LUDOVIKA
EGYETEMI KIADÓ

Tóth András

A digitális állam információbiztonsági kihívásai

Tóth András

A digitális állam információbiztonsági kihívásai

Tóth András

A digitális állam információbiztonsági kihívásai

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2025

A mű a TKP2020-NKA-09 számú projekt a Nemzeti Kutatási Fejlesztési
és Innovációs Alapból biztosított támogatással,
a Tématerületi Kiválósági Program 2020 pályázati program finanszírozásában valósult meg.

Nemzeti Kutatási Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL
MEGVALÓSULÓ PROJEKT

A kötet megjelenését a Nemzeti Média- és Hírközlési Hatóság támogatta.

NMHH
Nemzeti Média- és Hírközlési Hatóság

Szakmai lektor
Farkas Tibor

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Pordány Katalin
Olvasószerkesztő: Nagy Judit, Tomka Eszter
Korrektor: Bujdosó Hajnalka, Pokorádi Zsófia
Tördelőszerkesztő: Tihanyi József

DOI: https://doi.org/10.36250/01048_00

Második, javított kiadás.

ISBN 978-963-653-193-5 (nyomtatott)
ISBN 978-963-653-194-2 (ePDF) | ISBN 978-963-653-195-9 (ePub)

Tartalom

Rövidítések jegyzéke 7

Szakkifejezések jegyzéke 11

Bevezetés 17

Európa és Magyarország digitalizációja 19
- A Digitális Európa Program 19
- Az Európai Digitális Egységes Piac 38
- Magyarország Digitális Jólét Programja 41
- A digitális állampolgárság alapjai 74
- Az állami adatvagyon hasznosítása 75
- Felhőtechnológia 76
- A felhasználói élmény javítása 77
- Digitális kormányzati eredmények Magyarországon 78
- Nemzeti digitális stratégiai ütemterv 78
- Digitális infrastruktúra és technológia 79
- A kkv-k digitalizációja 79
- Kiberbiztonság 80
- Digitális készségek és közszolgáltatások 80
- Digitális jogok és elvek 81
- Fenntarthatóság és zöld digitalizáció 81
- Összefoglalás 82

A digitális állam kialakításának kérdései és kihívásai 83
- Digitális kompetenciák az Európai Unióban és Magyarországon 83
- A digitális állam alapvető elemei 100
- Digitális kormányzati átalakítási keretrendszer 108
- A digitális állam adatvezérelt közértékteremtése 122
- A bizalom és a magánélet védelme a digitális államban 133
- Összefoglalás 145

Biztonsági fenyegetések a digitális államban 147
- A kiberbiztonság és az információbiztonság fogalma és tartalma 147
- Potenciális sérülékenységek és veszélyek a digitális államban 152
- Összefoglalás 222

Felhasznált irodalom 225
- Törvények, rendeletek, egyéb kormányzati és uniós dokumentumok 225
- Nyomtatott és internetes források 229

Rövidítések jegyzéke

2FA	Two-factor Authentication	kétfaktoros hitelesítés
5GK		Magyarországi 5G Koalíció
AES	Advanced Encryption Standard	fejlett titkosítási szabvány
AI/MI	Artificial Intelligence	mesterséges intelligencia
AKG		agrár-környezetgazdálkodási
API	Application Programming Interface	alkalmazásprogramozási felület
APT	Advanced Persistent Threats	fejlett tartós fenyegetések
ARP	Address Resolution Protocol	címfeloldási protokoll
ASP	Application Service Provider	alkalmazásszolgáltató
CDO	Chief Data Officer	adatvédelmi tisztviselő
CDO	Chief Digital Officer	digitális igazgató
CDN	Content Delivery Network	tartalomszolgáltató hálózat
CIO	Chief Information Officer	informatikai vezető
CSIRT	Computer Security Incident Response Team	számítógép-biztonsági eseményekre reagáló csoport
DAI	Dynamic ARP Inspection	dinamikus ARP-ellenőrzés
DAS		Magyarország Digitális Agrár Stratégiája
DDoS	Distributed Denial of Service	elosztott szolgáltásmegtagadás
DEFS		Digitális Egészségipar-fejlesztési Stratégia
DES		Magyarország Digitális Exportfejlesztési Stratégiája
DETB		Digitális Exportfejlesztési Tárcaközi Bizottság
DGYS		Magyarország Digitális Gyermekvédelmi Stratégiája
DiD	Defense-in-Depth	mélységi védelem
DJA		Digitális Jólét Alapcsomag
DJP		Digitális Jólét Program
DJPP		Digitális Jólét Pénzügyi Program
DMP		Digitális Munkaerő Program
DNS	Domain Name System	tartománynévrendszer
DOM	Document Object Model	dokumentum objektum modell
DOS		Magyarország Digitális Oktatási Stratégiája
DoS	Denial of Service	szolgáltatásmegtagadással járó támadás, túlterheléses támadás
DPMK		Digitális Pedagógiai Módszertani Központ
DSS		Magyarország Digitális Startup Stratégiája
EHE/CEF	Connecting Europe Facility	Európai Hálózatfinanszírozási Eszköz
EKSZ	European External Action Service	Európai Külügyi Szolgálat
ERC/EKT	European Research Council	Európai Kutatási Tanács
ERDF/ERFA	European Regional Development Fund	Európai Regionális Fejlesztési Alap
ERP	Enterprise Resource Planning	vállalatirányítási tervezés
ESF/ESZA	European Social Fund	Európai Szociális Alap
FTP	File Transfer Protocol	fájlátviteli protokoll
G2B	Government to Business	a gazdasági szereplők és a kormányzat közötti kapcsolatok

G2C	Government to Citizens	az állampolgárok és a kormányzat közötti kapcsolatok
G2E	Government to Employees	a közszolgálatban dolgozók közötti kapcsolatok
G2G	Government to Government	közigazgatási szervek közötti kapcsolatok
G2NGO	Government to Non-governmental Organizations	a civil szervezetek és a kormányzat közötti kapcsolatok
GDPR	General Data Protection Regulation	Általános Adatvédelmi Rendelet
GÉANT	Gigabit European Academic Network Technology	gigabites európai kutatási gerinchálózat
HBONE	Hungarian Backbone	az első magyarországi internetes gerinchálózat
HPC	High Performance Computing	nagy teljesítményű számítástechnika
HTML	HyperText Markup Language	hiperszöveges jelölőnyelv
HTTP	Hyper Text Transfer Protocol	hiperszöveg-átviteli protokoll
HTTPS	Hyper Text Transfer Protocol Secure	biztonságos hiperszöveg-átviteli protokoll
I4.0 NTP		Ipar 4.0 Nemzeti Technológiai Platform
IAM	Identity and Access Management	identitás- és hozzáférés-kezelés
ICT/IKT	Information and Communication Technology	információs és kommunikációs technológia
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IKER		Infokommunikációs Egységes Referenciakeret
IoT	Internet of Things	tárgyak internete
ISA²	Interoperability Solutions for Public Administrations, Businesses and Citizens	az európai közigazgatások, üzleti vállalkozások és polgárok rendelkezésére álló interoperabilitási megoldások és közös keretek
ISACA	Information Systems Audit and Control Association	Informatikai Auditorok és Ellenőrök Nemzetközi Szövetsége
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
ITS		Integrált Területfejlesztési Stratégia
JSZP		Járműszolgáltatási Platform
K+I		kutatási és innovációs
KDS		Közgyűjteményi Digitalizálási Stratégia
KKSZB		Központi Kormányzati Szolgáltatási Busz
Kkv		kis- és középvállalkozások
MAC	Media Access Control	közeghozzáférés-vezérlő
MiTM	Man-in-The-Middle	közbeékelődéses
NAV		Nemzeti Adó- és Vámhivatal
NGA	Next Generation Access	új generációs hozzáférés
NGO	Non-governmental Organization	civil szervezet
NIIF		Nemzeti Információs Infrastruktúra Fejlesztési Program
NTG		Nemzeti Távközlési Gerinchálózat
OECD	Organisation for Economic Co-operation and Development	Gazdasági Együttműködési és Fejlesztési Szervezet
OTP	One-time PIN	egyszeri PIN-kód

P2P	Peer-to-Peer	egyenrangú résztvevők együttműködésén alapuló
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
PRACE	Partnership for Advanced Computing in Europe	az Európai Unió támogatásával létrehozott közös európai szuperszámítógépes infrastruktúra és együttműködés
RAT	Remote Administration Tool	távfelügyeleti eszközök
SFTP	SSH File Transfer Protocol	SSH fájlátviteli protokoll
SMS	Short Message Service	rövidüzenet-szolgáltatás
SSH	Secure Shell	biztonságos bejelentkezés távoli számítógépre egy nem biztonságos csatornán
SSL	Secure Socket Layer	védett socketréteg
SSC	Shared Service Center	szolgáltatóközpont
SSO	Single Sign-on	egyszeri bejelentkezési
SZEÜSZ		Szabályozott Elektronikus Ügyintézési Szolgáltatások
SZIP		Szupergyors Internet Program
TEN-T	Trans-European Transport Network	transzeurópai közlekedési hálózat
TLS	Transport Layer Security	szállítási réteg biztonsága
URL	Uniform Resource Locator	egységes erőforrás-helymeghatározó, webcím
VHCN	Very High Capacity Network	nagyon nagy kapacitású hálózat
VPN	Virtual Private Network	virtuális magánhálózat
XHTML	Extensible Hypertext Markup Language	bővíthető hiperszöveges jelölőnyelv
XML	Extensible Markup Language	kiterjeszthető jelölőnyelv
XSS	Cross-Site Scripting	keresztoldali szkriptelés
XXE	XML External Entities	XML külső entitások

Szakkifejezések jegyzéke

adatalany/ érintett	Az a természetes személy, aki bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.[1]
adatfeldolgozó	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.[2]
adatfelelős	Az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.[3]
adatkezelő	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.[4]
adatközlő	Az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi.[5]
biometrikus adat	Egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.[6]
biztonsági esemény	Minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.[7]

[1] 2011. évi CXII. törvény.
[2] 2011. évi CXII. törvény.
[3] 2011. évi CXII. törvény.
[4] 2011. évi CXII. törvény.
[5] 2011. évi CXII. törvény.
[6] 2011. évi CXII. törvény.
[7] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről.

bűnügyi személyes adat	A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.[8]
deepfake	A kifejezést olyan médiára (általában képre vagy videóra, de akár hangra is) használják, amelynél egy személy valamely ismertetőjegyét mesterséges intelligencia segítségével úgy változtatták meg, hogy az illető valaki másnak tűnjön.[9]
DNS-szolgáltató	Olyan szervezet, amely DNS-szolgáltatásokat nyújt az interneten.[10]
dolgok internete	Különböző, egyértelműen azonosítható elektronikai eszközök egysége, amelyek egymással egy internetalapú hálózaton keresztül kommunikálnak. A gépek a bennük található szenzorok segítségével kapcsolódnak a hálózathoz, ilyen módon osztanak meg egymással minden lényegi információt.[11]
egészségügyi adat	Egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.[12]
exaflop teljesítmény nagyságrendű szuperszámítógép	Olyan számítógépes rendszer, amely másodpercenként tíz a tizennyolcadikon művelet (azaz 1 exaflop) elvégzésére képes, így alkalmas olyan alkalmazások futtatására, amelyek kevesebb idő alatt találnak nagy megbízhatóságú megoldásokat, illetve amelyek összetettebb problémák kezelésére képesek.[13]
fejlett digitális készségek	A Digitális Európa Program által támogatott technológiák, termékek és szolgáltatások megértéséhez, tervezéséhez, fejlesztéséhez, irányításához, teszteléséhez, bevezetéséhez, alkalmazásához és fenntartásához szükséges ismereteket és tapasztalatokat igénylő készségek és szakmai kompetenciák.[14]
felhőalapú számítástechnikai szolgáltatás	Olyan digitális szolgáltatás, amely megosztható számítástechnikai erőforrások méretezhető és rugalmas pooljához enged hozzáférést.[15]
féreg	Olyan rosszindulatú számítógépes program, amely egy hálózaton keresztül példányokat küld saját magáról a többi számítógépre.[16]

[8] 2011. évi CXII. törvény.
[9] Lexiq: *Deepfake,* 2020.
[10] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[11] IFKA: *Ipar 4.0 fogalomtár,* 2020.
[12] 2011. évi CXII. törvény.
[13] A Tanács (EU) 2018/1488 rendelete.
[14] Az Európai Parlament és a Tanács (EU) 2021/694 rendelete.
[15] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[16] McAfee: *Mik azok a kártevő programok?* (2021. szeptember 1.).

genetikai adat	Egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.[17]
hálózati és információs rendszerek biztonsága	A hálózati és információs rendszer arra való képessége, hogy adott bizonyossággal ellenálljon az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszeren nyújtott vagy rajta keresztül elérhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát.[18]
hátsó kapu	Szoftverbe (vagy ritkább esetben hardverbe) épített olyan funkció, amelynek segítségével illetéktelen személyek hozzáférnek a programhoz, a géphez vagy annak bizonyos részeihez.[19]
informatikai biztonság	Olyan előírások, szabványok betartásának eredménye, amelyek az információ elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni.[20]
innovációs tevékenység	Elsősorban olyan tevékenységeket foglal magában, amelyek közvetlenül új, módosított vagy jobb minőségű termékek, eljárások vagy szolgáltatások terveinek és kialakításmódjának megtervezésére, elkészítésére irányulnak, és amelyeknek része lehet a prototípusgyártás, a tesztelés, a demonstrációs tevékenységek, a kísérleti bevezetés, a nagy léptékű termékvalidálás és a piaci elterjesztés.[21]
kémprogram	Olyan rosszindulatú program, amely adatokat gyűjt az emberekről anélkül, hogy tudomásuk lenne róla.[22]
kiberbiztonság	A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.[23]
kibervédelem	A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertérképességek megőrzését.[24]

[17] 2011. évi CXII. törvény.
[18] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[19] Lexiq: *Backdoor,* 2020.
[20] Szádeczky (2018): i. m. 5–6.
[21] Az Európai Parlament és a Tanács (EU) 2021/695 rendelete.
[22] McAfee (2021): i. m.
[23] 2013. évi L. törvény.
[24] 2013. évi L. törvény.

kockázat	Minden olyan észszerűen azonosítható körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára.[25]
kockázatelemzés	Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.[26]
kockázatkezelés	Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.[27]
kockázatokkal arányos védelem	Az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.[28]
közbeékelődéses támadás	Olyan, a hálózati lehallgatáshoz sokban hasonlító kibertámadás, amely során a támadó az elektronikus hírközlési hálózaton továbbított adat küldője és fogadója közé „ékelődik be", és a továbbított információt, adatot megváltoztatja. A cél, hogy a fogadó személyt megtévessze, és tőle érzékeny információkat (pl. jelszót) szerezzen meg, amelyekkel utána visszaélhet.[29]
közérdekből nyilvános adat	A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.[30]
közérdekű adat	Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.[31]
kulturális javak	Az élettelen és élő természet keletkezésének, fejlődésének, az emberiség, a magyar nemzet, Magyarország történelmének kiemelkedő és jellemző tárgyi, képi, hangrögzített, írásos emlékei és egyéb bizonyítékai – az ingatlanok kivételével –, valamint a művészeti alkotások.[32]

[25] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[26] 2013. évi L. törvény.
[27] 2013. évi L. törvény.
[28] 2013. évi L. törvény.
[29] Hírközlési és Informatikai Tudományos Egyesület: *Fogalomtár.* 2021.
[30] 2011. évi CXII. törvény.
[31] 2011. évi CXII. törvény.
[32] 2001. évi LXIV. törvény.

kutatási és innovációs tevékenység	Elsősorban olyan tevékenységeket foglal magában, amelyek új ismeretek létrehozására vagy egy új vagy jobb minőségű technológia, termék, eljárás, szolgáltatás vagy megoldás megvalósíthatóságának vizsgálatára irányulnak. Ez magában foglalhatja az alapkutatást, az alkalmazott kutatást, technológiák fejlesztését és integrálását, kis léptékű prototípusokkal laboratóriumi vagy szimulált környezetben végzett tesztelést, demonstrációs tevékenységeket és validálást.[33]
külföldi minősített adat	Megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.[34]
különleges adat	A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.[35]
nemzeti minősített adat	A minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.[36]
nyílt adat	Olyan adat, amely bárki által szabadon felhasználható, újrafelhasználható és terjeszthető.[37]
nyílt kormányzati (állami) adat	A nyílt adat valamely kormány által került előállításra.[38]

[33] Az Európai Parlament és a Tanács (EU) 2021/695 rendelete.
[34] 2009. évi CLV. törvény.
[35] 2011. évi CXII. törvény.
[36] 2009. évi CLV. törvény.
[37] Van Ooijen – Ubaldi – Welby (2018): i. m.
[38] Van Ooijen – Ubaldi – Welby (2018): i. m.

online piactér	Olyan digitális szolgáltatás, amely a fogyasztók és/vagy kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek.[39]
reklámprogram	Olyan szoftver, amely egy számítógépen automatikusan hirdetéseket játszik le, jelenít meg vagy tölt le.[40]
rosszindulatú program	Olyan szoftver, amelyet a számítógépek károsítására hoztak létre. A rosszindulatú programok bizalmas jellegű adatokat lophatnak a számítógépről, fokozatosan lelassíthatják a számítógépet, vagy akár hamis e-maileket is küldhetnek a felhasználó e-mail-fiókjából az ő tudta nélkül.[41]
személyes adat	Az érintettre vonatkozó bármely információ.[42]
tartománynév-rendszer (DNS)	Olyan hierarchikusan felépülő elnevezési rendszer, amely a hálózatban tartománynév-lekérdezéseket szolgál ki.[43]
trójai program	Olyan kártékony program, amely hasznos alkalmazásként tünteti fel magát, de árt a számítógépnek, vagy a telepítést követően ellopja a felhasználó adatait.[44]
vírus	Olyan kártékony számítógépes program, amely önmagát másolja, és megfertőzi a számítógépet.[45]
zsarolóprogram	Olyan rosszindulatú szoftver, amely korlátozza a megfertőzött számítógéphez a hozzáférést, a feloldást pénz megfizetéséhez kötve. Az áldozat gépét általában fertőzött e-mail-csatolmánnyal, applikációval vagy külső hardware-eszközön keresztül fertőzi meg.[46]

[39] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[40] McAfee (2021): i. m.
[41] ORFK Kommunikációs Szolgálat: *Digitális kártevők és biztonsági mentés.* 2021.
[42] 2011. évi CXII. törvény.
[43] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[44] McAfee (2021): i. m.
[45] McAfee (2021): i. m.
[46] Hírközlési és Informatikai Tudományos Egyesület (2021): i. m.

Bevezetés

Az elmúlt évtizedekben végbement technológiai fejlődéseknek köszönhetően egyre szélesebb körben terjedtek el a digitális technológiák. Ezek a technológiák komoly hatással vannak a mindennapi életünkre, a munkánkra, és sokkal több mindenre képesek, mint amire jelenleg használjuk őket. Ahhoz, hogy ezeket a képességeket a lehető legjobban ki tudjuk használni, az abban rejlő előnyöket a hasznunkra tudjuk fordítani, a rendelkezésre álló technológiákat elérhetővé kell tenni mind a lakosság, mind a vállalati szektor, illetve a közigazgatás és a kormány számára is. Ehhez elsősorban komoly kapacitásnövelésre van szükség, ami biztosítja a különböző szinten megjelenő felhasználók mindegyikének a hozzáférést a meglévő technológiákhoz, szolgáltatásokhoz.

Jelen monográfia a digitális állam információbiztonsági kihívásait tárgyalja. Azonban ahhoz, hogy ezeket a kihívásokat megértsük, először magával a digitális állam koncepciójával kell tisztában lennünk. A digitális állam fogalmát Magyarországon a 2013-ban kiadott Nemzeti Infokommunikációs Stratégia, az infokommunikációs szektor fejlesztési stratégiája fogalmazta meg. A stratégia alapján a digitális állam feladata „a kormányzat működését támogató belső IT, a lakossági és vállalkozói célcsoportnak szóló elektronikus közigazgatási szolgáltatások, illetve az állami érdekkörbe tartozó egyéb elektronikus (pl. egészségügyi, oktatási, könyvtári, kulturális örökséghez kapcsolódó vagy az állami adat- és információs vagyon megosztását célzó) szolgáltatások, valamint e szolgáltatások biztonsági hátterének biztosítása". A digitális állam megfelelő működéséhez elengedhetetlen a minden követelményt kielégítő digitális infrastruktúrák megléte, valamint a lakosság folyamatos képzésével a digitális kompetenciák kialakítása. A digitális infrastruktúrák azok a hírközlési infrastruktúrák, amelyek biztosítják a digitális szolgáltatások nyújtásához és igénybevételéhez szükséges sávszélességet, valamint a folyamatos rendelkezésre állást a hálózat valamennyi szegmensében (gerinc-, körzet- és helyi hálózat). A digitális kompetenciák „a lakosság, a mikro- és kisvállalkozások, illetve a közigazgatásban dolgozók digitális kompetenciáinak fejlesztése, az elsődleges (digitális írástudatlanság) és másodlagos (alacsony szintű használat) digitális megosztottság mérséklése, illetve a tartósan leszakadók részesítése a digitális ökoszisztéma előnyeiből (eBefogadás)". A megfelelő infrastrukturális környezet, valamint a kompetenciák megteremtéséhez elengedhetetlen egy erős digitális gazdaság kialakítása. A digitális gazdaság „egyrészt a szűkebben értelmezett infokommunikációs

szektor, másrészt az általa biztosított elektronikus (kereskedelmi, banki stb.) szolgáltatásokat igénybe vevő vállalkozások külső és belső informatikai rendszereinek fejlesztése, illetve az infokommunikációs fejlesztésekre és az információs és kommunikációs technológiákon alapuló fejlesztésekre irányuló kutatás-fejlesztési és innovációs tevékenység ösztönzése".[47]

A monográfia a jelenleg hatályos jogszabályi környezetet, valamint a hazai és nemzetközi digitalizációs programok jellemzőit foglalja össze. A vizsgált szabályozói környezet segít megérteni a digitális államhoz kapcsolódó egyes fogalmakat, a különböző keretrendszereket és stratégiai célokat, ezt követően az Európai Unió és Magyarország digitális kompetenciájának szintjét ismerteti. Ehhez a jelenleg rendelkezésre álló uniós jelentések és statisztikák nyújtanak megfelelő ismereteket, ezek alapján összehasonlíthatók a különböző területek, amelyek befolyásolják a digitális állam megfelelő működését úgy, mint például a széles sávú hozzáférés, az információs és kommunikációs szakemberek és a technológiák alkalmazása, valamint az e-kormányzatban alkalmazott egyes szolgáltatások száma, kihasználtsága. A monográfia alaptémájaként megvizsgáljuk azokat a területeket, amelyek potenciális fenyegetéseknek vannak kitéve a digitális térben. Ennek alapján a bizalom kialakításának és fenntartásának a lehetőségét, valamint a magánélet védelmét elemzi a szerző. Ezt követően az utolsó fejezet ismerteti a napjainkra jellemző támadási vektorokat és lehetséges védelmi megoldásokat, amelyek a digitális állam működését, az azt működtető információs és kommunikációs hálózatokat, valamint a lakosságot mint felhasználót fenyegetik.

A monográfia a témából adódóan számos olyan kifejezést tartalmaz, amelynek nincs pontos magyar megfelelője, így azokat első előfordulásuk során a szerző megmagyarázza, majd azok angol nyelvű megfelelőjét vagy annak rövidítését alkalmazza a szaknyelvnek megfelelés céljából. A kiadvány egy összefoglaló mű, célja megválaszolni azokat az alapvető kérdéseket, hogy a digitális államoknak milyen kihívásokkal kell szembenézniük a személyes és az egyéb érzékeny adatok védelme érdekében, valamint hogy melyek azok a potenciális fenyegetések, amelyek veszélyeztetik az adatok, a hálózatok védelmét, illetve a teljes digitális állam működését.

[47] *Nemzeti Infokommunikációs Stratégia 2014–2020,* 2014. 5.

Európa és Magyarország digitalizációja

A napjainkra jellemző digitalizáció eredményeinek és az azokból fakadó lehetőségeknek a lehető legjobb kihasználására van szükség a digitális államokban. Ez azt jelenti, hogy mind kormányzati, mind vállalati, mind lakossági szinten elérhetővé kell tenni az új digitális szolgáltatásokat, ahhoz megfelelő technikai, technológiai hátteret kell biztosítani, valamint a lakosság körében olyan képességeket kell fejleszteni, amelyek hozzájárulnak e megoldások lehető leghatékonyabb kihasználásához. Ennek kialakítása és biztosítása érdekében hozta létre az Európai Parlament és a Tanács a Digitális Európa elnevezésű programot, amelynek az a célja, hogy az európai társadalmak és gazdaságok digitális transzformációjának felgyorsítása érdekében előremozdítsa a legmodernebb technológiák széles körű bevezetését.

A Digitális Európa Program[48]

A Digitális Európa Programot létrehozó Európai Parlament és a Tanács (EU) 2021/694 számú rendeletét a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről 2021. április 29-én fogadták el. A rendelet a 2021 és 2027 közötti időszakra határoz meg célokat és feladatokat az unió és a tagállamok részére, és kimondja, hogy a program nem egy kutatás-fejlesztési program, hanem a már meglévő eredmények és kialakított technológiák beillesztésére fókuszál, ezzel támogatva a lakosság, a vállalkozások, a közigazgatás és a kormány mindennapi tevékenységeit. A program alapvető célja az európai gazdaság, az ipar és a társadalom digitális transzformációjából fakadó előnyök kihasználása, azok eljuttatása a polgárokhoz, a közigazgatásokhoz és a vállalkozásokhoz az egész unióban. Szintén kiemelt cél Európa versenyképességének javítása a globális digitális gazdaságban, illetve a határokon átnyúló támogatások és erősebb uniós hozzájárulások révén az unió stratégiai autonómiájának megerősítése, a meglévő digitális szakadékok áthidalása az egész unióban. A program kialakítása során megállapították, hogy azt csak

[48] Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről.

más uniós programokkal szoros koordinációban lehet végrehajtani. Mindezek alapján a következő sarokpontokat határozták meg a rendelet megalkotása során:

- a digitális technológia kulcsterületein Európa kapacitásainak megerősítése és előmozdítása széles körű bevezetés révén;
- a magánszektorban és a közérdekű területeken Európa kulcsfontosságú digitális technológiái terjesztésének és elterjedésének kiszélesítése, előmozdítva a digitális transzformációt és a digitális technológiákhoz való hozzáférést.

A rendelet a program öt egyedi, egymással összefüggő célkitűzést határoz meg, ezek a következők:

- nagy teljesítményű számítástechnika;
- mesterséges intelligencia;
- kiberbiztonság és bizalom;
- fejlett digitális készségek;
- digitális kapacitások telepítése, legjobb felhasználása és interoperabilitás.

Nagy teljesítményű számítástechnika

A nagy teljesítményű számítástechnika (High Performance Computing – HPC) vonatkozásában egy integrált, keresletorientált és alkalmazásvezérelt szuper-számítástechnikai és adat-infrastruktúra telepítését, uniós szintű összehangolását és működtetését kell megvalósítani. Az infrastruktúrának mindenki számára könnyen hozzáférhetőnek kell lennie, függetlenül attól, hogy melyik tagállamban található. Alkalmasnak kell lennie a különböző kutatások támogatására, magas biztonság és adatvédelem mellett biztosítania kell minden olyan hardvert, szoftvert, összeköttetést, alkalmazást és szolgáltatást, valamint digitális készséget, amely szükséges a kutatás és innováció eredményeképpen létrejött, felhasználásra kész, működőképes technológia telepítéséhez egy integrált uniós HPC-ökoszisztéma kiépítése érdekében. Célként rögzítették a kvantuminformatikai technológiák és a modern számítástechnika-tudomány kutatási infrastruktúrák integrációját, ezzel az exaflopot (másodpercenként 10^{18} műveletet) meghaladó teljesítmény nagyságrendű infrastruktúra telepítését és működtetését, valamint az ilyen telepítéshez szükséges hardver és szoftver unión belüli fejlesztésének ösztönzését.

A rendeletben meghatározott célokat és feladatokat a Tanács (EU) 2018/1488 rendeletével az európai nagy teljesítményű számítástechnikai közös vállalkozás létrehozásáról összhangban kell végrehajtani és megvalósítani. Ennek megfelelően és a fentiekkel összhangban a vállalkozás küldetése egy világszínvonalú integrált szuperszámítógépes és adat-infrastruktúra kifejlesztése, működésbe helyezése, bővítése és fenntartása az unióban, valamint egy versenyképes és innovatív ökoszisztéma kialakítása és támogatása a nagy teljesítményű számítástechnika vonatkozásában. Mindezek eléréséhez meghatározták az általános és a konkrét célokat, valamint a megvalósításhoz szükséges tevékenységeket.

Általános célok:

- hozzáférés biztosítása az unióhoz vagy a Horizont 2020-hoz társult országok kutatói és tudományos közössége, ipara – ezen belül a kis- és középvállalkozások (kkv) – és közszektora számára az elérhető legjobb, versenyképes, nagy teljesítményű számítástechnikai és adat-infrastruktúrához, valamint a hozzá kapcsolódó technológiák fejlesztésének, illetve különféle területeken történő alkalmazásának a támogatása;
- keret biztosítása egy világszínvonalú, exaflophoz közelítő teljesítményű integrált, keresletorientált és felhasználóközpontú szuperszámítógépes és adat-infrastruktúra beszerzéséhez az unióban;
- uniós szintű koordináció és megfelelő pénzügyi források biztosítása az említett infrastruktúra fejlesztésének és beszerzésének támogatásához, amely elsősorban kutatási és innovációs célokból fog rendelkezésre állni az állami és a magánszektor felhasználói számára;
- olyan ambiciózus kutatási és innovációs menetrend támogatása, amely az unióban egy világszínvonalú, nagy teljesítményű – exaflop vagy azt meghaladó teljesítményű – számítástechnikai ökoszisztémát fejleszt ki és tart fenn, amely kiterjed a tudományos és ipari értéklánc minden szegmensére – ideértve az alacsony teljesítményű processzor- és köztesszoftver-technológiákat, az algoritmusokat és a kódtervezést, az alkalmazásokat és a rendszereket, a szolgáltatásokat, a mérnöki munkát, valamint a gyakorlati ismereteket és a készségeket is – a szuperszámítógépek következő generációjára való felkészülés céljából;
- az unióban született kutatási és innovációs eredményeknek a tudományos, az ipari – ideértve a kkv-kat is – és a közszférabeli felhasználók körében való elterjedésének és szisztematikus használatának elősegítése.

Konkrét célok:

– a tagállami és uniós stratégiák összehangolása egy koordinált európai nagy teljesítményű számítástechnikai stratégia keretében, továbbá hozzájárulás a közpénzből finanszírozott támogatás eredményességéhez a felesleges párhuzamosságok és az erőfeszítések szétaprózódásának elkerülése révén;
– az uniós források, a nemzeti források és a magánberuházások összevonása, valamint a nagy teljesítményű számítástechnikába irányuló beruházásoknak a globális versenytársakéhoz összehasonlítható szintre hozatala;
– a tudományos kiválóságnak, valamint az ipar és az állami szektor digitalizálásának alapvető összetevőjeként és az unión belüli gazdasági növekedés és foglalkoztatásnövekedés megteremtését szolgáló innovációs képességek és globális versenyképesség megerősítése érdekében az uniót behálózó világszínvonalú, integrált, a különféle felhasználói igényeknek való megfeleléshez szükséges architekturális változatossággal rendelkező szuperszámítógépes és adat-infrastruktúra létrehozatala és üzemeltetése;
– hozzáférés biztosítása a nagy teljesítményű számítástechnikán alapuló infrastruktúrákhoz és szolgáltatásokhoz a tudományos és a kutatóközösség, valamint az ipar – ezen belül a kkv-k – és az állami szektor felhasználóinak széles köre, továbbá új és kialakulóban lévő, nagy adat- és számításigényű alkalmazások és szolgáltatások számára;
– világszínvonalú, nagy teljesítményű – exaflop vagy azt meghaladó teljesítményű – számítógépes technológiák unión belüli kifejlesztésének támogatása, ideértve az alacsony teljesítményű mikroprocesszorokat és a kapcsolódó köztesszoftver-technológiákat, továbbá a rendszerbe való, közös tervezésen alapuló megközelítésen keresztül történő integrációjukat, valamint e technológiák különféle nagy léptékű és újonnan létrejövő alkalmazási területeken való elterjedésének elősegítése;
– a kutatás-fejlesztés és az exaflop teljesítmény nagyságrendű szuperszámítástechnikai rendszerek megvalósítása közötti szakadék megszüntetése az unió digitális technológiai ellátási láncának megerősítésével, valamint annak lehetővé tételével, hogy a közös vállalkozás világszínvonalú szuperszámítógépeket szerezhessen be, esetlegesen európai technológiák beépítésével;

– a világ élvonalába kerülés érdekében kiemelkedő teljesítmény biztosítása a nagy teljesítményű számítástechnikai alkalmazások terén a programkódok, alkalmazások, valamint a nagy teljesítményű számítástechnika által lehetővé tett egyéb nagy léptékű, illetve újonnan létrejövő, vezető piaci alkalmazási területek közös tervezésen alapuló megközelítés keretében való fejlesztése és optimalizálása, egyrészt a nagy teljesítményű számítástechnika felhasználására irányuló kiválósági központok támogatása, másrészt a nagy adathalmazokat kezelő alkalmazásokra és szolgáltatásokra irányuló, a nagy teljesítményű számítástechnikán alapuló, különféle tudományos és ipari területeket érintő, nagyszabású demonstrációs és kísérleti projektek támogatása révén;
– a regionális, nemzeti és európai nagy teljesítményű szuperszámítógépek és más számítástechnikai rendszerek, adatközpontok, valamint kapcsolódó szoftverek és alkalmazások hálózatba kapcsolása és összekötése a PRACE[49]-vel; és
– a GÉANT[50]-hálózattal együttműködésben;
– az ipar – különösen a kkv-k – innovációs potenciáljának növelése nagy teljesítményű, fejlett számítástechnikai infrastruktúrák és szolgáltatások alkalmazásával, nagy teljesítményű számítástechnikai kompetenciaközpontok uniószerte történő létrehozása és különösen ezek hálózatba kapcsolása és összehangolása révén;
– a nagy teljesítményű számítástechnika megértésének javítása, valamint hozzájárulás a nagy teljesítményű számítástechnika területén tapasztalható unióbeli készséghiány csökkentéséhez tájékoztatás, képzés és a gyakorlati ismeretek elterjesztése révén;
– a nagy teljesítményű számítástechnika alkalmazási körének kibővítése.

A közös vállalkozásnak a fenti célokat a következő három tevékenységi kör révén kell megvalósítania:

– a közös vállalkozás működtetését és irányítását célzó általános adminisztratív tevékenységek;

[49] PRACE (Partnership for Advanced Computing in Europe) – az Európai Unió támogatásával létrehozott közös európai szuperszámítógépes infrastruktúra és együttműködés.
[50] GÉANT (Gigabit European Academic Network Technology) – gigabites európai kutatási gerinchálózat.

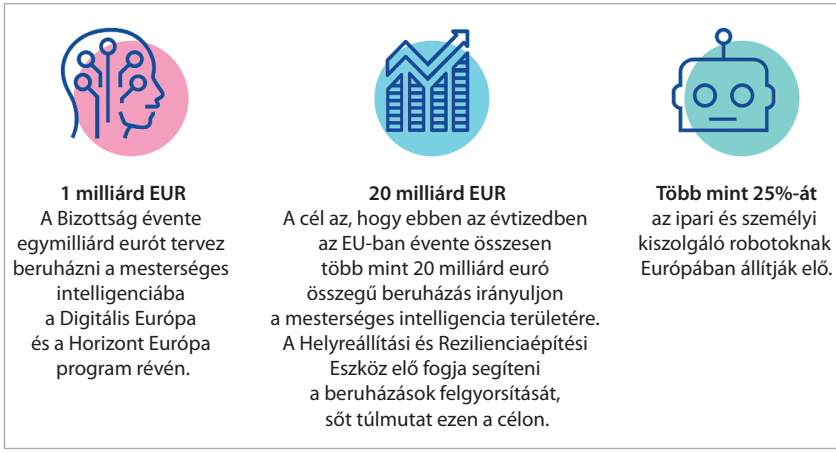
– a világszínvonalú szuperszámítógépek és adat-infrastruktúrák beszerzésére, üzembe helyezésére, összekapcsolására, üzemeltetésére, valamint a hozzáférésiidő-gazdálkodásra irányuló tevékenységek;
– a szuperszámítógépes szoftver- és hardvertechnológiákra és exaflop teljesítmény nagyságrendű szuperszámítógépes rendszerekbe való beépítésükre, továbbá a fejlett alkalmazásokra, szolgáltatásokra és eszközökre, valamint készségekre és gyakorlati ismeretek felhalmozására irányuló innovációs ökoszisztéma létrehozását szolgáló kutatási és innovációs menetrendet támogató tevékenységek.[51]

Mesterséges intelligencia

A mesterséges intelligencia (MI) célkitűzése esetében alapvető cél a már meglévő és a jövőben kialakítandó algoritmuskönyvtárak és kapacitások megosztása, a már meglévő ismeretek átadása. Ehhez közös európai adattereket kell létrehozni, amelyek lehetővé teszik, hogy minden tagállamból elérhetővé váljanak a meglévő adatok, amelyek ezáltal felhasználhatóvá válnak minden, MI-hez kapcsolódó tevékenység számára. Ehhez elengedhetetlen, hogy a meglévő adatok interoperábilisak legyenek, azaz azokat olyan formában kell tárolni, hogy az minden felhasználó számára olvasható, értelmezhető legyen mind az állami, mind a magánszektoron belül. Az algoritmuskönyvtárak lehetővé teszik, hogy valamennyi potenciális európai felhasználó számára elérhetők legyenek a már kifejlesztett algoritmusok, ezzel támogatva, hogy képesek legyenek azonosítani a számukra leginkább alkalmas megoldásokat, és hozzáférni azokhoz. A rendelet kimondja, hogy kiemelt figyelmet kell fordítani az említett kapacitásokhoz való hozzáférés biztosítására valamennyi vállalkozás, különösen a kkv-k és a startupok, valamint a civil társadalom, a nonprofit szervezetek, a kutatóintézetek, az egyetemek és a közigazgatások számára. Szorosan kapcsolódik ehhez az egyes tagállamokban már meglévő, az MI-vel kapcsolatos tesztelési és kísérleti létesítmények megerősítése és hálózatba kapcsolása, amivel növelhető az európai társadalom és gazdaság számára elérhető lehetőségek száma, ezzel komoly előnyöket érhetnek el világszinten. Ehhez világszínvonalú referencialétesítmények szükségesek, amelyek célja a valós

[51] A Tanács (EU) 2018/1488 rendelete (2018. szeptember 28.) az európai nagy teljesítményű számítástechnika közös vállalkozás létrehozásáról, 11.

körülmények közötti tesztelés és kísérletezés. Ezekben az eljárásokban az MI olyan alapvető ágazatokban történő alkalmazására koncentrálva járnak el, mint az egészségügy, a Föld- és környezetvédelmi monitoring, a közlekedés és a mobilitás, a biztonság, a gyártás és a pénzügyek, valamint egyéb közérdekű területek. Ehhez olyan létesítményeket kell létrehozni, amelyek jelentős számítástechnikai és adatkezelési eszközökkel, valamint az MI-hez kapcsolódó legújabb technológiákkal vannak felszerelve. Szintén kiemelt figyelmet kapott az MI-n alapuló megoldások elterjedésének előmozdítása a közérdekű területeken és a társadalomban. Az 1. ábrán az Európai Unió mesterségesintelligencia-fejlesztésre tervezett összegei láthatók, illetve az eddigi fejlesztések eredményeként megjelenő ipari és személyi robotok előállításának részesedése a világ egyéb területeihez képest.



1. ábra: A mesterséges intelligencia és az EU számokban

Forrás: Európai Bizottság: *Kiválóság és bizalom a mesterséges intelligencia terén,* 2021

Kiberbiztonság és bizalom

A Digitális Európa Program célja, hogy fejlett kiberbiztonsági berendezések, eszközök és adatinfrastruktúrák kiépítése és beszerzése valósuljon meg az adatvédelmi jogszabályok és az alapvető jogok teljes körű tiszteletben tartásával, ezzel biztosítva, hogy az unió kiberbiztonsága és stratégiai autonómiája egy-

ségesen magas szintre kerüljön és folyamatosan biztosított legyen. Támogatja a kiberbiztonsággal kapcsolatos európai ismeretek, kapacitások és készségek lehető legjobb módon történő felhasználását, valamint a legjobb gyakorlatok megosztásait az egyes tagállamok között. Mindegyik alapvető fontosságú a kritikus infrastruktúrák és a digitális egységes piac védelme vonatkozásában. Ezek a tevékenységek olyan beruházásokat vonnak maguk után, mint például a kvantumlétesítményekbe és a kiberbiztonságot szolgáló adatforrásokba, a kibertérbeli helyzetismeretbe, valamint egyéb olyan eszközökbe történő befektetések, amelyeket az állami és a magánszektor rendelkezésére kell bocsátani egész Európában.

Szintén alapvető célként szerepel a legkorszerűbb és leghatékonyabb kiberbiztonsági megoldások széles körű bevezetésének biztosítása az egész európai gazdaságban, különös figyelmet fordítva a közjogi hatóságokra és a kkv-kre. Ehhez igényként határozza meg a tagállami kompetencia-központok hálózatba szervezését, illetve a meglévő technológiai kapacitások továbbfejlesztését. Alapvető követelménye ennek, hogy a rendelkezésre álló kapacitások reagáljanak a közszektorbeli és az ipari igényekre, többek között olyan termékek és szolgáltatások révén, amelyek megerősítik a kiberbiztonságot és a bizalmat a digitális egységes piacon belül. Az állami és magánszervezetek vonatkozásában támogatja azokat az alapvető szolgálatásokat, amelyek hozzájárulhatnak a kiberbiztonság alapszintjének eléréséhez. Ilyen többek között az adatok végponttól végpontig terjedő titkosítása és a szoftverfrissítések, valamint az egyes alkalmazások, szolgáltatások és termékek biztonságának és védelmének megerősítése a tervezésüktől kezdve a kereskedelmi forgalmazásukig.

Emellett célként említi a kiberbiztonsági folyamatokkal kapcsolatos kockázatok jobb felismeréséhez és az e folyamatokkal kapcsolatos ismeretek bővítéséhez való hozzájárulást, valamint a kibertámadásokkal szembeni rugalmas ellenálló képesség javítását, amit a kiberbiztonsági készségeket célzó programok összhangba hozásával, azok konkrét ágazati szükségletekhez igazításával és a célzott specializált képzéshez való hozzáférés megkönnyítésével próbálnak biztosítani minden tagállam magán- és állami szereplői számára.

Mindezt úgy kell megvalósítani, hogy az egyes tagállamok és a magánszektor képesek legyenek megfelelni az Európai Parlament és a Tanács (EU) 2016/1148 számú, a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvének, többek között a kiberbiztonsági legjobb gyakorlatok elterjedését támogató intézkedések révén. Az irányelv a hálózati és információs rendszerek unión belüli

egységesen magas szintű biztonságának megvalósítása céljából az alábbiakat határozza meg:

- valamennyi tagállam számára kötelezettségeket állapít meg a hálózati és információs rendszerek biztonsága nemzeti stratégiájának elfogadására vonatkozóan;
- létrehoz egy együttműködési csoportot a tagállamok közötti stratégiai együttműködés és információcsere támogatása és elősegítése, valamint a közöttük lévő bizalom erősítése céljából;
- létrehozza a számítógép-biztonsági eseményekre reagáló csoportok hálózatát (Computer Security Incident Response Team – CSIRT) a tagállamok közötti bizalom erősítéséhez való hozzájárulás, valamint a gyors és hatékony operatív együttműködés előmozdítása céljából;
- biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára;
- a tagállamok számára kötelezettségeket állapít meg arra vonatkozóan, hogy a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására jelöljenek ki nemzeti illetékes hatóságokat, egyedüli kapcsolattartó pontokat, valamint CSIRT-eket.[52]

Fejlett digitális készségek

A fejlett digitális készségek célkitűzés esetében az unió támogatja az olyan személyek képzését, akik a digitális készségek tekintetében kiemelkedő képességűek. Ezzel alapvető célja az uniónak, hogy az Európában élő tehetségeket támogassa, bővítse körüket, ezzel ösztönözve a nagyobb szakmai hozzáértést, illetve hozzájáruljon az esetlegesen fennálló digitális szakadékok áthidalásához. Olyan szakemberek képzése az alapvető cél, akikkel a fennálló munkaerőhiány kezelhető, és akik komoly elméleti és gyakorlati tudással rendelkeznek a nagy teljesítményű és felhőalapú számítástechnika, a nagy adathalmaz (big data) elemzés, a kiberbiztonság, a megosztott könyvelési technológiák (pl. blokklánc), a kvantumtechnológiák, a robotika, az MI területén. Mindezekhez olyan operatív célkitűzéseket határoztak meg, mint:

[52] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, 11–12.

– magas színvonalú, hosszú távú képzések és tanfolyamok – többek között vegyes tanulás – tervezésének és nyújtásának támogatása a diákok és a munkaerő számára, amelyeket a kompetencia-központokban és a fejlett digitális technológiákat telepítő vállalkozásoknál kínált szakmai gyakorlatokon való részvétel révén valósíthatnak meg;
– magas színvonalú rövid távú képzések és tanfolyamok tervezésének és nyújtásának támogatása a munkaerő, különösen a kkv-k és a közszektor munkavállalói számára, amely tanfolyamokat a programban részt vevő szervekkel együttműködésben felsőoktatási intézményeknek, kutatóintézeteknek és ágazati szakmai tanúsító szerveknek kell nyújtaniuk;
– magas színvonalú munkahelyi képzések és szakmai gyakorlatok – többek között gyakornoki állások – támogatása diákok, továbbá a munkaerő, különösen a kkv-k és a közszektor munkavállalói számára.

Digitális kapacitások telepítése, legjobb felhasználása és interoperabilitás

A digitális kapacitások telepítése, legjobb felhasználása és az interoperabilitás célkitűzése hozzájárul, hogy a közszektor és az unióban letelepedett releváns vállalkozások képesek legyenek eredményesen telepíteni a legkorszerűbb digitális technológiákat, és azokat folyamatosan elérjék úgy, mint például a HPC-t, az MI-t és a kiberbiztonságot. Ennek megfelelően támogatásban részesül többek között az egészségügy és a gondozás, az oktatás, az igazságszolgáltatás, a vámügy, a közlekedés, a mobilitás, az energia, a környezetvédelem, továbbá a kulturális és kreatív ágazatok. A program során támogatják a legkorszerűbb transzeurópai interoperábilis digitális szolgáltatási infrastruktúrák telepítését, működtetését és fenntartását az egész unióban, valamint a jóváhagyott európai digitális szabványok integrálását és felhasználását a költséghatékony végrehajtás és az interoperabilitás elősegítése érdekében.

A célkitűzés hozzájárul, hogy a közigazgatások, vállalkozások és polgárok által kifejlesztett megoldások és keretek folyamatosan aktualizálva lehessenek, biztosítja azok felhasználhatóságát.

A program könnyű hozzáférést nyújt a közszektor és az uniós ipar, különösen a kkv-k számára a digitális technológiák teszteléséhez és kísérleti üzemeltetéséhez, valamint támogatja a fejlett digitális és kapcsolódó technológiák elterjedését a közszektorban és az uniós iparban, különösen a kkv-k és a startupok körében. Szintén támogatja az interoperábilis digitális megoldá-

sokat – ideértve a digitális kormányzási megoldásokat is – tervezését, tesztelését, végrehajtását, telepítését és fenntartását. A digitális fejlődés vezetése érdekében uniós szinten folyamatos kapacitásbiztosítás valósul meg, emellett biztosítja a legjobb gyakorlatok megosztásait is. Kialakít továbbá a megbízható adatmegosztó és digitális infrastruktúrák számára egy európai ökoszisztémát, amely támogatja az interoperabilitást és a szabványosítást. Ezzel párhuzamosan ösztönzi a magán- és állami felhasználókat, hogy a beépített biztonságon és adatvédelmen alapuló, határokon átnyúló uniós alkalmazásokat telepítsék, ezzel megfelelve a fogyasztó- és adatvédelmi jogszabályoknak. Mindezek mellett segíti az európai digitális innovációs központok és hálózatuk kiépítését és megerősítését.

Szinergiák más uniós programokkal

A Digitális Európa Programot a célkitűzések eléréséhez és a megvalósítás szakmai és technikai biztosításához a következő programokkal összhangban valósítják meg:

- a Horizont Európa keretprogrammal;
- megosztott irányítás alá tartozó uniós programokkal, mint például az Európai Regionális Fejlesztési Alappal (ERFA), az Európai Szociális Alap Plusszal (ESZA+);
- az Európai Hálózatfinanszírozási Eszközzel;
- az InvestEU programmal.

A Horizont Európa kutatási és innovációs keretprogram

A keretprogram általános célja a kutatási és innovációs (K+I-) tevékenységek támogatása. Alapvető cél, hogy az ezen a területen végbemenő uniós beruházások tudományos, technológiai, gazdasági és társadalmi hatást fejtsenek ki az unió tudományos és technológiai bázisainak megerősítése, versenyképességének fokozása, valamint stratégiai prioritásainak megvalósítása érdekében. Mindezekhez olyan ismeretek, készségek, technológiák és megoldások kialakítását tűzték ki célul, amelyek hozzájárulnak a tudományos kiválóság fejlesztéséhez, ösztönzéséhez és előmozdításához. Támogatást kapnak az olyan megoldásokhoz való hozzáférések, amelyek hozzájárulnak a tudás-

teremtéshez, erősítik az uniós szakpolitikák kidolgozására, támogatására és végrehajtására gyakorolt hatásokat. A hozzáférés mellett fontos, hogy az így kialakított tudás és legjobb gyakorlatok elterjedjenek a társadalomban, illetve alkalmazzák ezeket az európai iparban, különösen a kkv-k körében. Megfogalmazták azt is, hogy minden tagállam részére lehetőséget kell biztosítani a K+I-tevékenységekben való aktív részvételre, ehhez az Európai Kutatási Tanács (EKT) tevékenységeit úgy kell összehangolni és optimalizálni, hogy az hozzájáruljon az Európán belüli K+I-célú együttműködések megkönnyítéséhez.[53]

Megosztott irányítás alá tartozó uniós programok

A megosztott irányítású programokra jellemző, hogy nem közvetlenül az Európai Bizottság irányítja őket, hanem a tagállamokkal való együttműködés során történik azok alapvető működésének koordinálása. A Digitális Európa Program szempontjából releváns, ilyen megosztott irányítás alá tartozó uniós programok az alábbiak:

Európai Regionális Fejlesztési Alap

Az alap célja az Európai Unióban az egyes régiók közötti egyenlőtlenségek csökkentése. Ezen belül az ERFA a kutatás és innováció, a kis- és középvállalkozások, valamint a digitalizáció támogatását, az abban végbemenő folyamatok segítését tűzte ki alapvető célként. Az alap hozzájárul a kutatás, a technológiai fejlesztés és az innováció megerősítéséhez, ezen belül a K+I-infrastruktúrák és -kapacitások megerősítésével hozzájárul az európai érdekeltségű kompetencia-központok támogatásához. Elősegíti a hozzáférést a rendelkezésre álló infokommunikációs technológiákhoz (IKT), ezen belül támogatja a nagy sebességű hálózatok kiépítését, valamint a digitális gazdasá-

[53] Az Európai Parlament és a Tanács (EU) 2021/695 rendelete (2021. április 28.) a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról, továbbá az 1290/2013/EU és az 1291/2013/EU rendelet hatályon kívül helyezéséről.

got szolgáló feltörekvő technológiák és hálózatok bevezetését. Közreműködik az e-kereskedelem megerősítésében, az e-kormányzás, az e-tanulás, az e-befogadás, az e-kultúra és az e-egészségügy infokommunikációs alkalmazásainak megerősítésében. Segíti a kkv-kat, hogy növekedni tudjanak a regionális, nemzeti és nemzetközi piacokon, és hogy az innovációs folyamatokban részt tudjanak venni. Az ERFA támogatja a fenntartható városfejlesztést olyan stratégiai intézkedések révén, amelyek hozzájárulnak a városi területeket érintő gazdasági, környezetvédelmi, éghajlati, demográfiai és társadalmi kihívások kezeléséhez, szem előtt tartva a város és a vidék közötti összeköttetések előmozdításának szükségességét.[54]

Az Európai Szociális Alap Plusz

Az Európai Szociális Alapot a Római Szerződés hozta létre abból a célból, hogy javítsa az Európai Unión belüli foglalkoztatás lehetőségeit, valamint hozzájáruljon a munkavállalói mobilitás fejlesztéséhez. Az ESZA+ támogatja a munkahelyteremtésre, az oktatásra és képzésre, valamint a társadalmi befogadásra és az egészségügyi ellátás igénybevétele lehetőségének javítására irányuló projekteket és beruházásokat, a tagállamokat a Covid–19-világjárvány okozta válság kezelésében, továbbá a zöld és digitális gazdaságra való átállást.

Az alap célja a digitális jártasság és az e-tanulás fejlesztése, valamint a digitális társadalmi befogadással, a digitális készségekkel és a megfelelő vállalkozói készséggel kapcsolatos beruházások révén az információs és kommunikációs technológiákhoz való hozzáférésnek és azok használatának és minőségének javítása.[55]

Az 1. táblázat bemutatja a Digitális Európa Program célkitűzéseinek eléréséhez legszorosabban kapcsolódó beruházási prioritásokat az Európai Regionális Fejlesztési Alap és az Európai Szociális Alap Plusz vonatkozásában.

[54] Az Európai Parlament és a Tanács 1301/2013/EU rendelete (2013. december 17.) az Európai Regionális Fejlesztési Alapról és a „Beruházás a növekedésbe és munkahelyteremtésbe" célkitűzésről szóló egyedi rendelkezésekről, valamint az 1080/2006/EK rendelet hatályon kívül helyezéséről.

[55] Az Európai Parlament és a Tanács 1304/2013/EU rendelete (2013. december 17.) az Európai Szociális Alapról és az 1081/2006/EK tanácsi rendelet hatályon kívül helyezéséről.

1. táblázat: Beruházási prioritások a Digitális Európa Program vonatkozásában

Tematikus célkitűzések	Beruházási prioritások ERFA	Beruházási prioritások ESZA+
A kutatás, technológiai fejlesztés és innováció erősítése.	A kutatási és innovációs (K+I-) infrastruktúra és kapacitás fejlesztése a kutatási és innovációs kiválóság kialakítása érdekében, valamint kompetencia-központok előmozdítása, különös tekintettel azokra, amelyek európai érdeket képviselnek.	
Információs és kommunikációs technológiák hozzáférésének, használatának és minőségének javítása.	Az IKT-termékek és szolgáltatások, valamint az e-kereskedelem továbbfejlesztése és az IKT iránti kereslet fokozása. Az e-kormányzás, az e-tanulás, az e-befogadás, az e-kultúra és az e-egészségügy IKT-alkalmazásainak megerősítése. A széles sáv alkalmazásának kiterjesztése, nagy sebességű hálózatok kiépítése, valamint feltörekvő technológiák és hálózatok fejlesztése a digitális gazdaság érdekében.	
Kis- és középvállalkozások versenyképességének növelése.	A vállalkozói szellem előmozdítása, különösen az új ötletek gazdasági hasznosításának megkönnyítésével, valamint új cégek alapításának ösztönzésével, többek között üzleti inkubátorházak segítségével. A kkv-k segítése abban, hogy növekedni tudjanak a regionális, nemzeti és nemzetközi piacokon, és részt tudjanak venni az innovációs folyamatokban.	

Tematikus célkitűzések	Beruházási prioritások ERFA	Beruházási prioritások ESZA+
A fenntartható közlekedés előmozdítása és szűk keresztmetszetek megszüntetése a kulcsfontosságú hálózati infrastruktúrákban.	Multimodális egységes európai közlekedési térség támogatása a transzeurópai közlekedési hálózatba (TEN-T) való beruházás által. Környezetbarát – többek között alacsony zajkibocsátású – és alacsony szén-dioxid-kibocsátású közlekedési rendszerek – többek között belvízi és tengeri hajózási útvonalak, kikötők, multimodális összeköttetések és repülőtéri infrastruktúra fejlesztése és javítása, a fenntartható regionális és helyi mobilitás előmozdítása érdekében. A regionális mobilitás fokozása a másodrangú és harmadrangú csomópontok TEN-T-infrastruktúrához – többek közt a multimodális csomópontokhoz – történő kapcsolásával. Az energiahatékonyság és az ellátásbiztonság javítása intelligens energiaelosztó, -tároló és -átviteli rendszerek kialakítása és a megújuló forrásokból származó elosztott termelés integrálása révén.	
A fenntartható és minőségi foglalkoztatás, valamint a munkavállalói mobilitás ösztönzése.	Üzleti inkubátorházak létrehozásának támogatása, valamint az önfoglalkoztatás, a mikrovállalkozások és a cégalapítás támogatása beruházásokkal. Beruházás a foglalkoztatási szolgálatok infrastruktúrájába.	A munkakeresők és inaktívak foglalkoztatáshoz való hozzáférése, beleértve a tartós munkanélkülieket és a munkaerőpiactól távol esőket, a helyi foglalkoztatási kezdeményezések és a munkavállalói mobilitás ösztönzése révén is. Önfoglalkoztatás, a vállalkozói készség, a vállalkozások létrehozása, beleértve a mikro-, kis- és középvállalkozásokat (kkv-k), valamint a mikrovállalkozásokat.

Tematikus célkitűzések	Beruházási prioritások ERFA	Beruházási prioritások ESZA+
		A munkaerőpiaci intézmények, például az állami és magán foglalkoztatási szolgáltatások modernizálása és a munkaerőpiaci igényekhez való igazodás javítása, beleértve a munkavállalók transznacionális földrajzi mobilitását a mobilitási programok, valamint az intézmények és az érdekeltek közötti együttműködés javítása révén ösztönző tevékenységeket is.
Az oktatásba, a képzésbe és szakképzésbe történő beruházás a készségek fejlesztése és az egész életen át tartó tanulás érdekében.	Beruházás az oktatásba, készségekre vonatkozó képzésbe, a szakképzésbe és az egész életen át tartó tanulásba oktatási és képzési infrastruktúrák fejlesztésével.	Az oktatási és képzési rendszerek munkaerőpiaci igényekhez való igazításának javítása, a tanulásból a munkába történő átállás megkönnyítése, a szakképzés és a képzési rendszerek megerősítése és minőségének javítása többek között a készségek iránti igény előzetes felmérésén alapuló mechanizmusok révén, a szakmai életút rugalmasabbá tétele, munkaalapú tanulási rendszerek – többek között a duális tanulási rendszerek és a gyakornoki képzések – létrehozása és továbbfejlesztése.
A hatóságok és az érdekelt felek intézményi kapacitásának növelése és hatékony közigazgatás.	A közjogi hatóságok és az érdekeltek intézményi kapacitásának és a közigazgatás hatékonyságának fokozása az intézményi kapacitás és az ERFA végrehajtásához kapcsolódó közigazgatási szervek és közszolgálatok hatékonyságát megerősítő intézkedések által, valamint az ESZA általi, az intézményi kapacitásra és a közigazgatás hatékonyságának megerősítésére irányuló intézkedések támogatása.	Azon közigazgatási szervek és közszolgálatok intézményi kapacitásának és hatékonyságának növelésébe történő beruházások nemzeti, regionális és helyi szinten, amelyek célja a reformok, a jobb szabályozás és a jó kormányzás megvalósítása.

Forrás: Az Európai Parlament és a Tanács 1303/2013/EU rendelete

Az Európai Hálózatfinanszírozási Eszköz

Az Európai Hálózatfinanszírozási Eszköz (EHE) célja a közlekedési, a távközlési és az energetikai fejlesztés során új infrastruktúrák és szolgáltatások kifejlesztése és kiépítése, illetve a meglévő infrastruktúrák és szolgáltatások korszerűsítése az Európai Unión belül. A közlekedési ágazatban prioritást élveznek az olyan projektek, amelyek során az eddig még meg nem lévő közlekedési kapcsolatok kiépítése a cél. Ennek megfelelően az EHE hozzájárul a vasúti, közúti, belvízi és tengeri infrastruktúra fejlesztéséhez és korszerűsítéséhez multimoduláris hálózatok kialakításával, valamint biztonságos mobilitás biztosításával. A program során elsőbbséget élvez az ERFA által is támogatott transzeurópai közlekedési hálózat továbbfejlesztése, különös tekintettel a határon átnyúló projektekre. Az Európai Hálózatfinanszírozási Eszköz 2.0 program a 2021–2027 közötti időszakra vonatkozóan a közlekedési infrastruktúrák esetében kiemelt figyelmet fordít az egyes közlekedési hálózatok katonai mobilitást támogató fejlesztésére is, és az így kialakított infrastruktúrák használhatóak lennének mind katonai, mind polgári célokra.

A program támogatja a határokon és ágazatokon átívelő hálózatok interoperabilitásának javítását, a dekarbonizáció előmozdítását és az ellátásbiztonság fejlesztését, ezzel növelve a belső energiapiac integrációját. Alapvető cél a megújulóenergia-megoldások fejlesztése, ahol szintén kiemelt figyelmet kap a határokon átnyúló együttműködések integrálása, továbbá az intelligens és hatékony energiarendszerek kifejlesztése, amelyek segítik a megfelelő tárolási, hálózathasználati és ellátásbiztonsági megoldások kialakítását és üzemeltetését, valamint az unió nagyobb fokú energiafüggetlenségének biztosítására is törekednek. Mindezek alapján a program támogatja a közlekedés, az ipar, a fűtés és a hűtés dekarbonizációját, valamint a villamosenergia-hálózatok összekapcsolásával, a villamos energia tárolásával, az intelligens energiahálózatok kialakításával a transzeurópai energia-infrastruktúra folyamatos fejlesztését. Az így kialakítandó intelligens energiahálózatok valós idejű irányítási rendszerek alkalmazásával integrálják a villamos energia termelését, elosztását vagy fogyasztását, illetve támogatják a határokon átnyúló energiaáramlást.

Az Európai Unió által kialakításra kerülő egységes piac alapját a digitális konnektivitási infrastruktúra adja. A digitális konnektivitás a gazdasági, társadalmi és területi szakadékok áthidalásának alapvető eleme, ami támogatja a helyi gazdaságok modernizációját, és segíti a gazdasági tevékenységek diverzifikációját, ezzel hozzájárulva az uniós ipar digitalizációjához és az olyan ágazatok

modernizációjához, mint a közlekedés, az energia, az egészségügy és a közigazgatás, valamint biztosítja a megbízható, megfizethető, nagy és rendkívül nagy kapacitású hálózatokhoz való egyetemes hozzáférést. Az EHE célja, hogy az unión belül a háztartásoknak, a vállalkozásoknak és a helyi közösségeknek hozzáférést biztosítson a legjobb szolgáltatásokhoz és alkalmazásokhoz. Így biztosítva, hogy minden olyan szervezetnek vagy intézménynek mint társadalmi-gazdasági mozgatórugónak, amely hatással lehet fontos társadalmi-gazdasági fejleményekre az elhelyezkedésük szerinti területeken, beleértve a vidéki és ritkán lakott területeket is, élen kell járnia a gigabites konnektivitás terén. Ilyen intézmények és szolgáltatások lehetnek a következők:

- az iskolák;
- az egyetemek;
- a könyvtárak;
- a helyi, regionális vagy nemzeti közigazgatások;
- a főbb közszolgáltatási intézmények;
- a kórházak és az egészségügyi központok;
- a közlekedési csomópontok;
- a digitálisan intenzív vállalkozások.

A digitális konnektivitás kialakítása során az unió törekszik az internetkapcsolattal nem rendelkező területek számára jó minőségű internetkapcsolatot biztosítani, ezzel megszüntetni a jelenleg fennálló digitális szakadékokat, és megelőzni a további elszigetelődéseket és elnéptelenedéseket az egész unióban. Ez új gazdasági lehetőségeket is jelent, hozzájárulhat a precíziós mezőgazdasági termelés vagy a vidéki területeken a biogazdaság kialakításához, fejlesztéséhez. A program része a WiFi4EU kezdeményezés, amely során az EHE támogatja az ingyenes, biztonságos és jó minőségű helyi vezeték nélküli konnektivitás kialakítását és biztosítását a helyi közélet központjaiban (középületekben, könyvtárakban, egészségügyi központokban és múzeumokban) – beleértve a közfeladatot ellátó szervezeteket, így például a hatóságokat és a közszolgáltatókat –, valamint a köz számára hozzáférhető kültéri területeken, többek között parkokban, tereken, az unió digitális jövőképének a helyi közösségekben történő előmozdítása érdekében.[56]

[56] A Bizottság javaslata: az Európai Parlament és a Tanács rendelete az Európai Hálózatfinanszírozási Eszköz létrehozásáról, valamint az 1316/2013/EU és a 283/2014/EU rendelet hatályon kívül helyezéséről (COM/2018/438 végleges).

Az InvestEU program

Az InvestEU program célja, hogy támogassa az unión belül az európai beruházásokat, az innovációt és a munkahelyteremtést, továbbá fokozza a vállalkozói kedvet. A program a kis- és középvállalkozások, a kutatás, az innováció és a fenntartható infrastruktúra-fejlesztések támogatásán túl az oktatás, az egészségügy és a szociális lakhatás támogatásával igyekszik áthidalni a szociális infrastruktúrák terén tátongó szakadékokat is az unión belül.

Az új program a következő pillérekből épül fel:

- az InvestEU Alapból;
- az InvestEU Tanácsadó Platformból;
- az InvestEU Portálból.

Az InvestEU Alap az innováció és a digitalizáció fejlesztésével hozzájárul az unió versenyképességének, társadalmi-gazdasági konvergenciájának és kohéziójának javításához, valamint segíti a tagállamok uniós forrásainak hatékonyabb mozgósítását. Az InvestEU Tanácsadó Platform integrálja a különböző tanácsadó szolgálatokat, valamint technikai támogatást és tanácsadást nyújt a projektek előkészítéséhez, kidolgozásához, strukturálásához és végrehajtásához, beleértve a kapacitásépítést. Az InvestEU Portál könnyen hozzáférhető és felhasználóbarát adatbázisokat biztosít, amelyek lehetővé teszik, hogy az egyes szektorokban megjelenő különböző projektlehetőségek kereshetők, jobban hozzáférhetők legyenek, ezáltal az egyes projektek ismertebbé, népszerűbbé válhatnak.

Az InvestEU program célja, hogy hozzájáruljon:

- az unió versenyképességéhez, ideértve a kutatást, az innovációt és a digitalizációt;
- az uniós gazdaság növekedéséhez, a foglalkoztatás fellendítéséhez, az uniós gazdaság fenntarthatóságához, továbbá a minőségi munkahelyek létrehozásához;
- az unió társadalmi rezilienciájához, inkluzivitásához és innovációs képességéhez;
- a tudományos és technológiai fejlődés, a kultúra, az oktatás és a képzés előmozdításához;
- az uniós tőkepiacok integrációjához és a belső piac megerősítéséhez;
- a gazdasági, társadalmi és területi kohézió előmozdításához;
- az uniós gazdaság Covid–19-válságot követő fenntartható és inkluzív helyreállításához.

További célkitűzések a kutatással, az innovációval és a digitalizációval, valamint a fenntartható infrastruktúrával kapcsolatos finanszírozási és beruházási műveletek támogatása, illetve a kis- és középvállalkozások, valamint a kis méretű, közepes piaci tőkeértékű vállalatok finanszírozáshoz jutásának és a finanszírozás rendelkezésre állásának bővítése.[57]

Az Európai Digitális Egységes Piac

Az Európai Bizottság tevékenysége során mindig vannak prioritással kezelt projektek és eljárások, amelyek ciklusonként változnak. Ezeknek a kulcsfontosságú területeknek az egyik eleme a digitális egységes piac, ami a COM/2015/0192 végleges dokumentumban került lefektetésre az Európai Bizottságnak az Európai Digitális Egységes Piac stratégiáról szóló közleményében 2015-ben, ami a 2024-ig terjedő időtartamra határozza meg az unió számára az elérendő célokat és a végrehajtandó feladatokat az egységes piac kialakítása és működtetése céljából. A stratégia célja, hogy az Európai Unió gazdasága, ipara és társadalma számára biztosítsa az új, digitális korszakkal járó megoldásokat és előnyöket, és megszüntesse az online és az offline világ közötti határokat. A stratégiában megfogalmazottaknak megfelelően a Digitális Egységes Piac olyan piac, amelyben biztosított az áruk, a személyek, a szolgáltatások és a tőke szabad mozgása, és ahol az egyének és vállalkozások akadálymentesen, a fogyasztó- és adatvédelmi szabályok messzemenő betartása és tisztességes versenyfeltételek mellett végezhetik internetes tevékenységeiket. A Digitális Egységes Piac megvalósítása révén Európa megtarthatja a digitális gazdaságban elfoglalt vezető pozícióját, elősegítve az európai vállalkozások globális növekedését. A digitális egységes piaci stratégia az alábbi három pillérre épül:

- Az internetes termékek és szolgáltatások elérhetőbbé tétele az európai fogyasztók és vállalkozók számára.
- A digitális hálózatok és szolgáltatások fellendülését elősegítő feltételek megteremtése.
- Az európai digitális gazdaság növekedési potenciáljának maximalizálása.

[57] Az Európai Parlament és a Tanács (EU) 2021/523 rendelete (2021. március 24.) az InvestEU program létrehozásáról és az (EU) 2015/1017 rendelet módosításáról.

Európa-szerte jobb fogyasztói és vállalkozói hozzáférés az internetes termékekhez és szolgáltatásokhoz

A pillér alapvető célja megszüntetni a tagállamközi internetes tevékenység útjában álló akadályokat, valamint az uniós alapelvekkel ellentétes eljárásokat, ezzel biztosítva, hogy az online áruk és szolgáltatások könnyebben hozzáférhetők legyenek a fogyasztók és vállalkozások számára. Ennek megfelelően egy olyan e-kereskedelmi keret kialakítása a cél, amely megakadályozza a fogyasztók és a vállalkozások közötti igazságtalan különbségtételt akkor, amikor megpróbálnak a tartalmakhoz hozzáférni vagy online árut és szolgáltatást vásárolni az EU-n belül. Szintén kiemelt figyelmet fordítanak a stratégia megvalósítása során a határokon átnyúló internetes értékesítés megbízhatóságára, ami bizalmat kelt a fogyasztók körében. Mindezeket figyelembe véve az alábbi intézkedéseket és feladatokat határozták meg:

- a határon átívelő elektronikus kereskedelemre vonatkozó szabályok könnyítése, hatékonyabb és megfizethetőbb határon átívelő csomagkézbesítés;
- a fogyasztóvédelmi együttműködésről szóló rendelet felülvizsgálata a fogyasztóvédelmi szabályok gyorsabb és következetesebb érvényesítése érdekében;
- az indokolatlan területi alapú tartalomkorlátozás megszüntetése, és ezáltal a választék és a hozzáférés bővítése az európai online fogyasztók részére;
- az európai elektronikus kereskedelmi piacokat befolyásoló, versennyel kapcsolatos aggályok azonosítása;
- egy modern, európaibb szerzői jogi keret kialakítása, ezzel a digitális tartalomhoz való hozzáférés javítása;
- az eltérő hozzáadottértékadó-szabályozások miatt a fogyasztókra és a vállalkozásokra háruló adminisztratív terhek csökkentése.

Megfelelő feltételek és egyenlő versenyfeltételek a fejlett digitális hálózatok és az innovatív szolgáltatások számára

A Digitális Egységes Piac célja, hogy megfelelő szabályozási feltételekkel támogatott nagy sebességű, megbízható és biztonságos infrastruktúrák és szolgáltatások biztosításával megteremtsen a digitális hálózatok és szolgáltatások számára egy minden követelményt kiszolgáló működési és üzemeltetési környezetet. Mindezek eléréséhez az üzemeltetésnek komoly hangsúlyt kell fektetnie a tech-

nológia folyamatos fejlesztése mellett az olyan területekre is, mint a kollektív kiberbiztonság, az adatvédelem, valamint a kialakított online platformok átláthatósága, felhasználóbaráttá tétele. Mindezeket figyelembe véve az alábbi intézkedéseket és feladatokat állapították meg:

- az EU távközlési szabályainak reformja, ezzel a céloknak megfelelően naprakésszé tétele;
- az audiovizuális médiáról szóló keret felülvizsgálata, valamint a 21. századi követelményekhez és módszerekhez igazítása;
- az olyan internetes platformoknak (pl. keresőprogramok, közösségi média, elektronikus kereskedelmi platformok, alkalmazás-áruházak, ár-összehasonlító oldalak) a Digitális Egységes Piacon betöltött szerepének elemzése, amelyek központi szerepet játszanak a társadalmi és gazdasági életben;
- annak felmérése, hogy miként vehető fel a küzdelem az interneten megtalálható illegális tartalmak ellen;
- a fogyasztók és a vállalkozások körében a bizalom megerősítése a digitális szolgáltatások, valamint a személyes adatok kezelése vonatkozásában, valamint e szolgáltatások biztonságának megerősítése.

A digitális gazdaság növekedési potenciáljának maximalizálása

A Digitális Egységes Piac stratégia egyik alapvető célja, hogy maximalizálja az európai digitális gazdaság növekedési potenciálját. Ehhez elengedhetetlenül szükséges, hogy a digitális technológiák előnyeit a lehető legtöbb EU-állampolgár képes legyen kihasználni, amihez a digitális készségek fejlesztése kiemelten fontos.[58] Mindezeket figyelembe véve az alábbi intézkedéseket és feladatokat sorolták fel:

- adatgazdaság építése, amelynek megalapozásához feltétlenül meg kell szüntetni a tagállamközi adatáramlást és az új szolgáltatások kifejlesztését gátló, EU-n belüli technikai és jogi akadályokat;
- a szabványokra, valamint az eszközök, alkalmazások, adatraktárak, szolgáltatások és hálózatok interoperabilitására vonatkozó prioritások meg-

[58] Horváth Gábor: A Digitális Európa Program és a BME VIK. *Híradástechnika,* 75. (2020), 1. 2–5.

határozása, amelyhez a Bizottság felülvizsgálja és kiterjeszti az európai interoperabilitási keret hatókörét;
– az inkluzív digitális társadalom támogatása, ahol alapvető cél annak elérése, hogy a polgárok és a vállalkozások rendelkezzenek a szükséges készségekkel és lehetőségekkel ahhoz, hogy részesedjenek az összekapcsolt és többnyelvű e-szolgáltatások, az e-kormányzat, e-igazságügy, e-egészségügy, e-energia vagy az e-szállítás előnyeiből.[59]

Magyarország Digitális Jólét Programja

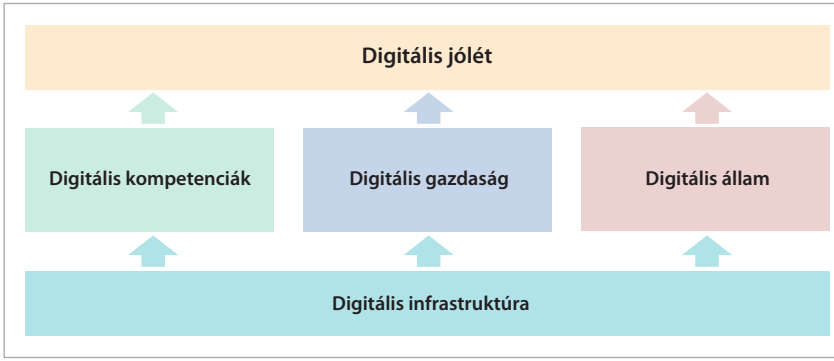
A kormány 2012/2015. (XII. 29.) számú határozata az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a kormány által végrehajtandó Digitális Jólét Programjáról hozta létre Magyarország Digitális Jólét Programját (DJP), amelynek célja felkészíteni az ország polgárait, gazdasági szereplőit, állami rendszereit a digitalizáció által eredményezett globális átalakulásra. A program alapvető célkitűzése, hogy Magyarország állami rendszerei, közigazgatása, vállalkozásai és minden polgára a digitalizáció és az informatikai forradalom nyertese lehessen.[60] Ennek megfelelően 2017-ben megjelent a DJP 2.0 elnevezésű stratégiai dokumentum, amely magában foglal minden olyan tervet és tevékenységet, amellyel elérhetők a digitalizáció során a kormány által felállított célkitűzések. Ezek a következők:

– minden magyar polgárnak legyen lehetősége arra, hogy digitális felkészültségét folyamatosan gyarapítsa;
– minden magyar vállalkozásnak legyen esélye arra, hogy – a digitalizáció fontosságát és hasznosságát felismerve és kihasználva – növelje versenyképességét;
– a nemzetgazdaságnak legyen esélye arra, hogy a nemzetközi versenyben a történelmi léptékű digitális átalakulás nyerteseként lépjen előre.

[59] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai digitális egységes piaci stratégia, COM/2015/0192 végleges (2015. május 6.).

[60] 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a kormány által végrehajtandó Digitális Jólét Programjáról.

Ezek eléréséhez és a szükséges jogi és szakmai háttér biztosításához 2017. július 19-én megjelent a kormány 1456/2017. (VII. 19.) határozata a DJP 2.0 elfogadásáról és annak végrehajtásáról. A DJP 2.0 a 2015-ben elfogadott Digitális Jólét Program kibővítése, ami több mint húsz új, a digitalizációt támogató fejlesztési programot fogalmaz meg a magyar gazdaság, az állami működés és a magyar társadalom digitális fejlesztésének szinte valamennyi területével kapcsolatosan. Célja a fenti pontokkal összhangban az internet mindenki számára történő hozzáférésének biztosítása azáltal, hogy a megfelelő infrastruktúrák kiépítése mellett biztosítja annak megfizethetőségét. Egy megfelelő alapot biztosít minden olyan terület számára, ahol elengedhetetlen a digitalizáció megkezdése vagy folytatása. Ilyen többek között az oktatás, a honvédelem és a közigazgatás.[61] A DJP 2.0 stratégiában megfogalmazottaknak megfelelően a digitális jólét elérését a digitális infrastruktúra fejlesztése alapozza meg, amely hozzájárul a digitális kompetenciák, a digitális gazdaság és a digitális állam alappillérek megerősítéséhez. Ezek szemléltetik összességében a DJP 2.0-ban megfogalmazott digitális jóléti célok elérésének alapjait, amelyek a 2. ábrán láthatók.



2. ábra: A Digitális Jólét Program stratégiai közelítése

Forrás: Digitális Jólét Program 2.0 stratégiai tanulmány, 2017. 6.

[61] 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről.

A Digitális Jólét Program jövőjét a DJP 1.0, valamint 2.0 sikereire építő DJP 2030 stratégiai keret adja, és alapvető feladata, hogy olyan új intézkedésekre, megoldásokra és intézményekre tegyen javaslatot, amelyek a hazai feladatok mellett a nemzetközi együttműködésben is hatékonyan tudják értelmezni, kezelni a digitalizáció által folyamatosan megjelenő új globális kihívásokat és lehetőségeket. A digitális államkormányzás esetében az elkövetkező években is érvényes marad az „analóg" közigazgatás négy alappillére, úgymint szervezet, feladat, eljárás és személyzet, azonban ezekre épül a digitális államkormányzás három fő alkotóeleme, amelyek a következők:

- a tiszta adat;
- a hasznos robot;
- az érthető hálózat.

A DJP 2030 központi témája a digitális államkormányzás. E dokumentum a stratégiai célokat és beavatkozási területeket hármas felosztásban, az ember-gép-rendszer viszonylatában határozza meg.

- Az ember oldaláról a következő évtizedben már nem feltétlenül a digitális kompetenciák kialakítása lesz az alapvető feladat, hanem olyan keretek kialakítása, amelyben Magyarország lakossága a munkaerőpiacon, a közösségekben (kivált a családban) és állampolgárként is értékesen működő emberré tud válni a digitális környezetben.
- A gépekhez tartozik többek között a digitális gazdaság és a digitális infrastruktúra. Ezen a területen alapvetően olyan gazdasági környezetet kell létrehozni, amelybe szívesen fektetnek be a high-tech cégek, a korábbinál erősebb, proaktív fogyasztóvédelmet kell kialakítani, továbbá kiemelt figyelmet kell arra fordítani, hogy a globális nyomás ellenére is legyen megtartó ereje a hazai munkaerőpiacnak, a jól képzett hazai munkaerő ne áramoljon ki az országból.
- A rendszer oldaláról az elsődleges cél az automatizálás, ennek során a digitális államkormányzás keretén belül tiszta adatokkal dolgozó hasznos robotokkal és közérthető hálózaton keresztül történne az alapvető feladatok ellátása.[62]

A Digitális Jólét Program egyes elemeit a 2. táblázat szemlélteti.

[62] Gál András Levente: *A polgárokra fókuszáló patrióta közadat-politikára van szükség.* (2020. március 12.).

2. táblázat: A Digitális Jólét Program stratégiai elemei

Stratégiák	Digitális hozzáférés	Digitális hálózatok	Digitális tudás	Digitális állam	Digitális gazdaság
Magyarország Digitális Oktatási Stratégiája (DOS)	Digitális adócsökkentés	Szupergyors Internet Program (SZIP)	Digitális tudásfejlesztés	Digitális biztonság	Ipar 4.0
Magyarország Digitális Startup Stratégiája (DSS)	Digitális Jólét Alap-csomag (DJA)	Magyarországi 5G Koalíció (5GK)	Digitális Jólét Program Hálózat	Okos Város – Smart city	Digitális Munkaerő Program (DMP)
Magyarország Digitális Exportfejlesztési Stratégiája (DES)	Digitális Jólét WiFi	Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF)	OkosÓvoda Program	Digitális közigazgatás	Digitális Egészségipar-fejlesztési Stratégia (DEFS)
Magyarország Digitális Gyermekvédelmi Stratégiája (DGYS)		Nemzeti Távközlési Gerinchálózat (NTG)	Digitális Kompetencia Keretrendszer		Magyarország Digitális Agrár Stratégiája (DAS)
DJP 2.0 – Stratégiai tanulmány		Mobilinternet Hálózatfejlesztés	DJP Lab		Digitális Jólét Hitelprogram
Közgyűjteményi Digitalizálási Stratégia (KDS)			Digitális Sport Tudásközpont		Digitális Jólét Tőkeprogram
					Mesterséges Intelligencia Koalíció (MI Koalíció)
					Digitális Fogalomtár
					Fintech Stratégia
					Digitális Jólét Pénzügyi Védjegy

Forrás: Digitális Jólét Program 2.0 stratégiai tanulmány, 2017

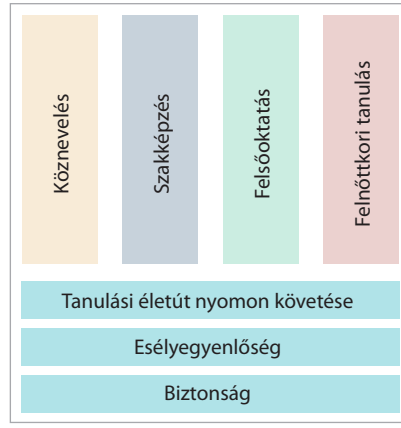
Magyarország Digitális Oktatási Stratégiája

Magyarország kormánya 2016. október 13-án elfogadta az 1536/2016. számú kormányhatározatot, amely alapján döntött a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról, illetve annak végrehajtásáról. A határozat alapján elfogadták a Digitális Jólét Program részeként bemutatott Magyarország Digitális Oktatási Stratégiáját (DOS). A kormány az oktatás digitális megújítása érdekében:

- Létrehozta a Digitális Pedagógiai Módszertani Központot, amely beépíti a tanulókkal és a pedagógusokkal szembeni elvárások közé a digitális képességeket, és ehhez különböző kompetencia-keretrendszereket alakít ki. Ennek megfelelően senki sem hagyhatja el az oktatást a megfelelő digitális képességek nélkül.
- Biztosítja a köznevelés és szakképzés valamennyi intézménye számára a digitális oktatáshoz szükséges magas sávszélességű, szupergyors internetelérést, továbbá az épületeken belüli wifihálózatokat.
- Biztosítja a stratégia által meghatározott digitális eszközállományokat a köznevelési és szakképzési intézményekben, külön figyelmet fordítva a sajátos nevelési igényű tanulókra, valamint fontos elem, hogy a tanulók saját eszközei is beépülnek az eszközrendszerbe.
- A köznevelési és szakképzési intézményekben a pedagógusok munkáját IKT pedagógiai asszisztensek támogatják, továbbá minden köznevelési és szakképzési intézményben elérhetővé vált a rendszergazda-szolgáltatás.
- Felmérte a pedagógusok digitális kompetenciáit, és ennek alapján a fejlesztési igényeknek megfelelő tananyagok és oktatási módszerek fejlesztése szintén megvalósult, amellyel végrehajtható a pedagógusok képzése.
- Megtörtént a Nemzeti Köznevelési Portál (Okosportál) továbbfejlesztése, valamint összekapcsolása a közgyűjteményi tartalomtárakkal.
- Valamennyi magyar polgár számára biztosítottá vált a lehetőség az alapszintű digitális írástudás elsajátítására térítésmentes képzéseken lakó- vagy tartózkodási helyén, vagy annak legfeljebb 30 kilométeres környezetében.
- Digitális Felsőoktatási Kompetencia-központot hozott létre, amely közreműködik a felsőoktatás szabályozási és akkreditációs feltételeinek felülvizsgálatában és a képzési kínálat megújításában.

– Kibővítette az elektronikus oktatásadminisztrációs szolgáltatások körét, összekapcsolta a tanulói életút szempontjából meghatározó adatbázisokat, valamint közhiteles és elektronikus módon hozzáférhetőek lettek a megszerzett oktatási tanúsítványok az Oktatási Anyakönyv Rendszeren keresztül.[63]

A Digitális Oktatási Stratégia a köznevelés, a szakképzés, a felsőoktatás, valamint a felnőttkori tanulás négy alapvető pillérére épül (lásd 3. ábra).



3. ábra: A Digitális Oktatási Stratégia pillérszerkezete
Forrás: Magyarország Digitális Oktatási Stratégiája, 2016

Minden egyes terület esetében rögzítették a stratégiai célokat, a jövőképet, az eszközrendszert, amelyekkel az adott terület fejleszthető, kidolgoztak olyan cél-eszköz mátrixokat, amelyek bemutatják, hogy melyik eszközcsoportok mit fejlesztenek, valamint az egyes területek finanszírozási formáit. A DOS kiterjed az oktatás minden szintjére és tényezőjére, úgymint:

– az alkalmazott módszertanra (tanárképzés és továbbképzés, valamint intézményi fejlesztések);
– a pedagógusok digitális felkészültségére és attitűdjeire;
– a fizikai infrastruktúrára, hozzáférésre, belső hálózatokra;

[63] 1536/2016. (X. 13.) Korm. határozat a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról.

– az oktatási intézmények eszközellátottságára;
– a Nemzeti Alaptanterv és Kerettanterv felülvizsgálatával és a digitális tartalomfejlesztéssel a tartalomra;
– az oktatásirányításra (az adminisztrációra és a minőségirányításra, a törzsinformációs rendszerre, a tanulói mérésértékelésre, a vezetői információs rendszerre).[64]

Magyarország Digitális Startup Stratégiája

Magyarország kormánya 2016. december 27-én elfogadta az 1858/2016. számú kormányhatározatot, amelynek alapján döntött a hazai innovatív vállalkozói környezet fejlesztéséről, a feltörekvő digitális vállalkozások versenyképességének javításáról és Magyarország Digitális Startup Stratégiájáról, illetve annak végrehajtásáról. A határozat kimondja, hogy elfogadták a Digitális Jólét Program részeként bemutatott Magyarország Digitális Startup Stratégiáját (DSS). A stratégia megvalósítása érdekében létrehozták a Startup Hungary Koordinációs és Módszertani Központot a startup-ökoszisztéma fejlesztését célzó programok összehangolása, az állami programok, pályázati lehetőségek hatékonyabb kommunikációja, valamint a stratégia monitoringrendszerének kialakítása és működtetése érdekében.[65] A DSS célja az innovatív, komoly növekedési potenciállal rendelkező startupvállalkozások létrejöttének és fejlődésének támogatása. A stratégiában megfogalmazottaknak megfelelően olyan szabályozási környezetet alakítanak ki, amely rugalmasan és nyitottan áll az új technológiák nyújtotta változásokhoz, felismerve, hogy a gyors reagálás versenyelőnyt jelent a globális gazdaságban. A DSS támogatja a digitális és nyelvi, illetve a kommunikációs és marketingkompetenciák fejlesztését valamennyi startupvállalkozás körében, valamint biztosítja, hogy létrejöjjenek és megerősödjenek a startup-ökoszisztéma megfelelő működése érdekében elengedhetetlen olyan intézmények, mint például az inkubátorházak vagy mentori hálózatok, továbbá biztosítja a megfelelő finanszírozási források elérhetőségét a különböző életszakaszban lévő startupvállalkozások számára. A stratégia alapvető célja, hogy biztosítsa a startup-ökoszisztéma kiegyensúlyozott fejlődését

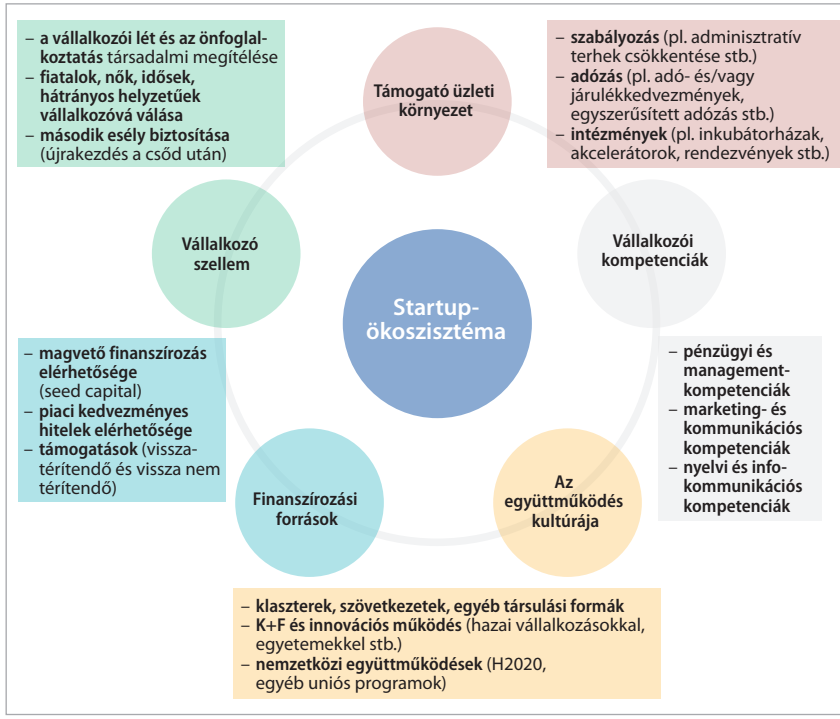
[64] 1536/2016. (X. 13.) Korm. határozat.

[65] 1858/2016. (XII. 27.) Korm. határozat a hazai innovatív vállalkozói környezet fejlesztéséről, a feltörekvő digitális vállalkozások versenyképességének javításáról és Magyarország Digitális Startup Stratégiájáról.

a vállalkozószellem, a vállalkozói kompetenciák és az együttműködés kultúrája megerősítésével, a támogató üzleti környezet fejlesztésével és a finanszírozási források célzott elérhetővé tételével. Mindezek megvalósításához a DSS öt pillért azonosít:

- vállalkozószellem;
- vállalkozói kompetenciák;
- az együttműködés kultúrája;
- támogató üzleti környezet;
- finanszírozási források.

A 4. ábra ismerteti az egyes pillérek által lefedett területeket.



4. ábra: A Digitális Startup Stratégia pillérei által lefedett területek

Forrás: Magyarország Digitális Startup Stratégiája, 2016. 9.

Magyarország Digitális Exportfejlesztési Stratégiája

Magyarország kormánya 2016. szeptember 15-én elfogadta az 1491/2016. számú kormányhatározatot, amely alapján döntött a digitális termékek és szolgáltatások exportjának növeléséről, Magyarország Digitális Exportfejlesztési Stratégiájáról, illetve annak végrehajtásáról. A határozat kimondja, hogy elfogadták a Digitális Jólét Program részeként bemutatott Magyarország Digitális Exportfejlesztési Stratégiáját (DES). A határozat alapján:

- a digitális ipar területén tapasztalható jelentős munkaerőhiány mérséklése és a munkaerőpiaci szereplők digitális kompetenciáinak javítása érdekében meghirdették a Digitális Munkaerő Programot;
- kiemelt célként rögzítették az informatikai szakemberképzés folyamatos bővítését;
- biztosítottá vált az informatikai szolgáltatóközpontok (Shared Service Center – SSC) magyarországi jelenlétének erősítése, valamint bővítették az informatikai szolgáltatóközpontok szakemberigényének kielégítését szolgáló képzések körét;
- a stratégia végrehajtásának elősegítése érdekében megalapították a Digitális Exportfejlesztési Tárcaközi Bizottságot (DETB).[66]

A Digitális Exportfejlesztési Stratégia átfogó célja intenzív digitális termékexport-növekedéssel elérni, hogy erős digitalizációs tudás alakuljon ki Magyarországon, amely:

- erős modernizációs hatást fejt ki a gazdaságra, különösen a kkv-szektorra;
- a fiatalok számára nagyszámú vonzó munkahelyet teremt;
- segíti Magyarország külpiaci megítélését, javítja országimázsát;
- segíti az az innovatív iparfejlesztés irányainak meghatározásáról szóló Irinyi-terv végrehajtását az egész gazdaságban;
- iparági pilotként más iparágak export- és kkv-fejlesztési terveihez is példaként szolgálhat.[67]

[66] 1491/2016. (IX. 15.) Korm. határozat a digitális termékek és szolgáltatások exportjának növeléséről, Magyarország Digitális Exportfejlesztési Stratégiájáról.

[67] Magyarország Digitális Exportfejlesztési Stratégiája, 2016. 6.

A stratégia összességében hozzájárul ahhoz, hogy Magyarország a digitalizációs trend haszonélvezője legyen. A DES egy olyan átfogó kormányzati intézkedéscsomagot határoz meg, amely hozzájárul az informatikai kkv-k exportképességének javításához. A digitális gazdaság exportteljesítményének javulása jelentős mértékben hozzájárul a magyar gazdaság növekedéséhez, számos olyan új munkahelyet teremt, ami a fiatalok számára is vonzó, növeli a hazai digitális innovációt, valamint a magyar tudás és innováció hasznosításával javítja Magyarország nemzetközi megítélését. A stratégiában meghatározott célok elérése érdekében végrehajtandó feladatokat a 3. táblázat szemlélteti.

3. táblázat: A magyar digitális ipar exportteljesítmény-növelése érdekében végrehajtandó feladatok

Fő célok	**A magyar digitális ipar exportteljesítményének növelése**			
Alcélok	Magyarország digitális versenyképességének javítása	Digitális termékek és szolgáltatások exportha-tékonyságának növelése	Digitális kompetencia- és szolgáltatásfejlesztés	
Intézkedés (pillér)	Állami digitális megoldások exportja	Startupok exportfejlesz-tése (Digitális Startup Stratégia)	Kkv-k exportfejlesztése	SSC-k exportfej-lesztése
Horizontá-lis terület	Emberi erőforrások biztosítása			
	Gazdasági hatás mérése (GDP, export, munkahelyek)			

Forrás: Magyarország Digitális Exportfejlesztési Stratégiája, 2016. 9.

Magyarország Digitális Gyermekvédelmi Stratégiája

Magyarország kormánya 2016. szeptember 2-án elfogadta az 1488/2016. számú kormányhatározatot, amely alapján döntött a gyermekek számára biztonságos internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról, illetve annak végrehajtásáról. A határozat kimondja, hogy elfogadták a Digitális Jólét Program részeként bemutatott Magyarország Digitális Gyermekvédelmi Stratégiáját (DGYS). A határozat alapján:

– ingyenesen hozzáférhető, magyar nyelvű, korszerű gyermekvédelmi szűrőszoftvereket kell kifejleszteni annak érdekében, hogy a gyermekek

számára veszélyes és káros tartalmak szűrése lehetővé váljon minden család számára;
- egy olyan adatbázist állítottak össze, amely megfelel a nemzetközi jó gyakorlatoknak, és tartalmazza a gyermekek számára veszélyes és káros (black list), illetve a gyermekek számára javasolt (white list) online tartalmakat;
- a gyermekek számára biztonságos tartalmakat, valamint az online gyermekvédelemmel kapcsolatos fontos információkat összegyűjtő és ezeket a gyermekek, a szülők és pedagógusok számára bemutató honlapokat hoztak létre (például: http://saferinternet.hu/, https://biztonsagosinternet.hu/, www.digitaliscsalad.hu, http://televele.hu/, http://mediatudor.hu/, www.kamaszpanasz.hu).[68]

Magyarország Digitális Gyermekvédelmi Stratégiájának célja, hogy megvédje a gyermekeket az internet káros tartalmaitól és módszereitől, a kockázataitól, valamint összehangolt lépésekkel felkészítse őket, a szüleiket és tanáraikat a tudatos és értékteremtő internethasználatra. A tudatos internethasználat egy nagyon fontos képesség, amellyel a gyermekeket mindenképpen fel kell vértezni, hogy a digitalizáció nyertesei lehessenek. A stratégia három pilléren nyugszik, és ez a szerkezet megjelenik a helyzetértékelésben, a célok meghatározásában, valamint az eszközök azonosításában is:
- tudatosítás és médiaműveltség;
- védelem és biztonság;
- szankcióalkotás és segítségnyújtás.[69]

A stratégiában meghatározott pillérekhez rendelt átfogó, stratégiai célkitűzéseket és feladatokat a 4–6. táblázat szemlélteti.

[68] 1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról.
[69] *Magyarország Digitális Gyermekvédelmi Stratégiája,* 2016.

4. táblázat: A tudatosítás és médiaműveltség pillér átfogó célkitűzései és feladatai

Célok	Feladatok
Monitoringrendszer felállítása és rendszeres mérések, kutatások végzése	Rendszeres, átfogó internetes gyermekvédelmi mérések, kutatások elvégzése
A gyermekek médiaműveltség-oktatása	A gyermekek médiaoktatásának átalakítása
Tanárképzés és tananyagfejlesztés	A tanárok képzésének átalakítása és a szükséges tananyagok előállítása
Az egyéb érdekeltek képzése	Az igazságszolgáltatás érintett szereplőinek és az állami gyermekvédelem rendszerében dolgozók kötelező képzése, a szülők képzési lehetőségének megteremtése
Gyűjtőhonlap és hitelesítés	Az információk könnyű elérhetőségének megteremtése és a hitelesítés rendszerének felállítása

Forrás: Magyarország Digitális Gyermekvédelmi Stratégiája, 2016. 76–77.

5. táblázat: A védelem és biztonság pillér átfogó célkitűzései és feladatai

Célok	Feladatok
Megfelelő szűrőszoftver-megoldások folyamatos biztosítása	A törvényi követelményeknek és a technológiai kívánalmaknak eleget tevő szűrőszoftver elérhetővé tétele
Káros tartalmak szűrésének alternatív megoldásai	Az alapbeállításként bevezetett hálózati szintű szűrőeszközök várható hatásainak, következményeinek előzetes értékelése
Hatékony műszaki megoldások alkalmazása	A hatékony műszaki megoldások alkalmazási lehetőségeinek átgondolása a médiaszabályozás által nem érintett internetes tartalmak vonatkozásában
Veszélyes és javasolt tartalmak kezelése (black list és white list)	Gyermekek számára káros, jogellenes, továbbá a kifejezetten számukra javasolt internetes oldalakat tartalmazó listák összeállítása és naprakészen tartása
Az iparági társszabályozás erősítése	Az ön- és társszabályozó szervezetekkel szorosabb és hatékonyabb együttműködés kialakítása
A büntetőjog ultima ratio jellege	A jogalkalmazás szereplői számára megfelelő képzés és továbbképzés biztosítása a jogsértő magatartások megfelelő szintű felismerése és értékelése érdekében
A gyermekek számára biztonságos és hasznos tartalmak körének bővítése	Kifejezetten a gyermekek számára készített tartalmak mennyiségének és sokszínűségének növelése

Forrás: Magyarország Digitális Gyermekvédelmi Stratégiája, 2016. 78–80.

6. táblázat: A szankcióalkalmazás és segítségnyújtás pillér átfogó célkitűzései és feladatai

Célok	Feladatok
Információgyűjtés	A hatékony fellépés érdekében össze kell gyűjteni és adatbázis keretei között rendszeresen frissíteni szükséges az elkövetett sérelmes magatartások számát, jellegét, típusát
Alternatív sérelemkezelési eljárások	A gyermekek által vagy sérelmére elkövetett online zaklatásokat, megfélemlítéseket (cyberbullying) indokolt esetben alternatív vitarendezési mechanizmusok keretében kell kezelni
Az online megfélemlítés (cyberbullying) kezelése	Kereteket és feltételeket kell biztosítani az online bántalmazások megfelelő szintű kezeléséhez és számuk lehetőség szerinti visszaszorításához
Feladatok a meglévő jogorvoslati mechanizmusok szélesebb körű megismertetése terén	A médiaoktatásban erőteljesen meg kell jeleníteni az elszenvedett károk kezelésének jogi lehetőségeit, az alkalmazható eljárásokat

Forrás: Magyarország Digitális Gyermekvédelmi Stratégiája, 2016. 81–83.

Közgyűjteményi Digitalizálási Stratégia

Magyarország kormánya 2017. június 28-án elfogadta az 1404/2017. számú kormányhatározatot, amely alapján döntött a Digitális Nemzet Fejlesztési Program megvalósítása során elkészült Közgyűjteményi Digitalizálási Stratégiáról, illetve annak végrehajtásáról. A határozat kimondja, hogy elfogadták a Digitális Jólét Program részeként bemutatott Közgyűjteményi Digitalizálási Stratégiát (KDS). A határozat alapján létrejött a Közgyűjteményi Digitalizálási Kollégium, ami alaprendeltetéséből adódóan felelős a közgyűjtemények együttműködéséért. Összeállították továbbá a Nemzeti Adattár Projektet és a projekt részeként a Kulturális Tanösvény alprojektet.[70]

A stratégia alapvető célja egy egységes közgyűjteményi keresőrendszer megalkotása, ami összekapcsolja a különböző tartalmakat, és az együttműködésre építve egy speciális közgyűjteményi, szabványosított kezelőfelületet hoz létre,

[70] 1404/2017. (VI. 28.) Korm. határozat a Digitális Nemzet Fejlesztési Program megvalósítása során elkészült Közgyűjteményi Digitalizálási Stratégiáról.

ezzel hozzájárulva, hogy a nemzeti öntudatra nevelés és a nemzeti alapműveltség elsajátítása során támaszkodni lehessen kulturális-szellemi örökségünk valamenynyi, közgyűjteményben fellelhető adattartalmára. Ehhez elengedhetetlen, hogy:

- a közgyűjtemények a kulturális örökség őrzőiből, a kulturális örökség első számú, autentikus, forrásértékű megosztóivá váljanak;
- a digitalizálás legyen eszköz ahhoz, hogy az emberek könnyebben juthassanak hozzá az egyéni élethelyzetüket javító tudáshoz;
- javuljon a digitális kulturális tartalmakat használók életminősége;
- javuljon a felhasználói komfortérzet;
- érzékelhetővé váljon az oktatás és a közgyűjteményi tartalomszolgáltatás egymásrautaltsága;
- javuljon az állampolgárok digitális kompetenciáinak minősége.

A KDS alapján a szolgáltatásorientált szemlélet megvalósítását három pillérre épülő célrendszer szolgálja:

- digitális közösség;
- digitális készség;
- digitális gazdaság.[71]

Az egyes pillérekhez tartozó célokat és indikátorrendszereket a 7. táblázat tartalmazza.

7. táblázat: A Közgyűjteményi Digitalizálási Stratégia pilléreken alapuló cél- és indikátorrendszere

Pillér	Célok	Indikátor
Digitális közösség	az egyes szolgáltatási célcsoportok meghatározása	felhasználók száma célcsoportonkénti bontásban
	virtuális kiállítások létrehozása	virtuális kiállítások száma
	e-kölcsönzés lehetőségének megteremtése	kölcsönzött dokumentumok mennyisége
	adatbázisok közötti interoperabilitás létrehozása	összekötött adatbázisok száma
	intézményközi együttműködések elősegítése	megkötött együttműködések száma

[71] *Közgyűjteményi Digitalizálási Stratégia (2017–2025),* 2017.

Pillér	Célok	Indikátor
Digitális készség	tanulási, informálódási szokások változásának lekövetése, új technológiák adaptálása	infokommunikációs eszközök terjedésének mértéke
	webaratás és -archiválás kifejlesztése	archivált és aratott oldalak száma, gyakorisága
	e-tananyag-fejlesztés	a formális oktatásban való elterjedés mértéke
	kompetenciafejlesztés	az akkreditált digitális kompetenciafejlesztést célzó képzések száma
	önálló tanulási kompetenciák fejlesztése	a tartalomszolgáltatás hasznosulása a nonformális és informális tanulás keretei között
Digitális gazdaság	innováció elősegítése	
	a tudományos teljesítmény fokozása	a tudományos kutatók Hirsch-indexének és impaktfaktoros reprezentációjának emelkedése, illetve a magyarországi közgyűjteményi tartalmak külföldi idézettségének emelkedése
	a hazai innovációs rendszer megerősítése	a felsőoktatás gazdasági szerepének megerősítésében való részvétel aránya
	fenntartható tudásgazdaság megteremtése	a kutatási és oktatási szegmensben történő összesített megjelenés mértékének emelkedése

Forrás: Közgyűjteményi Digitalizálási Stratégia (2017–2025), 2017. 42.

Digitális hozzáférés

A Digitális Jólét Program célja, hogy Magyarország minden lakosa internet-hozzáféréssel rendelkezzen. Ennek eléréséhez minden olyan akadályt igyekszik megszüntetni, amely annak az útjában áll, hogy valaki internethasználóvá válhasson. Ennek megfelelően alakították ki az alábbi három programot:

- Digitális adócsökkentés;
- Digitális Jólét Alapcsomag;
- Digitális Jólét WiFi.

Digitális adócsökkentés

A digitális adócsökkentéssel Magyarországon az internet-előfizetés áfája két lépésben 27%-ról 5%-ra csökkent, ezzel hazánkban lett a legalacsonyabb

az internetezés adója az Európai Unió tagállamai között, és nagymértékben hozzájárult, hogy az emberek internet-hozzáféréssel rendelkezzenek.[72]

Digitális Jólét WiFi

Magyarországon az elmúlt években a Digitális Jólét Program keretében közel minden településen legalább egy közintézményben és legalább egy közterületen ingyenes, széles sávú wifiszolgáltatást építettek ki, a polgárok digitális kompetenciáinak fejlesztése, valamint az egyre inkább elterjedő állami digitális szolgáltatások hozzáférésének biztosítása céljából.[73]

Digitális hálózatok

A digitális gazdaság, a polgárok és a vállalkozások digitális kompetenciáinak fejlesztéséhez, valamint az állami digitális szolgáltatások elterjedéséhez elengedhetetlenül szükséges a megfelelő hálózati infrastruktúra kialakítása. Ennek érdekében alakították ki a Digitális Jólét Program keretein belül a digitális hálózatok pillért, ami az alábbi elemeket foglalja magában:

- Szupergyors Internet Program (SZIP);
- 5GK – Magyarországi 5G Koalíció;
- NTG – Nemzeti Távközlési Gerinchálózat;
- NIIF – Nemzeti Információs Infrastruktúra Fejlesztési Program;
- Mobilinternet Hálózatfejlesztés.

Szupergyors Internet Program

Összhangban az Európai Unió digitális menetrendjével, Magyarország Nemzeti Infokommunikációs Stratégiájában alapvető célkitűzésként szerepel, hogy 2020-ra minden háztartás számára elérhető lesz a legalább 30 Mbps sebességű interneteléréshez való hozzáférés lehetősége, továbbá hogy a háztartások legalább 50%-ában 100 Mbps-os internet-hozzáférés álljon rendelkezésre. Ennek megvalósítása érde-

[72] Digitális Jólét Program: *Digitális adócsökkentés,* 2019.
[73] Digitális Jólét Program: *Digitális Jólét WiFi,* 2019.

kében született a Szupergyors Internet Program (SZIP) az 1486/2015. (VII. 21.) Kormányhatározattal a Digitális Nemzet Fejlesztési Program megvalósításával kapcsolatos aktuális feladatokról, valamint egyes kapcsolódó kormányhatározatok módosításáról. A fentiek mellett a határozatban megfogalmazták azt is, hogy a köznevelési intézmények által igénybe vett szolgáltatások által használt hálózatok érjék el az átlagosan 50 Mbps sávszélességet, valamint a felsőoktatási és más kutatási intézmények által végzett kutatás-fejlesztési és innovációs tevékenységek hatékonyságának a növelése érdekében a jelenlegi szuper-számítástechnikai kapacitásokat 75%-kal növelni kell. A digitális állam kialakításával kapcsolatosan a határozat kimondja, hogy ki kell alakítani és működtetni kell egy olyan szervezeti és tudásplatformot, amely összefogja és összehangolja az intelligens városi szolgáltatásokat, és nyomon követi a teljes rendszer működését.[74]

A megfogalmazott célkitűzésekkel összhangban a program feladatai között szerepel továbbá az országos internetlefedéshez szükséges fejlesztések előkészítése, a pénzügyi, infrastrukturális és a fejlesztési tervezés, valamint a teljes folyamat ellenőrzése. A 2019 januárjában indult Szupergyors Internet Program második fázisa során további új célokat és feladatokat fogalmaztak meg a „Gigabitalapú társadalom" és az 5G stratégiákban leírtaknak megfelelően, amelyek során a legalább 100 Mbit feletti és elsősorban optikai hálózati infrastruktúrák kialakítása került előtérbe.[75]

A Magyarországi 5G Koalíció

A Digitális Jólét Program által kezdeményezett Magyarországi 5G Koalíció (5GK) célja, hogy Magyarország az 5G fejlesztések egyik európai központjává váljon, és vezető szerepet töltsön be az 5G-re épülő alkalmazások fejlesztésében, tesztelésében a régióban, valamint hogy hazánk a világ élvonalába tartozzon az 5G bevezetése, elterjedése és gyakorlati alkalmazása területén. Az 5G Koalíció tevékenységét héttagú választott elnökség irányítja, szakmai munkáját öt munkacsoportjában folytatja, ezek az alábbiak:

1. *5G stratégia munkacsoport*

A stratégiai munkacsoport feladata javaslatok és ajánlások készítése a készülő Magyarországi 5G stratégiához.

[74] 1486/2015. (VII. 21.) Korm. határozat a Digitális Nemzet Fejlesztési Program megvalósításával kapcsolatos aktuális feladatokról, valamint egyes kapcsolódó kormányhatározatok módosításáról.
[75] Kormányzati Informatikai Fejlesztési Ügynökség: *Szupergyors Internet Program (SZIP),* 2019.

2. *Hálózatfejlesztés és infrastruktúra munkacsoport*

A munkacsoport feladata hálózatfejlesztési javaslatok kidolgozása az új hálózati architektúrára és az 5G bevezetése kapcsán felmerülő technológiai kihívásokra tekintettel.

3. *Alkalmazások és mintarendszerek munkacsoport*

A munkacsoport feladata az 5G-re épülő alkalmazások beazonosítása, a magyar piac számára potenciális versenyelőnyt biztosító alkalmazások kiemelésével.

4. *Tesztkörnyezet munkacsoport*

A munkacsoport feladata javaslatok és ajánlások kidolgozása a kialakítandó tesztkörnyezet vagy tesztkörnyezetek műszaki, technológiai, infrastrukturális igényeire, különös tekintettel a konfigurálható 5G hálózatokra.

5. *Nemzetközi együttműködések munkacsoport*

A munkacsoport feladata a lehetséges határ menti közös projektek kialakítása, együttműködések megvalósítása, EU-s kutatás-fejlesztési pályázatok és források beazonosítása, az 5G fejlesztéseket elősegítő további nemzetközi szakmai együttműködési lehetőségek feltérképezése.

Nemzeti Távközlési Gerinchálózat

2012. január 1-jével kezdte meg működését a Nemzeti Távközlési Gerinchálózat, amelynek működési alapjait a 346/2010. (XII. 28.) kormányrendeletben a kormányzati célú hálózatokról fektették le. A rendelet kimondja, hogy a Nemzeti Távközlési Gerinchálózat (NTG) biztosítja a kormányzati célú hírközlési szolgáltatás igénybevételére kötelezett és jogosult felhasználók számára az elektronikus hírközlési szolgáltatásokat.[76]

A Digitális Jólét Program keretében az NTG fejlesztése is megvalósul, így az állami, az önkormányzati és a közigazgatási szervezetek, intézmények által igénybe vett internethálózatot is megújítják.

Nemzeti Információs Infrastruktúra Fejlesztési Program

A Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF) feladata a magyarországi felső- és közoktatási intézmények, kutató-fejlesztő helyek,

[76] 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról.

közgyűjtemények és más oktatási, tudományos és kulturális szervezetek információs infrastruktúrájának és számítógépes hálózati szolgáltatásainak összehangolt fejlesztése, valamint az országos és nemzetközi hálózati kapcsolatok, információs szolgáltatások elérésének biztosítása. A program keretében valósul meg a magyar köznevelési, felsőoktatási, kutatási és közgyűjteményi hibrid hálózat fejlesztése és működtetése, továbbá szintén a program keretében biztosított a fenti közösségek számára az integrált országos számítógép-hálózati infrastruktúrához, valamint az erre épülő, kommunikációs, információs és kooperációs szolgáltatásokhoz való hozzáférés, továbbá egy élvonalbeli alkalmazási környezet és tartalomfejlesztési, illetve tartalomelérési háttér használata.[77]

Mobilinternet Hálózatfejlesztés

Magyarország kormánya nemzetgazdasági szempontból kiemelt jelentőségű üggyé nyilvánította a magyarországi távközlési szolgáltatók nagy sebességű mobil hírközlési (4G, 4G+, 5G) hálózatfejlesztési beruházásait a 484/2017. (XII. 28.) kormányrendelettel a nagy sebességű mobil hírközlési hálózatfejlesztési beruházások megvalósításával összefüggő közigazgatási hatósági ügyek nemzetgazdasági szempontból kiemelt jelentőségű üggyé nyilvánításáról. A rendelet a szolgáltatók 4G, 4G+ és 5G széles sávú mobilhálózati infrastruktúra beruházásait nemzetgazdasági szempontból kiemelt jelentőségű beruházásokká nyilvánította, amely beruházások révén a kiépülő 4G mobilhálózatok infrastrukturális alapját képezik a közeljövő ötödik generációs (5G) mobilhálózat-fejlesztéseinek is.[78]

Digitális tudás

A digitalizáció napjaink egyik legfontosabb eszköze, amellyel komoly sikerek érhetők el mind nemzeti, mind nemzetközi szinten. Ennek alapvető elemei a digitális alapkompetenciák, amelyek hiánya napról napra erőteljesebben rontja az érintett polgárok munkaerőpiaci kilátásait, ami egyrészt elmélyíti a társadalmi egyenlőtlenségeket, másrészt gyengíti a gazdaság versenyképességét is. Ezért a Digitális Jólét

[77] Kormányzati Informatikai Fejlesztési Ügynökség: *A KIFÜ lett a jogutódja a Nemzeti Információs Infrastruktúra Fejlesztési Intézetnek,* 2020.

[78] Digitális Jólét Program: *Mobilinternet Hálózatfejlesztés,* 2019.

Program (DJP) egyik legfontosabb célkitűzése, hogy minden polgárnak, minden vállalkozásnak esélye legyen arra, hogy egyet előrelépjen a digitális felkészültségében.

A digitális tudás növelése érdekében a DJP az alábbi pilléreket határozza meg:

- Digitális tudásfejlesztés;
- Digitális Jólét Program Hálózat;
- OkosÓvoda Program;
- Digitális Kompetencia Keretrendszer;
- DJP Lab;
- Digitális Sport Tudásközpont.

Digitális tudásfejlesztés

A Digitális Jólét Program 2.0 keretén belül dolgozták ki a digitális kompetenciák mérési rendszereit, valamint a digitális kompetenciafejlesztés hosszú távú, részletes koncepcióját, amellyel a polgárok és a vállalkozások digitális kompetenciái folyamatosan fejleszthetők. Ennek megvalósításához került kialakításra a Digitális Jólét Program Hálózat, amelyben az ott dolgozó Digitális Jólét Program-mentorok segítségével válik elérhetővé a digitális világgal való megismerkedés és az alapszintű digitális kompetenciák ingyenes elsajátítása.[79]

A Digitális Jólét Program Hálózat

A Digitális Jólét Program Hálózat a Digitális Jólét Koordinációs Központ által koordinált program, amelynek célja a magyar polgárok kompetenciafejlesztése mentorok segítségével a digitális írástudatlanság csökkentése érdekében.

OkosÓvoda Program

Az OkosÓvoda Program a Digitális Jólét Program keretében nyújt elsősorban honlapkialakítási és -kezelési lehetőséget a magyarországi óvodák számára. A program keretében már számos óvoda kapott lehetőséget honlap kialakítására és üzemeltetésére, valamint ingyenes felkészítésre a témában.

[79] Digitális Jólét Program: *Digitális tudásfejlesztés,* 2019.

A DJP Lab

A DJP Lab fő célkitűzése, hogy képzési programjain keresztül kutassa és támogassa a technológiai eredmények kreatív használatát és az innovatív lehetőségeket, amelyek a különböző tudástranszferek révén a nyílt innováció fejlesztését segíthetik. A Lab digitalizációval, mesterséges intelligenciával és fenntarthatósággal kapcsolatos kutatásai igyekeznek hozzájárulni a technológiai fejlődés nyomán keletkező kérdések megválaszolásához, valamint lehetőséget teremt a fiatal kreatívipari szakemberek számára új okosváros-megoldások kitalálására és fejlesztésére, továbbá az iparági partnerekkel való együttműködésre és kapcsolatépítésre.[80]

Digitális Sport Tudásközpont

A digitalizáció a sportökoszisztémára is komoly hatással van, hiszen a hordozható teljesítménymérők és összetett adatelemző szoftverek segítik a sportolók felkészülését, illetve hozzájárulnak a minél pontosabb és hatékonyabb kiválasztási és tehetséggondozási rendszerek működtetéséhez. Ezzel összhangban jött létre 2018 novemberében a Digitális Sport Tudásközpont, amely segíti a sport digitális átállási folyamatainak előmozdítását szakmai és közigazgatási szempontból. A Tudásközpont a Digitális Jólét Program 2.0 keretén belül 2019-ben elkészítette Magyarország Digitális Sport Stratégiáját, amely a sportágazat digitális fejlesztésével kívánja támogatni a magyar sport versenyképességének növelését. A tudásközpont tevékenységének fókuszában áll az iskolai testnevelés digitális átállási folyamatainak támogatása is, amely során célja a testnevelésórák élményalapúvá tétele a modern generációk igényeihez igazodva, digitális technológiák bevonásával.[81]

Digitális állam

A Digitális Jólét Program célja minél szélesebb rétegek bevonása a digitális ökoszisztémába, ahol a legjobb eredményeket a szolgáltatások fejlesztésével, valamint a polgárok kompetenciáinak növelésével lehet elérni. Ennek megfelelő kialakításához határozták meg a digitális állam pillért, ami három területet foglal magában:

- Digitális közigazgatás;

[80] Digitális Jólét Program: *DJP Lab,* 2019.
[81] Digitális Jólét Program: *Digitális Sport Tudásközpont,* 2021.

– Okos Város – Smart city;
– Digitális biztonság.

Digitális közigazgatás

A Digitális Jólét Program a teljes közigazgatás digitális átalakításához kapcsolódva olyan új javaslatokat fogalmaz meg, amelyek hozzájárulhatnak az állami szolgáltatások digitális átalakításához és elérhetővé tételéhez. A DJP 2.0-ban megfogalmazottaknak megfelelően a közigazgatás digitalizálása nem egy informatikai projekt, hanem egy társadalmi program, amely során számos, a teljes közigazgatás digitális átalakítását szolgáló átfogó digitális közigazgatási képzési és továbbképzési programot dolgoztak ki és indítottak el.[82]

A DJP 2.0-ban megfogalmazott célok és tevékenységek a digitális közigazgatás vonatkozásában:

– Meg kell teremteni a digitális közigazgatás-kutatás és -fejlesztés, valamint -felügyelet egységes és integrált intézményrendszerét.
– Felnőttképzési programot kell indítani a digitális ügyintézési kompetencia fejlesztése érdekében.
– Országos kampányt kell indítani a digitális közigazgatási szolgáltatások ismertségének megteremtése érdekében.
– Magyarország és különösen a kormányzat informatikai függetlensége elérésének egyik sarokpontja, hogy a kormányzat a megfelelő informatikai kompetenciával rendelkezzen a hazai fejlesztők számára is hozzáférhető nyílt megoldások bevezetéséhez, támogatásához, illetve továbbfejlesztéséhez, testreszabásához.[83]

Okos Város – Smart city

A 21. században zajló urbanizációnak köszönhetően a városok a gazdaság egyik alapvető tényezőjévé váltak. A DJP 2.0 célja, hogy a települések, a polgárok, a vállalkozások és a közösségek minél szélesebb körben ki tudják használni az okosváros-fejlesztések kínálta lehetőségeket, illetve hozzájárul ahhoz, hogy

[82] Digitális Jólét Program: *Digitális közigazgatás,* 2019.
[83] *Digitális Jólét Program 2.0 stratégiai tanulmány,* 2017.

az okosváros-fogalom és -intézményrendszer szervesen illeszkedjen a magyar közigazgatási, elsősorban önkormányzati és területi közigazgatási jogrendszerbe és jogalkalmazási gyakorlatba.[84]

A DJP 2.0-ban megfogalmazott célok és tevékenységek a digitális közigazgatás vonatkozásában:

- okosváros és okostérség közigazgatási mintaprojektek létrehozása;
- a jelenleg elérhető okosváros-megoldások tesztelése, ügyfél-elégedettség és -hatékonyság mérése;
- szabályozási és finanszírozási modellek kialakítása, képzésfejlesztés;
- okosváros-megoldások megjelenítése a kormánytisztviselői és kiemelten köztisztviselői képzésben, valamint a nappali tagozatos felsőoktatásban;
- okosváros munkacsoport-létrehozása a Digitális Jólét Program és Okos Város Platformok (Tudásplatform és Technológiai Platform) tevékenységeinek összehangolása érdekében;
- az Integrált Területfejlesztési Stratégia (ITS) felülvizsgálata az Okos Város Fejlesztési Modell alapján.[85]

Digitális biztonság

A Digitális Jólét Program 2.0 egyik kiemelt célja a biztonságos kibertér megteremtése is. Ennek megfelelően kerültek a következő célok és feladatok a DJP 2.0 tanulmányba:

- a nemzeti kiberbiztonsági stratégia felülvizsgálata a kibervédelmi és -támadási képességek fejleszthetőségének tükrében;
- a kibertámadási képességfejlesztés lehetőségének megvizsgálása a kibertérben érkező fenyegetések elleni hatékony fellépés érdekében;
- a hazai jogszabályi háttér uniós harmonizálása;
- digitális információbiztonsági és kiberbiztonsági oktatási és továbbképzési, átképzési koncepció kialakítása;
- a hazai ICT-szektor kiberbiztonsági innovációinak támogatása;
- nemzeti kiberbiztonsági eseménykezelő központ kialakítása;
- a közigazgatási szervek kibervédelmi kapacitásának bővítése;
- a kkv-k kibervédelmi kapacitásának javítása;

[84] Digitális Jólét Program: *Okos Város – Smart city,* 2019.
[85] *Digitális Jólét Program 2.0 stratégiai tanulmány,* 2017.

– az Infokommunikációs Egységes Referenciakeret (IKER) információbiztonsági és kiberbiztonsági részeinek felülvizsgálata.[86]

Digitális gazdaság

A magyar gazdaság versenyképességének kulcsa a digitális átalakulásra való vállalati és munkavállalói felkészülés és átállás. Ennek megfelelően Magyarország kormánya számos digitális munkahelyet kíván létrehozni az ipar, a mezőgazdaság és a szolgáltató szektor területein belül, másfelől folyamatosan fejleszteni kívánja a munkavállalók digitális felkészültségét, kompetenciáit. Mindezek biztosításához a DJP 2.0 tanulmányban az alábbi, a digitális gazdaság vonatkozásában kulcsfontosságú területeket nevezték meg:

– Ipar 4.0;
– DMP – Digitális Munkaerő Program;
– DEFS – Digitális Egészségipar-fejlesztési Stratégia;
– DAS – Magyarország Digitális Agrár Stratégiája;
– Digitális Jólét Hitelprogram;
– Digitális Jólét Tőkeprogram;
– Mesterséges Intelligencia Koalíció;
– Digitális Fogalomtár;
– Fintech Stratégia;
– Digitális Jólét Pénzügyi Védjegy.

Ipar 4.0

Az Ipar 4.0 kifejezés alatt alapvetően az ipari termelés területén zajló technológiai forradalmat értjük, amely többek között magában foglalja a digitalizált termelési láncokat, a robotikát, az automatizációt, az ember és a gépek együttműködésére épülő kiberfizikai rendszereket is. Az Ipar 4.0 jellemzője a digitalizáció, ami nagymértékben formálhatja át a megszokott gyártási, termelési folyamatokat és eljárásokat.[87]

2016 májusában megalakult az Ipar 4.0 Nemzeti Technológiai Platform (I4.0 NTP), amelynek feladata egy olyan felület biztosítása, ami gyártási és logiszti-

[86] *Digitális Jólét Program 2.0 stratégiai tanulmány,* 2017.
[87] Digitális Jólét Program: *Ipar 4.0,* 2019.

kai rendszerek vonatkozásában hidat képez a fizikai és a digitális világ között. A platform lehetőséget biztosít a gazdaság szereplői, különösen a kormányzati iparpolitika kiemelt ágazatai, valamint az állami gazdaságpolitika és az innovációs ökoszisztéma intézményei számára, hogy a lehető leggyorsabb és legjobb válaszokkal szolgáljanak a témában felmerült kérdésekre. A platform hangsúlyos céljai között szerepel:

- az Ipar 4.0 paradigma stratégiai fontosságának felismertetése és terjesztése elsősorban a kkv-körben, amelyek az élenjáró nemzetközi nagyvállalatok beszállítóiként különös jelentőségűek az ország versenyképességének erősítésében;
- a digitalizációs technológiák terjesztése;
- a hozzájuk kapcsolódó képességek fejlesztése;
- szakértői tevékenységek;
- mintalabor-hálózatok kialakítása;
- az Európában kialakult legjobb gyakorlatok, elsősorban a legfejlettebb németországi minták átvételének segítése;
- iparvállalatok Ipar 4.0-érettségének az állami pályázati rendszerben elismert minősítésének kidolgozása saját módszertan szerint;
- a teljes magyarországi szakemberképzés megújításának elősegítése.[88]

Digitális Munkaerő Program

A magyar kormány határozott törekvése, hogy a digitalizációval több új, magas hozzáadott értéket termelő munkahelyet hozzon létre, mint amennyi munkahely megszűnik. Ehhez mind a vállalkozások szemléletmódjában, mind digitális felkészültségükben, mind pedig a digitális munkaerő képzésében jelentős előrelépést kíván elérni. Ennek megvalósításához készült a Digitális Munkaerő Program (DMP), amely végrehajtásának első szakaszában a hangsúly elsősorban a rövid ciklusú, nem hagyományos informatikusképzési programokra helyeződött, azóta azonban megnövekedett a digitális értelemben magasan képzett szakemberek pótlását szolgáló képzések száma.[89]

A DMP legnagyobb bázisa, azaz akik a program keretein belül képzést kaphatnak, az aktív korú munkavállalókból kerül ki. Számukra a digitális továbbképzés vagy átképzés jelentheti a munkaerőpiaci reintegrációt, vagy egy magasabb jöve-

[88] I4.0 NTP: *Az Ipar 4.0 Nemzeti Technológiai Platform Szövetség,* 2021.
[89] Digitális Jólét Program: *DMP – Digitális Munkaerő Program,* 2019.

delmet kínáló munkahely megszerzését, illetve a jelenlegi munkahely megőrzésének esélyét. A DMP szintén támogatja a hátrányos helyzetűeket, akiknek nehézkes az informatikai képzésekre való bekerülés, illetve a program fontos eleme a kkv-k munkavállalóinak képzése, átképzése, valamint a digitális kompetenciák fejlesztése.[90]

Digitális Egészségipar-fejlesztési Stratégia

A Digitális Jólét Program keretén belül megkezdődött Magyarország Digitális Egészségipar-fejlesztési Stratégiájának (DEFS) kialakítása, amely elsősorban a polgárok egészségnyereségét helyezi a középpontba. A polgárok mellett a digitalizáció nyertesei lehetnek az egészségügyi szakdolgozók is, ami hozzájárulhat munkaterhelésük csökkentéséhez, a minőségi betegellátás kialakításához, valamint új munkahelyek kialakításához is. A digitális alkalmazásokhoz és megoldásokhoz való hozzáférések lehetőségének kialakítása nagymértékben növelheti a polgárok egészségtudatosságát, ami fejleszti hazánk egészségkultúráját.

A fentiek kialakítása érdekében a DJP 2.0 stratégiai tanulmányban megfogalmazottak az egészségügy digitalizációjának a lakossági felhasználás elterjedésétől a komplex intézményrendszeri integrációig minden területet fel kell ölelnie az alábbiak szerint:

- Egyéni felhasználás: általában mobil- vagy hordható okoseszköz-alkalmazások, amivel az egyének a saját adataikat gyűjthetik és követhetik.
- Közösségi használat: az online közösség támogatására, többnyire játékosításra (gamification), versenyzésre épülő modell, ami működő platformot és megfelelő kritikus tömeget igényel.
- Integrált rendszer: az egyéni és a kórházi adatbázisok, illetve a betegek és az orvosok összekötésével egy magasabb szintre emeli az egészségügyi ellátást.
- Komplex rendszer: big data, prediktív előrejelzések, és/vagy mesterséges intelligencia segítik az ellátási rendszer optimalizálását, a személyre szabott ellátás kialakítását.
- Kockázatok és veszélyek (adatvagyonnal kapcsolatos visszaélések, személyiségi jogi problémák, etikai problémák, kiforratlan megoldások azonnali implementációi, hatástanulmányok hiánya stb.) kezelése.[91]

[90] *Digitális Munkaerő Program stratégiai dokumentum,* 2018.
[91] *Digitális Jólét Program 2.0 stratégiai tanulmány,* 2017.

Az 1517/2020. (VIII. 14.) Kormányhatározattal Magyarország átfogó Egészségipari Stratégiájáról és annak végrehajtásáról a Digitális Egészségipar-fejlesztési Stratégia beépült az Innovációs és Technológiai Minisztérium Egészségipari Stratégiájába, amely öt pilléren nyugszik, és az alábbi kilenc, egészségüggyel kapcsolatos területre összpontosít:

- a gyógyszeripar;
- az orvostechnikai eszközök;
- a biotechnológia;
- a gyógynövényipar;
- a genomika;
- a bionika;
- a klinikai vizsgálatok;
- az egészségturizmus;
- e-health.[92]

Magyarország Digitális Agrár Stratégiája

2019-ben készült el Magyarország Digitális Agrár Stratégiája (DAS) a Digitális Jólét Program keretén belül. A stratégia célja a mezőgazdasági termelés jövedelmezőségének növelése az információk gyűjtésével, feldolgozásával és megfelelő elemzésével, valamint a technológiai műveletek automatizálásával és robotizálásával úgy, hogy ezek mellett a rendelkezésre álló környezeti erőforrásokat a lehető leghatékonyabban használják fel. A stratégiában megfogalmazott célok elérése érdekében a gazdálkodás alábbi ágazataiban kell a modernizációt végrehajtani:

- a szántóföldi növénytermesztésben;
- az állattenyésztésben;
- a kertészetben;
- a szőlészetben;
- a halászatban;
- az erdészetben.[93]

[92] 1517/2020. (VIII. 14.) Korm. határozat Magyarország átfogó Egészségipari Stratégiájáról és annak végrehajtásáról.

[93] Digitális Jólét Program: *DAS – Magyarország Digitális Agrár Stratégiája,* 2019.

A DAS átfogó céljának teljesülését három stratégiai, valamint négy horizontális területen nyolc horizontális cél támogatja, amelyek alapján tizenkét jövőképet fogalmaz meg az 5. ábra alapján.

Digitális Jólét Hitelprogram

A Digitális Jólét Hitelprogram 2018 szeptemberétől kedvezményes hitellel támogatta a hazai mikro-, kis- és középvállalkozások, illetve startupok digitálistermék- és szolgáltatás-fejlesztési projektjeit a Digitális Jólét Pénzügyi Program (DJPP) részeként. A támogatott projektek minden esetben illeszkedtek a DJP stratégiai célkitűzéseihez, így jellemzően az alábbi területeket támogatták:

- oktatás;
- állami szolgáltatások;
- egészségügyi és jóléti szolgáltatások;
- a digitális gazdaság különböző ágazatai;
- információbiztonság (Cyber security);
- digitális infrastruktúra, 5G fejlesztések és kapcsolódó innovációk;
- egyéb digitális innovációk.[94]

A hitelprogram jelenleg szünetel.

A Digitális Jólét Tőkeprogram

A Digitális Jólét Pénzügyi Program (DJPP) részeként igénybe vehető Digitális Jólét Tőkeprogram célja, hogy a magas növekedési potenciálú, érettségüket tekintve induló (pre-seed vagy seed), startup- és érettebb fázisban lévő vállalkozások infokommunikációs vagy új digitális megoldásokat megvalósító, a Digitális Jólét Program stratégiai célkitűzéseihez illeszkedő digitális fejlesztéseit, termékeit vagy szolgáltatásait támogassa a digitális infrastruktúra, a digitális kompetenciák, valamint a digitális gazdaság fejlesztése, továbbá a digitális állam kialakítása területeken.[95]

[94] Digitális Jólét Program: *Digitális Jólét Hitelprogram,* 2018.
[95] Digitális Jólét Program: *Digitális Jólét Tőkeprogram,* 2019.

5. ábra: A Digitális Agrár Stratégia jövőképe és célrendszere

Forrás: Magyarország Digitális Agrár Stratégiája 2019–2022, 2019

Mesterséges Intelligencia Koalíció

A Mesterséges Intelligencia Koalíció egy állandó szakmai és együttműködési fórumot biztosít az MI-fejlesztők, az MI felhasználói oldalát képviselő piaci és állami szereplők, illetve az akadémiai szféra, a szakmai szervezetek és az állami intézmények számára a mesterséges intelligencia hazai fejlesztési irányainak és kereteinek kialakítása, fejlesztése céljából.

A koalíció célja, hogy:

- Magyarország a mesterségesintelligencia-fejlesztések terén mihamarabb az európai élvonalba kerüljön, ezáltal hazánk a nemzetközi MI-közösség fontos referenciapontjává váljon;
- a mesterségesintelligencia-alapú fejlesztések széles körű elterjedésének és alkalmazásának köszönhetően jelentősen erősödjön a hazai vállalkozások versenyképessége;
- a magyar startupok és kkv-k nagy arányban vegyenek részt mesterségesintelligencia-fejlesztésekben, akár nagyvállalati, egyetemi vagy nemzetközi partnerségben;
- az állam a nemzeti adatvagyon átgondolt hasznosításával, valamint a digitális ökoszisztéma minden szereplője az adatvagyonok tisztességes, szabályozott és hatékony hasznosításával, illetve a mesterségesintelligencia-megoldások felhasználójaként vegye ki a részét a magyar társadalom és a nemzetgazdaság fejlesztésében.[96]

A fenti célok elérése érdekében 2020-ban elkészült Magyarország Mesterséges Intelligencia Stratégiája, hogy meghatározza azokat az alapvető belső és külső feltételeket, amelyek hozzájárulnak a magyar mesterségesintelligencia-fejlesztések véghezviteléhez. A megfogalmazott feltételek:

Belső feltételek:

- a köz- és magánadatok elérhetőségét biztosító adatgazdaság támogatása;
- alap- és igényvezérelt kutatói, fejlesztői közösség építése;
- a technológia magán- és vállalati alkalmazását segítő ökoszisztéma építése.

Külső feltételek:

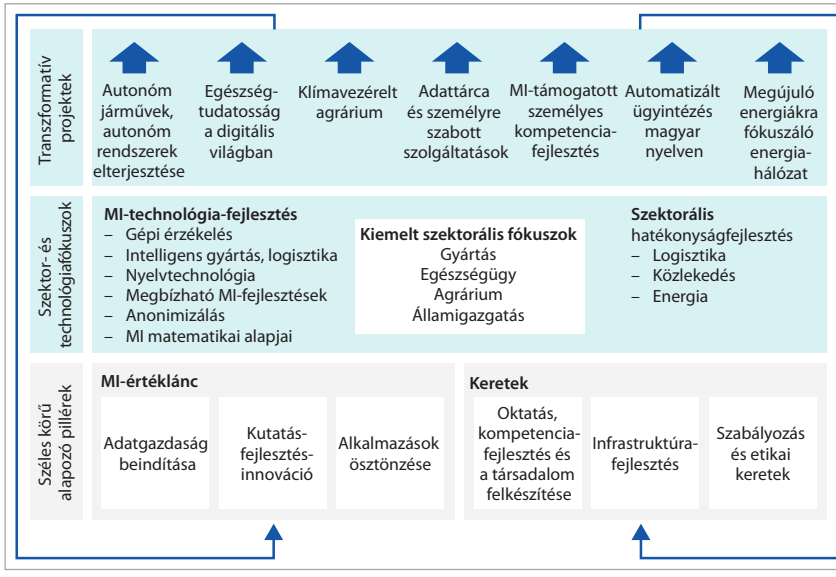
- a magabiztos MI-használathoz szükséges emberi képességek;
- a szoftveres és hardveres erőforrások rendelkezésre állása;

[96] Digitális Jólét Program: *Mesterséges Intelligencia Koalíció,* 2019.

– az egyértelmű és a további fejlődést és innovációt támogató szabályozási környezet.

A stratégia a fenti feltételekkel az alábbi területeket hivatott támogatni:
– gyártás;
– agrárium;
– egészségügy;
– államigazgatás;
– logisztika;
– közlekedés;
– energetika.

Az egyes pillérek, a kiemelt technológiák és szektorok szorosan illeszkednek egymáshoz, azok egymásra épülnek, a 6. ábrán látható módon.



6. ábra: A Mesterséges Intelligencia Stratégia egyes intézkedéscsoportjai, és azok egymáshoz való viszonya

Forrás: Magyarország Mesterséges Intelligencia Stratégiája 2020–2030, 2020, 22.

A stratégia számos, részben egymásra épülő intézkedésre, beavatkozásra tesz javaslatot a hazai technológiai adottságok felmérése alapján, amelyeket a következőképpen csoportosít:

- a mesterséges intelligencia jelentette gazdasági és társadalmi változásokra való felkészüléshez szükséges alapozó pillérek;
- a mesterséges intelligencia alkalmazása és bevezetése szempontjából kiemelten fontos szektorális és technológiai fókuszterületek;
- komplex, több ágazatot átfogó, már az állampolgárok felé is közvetlen hatást kiváltó transzformatív programok.[97]

Digitális Fogalomtár

A Digitális Jólét Program keretében összeállt egy folyamatosan bővülő Digitalizációs Fogalomtár, amely közérthetően, egységes szerkezetben, a lehető legkönnyebben elérhető és kereshető módon tartalmazza a digitalizációval kapcsolatos alapvető fogalmakat és szakkifejezéseket.[98]

Fintech Stratégia

A Digitális Jólét Program részeként létrehozták a hazai pénzügyi szektor digitalizációs stratégiáját, amelyben többek között megfogalmazták a rendkívül gyorsan fejlődő pénzügyi technológiai megoldások (Fintech) és a blokklánc-technológia (blockchain) széles körű alkalmazhatóságait. A dokumentum Magyarország Fintech Stratégiája címen került összeállításra, és meghatározott pillérek mentén építi fel az ágazati szakmai tevékenységeket és alakítja ki a szakmai együttműködéseket.[99]

[97] *Magyarország Mesterséges Intelligencia Stratégiája 2020–2030,* 2020.
[98] Digitális Jólét Program: *Digitális Fogalomtár,* 2019.
[99] Digitális Jólét Program: *Fintech Stratégia,* 2020.

Digitális Jólét Pénzügyi Védjegy

Magyarország kormánya kezdeményezte a Digitális Jólét Pénzügyi Védjegy pályázati rendszer kidolgozását a Digitális Jólét Program keretein belül. Ennek alapvető oka, hogy a kormány felismerte, hogy a digitális pénzügyi szolgáltatások mind az ágazati digitalizációhoz, mind pedig a digitális kompetenciafejlesztéshez hozzájárulnak, és szükséges egy olyan megoldás létrehozása, amely egyszerre jelent minőségi garanciát a ma még bizalmatlan felhasználók számára, ösztönzi a ma még távol maradókat a digitális szolgáltatások igénybevételére, illetve a pénzügyi szolgáltatókat a digitális (és akár fintech) megoldások és az ügyfélélmény fejlesztésére.[100]

A védjegy kidolgozása során kétszintű rendszer épült fel:

- Az első szintű minősítés a Digitális Hitelintézet/Biztosító DJP-partner, ahol a szolgáltatónak alapvető követelményeknek, biztonsági feltételeknek kell megfelelnie.
- A második szint, a Kiemelkedő Digitális Hitelintézet, illetve Biztosító védjegy, ahol szolgáltatók már oktatási és/vagy innovációs tevékenységet is végeznek.

A *Nemzeti Digitális Állampolgárság Program* a Digitális Magyarország Ügynökség (DMÜ) 2022-ben kidolgozott stratégiája, amelynek célja az állampolgári ügyintézés és az állam közötti kommunikáció digitális térbe történő áthelyezése, ezáltal megkönnyítve és felgyorsítva az adminisztrációs folyamatokat. A program a modern digitális infrastruktúrákra, integrált alapszolgáltatásokra és ügyfélbarát megoldásokra épül, figyelembe véve az Európai Unió irányelveit és stratégiáit.

A modern társadalmakban az állampolgári ügyintézés digitalizálása alapvető elvárás. A Magyarországon elsőként kialakított digitális megoldások sikeresnek mondható rendszerek voltak, például az eSZJA-felület, amely az adóbevallás területén jelentősen növelte a hatékonyságot. Ezekre a rendszerekre alapozva volt szükség további fejlesztésekre, hiszen számos közszolgáltatási terület nem rendelkezett hasonlóan fejlett digitális háttérrel, és az állami rendszerek közötti integráció is hiányos volt. A program célzott megoldásokat kínált és kínál ezekre a kihívásokra. A program fő célja egy modern, felhasználóbarát digitális ökoszisztéma kialakítása. Kiemelt irányelvek:

[100] Digitális Jólét Program: *Digitális Jólét Pénzügyi Védjegy,* 2020.

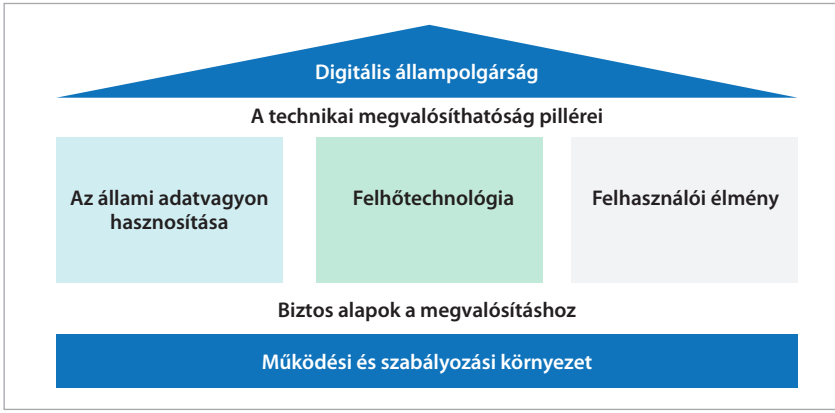
- Egyszerűség és elérhetőség: az ügyintézés legyen gyors, intuitív és könnyen hozzáférhető.
- Integráció: az állami rendszerek közötti adatáramlás megkönnyítése.
- Nemzetközi szabványok alkalmazása: az Európai Unió digitális irányelveivel összhangban történő fejlesztések.

A digitális állampolgárság alapjai

A program az alábbi négy digitális alapszolgáltatást határozza meg, amelyek a digitális átállás kulcsfontosságú elemei:

1. eSzemélyazonosítás: az online ügyintézés alapja, amely egyszerűen és biztonságosan azonosítja az állampolgárokat. A rendszer mobilalkalmazásokra épül, ami lehetővé teszi a gyors azonosítást akár arcfelismerés vagy biometrikus adatok segítségével.
2. ePosta: hivatalos kommunikációs platform, amely biztosítja az állam és az állampolgárok közötti hiteles, kétirányú levelezést. Az ePosta célja a papíralapú értesítések kiváltása és a költséghatékonyság növelése.
3. eDokumentumkezelés: egy központi tárhely az ügyintézés során keletkezett dokumentumok számára, amely könnyű hozzáférést és visszakereshetőséget biztosít az állampolgároknak.
4. eFizetés: egységes online fizetési rendszer, amely az állami és magánszolgáltatások díjainak egyszerű és biztonságos befizetésére alkalmas.

A program elsődleges célja a digitális állampolgárság hatékony megvalósítása, ami pozitív változásokat eredményez a lakosság számára. A korszerű digitális állampolgárság megvalósítása a fejlett technológiák használatát igényli a polgárok igényeinek figyelembevétele mellett. Ennek megfelelően a program három kulcsfontosságú pillért határoz meg, amelyek támogatják a digitális átállást, és irányítják annak fejlesztését. A három pillér a 7. ábrán látható.



7. ábra: A Digitális Állampolgárság pillérei
Forrás: Nemzeti Digitális Állampolgárság Program, 2022, 11.

Az állami adatvagyon hasznosítása

Az állami adatvagyon hatékony kezelése lehetővé teszi a gyorsabb ügyintézést az adatok biztonságos összekapcsolása révén. Innovációt biztosít a piaci szereplők számára megnyitott adatokból származó új szolgáltatásokkal, például közlekedési alkalmazásokkal vagy egészségügyi előrejelzésekkel. Az állami adatvagyon felhasználása azon az elven alapul, hogy a polgároknak joguk van az adatokhoz való hozzáféréshez, míg a közszervek csak az ügyintézéshez szükséges adatokat érhetik el. A program célja az adatokhoz való gyors és teljes körű hozzáférés biztosítása, ami növeli az ország versenyképességét. A Digitális Magyarország Ügynökség a polgárok tájékoztatására, a döntéshozatal támogatására és a közszolgáltatásokkal kapcsolatos adatok szolgáltatására összpontosít. Alapvető cél az adatok biztonságos kezelése, szavatolva a duplikációmentességet, a magas minőséget és a könnyű felhasználhatóságot. Az adatbázisok összekapcsolása támogatja a kormányzati döntéshozatalt és a polgárok életeseményeit. Az adatok átlátható interfészeken és API-okon (Application Programming Interface – API) keresztül, az uniós irányelvek betartásával, valós időben lesznek elérhetők.

A program meghatározása alapján az adatok hatékony felhasználásához háromszintű fejlesztésre van szükség: infrastruktúra, adatkezelés és felhasználási esetek. Az infrastruktúra adatbázisokból, adatintegrációból és felhasz-

nálói interfészekből áll. A meghatározás alapján az adatokhoz való hozzáférést szabványos API-okon keresztül valós idejűvé kell tenni, és egy felhasználóbarát interfész biztosítja, hogy az adatok a társadalom széles rétegeihez eljussanak, támogatva a döntéshozatalt és növelve a gazdasági versenyképességet. A hatékony adatkezelés javítja az adatok minőségét és hozzáférhetőségét, míg az adatstruktúra-kezelés a szervezetekben tárolt adatok részletes dokumentálására terjed ki. A program kimondja, hogy a hatékony adatkezeléshez szabályozási irányelvek és szoftvereszközök szükségesek. A szervezeteknek rögzíteniük és szabványosítaniuk kell az adatkezeléshez szükséges készségeiket és szervezeti egységeiket. Mindezek mellett a DMÜ célja az adatinfrastruktúra és az adatkezelési keretrendszerek kiépítése és fejlesztése, hogy azok a polgárok, a vállalkozások, a tudományos élet és a kormányzat számára a lehető legnagyobb hasznot hozzák.

Felhőtechnológia

Az állami felhőszolgáltatás célja a magyar versenyképesség növelése a rugalmas fejlesztési környezet, a költséghatékony üzemeltetés és a digitálisan élenjáró iparági szabványok bevezetése révén. A DMÜ a digitális fejlesztések során a skálázhatóságra, a kapacitáskiegyenlítésre és a gyorsabb fejlesztésre helyezi a hangsúlyt. Az első, digitális állampolgársághoz kapcsolódó alkalmazásokat már felhő-infrastruktúrára optimalizáltan fejlesztették. A szolgáltatásokat alapvetően egy globális felhőszolgáltató segítette elő, de a hosszú távú tervek alapján több szolgáltató is igénybe lesz véve. Elsőbbséget élveznek azok a partnerek, akik Magyarországon tervezik adatközpont létrehozását. A program kimondja, hogy a kormányzati felhőszolgáltatásokat elérhetővé teszik az állami szervek és vállalatok számára, és a befektetés megtérülésének felgyorsítása érdekében megvizsgálják a magánszektor bevonását is. Mivel a meglévő felhőszolgáltatásokat a jövőben folyamatosan fejleszteni és korszerűsíteni fogják, elengedhetetlen az olyan szakemberek képzése, akik a modern felhőtechnológiák területén szereznek használható elméleti és gyakorlati tudást. Ehhez képzési programokat alakít ki a DMÜ.

Az olyan országok, mint Magyarország, egyre inkább elfogadják a felhőalapú szolgáltatásokat, hogy javítsák a polgárok által ciklikusan igénybe vett elektronikus szolgáltatásaikat. Ezek a szolgáltatások rugalmasságot, megbízhatóságot, költséghatékonyságot, innovatív felhasználási eseteket, hatékonyabb fejlesztést és a közintézmények informatikai szabványosítását kínálják. A felhőtechnológia

lehetővé teszi az azonnali terheléselosztást, így az e-szolgáltatási platformok rugalmasak és megbízhatók lesznek. A felhőszolgáltatások a fejlesztőknek is innovatív lehetőségeket nyújtanak, lehetővé téve a nagyszabású szimulációt és a modern infrastruktúra-környezeteket. A magyar állam az összes állami intézményben központosítani tudja a fejlesztési elveket és az informatikai szabványokat, elkerülve az eltérő minőségű háttér-informatikai rendszerek okozta kompatibilitási problémákat. A program kimondja, hogy a magyar e-szolgáltatási ágazat a hatékonyabb fejlesztés, a rugalmasság, az innovatív felhasználói ügykezelés, a szabványosított IT-üzemeltetés és a költségcsökkentés érdekében a felhőszolgáltatások felé fordul. Az energiahatékony és környezetbarát adatközpontok az uniós irányelvekkel összhangban lesznek támogatva, ezzel is biztosítva a technológia környezetvédelmi előnyeit.

A felhasználói élmény javítása

A programban megfogalmazott irányelvek alapján a digitális állampolgársághoz kapcsolódó szolgáltatások és az adatokhoz való hozzáférés elsősorban egy mobilra optimalizált felületen keresztül lesz elérhető, amelyeket átmeneti webes felületek támogatnak. A fejlesztés egy egységes platformon lesz elindítva, a polgárok igényei és a tematikus platformok alapján. Egy jól átlátható platform segítségével a kormányzati szervezetek és az állami vállalatok digitális termékeinek teljes skálája elérhető lesz. A felületeket életkori alapon, egységes vizuális arculattal tervezik meg az összes közszolgáltatás és szervezet számára. Az e-szolgáltatásokban használt nyelvezet egyszerű, könnyen érthető és felhasználóbarát lesz. Az e-szolgáltatások mindenki számára hozzáférhetők lesznek, függetlenül a fizikai (testi és értelmi fogyatékosság) vagy a technológiai (digitálisan lemaradók) adottságoktól. Alapvető cél egy intelligens keresőmotor kialakítása, amely segíti az állampolgárokat a kívánt ügyintézési felület vagy szolgáltatás gyors megtalálásában. A dokumentum hangsúlyozza, hogy a digitális platformokat folyamatosan fejleszteni kell, az állampolgárok visszajelzései alapján. Az integrált mobilalkalmazások terjedése különösen fontos, mivel az okoseszközök egyre nagyobb szerepet kapnak az ügyintézésben, ennek megfelelően kell optimalizálni a kialakított platformokat.

Digitális kormányzati eredmények Magyarországon

Az Európai Bizottság 2024-ben kiadta a *Digitális évtized országjelentés 2024: Magyarország* című tájékoztató jelentését, amelyben összefoglalta az ország digitalizációjával kapcsolatban addig elért eredményeket. A jelentés az alábbi információkat tartalmazza:

A Bizottság megítélése alapján Magyarország képes hozzájárulni az Európai Unió digitális évtizedének célkitűzéseihez azáltal, hogy a sikeres digitalizáció révén elősegíti a versenyképességet, a rugalmasságot, a szuverenitást, az európai értékeket és az éghajlatvédelmi intézkedéseket. 2023-ban Magyarország jelentős előrelépést tett a széles sávú összeköttetés, az 5G-lefedettség és a kkv-k digitalizációja terén, különösen a felhő és az adatelemzés tekintetében. Ugyanakkor továbbra is kihívások állnak fenn a digitális készségek területén, kiváltképpen az idősebb generációk esetében, valamint a fejlett technológiák, például a mesterséges intelligencia bevezetésében. Magyarország célja, hogy 2030-ra a digitalizáció terén az EU tíz vezető gazdasága közé kerüljön, összhangban a 2022–2030-as nemzeti digitalizációs stratégiával.

Nemzeti digitális stratégiai ütemterv

Célok és kihívások

Magyarország 12 mutatóra állított fel célokat 2030-ra, mint például:

- 5G-lefedettség (99%);
- gigabit sebességű hálózatok (95%);
- alapvető digitális készségek (60%);
- felhőszolgáltatások és mesterséges intelligencia (MI) alkalmazása.

Az ország több területen elmarad az EU-s céloktól:

- például MI alkalmazása (cél: 24%; EU-cél: 75%);
- felhőmegoldások elterjedése (cél: 60%; EU-cél: 75%);
- digitális készségek (cél: 60%; EU-cél: 80%).

Az ütemterv prioritásai

- Digitális készségek és oktatás: jelentős forrásokat szánnak rá.
- E-egészségügy: az EgészségAblak (EESZT) mobilalkalmazás népszerűsítése.
- A kkv-k digitalizációja: programok indítása az MI és a big data alkalmazások terén.

Digitális infrastruktúra és technológia

Fejlesztések és kihívások

5G- és széles sávú hálózatok:

- Az ország 83,7%-os 5G-lefedettséget ért el (EU-átlag: 89,3%), cél a 99%-os lefedettség 2026-ra.
- A gigabites hálózatok lefedettsége 84,1%, meghaladva az EU átlagát (78,8%).
- Vidéken azonban még mindig jelentős lemaradás tapasztalható.

Félvezetők:

- Magyarország kísérletezik a kerámialapkák fejlesztésével chipgyártáshoz, de a félvezetőipar fejlesztésére jelenleg nincsenek nagyobb tervek.

Javaslatok

- Növelni kell a vidéki gigabithálózatok lefedettségét és az 5G fejlesztését.
- A félvezetők terén nagyobb fókusz az európai együttműködésekre.

A kkv-k digitalizációja

Eredmények

- A magyar kkv-k 53,2%-ának van legalább alapszintű digitális intenzitása, de ez elmarad az EU átlagától (57,7%).
- Jelentős növekedés történt a big data (53,2%) és a felhőalapú megoldások (37,1%) használatában, ami az EU-átlag közelében van.
- Az MI alkalmazása még alacsony (3,7%), de az MI Koalíció több mint 400 taggal dolgozik a technológia népszerűsítésén.

Javaslatok

- További támogatások a kkv-k számára MI- és big data megoldásokhoz.
- A felhőszolgáltatások elterjedésének ösztönzése.

Kiberbiztonság

Eredmények

- A kiberbiztonsági incidensek száma alacsonyabb az EU átlagánál, de a vállalatok felkészültsége gyenge (5,3%-uk rendelkezik biztosítással, EU-átlag: 25%).
- A Nemzeti Kibervédelmi Központ széles körű figyelemfelkeltő kampányokat és technikai auditokat végzett.

Javaslatok

- Növelni kell a vállalatok biztosítási lefedettségét és felkészültségét.
- Több erőforrást kell fordítani a kiberbiztonsági képzésre és a tudatosság növelésére.

Digitális készségek és közszolgáltatások

Digitális készségek

- A magyar lakosság 58,9%-ának vannak alapszintű digitális készségei, ami meghaladja az EU átlagát (55,6%), de az idősebb generációk lemaradása jelentős.
- 2023-ban több mint 260 ezer laptopot osztottak ki diákoknak és tanároknak a digitális készségek fejlesztése érdekében.

E-egészségügy

- Az EESZT alkalmazás több mint 2,5 millió felhasználóval rendelkezik, és a legnépszerűbb magyar mobilapplikáció.
- A laboratóriumi eredmények strukturált tárolása és megosztása 2024-ben kötelezővé vált.

Javaslatok

- Több forrás biztosítása az idősebb generációk és a sérülékeny csoportok digitális oktatására.
- Az e-egészségügyi infrastruktúra továbbfejlesztése és nemzetközi szabványokkal való összehangolása.

Digitális jogok és elvek

Főbb eredmények

- A magyarok 60%-a úgy véli, hogy az EU jól védi digitális jogait, ez magasabb az EU átlagánál (47%).
- Továbbá 68% elégedett az internet-hozzáférés megfizethetőségével és a környezetbarát online szolgáltatásokkal.

Javaslatok

- Fokozott figyelmet kell fordítani az online gyermekvédelemre és az internetes szólásszabadság biztosítására.
- A digitális jogokkal és elvekkel foglalkozó szabályzók szélesebb körű ismertetése.

Fenntarthatóság és zöld digitalizáció

Eredmények

- A vállalatok csupán 18,7%-a veszi figyelembe az ICT környezeti hatásait (EU-átlag: 48,7%).
- Az energiahatékonysági intézkedések növekvő számban jelennek meg az ICT-szolgáltatók között.

Javaslatok

- Az energiahatékonyság növelése a digitális infrastruktúrában, például adatközpontok és IoT-megoldások alkalmazásával.
- A digitális technológiák környezeti hatásainak pontosabb nyomon követése és csökkentése.

Összefoglalás

A fejezet az Európai Unió digitális stratégiáját és Magyarország digitalizációs célkitűzéseit tárgyalja, kiemelve a Digitális Európa Program hatását. Magyarország számára a digitalizáció elengedhetetlen az innovációs kapacitások növeléséhez, a versenyképesség erősítéséhez és a társadalmi jólét fokozásához. A legmodernebb technológiák – például mesterséges intelligencia (MI), nagy teljesítményű számítástechnika (HPC) és kiberbiztonsági rendszerek – széles körű alkalmazása biztosítja, hogy az ország lépést tartson az európai és globális trendekkel. A magyar kormányzat jelentős szerepet szán az infrastruktúra fejlesztésének, ideértve a gyors és biztonságos internetkapcsolatot, amely kulcsfontosságú a digitális szakadék csökkentésében. Az MI terén Magyarország aktívan részt vesz az európai adatterek létrehozásában, amelyek lehetővé teszik a kutatások és az ipari innovációk előmozdítását. Az ország külön hangsúlyt helyez a szuperszámítógépes rendszerek fejlesztésére, amelyek az egészségügy, a környezetvédelem és a közlekedés digitalizációját is támogatják. A kiberbiztonság területén Magyarország célja, hogy megerősítse a védelmi rendszereket a közszférában és a magánszektorban. Ehhez hozzájárulnak a digitális kompetencia-központok, amelyek nemcsak a technológiák telepítését, hanem a digitális készségek fejlesztését is elősegítik. A kkv-k számára elérhetővé teszik a legmodernebb digitális eszközöket, támogatva versenyképességüket és növekedési potenciáljukat a digitális gazdaságban. Az oktatás és képzés kiemelt szerepet kap Magyarország digitalizációs törekvéseiben. A fejlett digitális készségek fejlesztése érdekében támogatják az IT-szakemberek képzését, a munkaerőpiaci igényekhez igazított oktatási programokat, valamint a kkv-k és a közszféra munkavállalóinak célzott képzését. Az e-kormányzás fejlesztésével a közszolgáltatások digitalizációja egyszerűbbé és hatékonyabbá válik, elősegítve az állampolgárok számára nyújtott szolgáltatások minőségének javítását. A *Nemzeti Digitális Állampolgárság Program* központi eleme Magyarország digitalizációs törekvéseinek. Célja, hogy az állampolgárok széles körének biztosítson hozzáférést a digitális közszolgáltatásokhoz, fejlessze digitális írástudásukat és elősegítse a biztonságos online ügyintézést. A program külön figyelmet fordít az idősek, a hátrányos helyzetűek és a vidéken élők digitális kompetenciáinak bővítésére, hogy mindenki egyenlő eséllyel vehessen részt a digitális társadalomban. Az állampolgárok számára elérhetővé teszi a digitális azonosítást, és biztosítja a közszolgáltatások egyszerűbb és gyorsabb elérését, ezzel hozzájárul a társadalom digitális integrációjához, csökkenti a digitális szakadékot, és szavatolja, hogy Magyarország versenyképes legyen a digitális gazdaságban.

A digitális állam kialakításának kérdései és kihívásai

Az előző fejezetben bemutattuk azokat az uniós és hazai programokat és intézkedéseket, amelyek hozzájárulnak a digitális állam kialakításához, megfelelő alapot nyújtanak az egyes elemek digitalizációjához, fejlesztéséhez. Ebben a fejezetben pedig azokat a digitális kompetenciákat ismertetjük, amelyeket a fenti programokkal az Európai Uniónak, illetve Magyarországnak napjainkig sikerült elérnie. Ezt követően azokat a stratégiákat és keretrendszereket elemezzük, amelyek alapvető célja a digitális állam, az e-kormányzás kialakítása, üzemeltetésének és fenntartásának folyamatos biztosítása. A fejezetben szintén ismertetjük azokat a kihívásokat, amelyek a digitális államon belül a bizalom kiépítésére és fenntartására vonatkoznak, valamint a személyes adatok és a magánélet védelmével kapcsolatosan jelennek meg a jelenleg is rendelkezésre álló szigorú szabályzások ellenére is.

Digitális kompetenciák az Európai Unióban és Magyarországon

A digitális állam létrejöttéhez elengedhetetlen, hogy kialakuljanak a megfelelő kompetenciák a lakosság, a vállalkozások, illetve az állami intézmények minden szintjén. Ehhez nyújtanak megfelelő alapot és segítséget az előző fejezetben tárgyalt programok és stratégiák. Ebben az alfejezetben bemutatjuk azokat a kompetenciákat, amelyeket 2020-ig sikerült az uniónak és hazánknak elérnie. A felhasznált adatok az Európai Bizottság által kialakított és üzemeltetett adatbázisokból származnak. Ezek jelenleg 2020-ig tartalmazzák a különböző mutatókat, amelyek tematikus csoportokra osztva az európai információs társadalom néhány kulcsfontosságú dimenzióját szemléltetik. Ezek a mutatók lehetővé teszik az európai országok közötti és az időbeli fejlődés összehasonlítását. Az adatbázisokban megtalálható ágazatok és kulcsfontosságú dimenziók a következők:

- távközlési ágazat;
- széles sávú hozzáférés és lefedettség;
- széles sávú sebesség és árak;
- mobilpiac;
- internethasználat;
- audiovizuális és médiatartalom;

- az internetszolgáltatások igénybevétele;
- e-kormányzat;
- e-kereskedelem;
- eBusiness;
- digitális készségek;
- nők a digitális világban;
- IKT-szakemberek;
- eHealth;
- biztonság és adatvédelem;
- IKT-ágazat;
- EU-s kutatási és fejlesztési programok;
- háttérváltozók;
- megszűnt mutatók.[101]

A fentiek közül az alábbi, a téma szempontjából releváns területeket vizsgáljuk meg:

- széles sávú hozzáférés és lefedettség;
- internethasználat;
- az internetszolgáltatások igénybevétele;
- IKT-szakemberek;
- e-kormányzat.

Széles sávú hozzáférés és lefedettség az Európai Unióban és Magyarországon

A széles sávú hozzáférés esetében két területet mutatunk be: az új generációs hozzáférésű (Next Generation Access – NGA) széles sávú lefedettség/elérhetőség, valamint a vidéki vezetékes nagyon nagy kapacitású hálózati (Very High Capacity Network – VHCN) lefedettség.

Az új generációs hozzáférésű széles sávú lefedettség

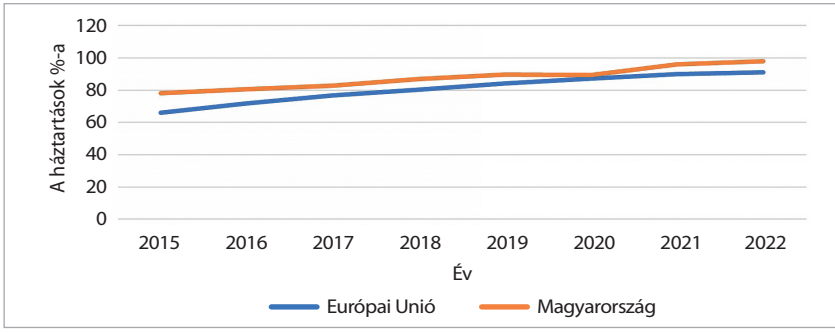
Az uniós és hazai NGA széles sávú lefedettségének alakulását a háztartások százalékos eloszlásának függvényében az alábbi táblázat és grafikon szemlélteti.

[101] European Commission: *Key Indicators of the European Information Society,* 2021.

8. táblázat: Az Európai Unió és Magyarország NGA széles sávú lefedettsége/elérhetősége

	2015 (%)	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)
Európai Unió	66	72	77	80	84	87	90	91
Magyarország	78	81	83	87	90	89	96	98

Forrás: European Commission: *Next Generation Access (NGA) Broadband Coverage/Availability (as a % of Households),* 2023



8. ábra: Az Európai Unió és Magyarország NGA széles sávú lefedettsége/elérhetősége
Forrás: European Commission: *Next Generation Access (NGA) Broadband Coverage/Availability (as a % of Households),* 2023

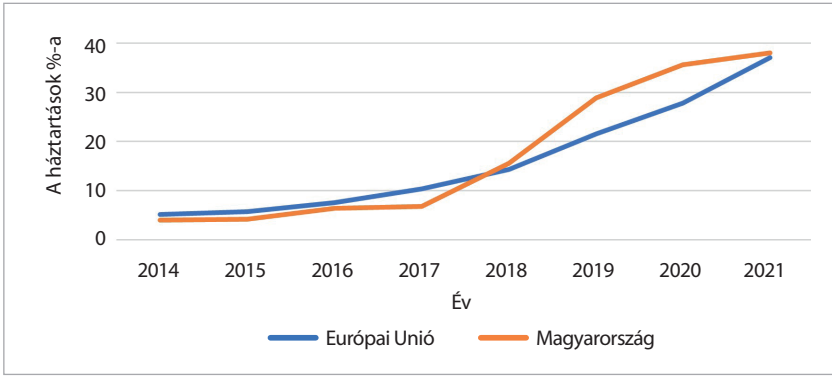
Vidéki vezetékes nagyon nagy kapacitású hálózati lefedettség

Az uniós és hazai vidéki vezetékes VHCN-lefedettség alakulását a háztartások százalékos eloszlásának függvényében a 9. táblázat és ábra szemlélteti.

9. táblázat: Az Európai Unió és Magyarország vidéki vezetékes VHCN-lefedettsége

	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)
Európai Unió	5	6	8	10	14	22	28	37
Magyarország	4	4	6	7	16	29	36	38

Forrás: European Commission: *Rural Fixed Very High Capacity Network (VHCN) Coverage in the European Union and Hungary,* 2022



9. ábra: Az Európai Unió és Magyarország vidéki vezetékes VHCN-lefedettsége
Forrás: European Commission: *Rural Fixed Very High Capacity Network (VHCN) Coverage in the European Union and Hungary,* 2022

Internethasználat az Európai Unióban és Magyarországon

Az internethasználat esetében két területet ismertetünk: a háztartások otthoni internethez való hozzáférését, valamint a lakosság azon részének vizsgálatát, akik soha nem használtak internetet.

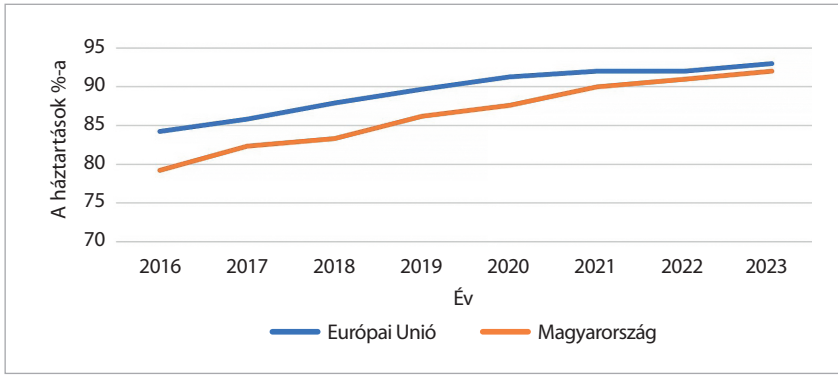
A háztartások otthoni internethez való hozzáférése

Az uniós és hazai háztartások otthoni internethez való hozzáférésének alakulását a háztartások százalékos eloszlásának függvényében a 10. táblázat és ábra szemlélteti.

10. táblázat: Az uniós és hazai háztartások otthoni internethez való hozzáférése

	2016 (%)	**2017 (%)**	**2018 (%)**	**2019 (%)**	**2020 (%)**	**2021 (%)**	**2022 (%)**	**2023 (%)**
Európai Unió	84	86	88	90	91	92	92	93
Magyarország	79	82	83	86	88	90	91	92

Forrás: European Commission: *Households With Access to the Internet at Home in the European Union and Hungary,* 2024



10. ábra: Az uniós és hazai háztartások otthoni internethez való hozzáférése
Forrás: European Commission: *Households With Access to the Internet at Home in the European Union and Hungary,* 2024

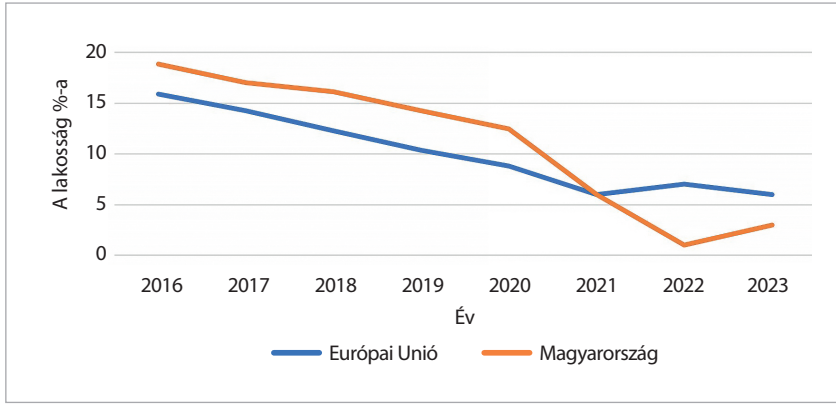
Lakosok, akik soha nem használtak internetet

Az Európai Unió és Magyarország 16 és 74 éves kor közötti lakosai közül azok százalékos eloszlását, akik soha nem használtak internetet, a 11. táblázat és grafikon szemlélteti.

11. táblázat: Az internetet soha nem használt uniós és hazai lakosság százalékos aránya

	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)	2023 (%)
Európai Unió	16	14	12	10	9	6	7	6
Magyarország	19	17	16	14	12	6	1	3

Forrás: European Commission: *Individuals Who Have Never Used the Internet in the European Union and Hungary,* 2024



11. ábra: Az internetet soha nem használt uniós és hazai lakosság százalékos aránya
Forrás: European Commission: *Individuals Who Have Never Used the Internet in the European Union and Hungary,* 2024

Az internetszolgáltatások igénybevétele az Európai Unióban és Magyarországon

Az internetszolgáltatások igénybevétele esetében négy területet mutatunk be: online információkeresés árukról és szolgáltatásokról, interneten keresztüli telefonálás vagy videóhívás (webkamera segítségével), online banki szolgáltatások használata, online tanfolyam elvégzése.

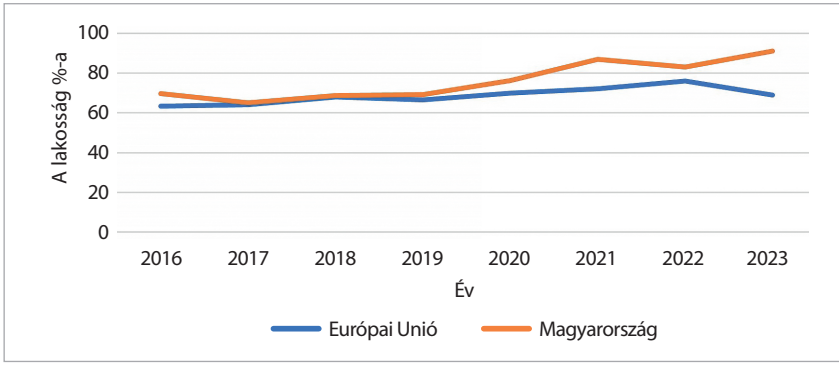
Online információkeresés árukról és szolgáltatásokról

Az Európai Unió és Magyarország 16 és 74 éves kor közötti lakosainak százalékos eloszlását a 12. táblázat és ábra szemlélteti, azok vonatkozásában, akik kerestek már online információkat árukról és szolgáltatásokról.

12. táblázat: Az árukról és szolgáltatásokról online információkat kereső uniós és hazai lakosság százalékos eloszlása

	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)	2023 (%)
Európai Unió	63	64	68	66	70	72	76	69
Magyarország	70	65	69	69	76	87	83	91

Forrás: European Commission: *Looking for Information About Goods and Services Online in the European Union and Hungary,* 2024



12. ábra: Az árukról és szolgáltatásokról online információkat kereső uniós és hazai lakosság százalékos eloszlása

Forrás: European Commission: *Looking for Information About Goods and Services Online in the European Union and Hungary,* 2024

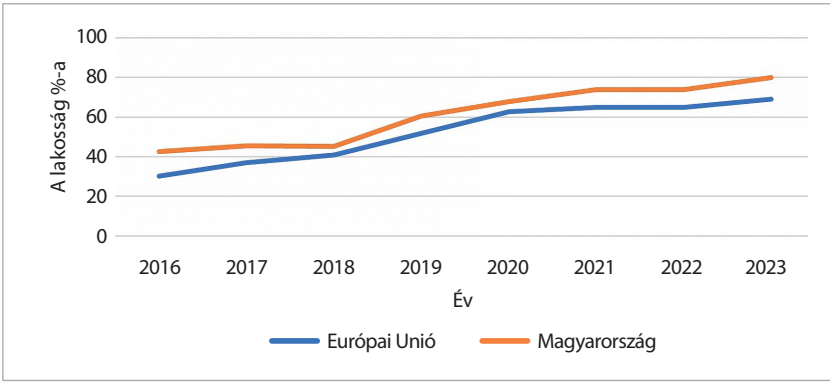
Interneten keresztüli telefonálás vagy videóhívás (webkamera segítségével)

Az Európai Unió és Magyarország 16 és 74 éves kor közötti lakosainak százalékos eloszlását a 13. táblázat és ábra szemlélteti, azok vonatkozásában, akik kezdeményeztek már interneten keresztül telefonálást vagy videóhívást webkamera segítségével.

13. táblázat: Az interneten keresztül telefonálást vagy videóhívást kezdeményező uniós és hazai lakosság százalékos eloszlása

	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)	2023 (%)
Európai Unió	30	37	41	52	63	65	65	69
Magyarország	42	45	45	61	68	74	74	80

Forrás: European Commission: *Telephoning or Video Calls (Via Webcam) Over the Internet in the European Union and Hungary,* 2024



13. ábra: Az interneten keresztül telefonálást vagy videóhívást kezdeményező uniós és hazai lakosság százalékos eloszlása
Forrás: European Commission: *Telephoning or Video Calls (Via Webcam) Over the Internet in the European Union and Hungary,* 2024

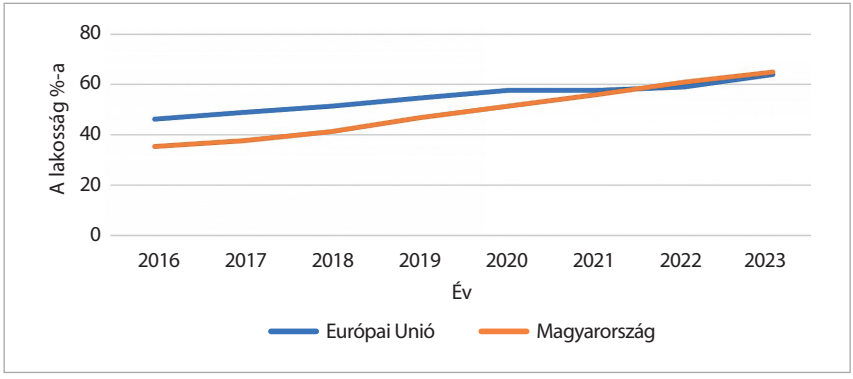
Online banki szolgáltatások használata

Az Európai Unió és Magyarország 16 és 74 éves kor közötti lakosainak százalékos eloszlását a 14. táblázat és ábra szemlélteti, azok vonatkozásában, akik használtak már online banki szolgáltatásokat.

14. táblázat: Online banki szolgáltatásokat használt uniós és hazai lakosság százalékos eloszlása

	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)	2023 (%)
Európai Unió	46	49	51	55	58	58	59	64
Magyarország	35	38	41	47	51	56	61	65

Forrás: European Commission: *Using Online Banking in the European Union and Hungary,* 2024



14. ábra: Online banki szolgáltatásokat használt uniós és hazai lakosság százalékos eloszlása
Forrás: European Commission: *Using Online Banking in the European Union and Hungary,* 2024

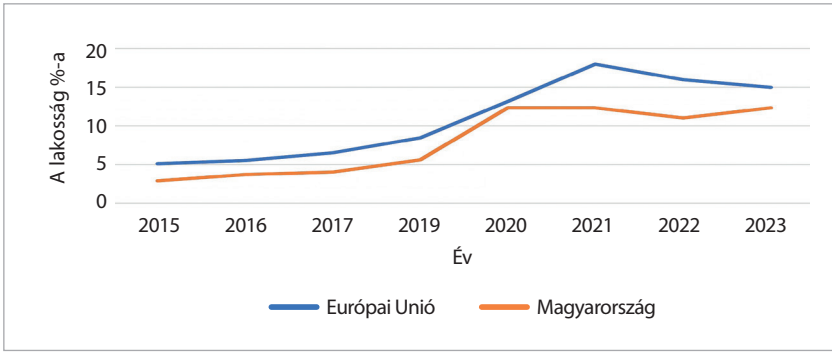
Online tanfolyam elvégzése

Az Európai Unió és Magyarország 16 és 74 éves kor közötti lakosainak százalékos eloszlását a 15. táblázat és ábra szemlélteti, azok vonatkozásában, akik végeztek már el online tanfolyamot.

15. táblázat: Az uniós és hazai lakosság százalékos eloszlása, akik végeztek már el online tanfolyamot

	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)	2023 (%)
Európai Unió	5	6	7	8	13	18	16	15
Magyarország	3	4	4	6	12	12	11	12

Forrás: European Commission: *Doing an Online Course in the European Union and Hungary,* 2024



15. ábra: Online tanfolyamot elvégzett uniós és hazai lakosság százalékos eloszlása
Forrás: European Commission: *Doing an Online Course in the European Union and Hungary,* 2024

IKT-szakemberek az Európai Unióban és Magyarországon

Az IKT-szakemberek esetében négy területet említünk: az IKT-szakembereket foglalkoztató vállalkozások számát, az IKT-szakértői készségekkel rendelkező foglalkoztatottak számát, azoknak a vállalkozásoknak a számát, amelyek képzést nyújtottak a munkavállalóknak, hogy fejlesszék/frissítsék az IKT-készségeiket, illetve a munkahelyen számítógépet használó, internet-hozzáféréssel rendelkező foglalkoztatottak (üzleti szektor) számát.

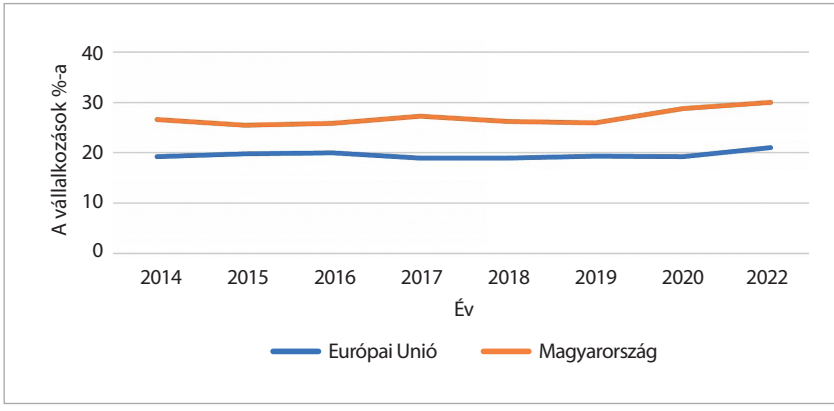
IKT-szakembereket foglalkoztató vállalkozások

Az uniós és hazai vállalkozások IKT-szakemberek alkalmazásának alakulását a vállalkozások százalékos eloszlásának függvényében az alábbi táblázat és grafikon szemlélteti.

16. táblázat: IKT-szakembereket alkalmazó uniós és hazai vállalkozások aránya

	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2022 (%)
Európai Unió	19	20	20	19	19	19	19	21
Magyarország	27	26	26	27	26	26	29	30

Forrás: European Commission: *Enterprises Employing ICT Specialists in the European Union and Hungary,* 2023



16. ábra: IKT-szakembereket alkalmazó uniós és hazai vállalkozások aránya
Forrás: European Commission: *Enterprises Employing ICT Specialists in the European Union and Hungary,* 2023

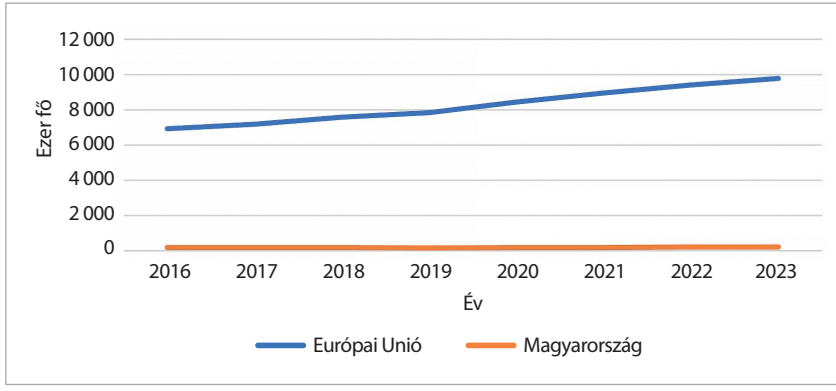
IKT-szakértői készségekkel rendelkező foglalkoztatottak

Az Európai Unióban és Magyarországon foglalkoztatott IKT-szakértői készségekkel rendelkező személyek számát az alábbi táblázat és grafikon szemlélteti.

17. táblázat: Az Európai Unióban és Magyarországon foglalkoztatott IKT-szakértői készségekkel rendelkező személyek száma (ezer fő)

	2016 (ezer fő)	2017 (ezer fő)	2018 (ezer fő)	2019 (ezer fő)	2020 (ezer fő)	2021 (ezer fő)	2022 (ezer fő)	2023 (ezer fő)
Európai Unió	6 908,3	7 173,4	7 570,3	7 846,2	8 431,3	8 956,2	9 403,9	9 789,2
Magyarország	158,1	157,7	165,6	152,4	170,6	181,2	193,6	197,7

Forrás: European Commission: *Persons Employed with ICT Specialist Skills (Broad Measure) in the European Union and Hungary,* 2024



17. ábra: Az Európai Unióban és Magyarországon foglalkoztatott IKT-szakértői készségekkel rendelkező személyek száma (ezer fő)

Forrás: European Commission: *Persons Employed with ICT Specialist Skills (Broad Measure) in the European Union and Hungary,* 2024

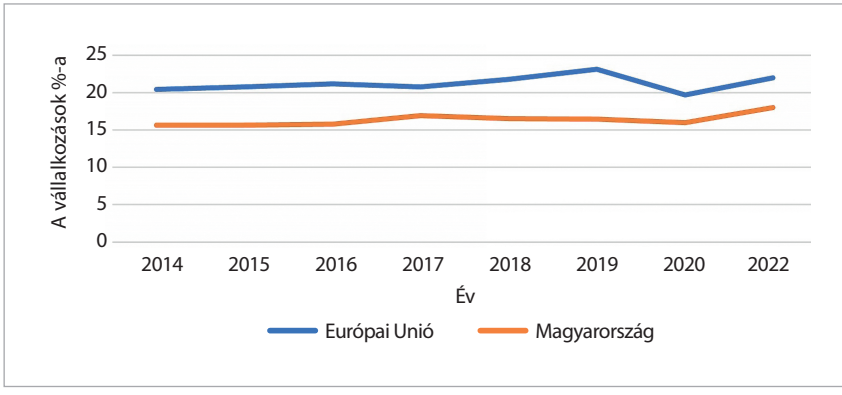
A munkavállalók IKT-készségeinek fejlesztéséhez/frissítéséhez képzést nyújtott vállalkozások

Az uniós és hazai vállalkozások számának alakulását, amelyek képzést nyújtottak a munkavállalóknak az IKT-készségek fejlesztéséhez/frissítéséhez, a vállalkozások százalékos eloszlásának függvényében a 18. táblázat és ábra szemlélteti.

18. táblázat: A munkavállalók IKT-készségeinek fejlesztéséhez/frissítéséhez képzést nyújtott uniós és hazai vállalkozások

	2014 (%)	**2015 (%)**	**2016 (%)**	**2017 (%)**	**2018 (%)**	**2019 (%)**	**2020 (%)**	**2022 (%)**
Európai Unió	20	21	21	21	22	23	20	22
Magyarország	16	16	16	17	17	16	16	18

Forrás: European Commission: *Enterprise Provided Training to Their Personnel to Develop/ Upgrade Their ICT Skills in the European Union and Hungary,* 2023



18. ábra: A munkavállalók IKT-készségeinek fejlesztéséhez/frissítéséhez képzést nyújtott uniós és hazai vállalkozások

Forrás: European Commission: *Enterprise Provided Training to Their Personnel to Develop/ Upgrade Their ICT Skills in the European Union and Hungary,* 2023

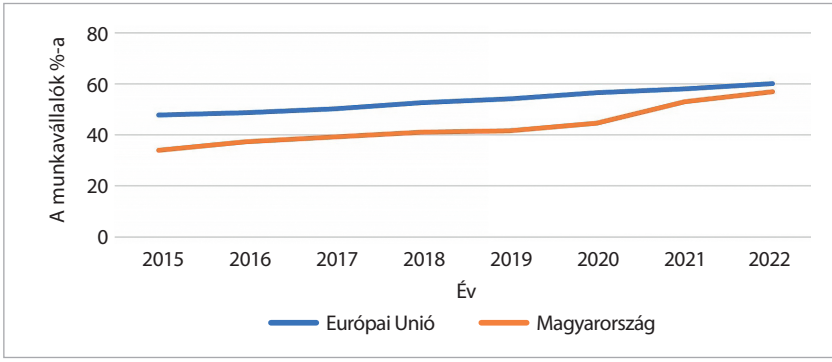
A munkahelyen számítógépet használó, internet-hozzáféréssel rendelkező foglalkoztatottak az üzleti szektorban

A munkahelyükön számítógéppel és internet-hozzáféréssel rendelkező uniós és hazai munkavállalók számának alakulását a munkavállalók százalékos eloszlásának függvényében a 19. táblázat és ábra szemlélteti.

19. táblázat: A munkahelyükön számítógéppel és internet-hozzáféréssel rendelkező uniós és hazai munkavállalók

	2015 (%)	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)
Európai Unió	48	49	50	53	54	56	58	60
Magyarország	34	37	39	41	42	45	53	57

Forrás: European Commission: *Persons Employed Using Computers with Access to the Web at Work (Business Sector) in the European Union and Hungary,* 2023



19. ábra: A munkahelyükön számítógéppel és internet-hozzáféréssel rendelkező uniós és hazai munkavállalók

Forrás: European Commission: *Persons Employed Using Computers with Access to the Web at Work (Business Sector) in the European Union and Hungary,* 2023

E-kormányzat az Európai Unióban és Magyarországon

Az e-kormányzat esetében három területet mutatunk be: a hatóságokkal online kapcsolatba lépő magánszemélyek számát, a kitöltött űrlapokat a hatóságokhoz benyújtó magánszemélyek számát, illetve a vállalkozások számára elérhető digitális közszolgáltatások számát.

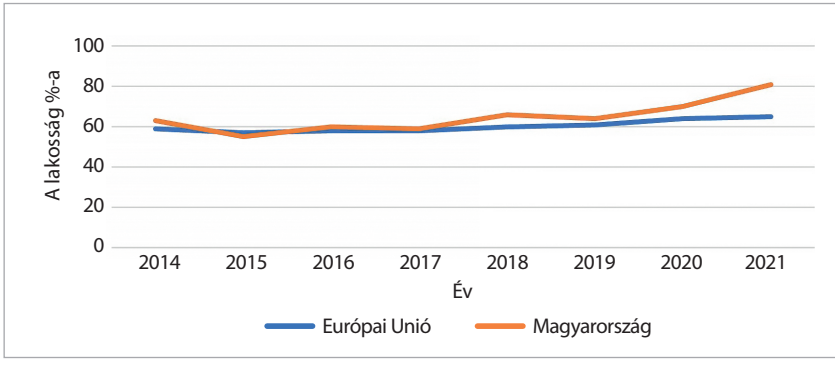
A hatóságokkal online kapcsolatba lépő magánszemélyek

A hatóságokkal már online kapcsolatba lépett uniós és hazai lakosok számának alakulását a lakosság százalékos eloszlásának függvényében a 20. táblázat és ábra szemlélteti.

20. táblázat: A hatóságokkal már online kapcsolatba lépett uniós és hazai lakosok százalékos aránya

	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)
Európai Unió	59	57	58	58	60	61	64	65
Magyarország	63	55	60	59	66	64	70	81

Forrás: European Commission: *Individuals Interacting Online with Public Authorities in the European Union and Hungary,* 2022



20. ábra: A hatóságokkal már online kapcsolatba lépett uniós és hazai lakosok százalékos aránya
Forrás: European Commission: *Individuals Interacting Online with Public Authorities in the European Union and Hungary,* 2022

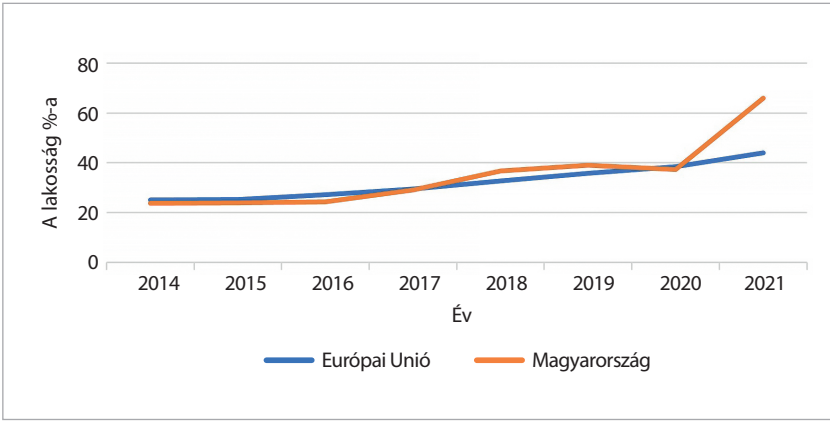
Kitöltött űrlapokat a hatóságokhoz benyújtó magánszemélyek

Az uniós és hazai magánszemélyek számának alakulását a lakosság százalékos eloszlásának függvényében a 21. táblázat és ábra szemlélteti, azok vonatkozásában, akik már nyújtottak be kitöltött űrlapokat a hatóságokhoz online.

21. táblázat: Kitöltött űrlapokat a hatóságokhoz online benyújtó uniós és hazai lakosok százalékos aránya

	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)
Európai Unió	25	25	27	29	33	36	38	44
Magyarország	24	24	24	29	37	39	37	66

Forrás: European Commission: *Individuals Submitting Completed Forms to Public Authorities in the European Union and Hungary,* 2022



21. ábra: Kitöltött űrlapokat a hatóságokhoz online benyújtó uniós és hazai lakosok százalékos aránya

Forrás: European Commission: *Individuals Submitting Completed Forms to Public Authorities in the European Union and Hungary,* 2022

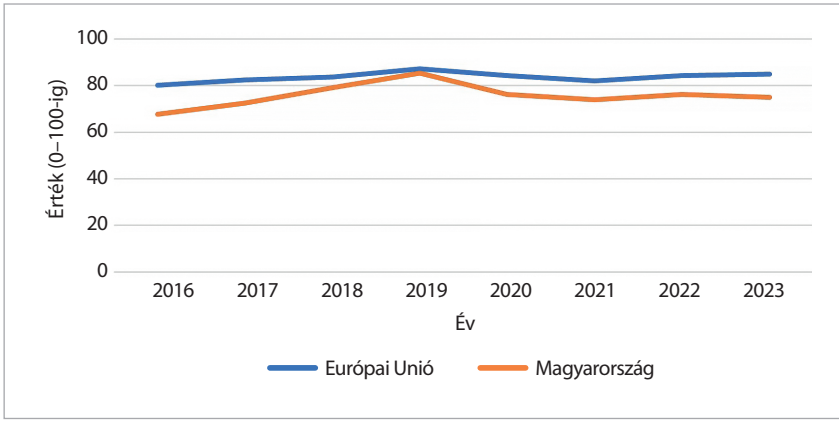
Digitális közszolgáltatások száma a vállalkozások számára

A vállalkozások számára kialakított uniós és hazai digitális közszolgáltatások számát a 22. táblázat és ábra szemlélteti, egy 0-tól 100-ig terjedő skálán, ahol a minimális érték 0, a maximális 100.

22. táblázat: A vállalkozások számára kialakított uniós és hazai digitális közszolgáltatások száma egy 0-tól 100-ig terjedő skálán

	2016 (%)	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)	2022 (%)	2023 (%)
Európai Unió	80	82	84	87	84	82	84	85
Magyarország	68	73	79	85	76	74	76	75

Forrás: European Commission: *Digital Public Services for Businesses in the European Union and Hungary,* 2024

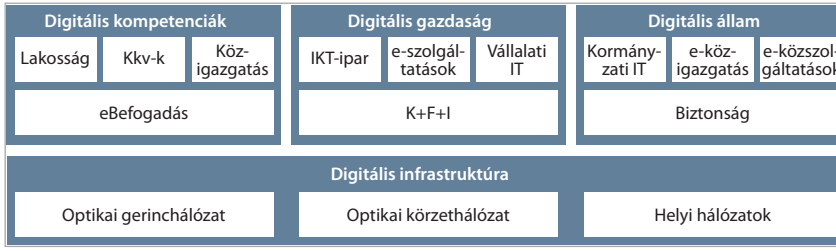


22. ábra: A vállalkozások számára kialakított uniós és hazai digitális közszolgáltatások száma egy 0-tól 100-ig terjedő skálán

Forrás: European Commission: *Digital Public Services for Businesses in the European Union and Hungary,* 2024

A digitális állam alapvető elemei

Magyarország Nemzeti Digitalizációs Stratégiája azzal a céllal jött létre, hogy egységes szerkezetbe foglalja, aktualizálja, illetve szükség szerint kiegészítse a digitalizációval kapcsolatosan készült intézkedéseket, szabályzatokat. A stratégia a Nemzeti Infokommunikációs Stratégia alapján a digitális ökoszisztémának négy pillért határozott meg, amelyeket a 23. ábra szemléltet.



23. ábra: A digitális ökoszisztéma pillérei

Forrás: Nemzeti Infokommunikációs Stratégia 2014–2020, 2014

A digitális infrastruktúra, mint ahogy az a fenti ábrán is látszik, minden másik pillérrel kapcsolatban áll, azoknak alapvető szolgáltatásokat nyújt, amelynek érdekében az alábbi célokat valósítja meg:

- gigabitképes hálózatok fejlesztése;
- oktatási intézmények digitálisinfrastruktúra-fejlesztése;
- felsőoktatási intézmények, kutatói hálózatok és közgyűjtemények digitálisinfrastruktúra-fejlesztése;
- a Nemzeti Távközlési Gerinchálózat továbbfejlesztése;
- a hivatásos szervezetek vezeték nélküli kommunikációjának továbbfejlesztése;
- kkv-kat, kutatási hálózatot és állami intézményeket kiszolgáló szuperszámítástechnikai (HPC) kapacitás bővítése;
- 5G hálózatok fejlesztésének ösztönzése.

A digitális kompetencia pillér célja tömeges lakossági digitáliskompetencia-fejlesztő programok indítása, az informatikusok és mérnökök számának mennyiségi és minőségi növelése, valamint a digitális kompetencia fejlesztéséhez szükséges struktúraváltás támogatása az oktatásban.

A digitális gazdaság pillér célja a kkv-k digitális ellátottságának és használatának növelése, digitális startupvállalkozások fejlesztése; az IKT-iparág célzott fejlesztése, valamint az állami adatvagyon gazdasági célú hasznosítása célzott stratégiával, intézkedésekkel.

A stratégia alapján a digitális állam a kormányzat, tágabb értelemben véve az állam működését támogató és a lakosságot kiszolgáló infokommunikációs technológiák, a lakossági és vállalkozói célcsoportnak szóló elektronikus államigazgatási, elektronikus ügyintézési szolgáltatások, az állami érdekkörbe tartozó egyéb (például egészségügyi, oktatási, könyvtári, kulturális örökséghez kapcsolódó vagy az állami adat- és információs vagyon megosztását célzó) digitális közszolgáltatások összessége, illetve az ezekhez kapcsolódó információbiztonság.

A digitális állam egyszerre jelenti:

- a saját működését a digitális technológiák felhasználásával hatékonyabbá tenni képes központi, területi és helyi közigazgatást és közszolgáltatásokat nyújtó intézményeket (például egészségügyi, oktatási, könyvtári, kulturális örökséghez kapcsolódó vagy az állami adat- és információs vagyon megosztását célzó); illetve
- a lakosság és a vállalkozások által igénybe vett állami (közigazgatási, egészségügyi stb.) szolgáltatások digitális platformon történő elérhetővé tételét és az ügyek online intézhetőségét.[102]

A digitális állam pillér alapvető célja a központi és területi közigazgatás digitális fejlesztése, az adatalapú közigazgatás megteremtése, az okostelepülések és okostérségek fejlesztése, a kormányzati elektronikus szolgáltatások információbiztonságának növelése, valamint a közszolgáltatások digitális fejlesztése, kiemelt hangsúllyal az egészségügyi megoldások továbbfejlesztésére.

A digitális államhoz tartozó fontosabb stratégiai területek:

- az igazságszolgáltatás;
- az adatpolitika;
- az egészségügy;
- a kulturális javak;
- a települési (digitális) fejlesztések;
- az informatikai és a kiberbiztonság.[103]

[102] *Nemzeti Digitalizációs Stratégia 2021–2030,* 2020.
[103] *Nemzeti Digitalizációs Stratégia 2021–2030,* 2020.

Az igazságszolgáltatás olyan egyedi jogvitát véglegesen eldöntő, egyéni jogsérelmet megállapító és azt helyreállító közhatalmi tevékenység, amely állami jogalkalmazás útján, a törvényesség, az eljárásban érintett személyek jogainak tiszteletben tartása mellett megvalósítja az általános jogvédelem rendszerét. Az igazságszolgáltatás mint tevékenység büntető-, polgári és közigazgatási bíráskodásra tagozódik. Szervezeti értelemben az igazságszolgáltatás a hatalommegosztás rendszerében a bírói hatalom kizárólagos megtestesítője, a bíróság és az igazságszolgáltatás egymást feltételező fogalmak, amelyekben kifejeződik a szervezet és a funkció egysége.[104]

Az igazságszolgáltatási rendszerek minőségének fontos része, hogy az igazságszolgáltatási eljárás egyes lépései elektronikus úton is elvégezhetők legyenek. Ezzel a keresetek elektronikus benyújtása, az eljárások előrehaladásának online nyomon követése megkönnyítheti az igazságszolgáltatáshoz való hozzáférést, és csökkentheti a késedelmeket és a költségeket. A bírósági IKT-rendszerek egyre nagyobb szerepet játszanak az igazságügyi hatóságok közötti, határokon átnyúló együttműködésben is, és megkönnyítik az uniós jogszabályok végrehajtását, például a kis értékű követelésekkel kapcsolatos eljárások esetében.[105]

Mindezekhez elengedhetetlen az igazságszolgáltatás digitalizációja mind hazai, mind uniós szinten. Ennek ad kiváló alapot az Európai Parlament és Tanács 2021 májusában kiadott rendelettervezete a határokon átnyúló polgári és büntetőeljárásokban történő kommunikációra szolgáló számítógépes rendszerről (e-CODEX rendszer), amely kimondja, hogy az igazságszolgáltatás digitalizációjának alapvető célja, hogy könnyebbé váljon az igazságszolgáltatás igénybevétele, javuljon az igazságszolgáltatás hatékonysága, és az igazságszolgáltatási rendszerek ellenállóbbá váljanak az olyan válságok idején, mint például a Covid–19-világjárvány.[106]

A nemzeti adatpolitika azokat a döntéseket és intézkedéseket foglalja magában, amelyek célja megteremteni az országban az információk kezelésének és

[104] Dezső Mária et al.: *Alkotmánytan I. Alapfogalmak, alkotmányos intézmények.* Budapest, Osiris, 2007.

[105] European Commission: *The 2019 EU Justice Scoreboard,* 2019.

[106] COM (2020) 712: Javaslat: Az Európai Parlament és a Tanács rendelete a határokon átnyúló polgári és büntetőeljárásokban történő kommunikációra szolgáló számítógépes rendszerről (e-CODEX rendszer) és az (EU) 2018/1726 rendelet módosításáról.

felhasználásának koherens környezetét, az úgynevezett nemzeti adat-ökoszisztémát. Ez többek között az alábbi területeket öleli fel:

- adatok előállítása és felhasználása, ennek során modern technológiák alkalmazása (számítási felhő, térinformatika, adatbányászat, big data technológiák stb.);
- adatszabványok alkalmazása;
- adatvédelem és adatbiztonság;
- szerzői jogi védelem;
- a nyilvántartás-vezetés szabályozása, a kezelt adatok minősége és interoperabilitása;
- szervek közötti (közvetlen és közvetett) adatcsere;
- közadatokhoz való hozzáférés biztosítása;
- egyéb nyílt adatokhoz való hozzáférés, nyílt adatok felhasználása;
- közadatok újrahasznosítása;
- együttműködés a releváns piaci, civil és tudományos szereplőkkel;
- az információs piac monitorozása.[107]

A digitalizációnak köszönhetően már nemcsak a közadatok újrahasznosításának van nagy szerepe a gazdaság egészének fejlődésében, hanem a teljes adatgazdaságnak is, amely magában foglalja az adatipart, adatkereskedelmet és adathasznosítást, amelyek kiterjednek az üzleti, a tudományos szférában, sőt az egész társadalomban keletkező adatokra is.

Magyarország kormányának alapvető célja az egészségügy megújítása, valamint fenntartható alapokra helyezése, továbbá egy hatékonyan működő, minőségorientált, betegközpontú egészségügyi rendszer létrehozása. E célok megvalósításához a kormány növelni kívánja az egészségügyben az állami szerepvállalást, valamint egészségügyi struktúraátalakítást kíván megvalósítani, ami a szervezeti integrációkra épül. A teljes fejlesztéshez az alábbi öt célfeladatot tűzték ki:

- a központi szolgáltatásfejlesztés és az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) továbbfejlesztése;
- központi távkonzultációs és távgyógyászati keretrendszer kialakítása, a távkonzultációhoz szükséges képalkotási adatközpont létrehozása;
- ágazati adatvagyon hasznosítása;

[107] Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete: *Fehér Könyv a nemzeti adatpolitikáról,* 2016.

– lakossági e-egészségügyi kompetenciafejlesztés, üzleti célú hasznosítási funkciók és hiteles elektronikus információk biztosítása;
– ágazati informatikai infrastruktúra-fejlesztés.[108]

A kulturális javak fogalmát a 2001. évi LXIV. törvény a kulturális örökség védelméről határozza meg a következők szerint: „Kulturális javak: az élettelen és élő természet keletkezésének, fejlődésének, az emberiség, a magyar nemzet, Magyarország történelmének kiemelkedő és jellemző tárgyi, képi, hangrögzített, írásos emlékei és egyéb bizonyítékai – az ingatlanok kivételével –, valamint a művészeti alkotások."[109]

A kulturális javak digitalizációjának megvalósítása érdekében született a fentiekben tárgyalt Közgyűjteményi Digitalizálási Stratégia, azzal a céllal, hogy a társadalom minél szélesebb köre számára biztosítsa az akadálytalan hozzáférést a kulturális javakból készített elektronikus tartalmakhoz.

A hazai település- és térségfejlesztési gyakorlat alapvető eleme az okosváros működési modell, amelynek fokozatos bevezetésével Magyarország alapvető célja a hosszú távon társadalmi, környezeti és pénzügyi szempontból fenntartható és élhető városok és térségek létrehozása. Az okosváros egy eredendően a digitális-technológiai megoldások széles körű alkalmazására támaszkodó településfejlesztési, illetve újabban térségfejlesztési megközelítés, ami ma már egy ennél jóval komplexebb városfejlesztési irányelvet, fejlesztési gondolkodásmódot takar.

Egy település akkor tekinthető okosnak, amikor a konkrét technológiai megoldások részévé válnak a város mindennapi életének, egyebek mellett a közlekedés (parkolás), a napi ügyintézés (közigazgatás), a közművek, városi terek fenntartása és használata, valamint egyéb, például humán szolgáltatások terén. Ezek a lakosság által napi szinten használt szolgáltatások az okosvárosban idővel egységes, összehangolt városi szintű működtetési rendszert alkotnak. Okos továbbá az a város, ahol a fejlesztésekhez újszerű döntéshozói (részvételen alapuló), szervezeti és működési megoldások kapcsolódnak, és minden fejlesztés alapja a fogyasztói igényekhez történő igazodás.

Az okosváros működési modell hátterében a látványos megoldásokon túl a folyamatos digitális információ- és adatgyűjtés, adatmenedzsment és az erre alapozott feladatszervezés áll. A települések okos működtetése felelősségteljes

[108] *Nemzeti Digitalizációs Stratégia 2021–2030,* 2020.
[109] 2001. évi LXIV. törvény a kulturális örökség védelméről.

üzleti szemléletű megközelítést is kíván, aminek nem a haszon, hanem a fejlesztésekre fordítható megtakarítás és így a fenntarthatóság az eredménye.[110]

Az informatikai biztonság olyan előírások, szabványok betartásának eredménye, amelyek az információ elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni.[111]

A kiberbiztonság „eszközök, politikák, biztonsági koncepciók, biztonsági garanciák, biztonsági technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék a számítógépes környezetet, továbbá az azt használó szervezetek és felhasználók eszközeit, rendszereit".[112]

A fentiekből is látszik, hogy a digitális állam kialakításához a két fogalom által felölelt módszerek és eljárásrendek alkalmazása elengedhetetlen. Az okosvárosok, a digitális kormányzás, az egyre összetettebb és egyre nagyobb digitális hálózatok egyre nagyobb kockázatot jelentenek a felhasználóknak, a vállalkozásoknak, illetve az állami szereplőknek egyaránt.

Kormányzati informatikai rendszerek

A digitális állam kialakításának alapvető követelménye egy egységes, központosított kormányzati informatikai rendszer kialakítása. Magyarországon ennek a rendszernek a kiépítése megtörtént a Nemzeti Infokommunikációs Stratégiával összhangban. A rendszer alapvető feladata az államigazgatási belső folyamatok támogatása és az elektronikus közigazgatási szolgáltatásokat támogató informatikai háttér biztosítása. Ezen belül kiemelt feladat a rendszer folyamatos üzemeltetése mellett az egységes kormányzati hardver- és szoftverinfrastruktúra-háttér továbbfejlesztése, a kormányzati intézmények belső folyamatait és szolgáltatásait támogató informatikai háttér biztosítása; az államigazgatási belső folyamatokat támogató informatikai rendszerek, központi kormányzati informatikai (pl. gazdasági támogató, személyügyi, dokumentumkezelő) és felhőalapú állami informatikai szolgáltatások fejlesztése; az ágazati intézményrendszerek

[110] *Nemzeti Digitalizációs Stratégia 2021–2030,* 2020.
[111] Szádeczky Tamás: *Az IT biztonság szabályozása.* Berlin, GlobeEdit, 2018. 5–6.
[112] ITU-T X.1205: *Overview of cybersecurity,* 2008. 2.

belső és külső folyamatainak digitalizálása; továbbá a területi közigazgatás működését támogató informatikai háttér fejlesztése (kormányhivatalok, járási hivatalok, kormányablakok).

A digitális állam kialakítása során szintén kiemelt feladat a közigazgatási belső folyamatok informatizálása, a közigazgatási reform infokommunikációs technológiákkal történő támogatása, ezzel hozzájárulva a központi közigazgatási intézményekben zajló folyamatok papírmentessé tételéhez; a Szabályozott Elektronikus Ügyintézési Szolgáltatások (SZEÜSZ) bevezetéséhez szükséges háttérfejlesztések összehangolásához; az önkormányzati informatikai fejlesztések és az önkormányzati alkalmazásszolgáltatók (ASP) portfóliójának bővítéséhez az önkormányzati szféra belső folyamatainak informatizálása és az intézmények működési hatékonyságának javítása érdekében.

A fentiek elérése érdekében elengedhetetlen az interoperabilitás kialakítása, valamint közös szabványok alkalmazása. Ehhez feltétlenül biztosítani kell az infokommunikációs technológiák átjárhatóságával kapcsolatos megfelelő jogszabályi hátteret, a széles körben elterjedt szabványok alkalmazására vonatkozó előírások és ajánlások rendszerének kialakítását az interoperabilitás biztosítása érdekében. Meg kell teremteni a biztonságos e-hitelesítési rendszerek határokon átnyúló elismerésével és interoperabilitásával kapcsolatos jogi kereteket, valamint folyamatosan korszerűsíteni és naprakészen kell tartani az állami nyilvántartásokat és az elektronikus azonosítások rendszerét (informatikai és szervezetfejlesztések, interoperabilitás, módszertan, humán feltételek, jogalkotás). Erősíteni kell az adatbázisok közötti együttműködést és átjárhatóságot, el kell végezni az adattisztítási folyamatokat, biztosítani kell a biztonságos adatcsere-lehetőségeket, ezekkel is erősítve az adatvédelmet. Ösztönözni kell a digitális államban tevékenykedő felhasználókat, vállalkozásokat és állami szereplőket a technológiasemlegességre, valamint az IT-biztonsági követelmények figyelembevétele mellett a nyílt forráskódú szoftverekre épülő fejlesztésekre.

E-közigazgatási szolgáltatások

A digitális állam fejlődésének alapfeltétele az elektronikus közigazgatás biztosításához szükséges, a fent leírt kiszámítható és stabil infrastrukturális és informatikai háttér, a közigazgatás belső folyamatainak átgondolt és az interoperabilitás elvét követő elektronizálása. Emellett szintén nagy szerepe van a lakosságnak és

a vállalkozásoknak nyújtott fejlett e-közigazgatási szolgáltatások kialakításának és működtetésének.

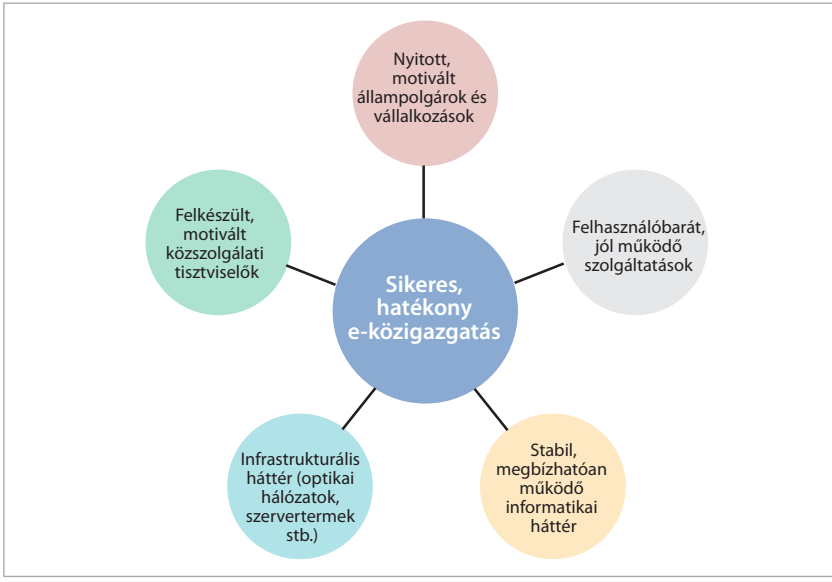
A magas szintű, korszerű lakossági és vállalati e-szolgáltatások bevezetéséhez elsősorban a lakosságnak és a vállalkozásoknak nyújtott közigazgatási szolgáltatások elektronizálására, az állam által kötelezően nyújtandó, illetve piaci alapon is elérhető SZEÜSZ-ök rendszerének kialakítására van szükség. Emellett meg kell határozni azoknak az ügyeknek a körét, amelyeket kizárólag elektronikusan lehet intézni, és ki kell alakítani a teljes átállás menetrendjét (roll-out terv).

A digitális állam fejlesztéséhez elengedhetetlen az elektronikus közszolgáltatások folyamatos fejlesztése és a digitális adatvagyon hozzáférhetővé tétele. Mindezekhez az alábbi feladatokat kell végrehajtani:

- e-egészségügyi akcióterv elkészítése;
- e-egészségügyi szolgáltatások fejlesztése;
- a digitalizálandó gyűjtemények körének felmérése (könyvtári, levéltári, kulturális, művészeti stb.), e-levéltári fejlesztések;
- az EU közadatok újrahasznosítását szabályozó irányelvének teljes körű implementálása, biztosítva a gyakorlatban is a közadatvagyon nyilvános hozzáférhetőségét, átlátható viszonyokat teremtve a közadatok újrahasznosításának piacain;
- köznevelési és felsőoktatási, illetve kutatási célú infokommunikációs infrastruktúra, szolgáltatások fejlesztése, az intézmények modern infokommunikációs eszközökkel történő ellátása, felhőalapú szolgáltatások bevezetése, a kutatási célú hálózati alap-infrastruktúra (GEANT, HBONE) és a nagy teljesítményű számítástechnikai kapacitás folyamatos bővítése;
- köznevelési és felsőoktatási, illetve kutatási célú digitális tartalmak és a hozzáférés bővítése az intézmények számára a képzési-oktatási és tudományos, valamint közgyűjteményi digitális tartalmak elérhetőségének bővítése, tartalomfejlesztési akciók lebonyolítása.[113]

A fentiek megvalósításához és sikeréhez szükséges tényezőket a 24. ábra szemlélteti.

[113] *Nemzeti Infokommunikációs Stratégia 2014–2020,* 2014.

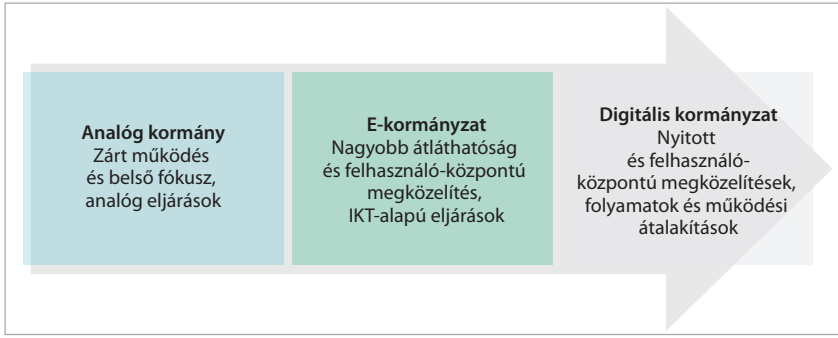


24. ábra: Az e-közigazgatás sikertényezői
Forrás: Nemzeti Infokommunikációs Stratégia 2014–2020, 2014

Digitális kormányzati átalakítási keretrendszer

A fenti kompetenciák és képességek megléte elengedhetetlen egy megfelelően működő digitális állam kialakításához. Azonban hogy a kialakított digitális kormányzás és egyéb elemei minden követelménynek megfeleljenek, és képesek legyenek ellátni alapvető feladataikat, szükséges egy olyan keretrendszer kialakítása, amely meghatározza a digitális kormányzás minden szintű igényt kiszolgáló kiépítéséhez szükséges alapvető irányvonalakat. Mindezekhez igazodva készítette el az Európai Bizottság a digitális kormányzati átalakítási tanulmányát. A tanulmányban meghatározták a digitális kormányzáshoz kapcsolódó alapvető fogalmakat, illetve kialakítottak benne egy olyan keretrendszert, ami segíti a tagállamokat digitális kormányzati rendszereik kialakításában. Ennek egyik alapdokumentuma *Az út az adatvezérelt közszektorrá váláshoz* című tanulmány, amelyet a Gazdasági Együttműködési és Fejlesztési Szervezet (Organisation for

Economic Co-operation and Development – OECD) készített. A tanulmány alapján paradigmaváltásra van szükség a digitális technológiák és adatok kormányzaton belüli használatában, leginkább az „e-kormányzásról" a „digitális kormányzatra" való áttérés esetében. Az „e-kormányzati" megközelítés a technológiát tekinti megoldásnak egy meglévő analóg folyamat digitalizálására a hatékonyság növelése érdekében, illetve a technológia bevezetését helyezi a középpontba. Ezzel szemben a digitális kormányzati gyakorlatok a technológiát másodlagosnak tekintik a felhasználói igényeknek a szolgáltatások és folyamatok e-tervezése és újratervezése révén történő kielégítésére való összpontosítással szemben. Ez a digitalizálás együtt jár a szervezet viselkedését átalakító, a tervezés által kialakított digitális kultúra kialakításával. Ennek vizualizációja is megjelenik a tanulmányban, amely az OECD OECD/LEGAL/0406 számú ajánlása alapján készült és a következő ábra szemlélteti.[114]



25. ábra: Átalakulás az analóg kormányzattól a digitálisig
Forrás: OECD: *Recommendation of the Council on Digital Government Strategies,* 2014

A 25. ábrán látható, hogy az e-kormányzat az információs és kommunikációs eszközök és technológiák kormányok általi használatát, különösen az internet alkalmazását mint a jobb kormányzás elérésének eszközét jelenti. Ezzel szemben a digitális kormányzat a digitális technológiák a kormányok modernizációs stratégiáinak integrált részeként történő, közértéket teremtő felhasználására utal.

[114] OECD: *The Path to Becoming a Data-Driven Public Sector.* Paris, OECD Publishing, 2019.

Ez a digitális kormányzati szereplőkből, nem kormányzati szervezetekből álló digitális kormányzati ökoszisztémára épül, és olyan vállalkozásokat, polgári társulásokat és magánszemélyeket foglal magában, amelyek támogatják a digitális kormányzás létrehozását és megvalósítását, továbbá biztosítják a kormányzattal való interakciókon keresztül az adatok, a szolgáltatások és a tartalmak előállítását és az azokhoz való hozzáférést.

A digitális kormányzat fogalma

Az Európai Bizottság digitális kormányzati átalakítási tanulmánya alapján a digitális kormányzat kihasználja a technológiai fejlődésekben rejlő előnyöket, támaszkodik az adatok és elemzések eredményeire, azokat folyamatosan felhasználja és újra felhasználja, abból a célból, hogy egyszerűsítse a (digitális és offline) tranzakciókat a végfelhasználók (polgárok, vállalkozások és kormányzati szervek) számára. A megszerzett adatok elemzése során olyan hasznos információkat állít elő, amelyek támogatják és javítják a kormányzati döntéshozatalt, továbbá elősegíti új, együttműködő és hatékonyabb szolgáltatásnyújtási modellek létrehozását. A kialakításra kerülő modellek nemcsak a küldetések hatékonyságának és eredményességének javítását támogatják, hanem hozzájárulnak az optimalizált eredmények eléréséhez is, mint például az átláthatóság és a nyitottság, a hosszú távú költségmegtakarítás, a jobb kormányzás, és ezáltal a polgárok jobb életminősége.[115]

A digitális kormányzat és a digitális kormányzás összehasonlítása

A fentiekből is látható, hogy a digitális kormányzat (más néven e-kormányzat) magában foglalja azokat az információs és kommunikációs technológiákat, amelyek hozzájárulnak a kormányzati tevékenységek javításához, a műveletek és struktúrák integrálásához, a polgárok bevonásához a kialakított digitális folyamatokba, növelik a közigazgatás hatékonyságát és átláthatóságát. Ez hozzájárul:

– a hatékonyság és eredményesség növeléséhez a kormányzati tevékenységekben és folyamatokban;

[115] European Commission: *Digital Government Benchmark, Study on Digital Government Transformation,* 2018.

– a közszolgáltatások minőségének javításához;
– az adminisztratív folyamatok egyszerűsítéséhez;
– az információkhoz való hozzáférés javításához;
– a kommunikáció növeléséhez a különböző kormányzati szervek között;
– a közrend támogatásának megerősítéséhez;
– a zökkenőmentes kormányzás lehetővé tételéhez.

Ezzel szemben a digitális kormányzás (más néven e-kormányzás) egy ország/állam vagy szervezet irányítását vagy adminisztrációját jelenti az információs és kommunikációs rendszerek alkalmazásával, amelyek biztosítják az információk terjesztését, a különböző modellek, folyamatok beépítését a kormányzati rendszerekbe és szolgáltatásokba. A digitális kormányzás olyan eszköz, amely hozzájárul:

– a kormányzati szolgáltatások minőségi biztosításához;
– a különböző csoportok közötti hatékonyabb együttműködéshez;
– a polgárok felhatalmazásához az információkhoz való hozzáférés révén;
– a hatékony kormányzati menedzsmenthez.[116]

A digitális kormányzás során kialakításra került alapvető modellek a következők:

– G2G (government to government): A közigazgatási szervek vagy szervezeti egységek közötti kapcsolatok és információcsere.
– G2C (government to citizens): Az állampolgárok és a kormányzat közötti kapcsolatok és információcsere. Ez magában foglalja olyan interfészek létrehozását, amelyek lehetővé teszik a nagyközönség számára az információk és szolgáltatások elérését bárhol, bármikor.
– G2B (government to business): A gazdasági szereplők és a kormányzat közötti kapcsolatok és információcsere, azzal a céllal, hogy növelje az átláthatóságot és az elszámoltathatóságot.
– G2E (government to employees): A közszolgálatban dolgozók közötti kapcsolatok és információcsere az alkalmazottak moráljának és elégedettségének növelése érdekében.
– G2NGO (government to non-governmental organizations): A civil szervezetek és a kormányzat közötti kapcsolatok.[117]

[116] Gadget-info: *Difference between e-government,* 2019.
[117] Zsom Brigitta: Az elektronikus közigazgatás és a területi kutatások kapcsolatáról. *Tér és Társadalom,* 28. (2014), 3. 21–22.

Az alábbi táblázat szemlélteti a digitális kormányzat és a digitális kormányzás közötti lényegi különbségeket.

23. táblázat: A digitális kormányzat és kormányzás közötti lényegi különbségek

Az összehasonlítás alapja	**Digitális kormányzat**	**Digitális kormányzás**
Jelentés	Az információs és kommunikációs rendszerek alkalmazása a kormányzati feladatok és műveletek támogatása, a polgárok tudatosítása érdekében, valamint a részükre nyújtott digitális szolgáltatások összessége	Az információs és kommunikációs rendszerek alkalmazása a nyilvánosság számára szolgáltatott információk és szolgáltatások széles körének és minőségének javítása érdekében
Mi ez?	Rendszer	Funkcionalitás
Kommunikációs protokoll	Egyirányú kommunikációs protokoll	Kétirányú kommunikációs protokoll

Forrás: Gadget-info: *Difference between e-government,* 2019

Az átalakulás szintjei

A digitális kormányzati átalakulás a kormányzati működés, a belső és külső folyamatok és struktúrák fokozatos átalakítását jelenti a nagyobb nyitottság és együttműködés elérése érdekében kormányzati körökben és azokon túl. Ez alapvetően a kormányzati szektoron belül és azon kívül meglévő IKT-k és/vagy új, adatvezérelt technológiák és alkalmazások kombinációját, valamint a szervezeti és kognitív gyakorlatok radikális átalakítását; a szolgáltatásnyújtás és a politikai ciklus egyes szakaszaiban a közszféra innovációjának különböző formáit foglalhatja magában a kulcsfontosságú célok elérése érdekében, úgymint a hatékonyság, az elszámoltathatóság és az átláthatóság növelése, a polgárközpontú szolgáltatások nyújtása, és olyan politikák kialakítása, amelyek növelik a befogadást és a kormányzatba vetett bizalmat.[118]

[118] Gianluca Misuraca – Egidijus Barcevičius – Cristiano Codagnone: *Exploring Digital Government Transformation in the EU – Understanding public sector innovation in a data-driven society,* EUR 30333 EN. Luxembourg, Publications Office of the European Union, 2020.

A közszolgáltatások átalakítása megköveteli, hogy a digitális átalakítási kezdeményezések vezetői felmérjék, hol áll a szervezetük a céljaihoz képest, és az eredményeknek megfelelően tegyenek lépéseket a digitális átalakulás fokozására. Ezekkel a lépésekkel lesznek képesek az Európai Bizottság által elkészített keretrendszerben meghatározott végcélokat elérni.

A keretrendszer öt szintből áll, kezdve egy kezdeti szinttel, ahol a szervezetek a hagyományos e-kormányzati elvek és eljárásmódok alapján működhetnek. Minél feljebb halad egy szervezet a digitalizáció szintjein, a digitális átalakulás annál inkább egy automatikus, önfenntartó folyamattá válik. A teljes digitalizáció nem minden esetben cél, bizonyos szervezetek dönthetnek úgy, hogy egy meghatározott szinten maradnak, és például különböző szolgáltatások esetében különböző digitális fejlettségi szinteket alakítanak ki. A digitális kormányzati átalakulási keretrendszerben meghatározott öt átalakulási szakasz a következő:

1. Az e-kormányzat: A hangsúly az online szolgáltatásokra helyeződik a felhasználók kényelme és a költségmegtakarítás érdekében.
2. Nyílt kormányzat: A nyílt kormányzat gyakran olyan állami programok formájában jelenik meg, amelyek célja az átláthatóság, a polgárok bevonásának és az adatgazdaság előmozdítása. Az e-kormányzati és a nyílt kormányzati programok gyakran egymás mellett léteznek, eltérő vezetéssel és prioritásokkal.
3. Adatközpontú kormányzat: Ezen a szinten a hangsúly a polgárok vagy a felhasználók igényeinek összegyűjtéséről áthelyeződik az adatok stratégiai gyűjtésében és hasznosításában rejlő új lehetőségek proaktív feltárására.
4. Teljesen átalakított kormányzat: Ezen a szinten a szervezet, ügynökség vagy minisztérium teljes mértékben elkötelezte magát az adatközpontú megközelítés, illetve a kormányzati innováció mellett.
5. Okoskormányzat: Ezen a szinten az adatközpontú digitális innováció folyamata az egész kormányzatra kiterjed.

Az adatközpontú kormányzat kialakításával érhető el az a fordulópont, amivel a valódi digitális átalakulás megkezdődik, és a digitalizálás lényegesen felgyorsul. Az átalakulási folyamat minősítéséhez hat témát határoztak meg a tanulmányban, amelyek a következők:

- Szolgáltatási modell: A kormányzati szolgáltatásokat kormányzati és nem kormányzati csatornák kombinációján keresztül biztosíthatják, a reaktív (azaz a választópolgár kifejezett kérésére válaszoló) és a proaktív (azaz

a választópolgár által kiváltott) szolgáltatások közötti változó egyensúlyt alkalmazva.

- Digitális rendszer: A digitális üzleti rendszer öt különböző rendszerből áll: IT-központú rendszerek, polgárközpontú rendszerek, adatközpontú rendszerek, dolog- és ökoszisztéma-központú rendszerek, valamint az adatfelhasználás/intelligencia. Bár mind az öt rendszer, az átalakulás különböző szintjein, az ügynökség küldetésétől függően beágyazható, az egyes átalakítási szintek általában más-más területre helyezik a hangsúlyt.
- Ökoszisztéma és felhasználók: A kormányok természetükből adódóan az elmúlt évtizedben belső kormányzati szektorbeli ökoszisztémákat működtettek annak érdekében, hogy jobb közszolgáltatásokat nyújtsanak felhasználóik (polgárok, vállalkozások és más kormányok) számára. A digitális kormányzati átalakulás megjelenésével egyre nagyobb hangsúlyt kap a beszállítókkal, partnerekkel és közvetítőkkel való együttműködés, hogy közösen hozzanak létre új, köz- és magánszféra közötti szolgáltatásokat, valamint a felhasználók bevonása a szolgáltatások továbbfejlesztésébe, a tervezésbe és a megvalósításba.
- Vezetés: Míg a technológiai és üzleti vezetők közötti együttműködés továbbra is a központi eleme a sikeres átalakulásnak, a digitális átalakulás előrehaladása során a különböző szinteken a kulcsszerepek eltérőek az egyes vállalatoknál.
- Technológiai fókusz: Számos technológia járul hozzá a digitális átalakuláshoz, de a digitális átalakulás minden egyes szakaszában más és más technológiák kapnak komolyabb figyelmet, amelyek eltérő készségeket kívánnak a végső siker eléréséhez. A folyamatok előrehaladtával a kormányzati vezetők felismerik az adatok stratégiai eszközként betöltött kritikus szerepét, és ennek megfelelően a vezetők a hatalmas adattárakat kihasználva biztosítják, hogy az adatok szemantikailag pontosan meghatározottak, hozzáférhetők és könnyen megoszthatók legyenek.
- Kulcsfontosságú mérőszámok: A fejlődési célok elérésének megfelelő mérése érdekében az intézkedések jellege a céloknak megfelelően változik. Az e-kormányzati mérőszámok elsősorban a szervezeten belüli munkafolyamatok – például a vállalkozások nyilvántartásba vétele és engedélyezése – működési hatékonyságára összpontosítanak. A digitális fejlettség magasabb szintjein a legfontosabb mérőszámok a teljesen új szolgáltatási és üzleti modellek hatékonyságát mérik a rendelkezésre álló adatok alapján.

Az e-kormányzat

Ebben a szakaszban a hangsúly az online szolgáltatásokra helyeződik a felhasználók kényelme és a költségmegtakarítás érdekében, ahol a mozgatórugók alapvetően a megfelelés és a hatékonyság. A szervezetek és a minisztériumok online csatornákon keresztül nyújtanak szolgáltatásokat, azzal a céllal, hogy megfeleljenek az alapvető követelményeknek és növeljék a hatékonyságot. Az e-kormányzat jellemzői:

- A szolgáltatási modell reaktív, a szolgáltatásokat a felhasználó kérésére nyújtják. A hozzáférés egy portálon és kormányzati alkalmazásokon keresztül történik. Továbbra is számos iroda és a humán szolgáltatás alkalmazása fennmarad, hogy segítséget tudjanak nyújtani a polgároknak a különböző kormányzati programokban és űrlapok kitöltésében.
- Az e-kormányzati szakaszban a rendszer alapvetően informatikai központú, amely például a munkatársak együttműködésére, a backoffice-rendszerekre, a kormányzaton belüli cserekapcsolati rendszerekre, az alapvető feladatkritikus alkalmazásokra és üzemeltetési rendszerekre épül.
- Az ezen a szinten kialakított ökoszisztéma kormányközpontú, ami főként más, ugyanabban az országban a kormányzati ágazatban vagy ágazatokon átnyúlóan működő ügynökségekből áll, amelyekkel a jobb megvalósítás érdekében vagy a programcélok eléréséhez, illetve a teljesítés javításához szolgáltatás- és adatintegrációra van szükség. Az ügynökségek között hatékony interoperabilitás kerül kialakításra és érvényesítésre keretrendszerek és/vagy ügynökségek közötti vállalati architektúra-megközelítések alkalmazásával. A kezelt adatok felhasználói és szolgáltatói egyértelműen azonosítottak.
- A technológia középpontjában a szolgáltatás-központú architektúra áll, amely megkönnyíti a szolgáltatások integrációját az ügynökségek között.
- Az e-kormányzati kezdeményezések irányítása általában az informatikai osztályon belül történik, és a stratégia végrehajtását a technológiai csapatok irányítják, nem pedig az üzleti szféra.
- A fő mérőszámok jellemzően az online szolgáltatások, a mobileszközökön keresztül elérhető szolgáltatások és az integrált szolgáltatások százalékos aránya, valamint az elektronikus csatornák kihasználtsága.

A nyílt kormányzat jellemzői:

- A nyílt kormányzás mozgatórugói az átláthatóság és a nyitottság. A szervezetek célja az adatforrások megnyitása, hogy harmadik felek is hasznosíthassák azokat.
- A szolgáltatási modell proaktív. Az adatok intenzívebb felhasználása lehetővé teszi a kormányzati szervek számára, hogy proaktívabbá váljanak. Ilyen például:
  - az olyan adóhivataloktól érkező adótanácsadás, amelyeknek valós idejű rálátásuk van az adófizetőkre;
  - megelőző egészségügyi ellátás a környezeti megfigyelésből származó adatok felhasználásával;
  - hatékonyabb irányítás a vészhelyzetek kezelése során több kormányzati és nem kormányzati forrásból származó adatok alapján.
- A digitális rendszer polgárközpontú. Az ügyfélportálok egyre fejlettebbé válnak, különösen a közösségi hálózatok terén. A nyílt adatok hasznosítása többnyire külső felhasználókra korlátozódik, mivel a kormányzati rendszer maga még nem elég fejlett ahhoz, hogy hasznosítani tudja a megszerzett adatokat.
- Az ökoszisztéma a szolgáltatások közös létrehozására összpontosít. Ebben a szakaszban az ökoszisztéma olyan külső közösségekre támaszkodik, amelyek segíthetnek a nyílt közadatok felhasználásában vagy hasznosításában. A felhasználók és az adatszolgáltatók egyértelműen azonosíthatók.
- A technológia középpontjában az alkalmazásprogramozási felületalapú (Application Programming Interface – API) architektúra áll. A nyílt adatok kezelése elveinek és technológiáinak elsajátítása alapvető fontosságú ebben a szakaszban. A fő hangsúly a nyílt adatokhoz való hozzáférést támogató API-ok kifejlesztésén és kezelésén van.
- A vezetés adatvezérelt. Mivel az egyes szervezetek és vállalatok vezetői nem feltétlenül hisznek a technológia átalakító erejében, így a nyílt kormányzati programok által megjelent feladatok és felelősségek olyan speciális szerepkörökre hárulnak, mint az adatvédelmi tisztviselő (Chief Data Officer – CDO) vagy a digitális igazgató (Chief Digital Officer – CDO).
- A legfontosabb mérőszámok általában a nyílt adatkészletek és a nyílt adatokon alapuló/azokat újrafelhasználó alkalmazások száma.

Adatközpontú kormányzat

Az adatközpontú kormányzat jellemzői:

- Az adatközpontú kormányzat mozgatórugója az állampolgári érték. A kormányzati szervek és a harmadik felek adatalapú szolgáltatásokat nyújtanak a felhasználóknak.
- A szolgáltatási modell közvetített, ahol a szolgáltatásokhoz aggregátorokon és közvetítőkön keresztül lehet hozzáférni, mint például a polgárok által fejlesztett vezérlőpultok vagy harmadik fél által fejlesztett alkalmazások, amelyeket nyílt adatokkal táplálnak, és amelyeket startupok vagy egyéni fejlesztők készítenek. A hangsúly külső, a tudósok és a polgárok adatai felé fordul.
- A digitális rendszer adatközpontú. Az adatok újrafelhasználása válik uralkodóvá. A hangsúly az adatelemzésre helyeződik át.
- Az ökoszisztéma a „tudatos" szinten van. A szervezetek kezdik megérteni saját célkitűzéseiket és a különböző szereplők szerepét (aktívan vagy passzívan), valamint az ökoszisztémák összetettségét, amelyben működnek.
- A technológia középpontjában a „több adat megosztása" áll. A szervezetek ugyanazokat az elveket kezdik alkalmazni az olyan üzleti adatokra is, amelyeket eredetileg nem nyilvános felhasználásra szántak, mint az előző szinteken.
- A nyílt adatok alkalmazása elősegíti az innovatív üzleti alkalmazások fejlesztését és a hatékonyabb elemzést döntéshozatal támogatása céljából. A „több adat megosztása" kifejezés itt olyan adatokra is vonatkozik, amelyek nem nyilvános felhasználásra készültek, azonban valamennyi kormányzati szervezet között megoszthatók.
- A vezetés az üzletből származik. Az egyes szervezetek vezetőinek feladata, hogy vezető szerepet vállaljanak az adatok innovatív felhasználásában.
- A fő mérőszámok jellemzően a megosztott üzleti adatokon alapuló új vagy átalakított szolgáltatások száma, valamint a nyílt adatokra szolgáltatásokat építő külső szereplők száma.

Teljesen átalakított kormányzat

A teljesen átalakított kormányzat szintjén a szervezet, ügynökség vagy minisztérium teljes mértékben elkötelezte magát a kormányzat fejlesztésének adatközpontú megközelítése mellett. Az adatok rendszeresen áramlanak a szervezeti határokat átlépve, ami könnyebb interakciókat eredményez, és jobb szolgáltatásokat nyújt a választópolgároknak. Ebben a szakaszban könnyen előfordulhat, hogy adatvédelemmel kapcsolatos visszásságok lépnek fel, mivel a polgárok szempontjából aggályos lehet, hogy az adataikat hogyan gyűjtik és használják fel. Ezért fontos biztosítani, hogy az adatok felhasználása a meglévő normák és szabályozások szerint történjen, és hogy ezt világosan kommunikálják. A teljesen átalakított kormányzat jellemzői:

- A teljesen átalakított kormányzat mozgatórugója az ismeretvezérelt átalakulás. A szervezet üzleti és informatikai vezetői a szolgáltatások szisztematikus és nagyobb léptékű „átalakítását" folytatják, amelyek az előző szintek tanulságain (sikerein) alapulnak.
- A szolgáltatási modell beágyazott, ahol a szolgáltatások számos csatornán keresztül elérhetők, beleértve a nem kormányzati csatornákat is. A kormányzati szolgáltatások beágyazódnak a kereskedelmi szolgáltatótól kapott személyes szolgáltatásokba, valamint a polgárokat körülvevő különféle eszközökbe, járművekbe és infrastruktúrákba.
- A teljesen átalakított kormányzat esetében a digitális rendszer tárgyközpontú, amely során a tárgyak adatgyűjtése és felhasználása folyamatosan növekszik. A digitális rendszerek a tárgyakhoz való kapcsolódásra (például a rendőrök testkamerái, a taxik GPS-e vagy a közös használatú kerékpárok távoli zárjai) és a tárgyak internete (internet of things – IoT) elemzésekre összpontosítanak.
- Az ökoszisztéma elkötelezett szinten van, és olyan külső közösségek felé irányul, amelyek segíthetnek az előnyök kihasználásában vagy a szabványosított és jól megformált nyílt közadatok hasznosításában. Az adatok felhasználója és szolgáltatója egyértelműen azonosított.
- A technológiai hangsúly a tárgyakon mint adatokon van. Ahhoz, hogy az átalakítás támogatása érdekében több forrásból származó adatokat és szolgáltatási elemeket össze lehessen gyűjteni, speciális szolgáltatási architektúra használatára van szükség. Ez magában foglalja a szolgáltatásokat, illetve több szinten és szervezeti határokon átnyúló API-okat tesz

elérhetővé, egyensúlyba hozva az igényeket a szolgáltatások összetételével és újrafelhasználásával.
- A vezetés információvezérelt, ennek megfelelően az adatok és információk értékét széles körben elismerik az egész szervezetben. Az informatikai vezető (Chief Information Officer – CIO) az innováció élére áll.
- A legfontosabb mérőszámok jellemzően a megszüntetett szolgáltatások százalékos aránya, valamint az új szolgáltatások és az igénybevételük aránya.

Okoskormányzat

Ezen a ponton a nyílt adatokat használó digitális innováció folyamata a politikai döntéshozók felső szintjének részvételével és vezetésével mélyen beágyazódik az egész kormányzatba. Az innovációs folyamat kiszámítható és megismételhető, még a gyors reagálást igénylő zavarok vagy hirtelen események esetén is. Az okoskormányzat jellemzői:

- Az okoskormányzás mozgatórugója, hogy a digitális szolgáltatások önmeghatározók; az intelligens kormányzással az átalakulás átadja helyét az új normának, azaz a digitális szolgáltatások folyamatos és tartós fejlesztésének.
- A szolgáltatási modell előrejelző jellegű, ahol a szolgáltatások és az interakciók számos érintkezési ponton keresztül zajlanak. Az interakciók ütemét az határozza meg, hogy a kormányzat képes-e előre jelezni egy igényt vagy megelőzni egy eseményt.
- A digitális rendszer az ökoszisztéma-központ, amelyen belül a szolgáltatások és a műveletek dinamikusan újrakonfigurálódnak, hogy alkalmazkodjanak a körülményekhez és a prioritások eltolódásához. Az API-menedzsmentszoftver az API-ok széles választékával és a kormányzati és magánszektorban futó ökoszisztémákkal foglalkozik.
- Az okoskormányzat esetében az ökoszisztéma folyamatosan fejlődik. Ezen a szinten a szervezetek kezdik megérteni az ökoszisztémák összetettségét, amelyekben működnek, az ügynökségek céljait és a különböző résztvevők szerepeit.
- A technológia középpontjában az intelligencia áll. A mesterséges intelligencia és a fejlett gépi tanulás alapvető fontosságúvá válik a megértés,

a tanulás és az előrejelzés területeken, valamint a nagy mennyiségű adatok kezelése során.
- A vezetés az innovációra épül. A CIO lesz a szervezet vezető átalakítási tisztviselője/innovációs vezetője. Az ő vezetésükkel válik a digitális átalakulás fenntartható üzleti tevékenységgé.
- A fő mérőszámok a fejlesztett adathasználat által helyettesített (vagy bevezetett) szolgáltatások száma.[119]

A fenti hat területre jellemző egyes főbb jellemzőket az alábbi táblázat szemlélteti, amely ismerteti az egyes szintekhez és területekhez tartozó alapvető fogalmakat.

24. táblázat: A digitális kormányzati fogalomtár táblázata

	E-kormányzat	**Nyílt kormányzat**	**Adatközpontú kormányzat**	**Teljesen átalakított kormányzat**	**Okoskormányzat**
Mozgatórugók	Megfelelés, hatékonyság	Átláthatóság és nyitottság	Állampolgári érték	Betekintésvezérelt átalakulás	Önmeghatározás
Szolgáltatási modell	Reaktív	Közvetített	Proaktív	Beágyazott	Előre jelző
Digitális rendszer	Informatikai központú	Állampolgár-központú	Adatközpontú	Tárgyközpontú	Ökoszisztéma-központú
Ökoszisztéma és felhasználók	Kormányzat-központú	Szolgáltatás-társalkotás	Tudatos	Elkötelezett	Fejlődő
Technológiai fókusz	Szolgáltatás-központú architektúra	API-támogatott architektúra	Bármely adatra nyitott	Tárgyak mint adatok	Intelligens
Vezetés	Technológia	Adat	Üzleti	Információs	Innovációs
Kulcsfontosságú mérőszámok	Az online szolgáltatások online %-a	A nyitott adatkészletek száma	Az adatvezérelt szolgáltatások száma	Az új és megszüntetett szolgáltatások %-a	Az új szállítási modellek száma

Forrás: European Commission: *Digital Government Benchmark, Study on Digital Government Transformation,* 2018

[119] European Commission (2018): i. m. 90–96.

A fenti lépések segítik a digitális kormányzat kialakítását, és hozzájárulnak az e-kormányzatról történő átálláshoz. Ehhez elengedhetetlen, hogy a keretrendszerben megfogalmazott képességek kialakításra kerüljenek, valamint hogy végbemenjenek azok a változások, amelyek átalakítják a vezetési rendet, illetve technológiai hátteret. Mindezeket segítik az OECD *A digitális kormányzat hatása a polgárok jólétére* című tanulmányában meghatározott dimenziók.

Az első ilyen dimenzió a tervezésalapú digitalizáció, amelynek során a kormányzat a teljes digitalizációhoz a sikeres és fenntartható átalakulás elősegítéséhez szükséges különböző stratégiai tevékenységek megértésével közelít. Ez azt jelenti, hogy a kezdetektől fogva figyelembe veszi a digitális, az adat- és a technológiai lehetőségeket annak érdekében, hogy a kormányzatot újragondolják, átalakítsák és egyszerűsítsék annak érdekében, hogy a felhasználó által használt csatornától függetlenül hatékony, fenntartható és polgárközpontú közszektort hozzanak létre.

A következő dimenzió az adatvezérelt közszféra, ahol a fókusz az adatok fontosságán van mint a közszféra alapvető és stratégiai eszközein, amelyek segítségével közösen meghatározhatók és előre jelezhetők az állampolgári és egyéb igények, és lehetővé válik az esetlegesen fellépő változásokra való egységes reagálás.

Szintén fontos elem az alapértelmezett nyitottság, ami a kormányok hajlandóságát jelenti a nyílt formátumú adatok közzétételére, a szervezeti határokon átnyúló együttműködésre és a kormányzaton kívüli harmadik felek bevonására. Fontos jellemzője, hogy olyan alapelvekre épül, mint az átláthatóság, integritás, továbbá megalapozza a digitális munkamódszereket és a nyílt kormányzást.

A felhasználóközpontúság mint megvalósítási dimenzió az átalakítás olyan megközelítése, amelyet egy nyitott kultúra tesz lehetővé, és amelyet a tervezésalapú digitalizációs törekvések támogatnak. Ez lehetővé teszi a kormányzatok számára, hogy olyan eszközöket foganatosítsanak, amelyek lehetőséget nyújtanak a nyilvánosság számára, hogy kommunikálhassák igényeiket a kormányzat felé, és a kormányzat bevonja őket a vezetésbe.

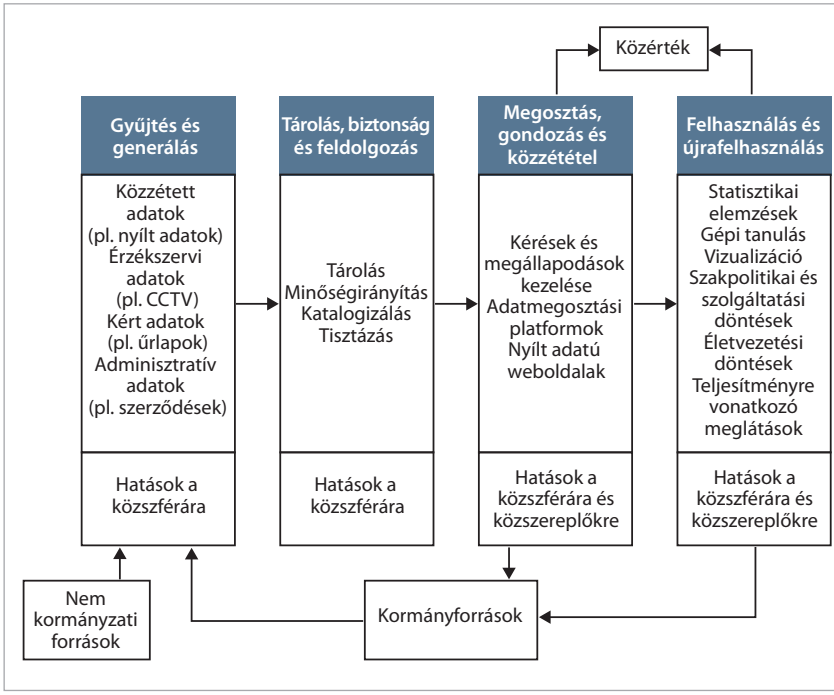
A kormányzat mint platform dimenzió célja egy olyan ökoszisztéma kiépítése a közszféra támogatására és felszerelésére, amely hozzájárul a hatékony politika kialakításához és a minőségi szolgáltatások nyújtásához, ami egyben ösztönzi a kormányzatot a polgárokkal, vállalkozásokkal és a civil társadalommal való együttműködésre.

A proaktivitás mint az utolsó dimenzió lehetővé teszi, hogy a fenti öt dimenzió alkalmazásával a kormányok előre lássák a polgárok igényeit, és gyorsan reagáljanak rájuk, még mielőtt a kérés valójában megfogalmazódna. Az átalakított kormányzat lehetővé teszi, hogy a problémákat az elejétől a végéig egységesen kezeljék, ahelyett hogy az egyes részeket külön-külön oldanák meg.[120]

A digitális állam adatvezérelt közértékteremtése

Az adatok felhasználása és alkalmazása során számos olyan közérték jön létre, amelyek hozzájárulhatnak a kormányzás sikeréhez, a döntéshozatal támogatásához, az egyes szolgáltatások javításához vagy átalakításához. Ahhoz, hogy az adatok ilyen formája ténylegesen értéket jelentsen a köz számára, a kormányzatnak tisztában kell lennie azzal, hogy milyen szerepet vár el az adatoktól a döntéshozatalban, és milyen erőfeszítésekre van szüksége ahhoz, hogy az adatokból információ váljon. Szintén kiemelt szerepe van az adatok azon jellemzőinek, hogy honnan származnak, hogyan használják fel őket, és kik vesznek részt a felhasználásban és újrafelhasználásban. A kormányzati adatok értékciklusának jobb kezelése segítheti a politikai döntéshozókat és a köztisztviselőket hatékonyságuk növelésében azáltal, hogy javítja a meglévő politikai problémákra és a különböző érdekeltekre vonatkozó ismeretek gyűjtésére, az új tendenciák és igények előrejelzésére, az innovatív politikai megközelítések kialakítására és adaptálására, a vállalt tevékenységek és a végrehajtott politikák nyomon követésére, valamint a politikai kihívások kezelésére mozgósított erőforrások (pénzügyi, időbeli, emberi és anyagi) kezelésére irányuló képességüket. A kormányzati adatok életciklusát a 26. ábra szemlélteti.

[120] Benjamin Welby: *The Impact of Digital Government on Citizen Well-Being.* Paris, OECD Publishing, 2019.



26. ábra: A kormányzati adatok életciklusa

Forrás: Charlotte van Ooijen – Barbara Ubaldi – Benjamin Welby: *A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance.* Paris, OECD Publishing, 2019. 11.

Az elemzési módszerek, amelyek az adatokat (nyers, elszigetelt és strukturálatlan adathalmazok) információvá (ahol az adatok közötti összefüggéseket azonosítják) és tudássá (ezen összefüggések megértése) alakítják, a kormányzat stratégiai, taktikai és operatív szintjén történő döntéshozatal (cselekvés) alapját képezik. Azoknak a döntéshozóknak, akik szeretnék kihasználni az adatvezérelt innovációból eredő jólétet, fejlődést és folyamatos növekedési lehetőségeket, meg kell érteniük azt a folyamatot, amelynek során az adatok átalakulnak, hogy végül innovációhoz vezessenek. Ez a folyamat, ahogy a fenti ábrán is látható, azonban

nem egy (lineáris) értéklánc, hanem egy értékciklus, amely az értékteremtési folyamat több fázisában visszacsatolási hurkokat tartalmaz. A továbbiakban az értékciklus-folyamat alapvető elemeit mutatjuk be, úgymint az adatok típusát, az adatelemzési módszereket és az adatvezérelt közszféra szereplőit.

A digitális állam adattípusai

A közintézmények számára releváns adatok számos különböző forrásból származnak, és számos különböző módon szerezhetők be. A kormányzati szervezetek, a polgárok, a vállalkozások, a kutatók és más társadalmi szereplők tudatosan vagy tudtukon kívül mind hozzájárulnak nagy és kis mennyiségű nyílt és minősített, strukturált és strukturálatlan, személyes és nem személyes jellegű adatok keletkezéséhez.

Nyílt adatok

A nyílt adatok bárki által szabadon felhasználhatók, újrafelhasználhatók és terjeszthetők. Nyílt kormányzati (állami) adatokról abban az esetben beszélünk, ha a nyílt adat valamely kormány által került előállításra. Ezek olyan adatok, amelyek az állam működéséhez szükségesek, de nem azonosíthatók belőlük egyének, vagy nem sértenek üzleti/állami titkot.

Magyarországon a nyilvánosan is megismerhető közérdekű és a közérdekből nyilvános adatok körét a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) szabályozza. A törvényben feltüntetett adatok meghatározásai a következők:

– Közérdekű adat: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a bir-

tokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.
- Közérdekből nyilvános adat: A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.[121]

Személyes adatok

Személyes adatnak minősül minden olyan információ, amely egy azonosított vagy azonosítható természetes személyre („érintett") vonatkozik. Azonosítható természetes személy az, aki közvetlenül vagy közvetve beazonosítható, különösen valamely azonosító (például név, azonosító szám, helymeghatározó adat vagy az adott természetes személy fizikai, fiziológiai, genetikai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző egy vagy több tényező) alapján.

Az Infotv. az alábbi személyes adatokkal kapcsolatos fogalmakat határozza meg:
- Biometrikus adat: Egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.
- Bűnügyi személyes adat: A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.
- Egészségügyi adat: Egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.
- Genetikai adat: Egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott

[121] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.

– Különleges adat: A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.[122]

Minősített adatok

A digitalizáció kialakítása és fejlesztése során elsősorban nyílt adatok kerülnek begyűjtésre, feldolgozásra és felhasználásra, azonban lehetnek olyan helyzetek, hogy egy-egy adat esetében szükséges annak minősítése, így mindenképpen fontos megemlíteni az ehhez kapcsolódó alapvető fogalmakat.

Magyarországon a minősített adatok kezeléséről a 2009. évi CLV. törvény a minősített adat védelméről rendelkezik, és ebben a törvényben határozták meg azokat az értelmező rendelkezéseket, amelyek ismertetik a minősített adatokhoz kapcsolódó alapvető fogalmakat, amelyek a következők:

– Nemzeti minősített adat: A minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.

[122] 2011. évi CXII. törvény.

– Külföldi minősített adat: Megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.[123]

Minősítői jogkört kizárólag meghatározott közhatalmi jogosítványokkal rendelkező személyek kaphatnak. A minősítésre csak a törvényben meghatározott védhető közérdek közvetlen sérelme, illetve veszélyeztetése esetén van mód. Ez abban az esetben állhat fenn, ha az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, károsítja a minősítéssel védhető közérdeket, és az adat nyilvánosságát, megismerhetőségét meghatározott ideig korlátozni szükséges. Minősített adathoz csak az a személy férhet hozzá és használhat fel, akinek ez állami vagy közfeladatai ellátásához indokolt, és aki – törvényben meghatározott kivétellel – rendelkezik érvényes személyi biztonsági tanúsítvánnyal, titoktartási nyilatkozattal, valamint felhasználói engedéllyel.

Big data

A digitalizációnak köszönhetően napjainkban egyre nagyobb és összetettebb adatbázisok jelennek meg, amelyek keletkezésének fő mozgatórugói az emberi tevékenységek fokozottabb nyomon követése és a tárgyak internetének elterjedése. Ezt a fejlődést általában big data néven emlegetik.

A big data fogalom egy komplex technológiai környezetet jelent, amely egyaránt tartalmazza az adatokat, a hálózati eszközöket és elemeket, valamint az óriási adatmennyiség tárolásához és feldolgozásához szükséges szoftvereket, hardvereket. Maga a big data nem egy konkrét technológia, hanem olyan régi, jól bevált és új technológiák összessége, amelyek alkalmasak a hatalmas adatmennyiségek kezelésére. A big data általában öt fő jellemzővel írható le, ez a big data 5V. A konkrét jellemzőket különböző vállalatok más-más módon definiálják. Általában az első három V mindenhol megegyezik, a többi pedig változhat:

[123] 2009. évi CLV. törvény a minősített adat védelméről.

– Volume: nagy mennyiség;
– Velocity: nagy sebesség, gyors változás;
– Variety: változatos formában, nagy heterogenitás;
– (Veracity: kérdéses pontosság, ellenőrizhetetlen megbízhatóság);
– (Variability: akár ellentmondó, inkonzisztens adatok);
– (Value: az adatok értéke, üzleti értéket teremtenek).

A digitális állam adatkezelési szereplői

Az OECD-nek az adatvezérelt közszférára vonatkozó tanulmánya alapján a digitális állam megvalósításában hat különböző szereplő vesz részt, amelyek a következők:

– az adatalany/érintett;
– az adatfelelős/adatközlő;
– az adatkezelő;
– az adatfeldolgozó;
– az adatelemző; és
– az állami döntéshozó.[124]

Az adatalany/érintett

Az érintett az a személy, akiről adatokat generálnak vagy gyűjtenek. Ezek lehetnek emberek (egyének és csoportok), állatok, tárgyak (pl. villanyórák, közlekedési lámpák, háztetők) vagy időnként kevésbé kézzelfogható entitások, például szervezetek (állami, magán és nonprofit) vagy természeti jelenségek (pl. a tenger, a levegő).

Az Infotv. alapján az adatalany vagy érintett az a természetes személy, aki bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg

[124] Charlotte van Ooijen – Barbara Ubaldi – Benjamin Welby: *A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance.* Paris, OECD Publishing, 2019.

egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.[125]

Az adatfelelős/adatközlő

Az Infotv. alapján az adatfelelős az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett. Az adatközlő az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi.[126]

A digitális kormányzati ökoszisztéma különböző szereplői ugyanabban a témában adatfelelősként/adatközlőként működhetnek közre, és ezáltal különböző nézőpontokat nyújthatnak ugyanarról a szakpolitikai kérdésről.

Az adatkezelő

Az adatkezelők azok, akik végső soron jogi felelősséggel tartoznak az adatok kezelésének biztosításáért.

Az Infotv. alapján az adatkezelő az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.[127]

Az adatfeldolgozó

Az adatfeldolgozók közé tartoznak azok a külső vállalatok, amelyek adatkezelési és elemzési eszközöket és kritikus számítástechnikai erőforrásokat kínálnak a kormányzat számára. Ezek többek között magukba foglalják az olyan technikai

[125] 2011. évi CXII. törvény.
[126] 2011. évi CXII. törvény.
[127] 2011. évi CXII. törvény.

megoldásokat, mint az adattároló szerverek, az adatbázis-kezelő vagy -elemző szoftverek, illetve a felhőalapú számítástechnikai erőforrások.

Az Infotv. alapján az adatfeldolgozó az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.[128]

Az adatelemző

Az adatelemzők közé tartoznak a kormányzaton belül azok, akik adatgyűjtési és -elemzési feladatokat látnak el, de olyan külső vállalatok is, amelyek ezeket a szolgáltatásokat nyújtják a kormányzatnak vagy a kormányzat számára. Idetartoznak az adatvizualizációs szolgáltatások is.

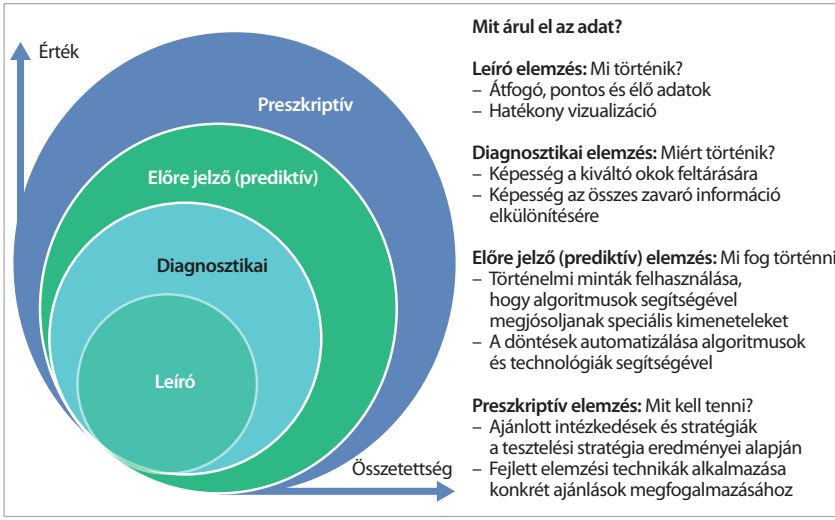
Az állami döntéshozó

Az állami döntéshozók azok a személyek, akik a kormányzat minden szintjén megtalálhatók, a miniszterektől kezdve a szakpolitikai tervezőkön, adóellenőrökön és utcai szintű bürokratákon át a költségvetési és humánerőforrás-menedzserekig. Ezek a személyek olyan döntések meghozatalára kapnak felhatalmazást, amelyek hozzájárulnak a jobb szakpolitikák és szolgáltatások kialakításához. Az adatok felhasználását folyamatosan biztosítani kell, hogy a lehető legjobb döntést lehessen meghozni, legyen szó akár a polgárok és a társadalom igényeinek kezdeti megértéséről, az ezekre adott válaszok megtervezéséről, szakpolitikák és szolgáltatások nyújtásáról vagy az elszámoltathatóságról. Ily módon az adatok olyan értékes eszközzé válnak a kormányok kezében, amelyek hozzájárulnak, hogy előremutatóvá, befogadóvá és a polgárok igényeire reagálóvá váljanak általuk, és amelyek hozzájárulhatnak ezzel a közbizalom erősítéséhez.[129]

[128] 2011. évi CXII. törvény.

[129] Van Ooijen – Ubaldi – Welby (2019): i. m.

Az adatok megnövekedett mennyisége, változatossága és gyorsasága új technikákat és eszközöket követel meg az adatok feldolgozásához és értelmezéséhez. A legújabb adatelemzési módszereket alapvetően arra használják, hogy képesek legyenek megfelelő összefüggéseket levonni, függőségeket megállapítani és előrejelzéseket készíteni a várható eredményekre és a viselkedésre vonatkozóan. Négy fő adatelemzési kategóriát különböztethetünk meg, amelyeket a 27. ábra szemléltet.



27. ábra: Az adatelemzés négy típusa

Forrás: Thomas Maydon: *The 4 Types of Data Analytics,* 2017

A leíró adatelemzés

A leíró elemzés az adatokat arra használja, hogy leírja, mi történt az összetett politikai kérdések elemzése során. A leíró elemzés a jelentéskészítés alapeleme, a „hányan, mikor, hol és mit" alapvető kérdéseire ad választ. Két kategóriára osztható: ad hoc és előkészített jelentések. Az előkészített egy olyan jelentés, amelyet már korábban megterveztek, és egy adott témakör köré gyűjtött információkat

tartalmaz. Az ad hoc jelentések ezzel szemben általában nincsenek ütemezve. Akkor jönnek létre, amikor egy adott kérdés megválaszolására van szükség.

A diagnosztikai adatelemzés

A diagnosztikai elemzés egy lépéssel továbbmegy az adatok gyűjtésénél és elemzésénél azzal a céllal, hogy megmagyarázza, miért történt egy adott szakpolitikai probléma, azonosítsa annak kiváltó okait, és megfejtse a mögöttes strukturális tendenciákat. Ehhez gyakran alkalmaznak olyan technikákat, mint az adatfeltárás, az adatbányászat és az összefüggések keresése. A többi kategóriához hasonlóan ez is két specifikusabb kategóriára oszlik: felfedezés és riasztások, valamint lekérdezés és mélyre ásás. A lekérdezés és a mélyre ásás arra szolgál, hogy a meglévő jelentésekből minél több részletet sikerüljön hasznosítani. A felfedezések és riasztások még a bekövetkezése előtt értesítést küldenek a potenciális problémáról. A diagnosztikai adatelemzéssel olyan információk is könnyedén begyűjthetők, mint például egy vállalatnál egy új pozícióra a legmegfelelőbb jelölt.

Előre jelző (prediktív) adatelemzés

Az előre jelző elemzés adatokat és algoritmusokat használ arra, hogy megjósolja a legvalószínűbb eseményeket, gyakran gépi tanulással, ennek alapján a kapott eredmények alapján nagy valószínűséggel megmondható, hogy mi fog történni. A leíró és diagnosztikai elemzés eredményeit használja fel a közös halmazok és a kivételek felismerésére, valamint a jövőbeli tendenciák meghatározására, ami értékes eszközzé teszi az előrejelzésben. Ezek az előrejelzések azonban csak becslések, amelyek pontossága nagymértékben függ az adatok minőségétől és a helyzet stabilitásától, ezért gondos kezelést és folyamatos optimalizálást igényelnek.

Preskriptív adatelemzés

A preskriptív (tételes) elemzés célja, hogy szó szerint előírja, milyen lépéseket kell tenni, hogy valamit előidézzünk vagy megakadályozzunk, egy jövőbeli problémát kiküszöböljünk vagy egy ígéretes fejlődési tendenciát teljes egészében

képesek legyünk kihasználni. Ez az adatelemzések legmodernebb típusa, ami nemcsak belső, múltbeli adatokra, hanem külső információkra is támaszkodik, és az alkalmazott algoritmusok ezeket elemzik. Az elemzésben a mesterséges intelligencia és a big data kombinációja segít megjósolni az eredményeket és azonosítani a szükséges intézkedéseket.[130]

A bizalom és a magánélet védelme a digitális államban

A hatékonyságon és eredményességen túl a kormányok számára a szolgáltatási innovációk bevezetésekor a törvényesség és a bizalom megteremtése is egy olyan fontos tényező, amelyet figyelembe kell venniük a digitális állam kialakítása során. Egyrészt ez jelentős akadályt jelenthet a digitális átalakulás előtt, másrészt pedig a lehetséges pozitív hatások egyikét jelentheti, amelyeket az új technológiák eredményezhetnek.

Amennyiben digitális államról beszélünk, fontos kitérni a közszféra szervezetei által történő etikus adatfelhasználásra, azok törvényességére, amelyek garantálhatják a közbizalmat, illetve a magánélet védelmére, az átláthatóságra és azokra a kockázatokra, amelyekkel a kormányoknak és az állampolgároknak tisztában kell lenniük. Ezek kiemelten fontosak abból a szempontból, hogy megértsük a következőket:

- a közszférába vetett bizalom milyen szerepet játszik az új digitális szolgáltatások elfogadásában az állampolgárok körében;
- az állampolgárok milyen feltételek mellett hajlandóak az új digitális közszolgáltatásokat elfogadni;
- az állampolgárok milyen kompromisszumokat kötnek a magánélet védelme és az új digitális közszolgáltatások használatából származó előnyök között a különböző területeken.

Számos kutatás kimutatta az elmúlt időszakban, hogy azok, akik általában bizalmatlanabbak és aggódnak a magánélet védelme miatt, alapvetően előnyben részesítették azokat a megoldásokat, ahol adataikat független szervezetek dolgozták fel, és nem a hatóságok vagy a kormányzat. Ez a tendencia különösen jelentős volt két érzékeny területen: az egészségügy és a szavazás területén. Ezek azt mutatják, hogy a kormányok nem tekinthetik magukat immunisnak

[130] Oracle: *What is Data Analytics?* 2021.

a polgárok magánélet védelmével kapcsolatos aggodalmaival szemben. Szintén levonható az a következtetés, hogy a lakosság megítélése szerint a kormányok és a hatóságok nem teljesen megbízhatóak adataik kezelésében, ami az elszámoltathatósággal kapcsolatos sürgető kérdéseket vet fel a digitális átalakítás során. A közszolgáltatások IKT-alapú átalakítása során figyelembe kell venni a polgárok megítélését és véleményét, és szükség esetén nemcsak szabályozással, hanem közvetlen konzultációk és tudatosságnövelő/oktatási kampányok révén meg kell alapozni a bizalmat, valamint folyamatos tudatosítási tevékenységet kell folytatni. Mindezek mellett egyelőre az a tendencia látszik, hogy a lakosság nem hajlandó a magánélet és a személyes adatok védelmét feláldozni az új digitális szolgáltatásokért cserébe. A magánélet védelmét és a személyes adatok feldolgozását illetően nem az tűnik lényegesnek, hogy az újonnan kialakított szolgáltatások milyen típusú előnyöket nyújtanak, hanem az, hogy a polgárok mennyire bíznak abban a szervezetben, amely hozzáfér az adataikhoz és azokat kezeli. Ennek megfelelően a kormányoknak komoly erőfeszítéseket kell tenniük annak érdekében, hogy növeljék legitimitásukat és elszámoltathatóságukat a személyes adatok feldolgozása során a közszolgáltatások javítása érdekében. A legitimitás és a bizalom egyszerre fontos folyamatszintű előfeltétele és végeredménye a digitális kormányzati átalakulásnak. A kormányzat, a közhivatalok és a tisztviselők által használt új adatközpontú technológiák természetére vonatkozó világos és átlátható kommunikáció a kiindulópontja a polgárokkal való bizalmi kapcsolatok kiépítésének.[131]

Ahhoz, hogy a digitális átalakulás teljes mértékben megvalósítható legyen, és a benne rejlő előnyöket a lehető leghatékonyabban tudjuk kihasználni, az egyéneknek, a vállalatoknak és a kormányoknak biztosnak kell lenniük abban, hogy a digitális környezetben való részvételük társadalmi és gazdasági tevékenységeik végzése során több előnnyel jár, mint hátránnyal. Az ilyen hátrányok a digitális technológiákat, az adatokat és a határokon átnyúló áramlásokat érintő különböző bizonytalansági forrásokból eredhetnek. Sok közülük a potenciális digitális biztonsági incidensekhez kapcsolódik (például az adatok, rendszerek vagy hálózatok rendelkezésre állásának, integritásának vagy bizalmas jellegének megsértése). A nemkívánatos események – például az üzleti vagyon vagy az egyén személyazonosságának ellopása, vagy a személyes adatokkal való visszaélés – következményei hatással lehetnek valamennyi szereplő hírnevére, pénzügyeire, szabadságára, autonómiájára, egészségére, jólétére, biztonságára, versenyképességére vagy haté-

[131] Misuraca–Barcevičius–Codagnone (2020): i. m.

konyságára, és végső soron korlátozhatják a digitális környezetben történő teljes körű részvételre való hajlandóságukat. Emellett veszélyeztethetik társadalmunk működését is, mivel a digitális biztonsági incidensek olyan kritikus tevékenységeket is érinthetnek, mint például az energia, a pénzügyek és a közlekedés. A bizalom biztosítása érdekében különböző területekre kell komoly figyelmet fordítani, többek között a digitális biztonságra, a magánélet védelmére és a fogyasztóvédelemre, különös tekintettel a kis- és középvállalkozásokra.

A bizalom

A bizalom alapvető fontosságú olyan helyzetekben, ahol a bizonytalanság és a kölcsönös függőség fennáll. A digitális környezetben ez a két tényező markánsan megjelenik, éppen ezért jelent a bizalom kialakítása és fenntartása komoly kihívást a digitális állam kialakítása és működtetése során. Az egyén szempontjából a bizalom a digitális korban arról szól, hogy hajlandó-e időt, pénzt áldozni, illetve személyes adatainak felfedését kockáztatni a kereskedelmi és társadalmi tevékenységekben való részvétel érdekében, továbbá hogy mennyire válik kiszolgáltatottá, ha egy vásárlás rosszul sül el, ha adatait ellopják, vagy ha azokat viselkedésének megfigyelésére, diszkriminációra vagy magánéletének megsértésére használják fel. A szervezetek szempontjából a bizalom azt jelenti, hogy a digitális átalakulás előnyeinek kihasználása érdekében az egyes szervezetek vállalnak bizonyos szintű kockázatokat az esetleges digitális biztonsági, adatvédelmi és fogyasztóvédelmi incidensek okán. Mindezek alapján látható, hogy a bizalom kulcsfontosságú feltétele annak, hogy a digitális korszakban rejlő növekedési és jóléti lehetőségeket teljes mértékben ki lehessen aknázni, még ha az jár is némi kockázattal. A digitális állam esetében is igaz, hogy a kockázatokat nem lehet teljesen elkerülni anélkül, hogy lemondanánk az adott tevékenység előnyeiről, amelyek bizonytalansághoz vezethetnek. Ezeket a bizonytalanságokat nem lehet kiküszöbölni, azonban lehet kezelni, és ennek leghatékonyabb módja a digitális kockázatok kezelése. Összességében megállapítható, hogy bizonyos mértékű kockázatot el kell fogadni ahhoz, hogy a digitális államban rejlő előnyöket ki lehessen használni, vagy más szóval, a kockázatokat az elérendő célok és előnyök fényében elfogadható szintre kell csökkenteni. Ehhez meg kell tanulni a kockázatok elemzését és kezelését, ami magában foglalja annak eldöntését, hogy elfogadjuk-e a kockázatot, hogyan, milyen módon csökkentjük azt, áthá-

rítjuk vagy esetleg elkerüljük, ez utóbbi azonban a digitális átalakulás és ezzel a fejlődés mellőzésével jár.

Kockázatkezelés a digitális államban

A digitális kockázatkezelés a kisvállalkozásoktól a nagyvállalatokon át az állami szervekig mindenkire vonatkozik, ez alól senki nem lehet kivétel. Minden szereplőnek közös felelőssége van abban, hogy szerepének, cselekvőképességének és a körülményeknek megfelelően kezelje a tevékenységét érintő digitális kockázatokat, és ehhez megfelelő készségekkel rendelkezzen. Mivel a kockázat határokon, ágazatokon és érdekcsoportokon átívelő kérdés, a digitális kockázatkezelés közös referenciakeretet biztosít a különböző szakpolitikai közösségek számára a bizalmi politikák integrált módon történő megvitatásához, valamint a különböző szereplők számára a kockázatok átfogóbb mérlegeléséhez és kezeléséhez, a kockázatkezelési ciklus alapvető összetevőire építve. Ezek az összetevők a következők:

- a tevékenység célkitűzéseinek és kontextusának meghatározása, valamint az elfogadható kockázati szint meghatározása;
- a kockázatok értékelése a kockázati tényezők azonosításával;
- a kockázatok bekövetkezésének, valószínűségének és súlyosságának értékelése;
- a kockázatok kezelése, ami magában foglalja a kockázatok egy részének elfogadását, a megfelelő intézkedésekkel az elfogadható szintre történő csökkentését, egy részének a megosztását vagy átruházását, és/vagy egy részének teljes elkerülését;
- a kockázatkezelési ciklus folyamatos nyomon követése és felülvizsgálata a folyamatosan változó környezethez való igazítás érdekében.[132]

A kormányzati szektorban jelentős mennyiségű gazdasági, társadalmi és katonai adatot, információt tárolnak, dolgoznak fel és kezelnek. Ez különösen igaz a digitális állam esetében, ahol az egyes elemek digitalizációjának köszönhetően az előállított adatok mennyisége és mérete lényegesen nagyobb (big data). Ezeknek az adatoknak a védelme prioritást élvez, így világszerte a kormányzati szektor fordítja a legtöbb anyagi, technikai és szakmai erőforrást az informatikai biztonságra, amely kezelésének problémája túlmutat az informatikai rendszere-

[132] OECD: *Going Digital Integrated Policy Framework.* Paris, OECD Publishing, 2020. 36.

ken; az egész szervezet (állami és nem állami) felépítését, üzletmenetét, folyamatait érintő kérdésről van szó. A különböző tevékenységeket végző szervezeteknek különböző típusú kockázatokkal kell szembenézniük, amelyek veszélyeztethetik a kezelt adataikat. Minden szervezetnek egyedi informatikai kockázati profilja van az alkalmazott eszközei, rendszerei és kapcsolódásai függvényében, amelyekre komoly hatással van a felhasználók és üzemeltetők kompetenciája, biztonságtudatossága. Ennek megfelelően nem lehetséges egy egységes iránymutatás megfogalmazása a kockázatok kezelésére. Minden egyes szervezetnek saját magának kell kialakítania a saját kockázatmenedzsmentjét az elvégzett kockázatelemzések eredményei és a jogszabályi előírások figyelembevételével.[133]

Magyarországon a 2013. évi L. törvény rendelkezik az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.). A törvény megfogalmazza az alapvető elektronikus információbiztonsági követelményeket, az azokhoz kapcsolódó feladatokat, felelősöket, intézményeket, hatóságokat, valamint a kockázatkezeléshez kapcsolódó elveket és alapvető fogalmakat, amelyek a következők:

- kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ezáltal okozott kár nagyságának a függvénye;
- kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
- kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;
- kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.[134]

A kockázatelemzésnek és kezelésnek igazodnia kell a vizsgált intézmény üzleti folyamataihoz, ki kell terjednie az alkalmazott informatikai rendszerek teljes életciklusára, és fel kell ölelnie a kiszervezés és az ellenőrzés területeit is. A kockázatelemzés támogatja a döntéshozatali folyamatokat, hozzájárul ahhoz, hogy a szervezet vezetői megalapozott döntéseket hozzanak azáltal, hogy támogatja a releváns információkon alapuló legjobb döntési alternatívák kidolgozását. A kockázatkezelés minden szervezeti folyamatnak részét alkotja, a stratégiai tervezéstől

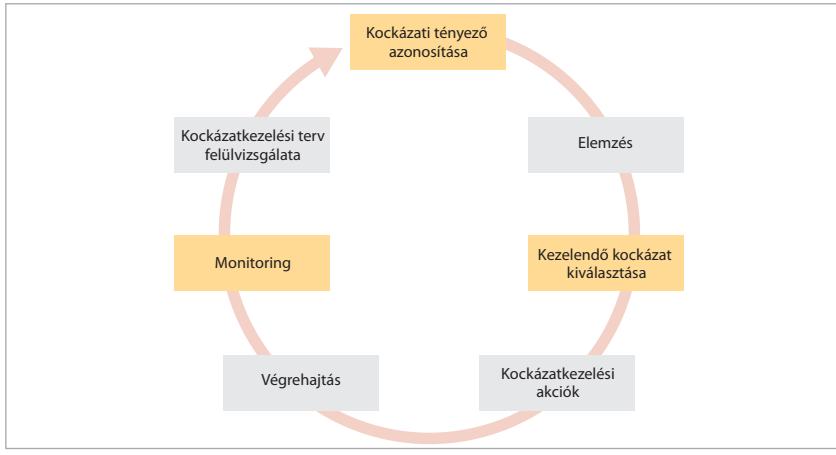
[133] László Gábor: *Kockázatértékelés, kockázatmenedzsment.* Budapest, NKE, 2014.

[134] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

a projektmenedzsmenten keresztül a változások kezeléséig minden területen áthatja a szervezeti működést. A kockázatkezelés dinamikus, ismétlődő és rugalmasan alkalmazkodik a változásokhoz azáltal, hogy érzékeli a szervezetben történő változásokat és folyamatosan alkalmazkodik hozzájuk, ezzel hozzájárul a szervezet folyamatos fejlődéséhez. Mivel a szervezetek folyamatosan fejlődnek, és ez különösen igaz a digitális állam esetében, ahol az egyes állami és közigazgatási szervezetek digitalizációja során a belső és a külső környezetük folyamatosan megújul, a kockázatkezelésről elmondható, hogy egy ciklikus folyamat.

A kockázatkezelési ciklus az alábbi elemekből épül fel, ezeket a 28. ábra szemlélteti:

- a kockázati tényezők feltárása;
- a feltárt kockázati tényezők elemzése;
- a kezelendő kockázatok kiválasztása;
- a kiválasztott kockázatokra kockázatkezelési akciók megfogalmazása;
- a kockázatkezelési feladatok végrehajtása;
- nyomonkövetési és monitoringfeladatok;
- a monitoringtevékenység során feltárt hiányosságok kezelése.[135]



28. ábra: A kockázatkezelési ciklus elemei

Forrás: Beláz (2018): i. m. 58.

[135] Beláz Annamária: A digitális állam információbiztonsága: kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban. *Bánki Közlemények,* 1. (2018), 3. 58.

A kockázatkezelési gyakorlatok valószínűleg különböznek a meghatározott célok függvényében, amelyek lehetnek például a digitális biztonság, a magánélet védelme, a fogyasztóvédelem vagy a termékbiztonság, de az alkalmazott házirendeknek figyelembe kell venniük a különböző kockázati kategóriák közötti összefüggéseket.

A digitális biztonság egy nagyon sokrétű terület, amely magában foglalja a gazdasági és társadalmi jóléthez, a technológiához, a bűnüldözéshez, valamint a nemzeti és nemzetközi biztonsághoz kapcsolódó kérdéseket. A kritikus tevékenységek digitális biztonsága és ellenálló képessége, valamint a digitális biztonságpolitika különösen fontos eleme a gazdasági jólétnek és a nemzetbiztonságnak, továbbá elengedhetetlenül szükségesek a gazdaság és a társadalom működéséhez. A digitális átalakulás jelentősen növeli a kritikus tevékenységek kölcsönös függőségét, a rendszerek összetettségét és az ágazatokon és határokon átívelő rendszerszintű hibák kockázatát.

Gazdasági és társadalmi szempontból a digitális biztonsági kockázatot hagyományosan technikai problémaként közelítették meg, amely technikai megoldásokat igényel. A digitális biztonsági kockázat változó jellege és nagyságrendje azonban arra készteti a kormányokat, hogy újraértékeljék stratégiáikat, és kulturális változást sürgessek ezen a területen. A kormányoknak olyan irányelveket kell elfogadniuk, amelyek arra ösztönzik a kritikus infrastruktúrák és szolgáltatások üzemeltetőit, hogy erősítsék meg digitális biztonsági kockázatkezelésüket. Ennek során lehetőségeket kell biztostani számukra, hogy képesek legyenek a lehető legtöbbet kihozni a digitális átalakulásból, többek között az olyan technológiák bevezetése és alkalmazása révén, mint például a tárgyak internete, a mesterséges intelligencia, a big data elemzés, valamint a blokklánc. Mindezek mellett az irányelveknek figyelembe kell venniük a meglévő ágazatspecifikus piaci, szabályozási és kulturális sajátosságokat. Míg a kritikus tevékenységek gyakran a nagy és a magánszektor szereplőire támaszkodnak, a digitális átalakulás a kkv-kat is képessé teszi arra, hogy részt vegyenek az alapvető szolgáltatások értékláncában. A digitális kockázatkezelést elősegítő irányelvek és házirendek kulcsfontosságúak a bizalom erősítéséhez, és lehetővé teszik az egyének és a szervezetek számára, hogy maximalizálják gazdasági és társadalmi célkitűzéseiket.[136]

[136] OECD: *Digital Security and Resilience in Critical Infrastructure and Essential Services.* Paris, OECD Publishing, 2019.

A magánélet védelme

A digitális átalakulás előrehaladtával a magánélet és különösen a személyes adatok védelme egyre inkább a bizalmat befolyásoló kritikus tényezővé válik. A személyes adatok egyre fontosabb szerepet játszanak a gazdaságunkban, a társadalmunkban és a mindennapi életünkben. A digitalizációnak köszönhetően megjelenő új technológiák és a felelős adatfelhasználás pedig nagy társadalmi és gazdasági előnyökkel járhatnak, amennyiben megfelelően használjuk őket. Ugyanakkor az összegyűjtött, feldolgozott és megosztott személyes adatok sokasága megnövelte az egyének magánéletét fenyegető kockázatokat, ami a digitális állam kialakítása és működtetése során komoly kihívásokat állít a szakemberek elé. A személyes adatokat egyre gyakrabban használják fel a gyűjtéskor nem várt módon, ennek megfelelően számos esetben felhasználtak személyes adatokat úgy, hogy érzékeny információk kerülhettek napvilágra, vagy hogy a feltételezhetően anonim adatokat konkrét személyekhez tudták kapcsolni. Az adatok felhasználásának és értékének növekedésével a személyes adatok megsértése is egyre gyakoribbá vált.[137]

A személyes adatok kezelése és védelme érdekében hozta meg az Európai Parlament és a Tanács a 2016/679 számú rendeletét a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről 2016 áprilisában (General Data Protection Regulation – GDPR). A GDPR 5. cikke tartalmazza a személyes adatok kezelésére vonatkozó elveket az Európai Unión belül, ami így minden tagállamra is érvényes és kötelező érvényű. Az egyes szabályozások ismertetése előtt fontos a 89. cikk (1) bekezdését megemlíteni, amelyre a személyes adatokra vonatkozó részek többször hivatkoznak, és ami az archiválás kérdéskörét dolgozza fel. A GDPR a személyes adatok archiválásáról a következőképpen rendelkezik:

> „A személyes adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelését e rendelettel összhangban az érintett jogait és szabadságait védő megfelelő garanciák mellett kell végezni. E garanciáknak biztosítaniuk kell, hogy olyan technikai és szervezési intézkedések legyenek érvényben, amelyek biztosítják különösen az adattakarékosság elvének betartását. Ezen intézkedések közé tartozhat az álnevesítés, amennyiben az említett célok ily módon megvalósíthatók. Amennyiben e célok megvalósíthatók az adatok oly módon történő további

[137] OECD: *OECD Digital Economy Outlook 2020.* OECD Publishing, 2020.

kezelése révén, amely nem vagy már nem teszi lehetővé az érintettek azonosítását, a célokat ilyen módon kell megvalósítani."[138]

A személyes adatok kezelése vonatkozásában a GDPR 5. cikk (1) bekezdése az alábbiakat határozza meg:

A személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság");

b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhozkötöttség");

c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság");

d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság");

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság");

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével,

[138] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, 89. cikk (1) bekezdés.

véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg").[139]

A GDPR 6. cikke alapján a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.[140]

A GDPR 9. cikke a személyes adatok különleges kategóriáinak kezelésével foglalkozik, amely alapján az (1) bekezdés kimondja, hogy a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos. Az (1) bekezdés nem alkalmazandó abban az esetben, ha:

a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy

[139] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, 5. cikk (1) bekezdés.
[140] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, 6. cikk (1) bekezdés.

tagállami jog úgy rendelkezik, hogy az (1) bekezdésben említett tilalom nem oldható fel az érintett hozzájárulásával;

b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;

c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;

d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;

e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;

f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;

g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a (3) bekezdésben említett feltételekre és garanciákra figyelemmel;

i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

j) az adatkezelés a 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.[141]

A GDPR alapján is látható, hogy a személyes adatok védelme komoly kihívásokat állít a szakemberek elé, ami kiemelten igaz a digitális államra, ahol lényegesen több adatot gyűjtenek, állítanak elő és dolgoznak fel, ami komoly kockázatokat is jelent. Ezek a kockázatok nemcsak az érintett személyeket érintik, hanem a magánélet védelmének alapértékeit és alapelveit is, mint például az egyéni autonómia, az egyenlőség és a szólásszabadság, amelyek szélesebb körű hatást gyakorolhatnak a társadalomra.

A digitalizációnak köszönhetően az egyének otthon és a munkahelyükön egyre több személyes adatot osztanak meg, akár szándékosan (például a közösségi felületeken), de tudtukon kívül is, például a webes böngészések vagy az okostelefonok használata során. Ugyanakkor az egyének nagyobb biztonságot és felügyeletet keresnek az adataik kezelésével kapcsolatban: tudni akarják, hogy gyűjtenek-e, és ha igen, akkor milyen személyes adatokat gyűjtenek és tárolnak róluk, hogyan használják fel azokat, és hogy törölhetik-e vagy javíthatják-e az adatokat, illetve ellenőrizhetik-e a másodlagos felhasználást. A technológiai fejlődés segíthet a bizalom növelésében a beépített adatvédelem révén, amelynek során a termék vagy szolgáltatás tervezésének kezdeti szakaszában figyelembe veszik az adatvédelemmel kapcsolatos következményeket. Ez lehetővé teheti a magánélet védelmének a technológiába való beágyazását vagy kódolását, és a személyes adatok gyűjtésének kezdettől fogva történő minimalizálását, illetve kezelésének nyomon követését. A titkosítás és egyéb biztonsági megoldások

[141] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, 9. cikk.

széles körben elterjedése fontos szerepet játszhat a magánélet védelme szempontjából, különösen az egyre inkább elterjedő mobileszközök és a tárgyak internete vonatkozásában.

Mindezeket figyelembe véve megállapítható, hogy a magánélet és a személyes adatok védelmével kapcsolatos kockázatokat sokkal átfogóbban, minden részletre kiterjedően kell kezelni, hogy az erre hivatott szervezetek képesek legyenek hatékony biztosítékokat nyújtani az állampolgároknak.

Összefoglalás

A fejezet a digitális állam fejlődését vizsgálja az Európai Unióban és Magyarországon, a stratégiákra, a célkitűzésekre és az eredményekre összpontosítva. Kiemeli a megfelelő kompetenciák fejlesztésének, az infrastruktúra bővítésének, az e-kormányzat előmozdításának, valamint a biztonság és az adatvédelem szavatolásának fontosságát. A digitális állam alapja a megfelelő készségek kialakítása a polgárok, a vállalkozások és a közintézmények körében. Az EU és Magyarország jelentős előrelépést ért el az internet-hozzáférés bővítése, az informatikai készségek fejlesztése és az IKT-szakemberek számának növelése terén. A háztartások többsége ma már rendelkezik internet-hozzáféréssel, miközben az e-kormányzat, az online banki ügyintézés, az e-egészségügy és az online oktatás egyre népszerűbbé válik.

A nemzeti stratégiák négy fő pillért határoznak meg: digitális infrastruktúra, digitális készségek fejlesztése, digitális gazdaság és digitális közigazgatás. E pillérek célja egy olyan koherens és fenntartható digitális ökoszisztéma létrehozása Magyarországon, amely lehetővé teszi a hatékony közszolgáltatásokat. A digitális állam központi eleme az e-kormányzat fejlesztése, amelynek kiemelt célja az elektronikus közigazgatás kiterjesztése, a szabályozott e-kormányzati szolgáltatások és a papírmentes közigazgatás.

A sikeres digitális államhoz elengedhetetlenek az intelligens városok és az adatvezérelt kormányzás. A digitális bizalom kiépítése, a személyes adatok védelme, a kiberbiztonsági kockázatok kezelése, valamint a polgárok és a vállalkozások körében a digitális készségek hiányának kezelése óriási kihívást jelent. A fejezet hangsúlyozza, hogy a digitális állam sikere az összehangolt és fokozatos lépésekben, az állami és piaci szereplők közötti együttműködésben, a technológiai semlegességben és a nyílt forráskódú fejlesztésekben rejlik.

Biztonsági fenyegetések a digitális államban

A fejezetben a digitális államot, illetve az azt működtető információs és kommunikációs rendszerek működését, valamint a kezelt és tárolt adatokat alapvetően fenyegető támadási vektorokat ismertetjük. Ehhez tisztázni kell olyan alapvető fogalmakat, mint az információbiztonság és a kiberbiztonság. Ezek elengedhetetlenek ahhoz, hogy megértsük a különbséget az információvédelmi tevékenységek, valamint a kibertérben végzett ellentevékenységek között. Mindez azért is fontos, mert a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatások napjaink életének egyre fontosabb, folyamatosan növekvő jelentőségű feltételét képezik, befolyásolják az állami működés hatékonyságát, a vállalkozások eredményességét és versenyképességét, az állampolgárok életminőségét. Emiatt egyre növekszik a szerepe a kibertérben jelentkező kockázatok és fenyegetések kezelésének, a megfelelő szintű kiberbiztonság garantálásának.[142]

A kiberbiztonság és az információbiztonság fogalma és tartalma

Az információbiztonság és a kiberbiztonság fogalom napjainkban is több esetben okoz még félreértéseket. Ennek egyik alapvető oka, hogy több esetben is félrefordítások vannak a rendelkezésünkre álló dokumentumokban. Emellett szintén probléma, hogy nemcsak ezt a két kifejezést, hanem ezek mellett még az informatikai biztonságot (vagy az elektronikus információs rendszerek biztonságát) is tévesen hozzák össze a többi biztonsági fogalommal összhangban. Erre hívja fel a figyelmet például Muha Lajos és Krasznay Csaba *Az elektronikus információs rendszerek biztonságának fogalma és tartalma* című könyvükben. Meglátásuk szerint általában a szövegkörnyezet egyértelművé teszi, hogy információvédelemről vagy elektronikus információs rendszerek védelméről van-e szó egy dokumentumban. Erre hozzák példának az ISO/IEC 27001:2005 nemzetközi szabványt, amelynek eredeti angol címe az *Information Technology – Security Techniques – Information Security Management Systems – Requirements,* amelynek a kezdetén lévő Information Technology kifejezés egyértelművé teszi, hogy itt az informatikáról van szó, majd

[142] Munk Sándor: Kiberbiztonsági szervezetek közötti interoperábilis információcsere-megoldások. *Hadmérnök,* 13. (2018), 4. 315–328.

ez után következik az Information Security, amely így informatikai biztonságot (az elektronikus információs rendszerek biztonságát) jelenti magyarul, hiszen az előtte lévő informatika kifejezésre utal. Ezt azonban a magyar szabványban szó szerint információbiztonságnak fordították. Már az ő megfogalmazásukban is feltűnik két olyan fogalom, amelyek szoros összefüggésben állnak egymással, de teljesen mást jelentenek. Ezek a biztonság és a védelem, ahol a védelem tevékenység, illetve tevékenységek sorozata, míg a biztonság egy állapot, amelyet a védelmi tevékenységgel lehet létrehozni. A védelem feladatai:

- megelőzés (prevention) és korai figyelmeztetés (early warning);
- észlelés (detection);
- reagálás (reaction);
- esemény- (incident management) vagy válságkezelés (crisis management).[143]

A továbbiakban ezeknek a kifejezéseknek a mélyebb vizsgálata következik, a hazai és nemzetközi szabályzók alapján.

A kibervédelem és a kiberbiztonság

A kiberbiztonsággal kapcsolatos kockázatok és aggodalmak azt eredményezték, hogy sokan, köztük a biztonsági megoldások szállítói is, a kiberbiztonságot olyan fogalommá alakították, amelyet minden, a biztonsággal kapcsolatos szempontot átfogó kifejezésként használnak, gyakran a felhasználók és a vezetőség „kiberfélelmein" lovagolva.

A különböző helyzeteknek és incidenseknek megfelelően a kiberbiztonságra különböző definíciókat és magyarázatokat adnak, és a kibertérrel kapcsolatban széles körben alkalmaznak olyan kijelentéseket, mint a következők:

- a kiberbiztonság valójában ugyanaz, mint az információbiztonság;
- az információbiztonság a kiberbiztonság része;
- egyes kiberbiztonsági támadásoknak semmi közük az információhoz és/vagy az adatokhoz;
- az információbiztonság valójában elavult; és a kiberbiztonság ma már a mindent magában foglaló kifejezés, amely felváltja az információbiztonságot.

[143] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, NKE, 2014. 122.

A fentieket figyelembe véve különböző értelmezések léteznek arról, hogy pontosan mit is tartalmaz, illetve mit nem tartalmaz a kiberbiztonság. Ebben az alfejezetben az egyes hazai és nemzetközi szabályzatokban, szabványokban megfogalmazott fogalmi magyarázatokat mutatjuk be.

A magyar szabályozói környezetben a 2013. évi L. törvény fogalmazza meg a kibervédelem és a kiberbiztonság fogalmát a következőképpen:

- kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertérképességek megőrzését;
- kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Az Európai Unióban a következő meghatározások kerültek megfogalmazásra:

- kibervédelem: a kommunikációs és irányítási rendszerek infrastruktúrája elleni kibertámadások elleni védelemre és az azokra való reagálásra irányuló biztonsági intézkedések alkalmazása;[144]
- kiberbiztonság: azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek.[145]

A fenti megfogalmazásokból látható, hogy az unióban a kiberbiztonság már nem feltétlenül egy állapot. Eltérően a magyar felfogástól, az uniós szabályokban a biztonság is egy tevékenység, a megkülönböztetés módját pedig a *Kézikönyv a kiberbiztonságról* című tanulmányban találhatjuk meg, amely *Az Európai Unió közös biztonság- és védelempolitikája* című kiadvány keretein belül jelent meg. A tanulmány úgy fogalmaz, hogy az EU és az Európai Külügyi Szolgálat (EKSZ) a kiberbiztonság kifejezést általános, elsősorban a polgári kontextusra vonatkozó fogalomként használja, míg a kibervédelem kifejezést általában a katonai kiberügyi

[144] Carmen-Cristina Cirlig: *Cyber Defence in the EU: Preparing for Cyber Warfare?* (h. n.), European Parliamentary Research Service, 2014. 4.

[145] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály).

vonatkozásokra használják. Mindazonáltal a két fogalom szorosan kapcsolódik egymáshoz, mivel ugyanazokkal a fenyegetésekkel foglalkozik, ugyanazokat az alapelveket követi, és hasonló intézkedéseket és eljárásokat igényel.[146]

Az információvédelem és az információbiztonság

Az információvédelmet Magyarországon a Miniszterelnöki Hivatal Informatikai Koordinációs Iroda által készített Informatikai Tárcaközi Bizottság-ajánlásokban az *Informatikai rendszerek biztonsági követelményei* című 12. sz. ajánlás tartalmazza (MeH ITB 12. számú ajánlás). Az ajánlás szerint az információvédelem a bizalmasság, a sértetlenség és a hitelesség elvesztése elleni védelmet, a megbízható működés a rendelkezésre állás és a funkcionalitás elvesztése elleni védelmet foglalja magába.

Az információbiztonság az MSZ ISO 27001:2014 szabványban került megfogalmazásra, a következőképpen: Az információbiztonság az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése, továbbá egyéb tulajdonságok, mint a hitelesség, a számonkérhetőség, a letagadhatatlanság és a megbízhatóság szintén idetartoznak.[147]

Az információvédelem kifejezés szakemberek által egyik leginkább elfogadott meghatározását a NATO-ban fogalmazták meg. E szerint az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából. A NATO-n belül az információvédelem mellett meghatároztak egy olyan fogalmat is, amely azoknak a biztonsági rendszabályoknak az alkalmazását jelenteni, amelyek a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen kerülnek foganatosításra.[148] Ez a vonatkozó szakirodalmakban az elektronikus információvédelem vagy néha elektroni-

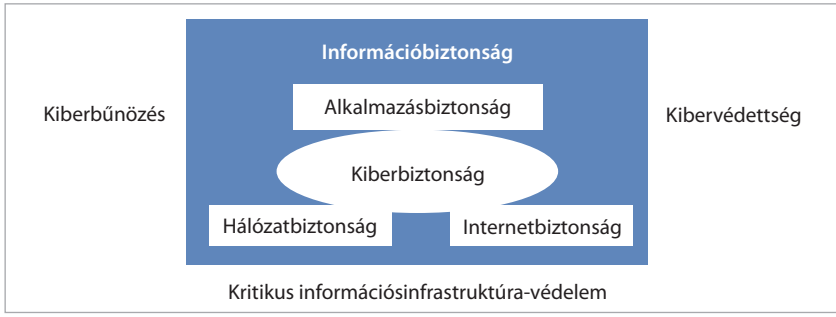
[146] Jochen Rehrl (szerk.): *Handbook on Cyber Security.* Luxembourg, Luxembourg Publications Office of the European Union, 2018.

[147] MSZ ISO 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.

[148] NATO Security Policy, C-M(2002)49, Security within the North Atlantic Treaty Organization (NATO), 2020.

kus dokumentumvédelem, a NATO-ban pedig az INFOSEC kifejezést jelenti, ami az INFOrmation SECurity kifejezés szavainak összevonásából született. Ez a meghatározás egyértelműen az információs és kommunikációs rendszerek, illetve az azokban kezelt adatok védelmére vonatkozik.[149]

A fenti fogalmi magyarázatokból is kiválóan látható, hogy a kiberbiztonság és az információbiztonság részben fedi egymást. Ezt támasztja alá a Nemzetközi Szabványügyi Szervezet és a Nemzetközi Elektrotechnikai Bizottság által 2012-ben létrehozott ISO/IEC 27032:2012 nemzetközi szabvány, ami a kiberbiztonságot úgy határozza meg, mint „az információk bizalmas jellegének, integritásának és rendelkezésre állásának megőrzését a kibertérben". Másrészt a szabvány az információbiztonságot úgy határozza meg, mint „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését". Ennek alapján tehát a kiberbiztonság és az információbiztonság közötti különbség az, hogy a kiberbiztonság a kibertérben lévő információkra korlátozódik, míg az információbiztonság az információ „mindenhol" jelen lévő védelmét jelenti.[150] A 29. ábrán látható a kiberbiztonság, illetve a többi biztonsági terület közötti kapcsolat.



29. ábra: A kiberbiztonság és a többi biztonsági terület kapcsolata
Forrás: ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity, 2012

A fenti ábra világosan szemlélteti, hogy a kiberbiztonság teljes mértékben az információbiztonság részét képezi. Az is látható, hogy a kiberbűnözés és a kibervédettség mind a kiberbiztonságon, mind az információbiztonságon kívülre esik.

[149] Muha–Krasznay (2014): i. m. 12.
[150] ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, 2012.

A kibervédettség a fizikai, a társadalmi, a szellemi, a pénzügyi, a politikai, az érzelmi, a foglalkozási, a pszichológiai, az oktatási vagy egyéb típusú vagy következményű meghibásodás, kár, hiba, baleset, sérülés vagy bármely más, nemkívánatosnak tekinthető esemény elleni védelem feltételét jelenti a kibertérben.

Az ISO/IEC szabványokkal megegyezően az Informatikai Auditorok és Ellenőrök Nemzetközi Szövetsége (Information Systems Audit and Control Association – ISACA) is elkészítette a témával kapcsolatos alapvető fogalmakat és meghatározásokat tartalmazó iránymutatásokat. Az ISACA szerint az információbiztonság magával az információval foglalkozik, függetlenül annak formátumától, magában foglalja a papíralapú dokumentumokat, a digitális és a szellemi tulajdont, valamint a szóbeli vagy vizuális kommunikációt. A kiberbiztonság ezzel szemben a digitális javak védelmével foglalkozik, a hálózatoktól kezdve a hardvereken át a szoftverekig, valamint az internetes rendszerek által feldolgozott, tárolt vagy szállított információkig. Emellett az olyan fogalmak, mint a nemzetállamok által támogatott támadások és a fejlett tartós fenyegetések (advanced persistent threats – APT) szinte kizárólag a kiberbiztonsághoz tartoznak. Mindezek alapján az ISACA is úgy fogalmaz, hogy a kiberbiztonságra az információbiztonság egyik összetevőjeként érdemes gondolni.

Mindezekkel szemben az ENISA úgy fogalmaz, hogy hagyományos értelemben nincs szükség a kiberbiztonságra vonatkozó definícióra, mivel a kiberbiztonság egy átfogó fogalom, és nem lehet olyan definíciót alkotni, amely lefedné a kiberbiztonság által lefedett dolgok teljes körét.[151]

Potenciális sérülékenységek és veszélyek a digitális államban

Napjainkban számos szervezet és vállalkozás vezetője felismerte, hogy az általuk üzemeltetett informatikai rendszerek és kezelt adatok védelme komoly vezetési-irányítási felelősség; következésképpen felelősséggel tartoznak a szervezetükben vagy vállalkozásukban az esetlegesen felmerülő kockázatokért és incidensekért, valamint az esetleges gondatlanság és/vagy tudatlanság miatt felmerülő jogi következményekért. Az információk biztonságával kapcsolatban a továbbiakban ismertetünk néhány olyan biztonsági szolgáltatást és incidenst, amelyek alapvető fenyegetést jelenthetnek a digitális állam informatikai és kommunikációs

[151] Basie von Solms – Rossouw von Solms: Cybersecurity and Information Security – What Goes Where? *Information and Computer Security,* 26. (2018), 1. 2–9.

rendszereire, valamint a kezelt adataira. Az információbiztonság legalapvetőbb fogalma a CIA-elv,[152] amelynek az egyes elemeit az Info tv. a következőképpen határozza meg:

- Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
- Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
- Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetők és az abban kezelt adatok felhasználhatók legyenek.[153]

A fentiek alapján elmondható, hogy a bizalmasság az a tulajdonság, amely megakadályozza, hogy az információ nyilvánosságra kerüljön vagy illetéktelen szervezetek vagy személyek számára hozzáférhetővé váljon, ezáltal megvédi az adatokat a jogosulatlan hozzáféréstől. A bizalmasság ellen irányuló tevékenységekre példák:

- eszközök eltulajdonítása (érzékeny információkat tartalmazó laptop ellopása) – fizikai behatolás vagy lopás;
- jelszólopás;
- érzékeny e-mailek elküldése jogosulatlan személyek számára;
- érzékeny információk felkerülése egy weboldalra hozzáférési korlátozások nélkül, ezzel az adatok nyilvánosságra kerülése – konfigurációs hiba;
- kulcsnaplózó szoftver vagy más kémprogram telepítése – malware.

Az adatsértetlenség az információbiztonságban az adatok teljességének és pontosságának biztosítására és fenntartására utal a teljes életciklus során. Ez megakadályozza, hogy az adatokat észrevétlenül vagy illetéktelenül megváltoztas-

[152] Confidentiality, Integrity, Availability – bizalmasság, sértetlenség és rendelkezésre állás.
[153] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

sák vagy módosítsák. A sértetlenség ellen irányuló legjellemzőbb tevékenység az illetéktelen hozzáférés, amely során a támadó engedély nélkül hozzáfér akár érzékeny adatokhoz is, és azokat tudja módosítani vagy letölteni.

Bármely információs rendszer működési és üzemelési céljainak elérése érdekében az információ rendelkezésre állása rendkívül fontos. Ez azt jelenti, hogy az információk feldolgozására és tárolására használt számítástechnikai rendszerek, a kommunikációs hozzáférési csatornák és a biztonsági ellenőrzések megfelelően működnek. A rendelkezésre állás biztosítása a szolgáltatásmegtagadásos támadások megelőzését is garantálhatja.

Az alábbi táblázat néhány lehetséges támadási vektort szemlétet, amelyek hatással lehetnek a CIA-triász egyes elemeire.

25. táblázat: A CIA-triász potenciális veszélyei

Biztonsági cél	Támadási vektor	Leírás
Bizalmasság	Elfogás Lehallgatás Kémkedés Forgalomelemzés	Az információk jogosulatlan, passzív elfogása, például a hálózat megfigyelése céljából történő lehallgatás. Üzenetek elfogása a kommunikációs mintákból érzékeny információk kinyerése céljából.
Sértetlenség	Megszakítás Módosítás Hamisítás Álcázás Ismétlés Visszautasítás	A lehallgató megpróbálja az információt a saját céljainak megfelelően módosítani. A támadó másnak adja ki magát. Egy már befejezett és engedélyezett szolgáltatást hamisít egy duplikált kéréssel, hogy megismételje az engedélyezett parancsokat.
Rendelkezésre állás	Megszakítás Módosítás Hamisítás Szolgáltatásmegtagadás	A hálózati erőforrás vagy gép elérhetetlenné tételének kísérlete a kiszemelt felhasználók számára.

Forrás: Preeti Sinha – Amit Kumar Rai – Bharat Bhushan: *Information Security threats and attacks with conceivable counteraction.* 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2020. 1208–1213.

A lehallgatásos támadások lehetővé teszik, hogy illetéktelen felhasználók hozzáférjenek adatainkhoz, alkalmazásainkhoz vagy környezetünkhöz, amelyek jellemzően a bizalmasság elleni támadást eredményeznek. A lehallgatás történhet fájlok jogosulatlan megtekintése vagy másolása, telefonbeszélgetések

lehallgatása vagy e-mail olvasása formájában, és végrehajtható nyugalmi vagy mozgásban lévő (információs csatornákon éppen megosztott) adatok ellen. A megfelelően végrehajtott lehallgatási támadásokat nagyon nehéz felderíteni.

A megszakításos támadások lényege, hogy alkalmazásával a támadó eléri, hogy eszközeink ideiglenesen vagy tartósan használhatatlanná válnak, illetve egyáltalán ne álljanak rendelkezésünkre. Ez a digitális állam működésében komoly fennakadásokat, a kritikus információs infrastruktúrák rendszereinek támadása esetén pedig súlyos károkat okozhat. A megszakításos támadások gyakran a rendelkezésre állást érintik, de a sértetlenséget is támadhatják. Egy levelezőszerver elleni szolgáltatásmegtagadással járó támadás, más néven túlterheléses támadás (Denial of Service – DoS) mindenképpen rendelkezésre állást érintő támadásnak minősül. Azonban abban az esetben, ha egy támadó manipulálja azokat a folyamatokat, amelyeken egy adatbázis fut, annak érdekében, hogy megakadályozza a benne lévő adatokhoz való hozzáférést, ezt az adatok esetleges elvesztése vagy sérülése miatt sértetlenségi támadásnak vagy a kettő kombinációjának tekinthetjük. Az ilyen adatbázis-támadást tekinthetjük módosítási támadásnak is, nem pedig megszakításos támadásnak.

A módosítási támadások az eszközeink manipulálását jelentik. Az ilyen támadások elsősorban sértetlenségi támadásnak tekinthetők, de jelenthetnek rendelkezésreállási támadást is. Ha a támadó jogosulatlanul hozzáfér egy fájlhoz, és megváltoztatja a benne lévő adatokat, akkor az a fájlban lévő adatok sértetlenségét befolyásolja, az kompromittálódik, így a továbbiakban már nem megbízható. Az ilyen típusú támadásokkal könnyen befolyásolhatók akár komoly döntési folyamatok is a digitális államban. Ha azonban megvizsgáljuk azt az esetet, amikor a kérdéses fájl egy konfigurációs fájl, amely egy adott szolgáltatás megfelelő működését biztosítja, például egy webkiszolgálóként működő szolgáltatást, akkor a fájl tartalmának megváltoztatásával befolyásolhatjuk a szolgáltatás rendelkezésre állását. Ha folytatjuk ezt a koncepciót, és azt mondjuk, hogy a webkiszolgáló fájlban megváltoztatott konfiguráció olyan, amely megváltoztatja, hogy a kiszolgáló hogyan kezeli a titkosított kapcsolatokat, akkor ezt akár bizalmasság elleni támadásnak is tekinthetjük.

A hamisítási támadások során a támadók adatokat, folyamatokat, kommunikációt vagy más hasonló tevékenységeket hoznak létre egy rendszeren belül, amelyek befolyásolják annak működését vagy rendelkezésre állását. A hamisítási támadások elsősorban a sértetlenséget érintik, de a rendelkezésre állásra is hatással lehetnek. Ha a támadók hamis információt generálnak egy adatbázisban, akkor az kihat a sértetlenségre. Létrehozhatnak hamis e-maileket is (ezt a módszert

általában e-mail-spoofingnak nevezzük), amelyek segítségével a hamisító például rosszindulatú programokat terjeszthet, úgymint férgek, vírusok, kémprogramok. A rendelkezésre állás elleni támadás esetében, ha elegendő káros folyamatot generál a támadó, mint például: hálózati forgalmat, e-mailt, webes forgalmat vagy szinte bármi mást, ami erőforrásokat fogyaszt, akkor potenciálisan elérhetetlenné teheti a forgalmat kezelő szolgáltatásokat a rendszer legitim felhasználói számára.

A sebezhetőségek

A fenti támadások sikere, illetve a továbbiakban tárgyaltaké egyaránt, nagyon sok esetben az eszközök és rendszerek sérülékenységétől és/vagy sebezhetőségétől függ. A sebezhetőségek a rendszerek biztonsági hiányosságai, amelyeket a támadók kihasználnak. A legfontosabb sebezhetőségek könnyen elérhetők az interneten a biztonsági szakemberek és a bűnöző hackerek számára egyaránt. Egy bűnözőnek jellemzően nem kell rendelkeznie semmilyen programozási vagy kódolási ismerettel a támadás végrehajtásához, mindössze egy rosszindulatú programkészletre és egy online oktatóanyagra van szüksége ahhoz, hogy ki tudja használni a sérülékenységeket, amelyekhez az interneten szintén hozzáfér. A célzott támadások munkaigényesebbek, de ott is megvan a támadónak az a lehetősége, hogy olyan eszközökre támaszkodjon, amelyeket a sebezhetőségek kihasználására terveztek. A sérülékenységek jellemző típusai, amelyek a digitális államban szintén megjelenhetnek:

- A hálózati sebezhetőségek: a nem biztonságos operációs rendszerekből és hálózati architektúrából adódnak. Idetartoznak a kiszolgálók és a hosztok (végberendezések) hibái, a rosszul konfigurált vezeték nélküli hálózati hozzáférési pontok és tűzfalak, valamint a nem biztonságos hálózati protokollok.
- A hardveres sebezhetőségek: a számítógépes hardverek kihasználható gyenge pontjai, amelyek szinte minden rendszert és rendszerelemet érintenek, beleértve az asztali számítógépeket, laptopokat, szervereket és okostelefonokat.
- A szoftverek és alkalmazások sebezhetőségei: idetartoznak a kódolási hibák vagy a bizonyos kérésekre nem kívánt módon reagáló szoftverek. A szoftveres sebezhetőségeket gyakran a szoftverben lévő hiba, hiányosság vagy gyengeség okozza.
- A nulladik napi sebezhetőségek (zero-day): olyan biztonsági hibák, amelyeket bűnözők fedeztek fel, de a szoftvergyártók nem ismerik, és ezért

nem javították ki őket. A kifejezés arra utal, hogy a gyártónak hány napja van a sebezhetőség javítására. (A nulladik napi exploitok olyan kódok, amelyek a nulladik napi sebezhetőségeket veszélyeztetik.)

Az OWASP által 2020-ban elkészített top 10-es lista alapvetően csak a webes alkalmazásokra jellemző sérülékenységeket mutatja be, azonban nagyon hasznos lehet az alkalmazások sebezhetőségének megértéséhez is. Az OWASP által megállapított legjellemzőbb sérülékenységek:

1. nem megfelelő naplózás és felügyelet (Insufficient Logging and Monitoring);
2. kódbefecskendezési hibák (Injection Flaws);
3. érzékeny adatok kitettsége (Sensitive Data Exposure);
4. ismert sebezhetőséggel rendelkező komponensek alkalmazása (Using Components with Known Vulnerabilities);
5. Cross-Site Scripting (XSS) hibák (Cross-Site Scripting [XSS] Flaws);
6. hibás autentikáció (Broken Authentication);
7. hibás hozzáférés-ellenőrzés (Broken Access Control);
8. XML[154] külső entitások (XML External Entities [XXE]);
9. hibás biztonsági konfiguráció (Security Misconfiguration);
10. nem biztonságos deszerializáció (Insecure Deserialization).

Nem megfelelő naplózás és felügyelet

Ez a sebezhetőség abból ered, hogy az alkalmazás nem naplózza a fontos eseményeket, amikor azok bekövetkeznek. Az alkalmazáson belüli naplózás nem megfelelő kialakítása vagy az alkalmazás naplóinak nem megfelelő nyomon követése és az azokra való reagálás hiánya lehetővé teheti a támadás folytatását, miközben a megfelelő ellenőrzésekkel a támadást el lehetett volna fogni és meg lehetett volna szüntetni. Emellett a nem megfelelő naplózás és felügyelet megnehezíti a támadás eseményeinek rekonstruálását, amelyek segíthetik a sebezhetőségek beazonosíthatóságát, hogy azokat a jövőben javítani lehessen. A legtöbb alkalmazás valamilyen szintű naplózást végez, de fontos megérteni, hogy mit kell naplózni, hol kell tárolni ezeket a naplókat, hogyan kell nyomon

[154] Az XML az angol Extensible Markup Language, vagyis „kiterjeszthető jelölőnyelv" rövidítése. Az XML lehetővé teszi az egyéni információs formátumok létrehozását, illetve elektronikus megosztását.

követni őket, és hogyan kell a biztonsági szakembereknek reagálniuk a feltételezett támadásokra.

A 26. táblázat szemlélteti, hogyan lehet azonosítani és megelőzni a sérülékenység kihasználását.

26. táblázat: A naplózási és riasztási feladatok

Azonosítás	Megelőzés és védelem
Annak megállapítása, hogy jelenleg milyen naplózással rendelkezik az alkalmazás.	Annak meghatározása, hogy milyen eseményeket és adatokat kell naplózni (idetartoznak például a bejelentkezési kísérletek, a bejelentkezési hibák, a korlátozott hozzáférésű oldalakhoz való hozzáférési kísérletek, a bemeneti érvényesítési hibák, az alkalmazás adatainak módosítása stb.).
Meg kell határozni, hogy hol történik a naplózás az alkalmazáson belül, és mire használják.	A naplóadatok tárolási helyének meghatározása. (Amennyiben lehetséges, a biztonsági naplókat az alkalmazást futtató eszköztől elkülönített központi helyre kell küldeni, és ott kell tárolni. Ha az alkalmazás felhőkörnyezetben került telepítésre, akkor célszerű a felhőszolgáltató naplózási szolgáltatásait használni.)
Annak meghatározása, hogy az adatokat hol naplózzák. (Ugyanazon a gépen tárolják-e a naplófájlokat, ahol az alkalmazás fut? Van-e egy központi naplózási rendszer? A biztonsági naplókat a hibakeresési vagy elemzési naplókkal együtt tárolják-e? A naplóadatokat felhőszolgáltatásban tárolják-e?)	A naplók nyomonkövetési módjának meghatározása. (Számos olyan szolgáltatás létezik, amely segíti a begyűjtött naplófájlok elemzését. Amennyiben felhőszolgáltatást használnak, akkor azok többsége rendelkezik naplóelemző és riasztási funkciókkal.)
Annak meghatározása, hogy a naplózott adatokat hogyan követik nyomon és hogyan reagálnak rájuk. (Az adatokat betáplálják-e egy behatolásjelző rendszerbe? Vannak-e szabályok a gyanús tevékenységre vonatkozó riasztások kiváltására? Vannak-e tervek az ilyen riasztásokra való reagálásra?)	Riasztások beállítása a gyanús tevékenységekre, és megfelelő válaszok adása. (A konkrét eseményekre vonatkozó megfelelő riasztások beállítása lehetővé teszi a biztonsági szakemberek számára, hogy figyelemmel kísérjék a tevékenységeket, és azonnali intézkedéseket tegyenek az adatok védelme érdekében. Meg kell határozni, hogy mely eseménytípusok és milyen küszöbérték esetén kell ezeket a riasztásokat elindítani. Rendelkezni kell egy incidensreagálási tervvel is a biztonsági rések kezelésére.)

Forrás: Andy Kofod: *OWASP Top 10 for Developers: Insufficient Logging and Monitoring,* 2021

Kódbefecskendezési hibák

A kódbefecskendezés akkor történik, amikor egy támadó érvénytelen adatokat küld a webes alkalmazásnak azzal a szándékkal, hogy olyasmire késztesse azt, amire az alkalmazást nem tervezték és programozták, azaz nem megbízható adatokat küld egy parancs vagy lekérdezés részeként, amellyel a célzott rendszert nem kívánt parancsok végrehajtására késztetheti. A támadók ezt arra használják, hogy az alkalmazásprogramozási felületen keresztül általuk megadott, nem szándékos parancsok végrehajtására késztessék a rendszert. Az ilyen típusú támadással a hackerek hozzáférhetnek a védett adatokhoz, vagy akár operációsrendszer-parancsokat is végrehajthatnak. Ez utóbbi sokkal veszélyesebbé teszi ezt a támadástípust.

A befecskendezés elkerülésének egyik alapvető módja a forráskód felülvizsgálata és a biztonságos API-ok használata. Szintén alkalmazhatók API-biztonsági megoldások, amelyek képesek minden esetben azonosítani az API-okat potenciálisan rosszindulatú adatokkal feltérképező támadókat.

Érzékeny adatok kitettsége

Érzékeny adatoknak való kitettségről akkor beszélünk, ha fontos tárolt vagy továbbított adatok kerülnek veszélybe. Ennek egyik alapvető kiváltó oka lehet, hogy nem védik megfelelően az olyan adatbázist, ahol az információkat tárolják. Ez következhet például abból, hogy nem alkalmaznak egyáltalán semmilyen titkosítást, vagy ha igen, akkor csak gyengét; szoftverhibákból, vagy amikor valaki tévedésből egy helytelen adatbázisba tölti fel az adatokat. Ezek különösen komoly problémát vethetnek fel a digitális állam vonatkozásában, amikor államtitkot vagy más, a nemzet működését érintő érzékeny adatokat tehetnek közzé felhasználói, biztonsági vagy szoftveres hibákból kifolyólag.

Az érzékeny adatok kiszivárgása megelőzésének lehetséges módjai közül az egyik legfontosabb az érzékeny adatok titkosítása minden körülmények között. Ez magában foglalja az adatok titkosítását azok megosztása, továbbítása és tárolása során egyaránt. Az extra érzékeny adatok esetében korlátozni kell a hozzáférhetőséget, amely alapján csak egy vagy két jogosult felhasználó fér hozzá az adatokhoz, lehetőség szerint külön privát kulcsokkal (titkosítás esetén). Minden egyes hozzáférés esetében erős jelszavak alkalmazása szükséges, amelyeket tanácsos rendszeresen módosítani, és minden egyes platformra egyedi jelszót fenntartani. Amennyiben megtörtént a probléma, és a kezelt információkhoz hozzáfértek, azo-

kat ellopták, abban az esetben a legtöbbször a legnagyobb veszteségeket az adatok megfelelő biztonsági mentésének hiánya okozza. Egy biztonságos és megfelelően őrzött biztonsági mentés fenntartása megkönnyítheti a veszteségek csökkentését. A webes alkalmazások esetében a probléma gyors megoldása a TLS[155] minden oldalon történő kikényszerítése. Kényszerített TLS-házirend nélkül vagy gyenge titkosítás esetén egy támadó megfigyelheti a hálózati forgalmat, a kapcsolatot HTTPS-ről[156] HTTP-re[157] minősítheti vissza, és az összes, tiszta szövegben átadott információt – felhasználói adatokat, jelszavakat, munkamenetsütiket stb. – rögzítheti. Az érzékeny adatokat érintő kockázati szintek esetében is elmondható, hogy azok az idővel folyamatosan változnak. Ajánlott rendszeresen figyelemmel kísérni ezeket a változásokat, és kockázatértékelést végezni az érzékeny adatokat fenyegető potenciális veszélyek tekintetében.

A fentiek, valamint az OWASP ajánlása alapján elmondható, hogy az alábbi eljárások és megoldások járulhatnak hozzá az érzékeny adatok illetéktelen személyek kezébe kerülésének megelőzéséhez, megakadályozásához:

- az érzékeny adatok azonosítása az adatvédelmi törvények, a szabályozási követelmények vagy az üzleti igények alapján;
- a feldolgozott, tárolt vagy továbbított adatok osztályozása;
- az osztályozásnak megfelelő biztonsági megoldások és ellenőrzések alkalmazása;
- érzékeny adatok szükségtelen tárolásának kerülése (meg nem őrzött adatokat nem lehet ellopni);
- az összes adat biztonságos protokollokkal, például TLS-sel történő titkosítása, a kiszolgáló által végzett titkosítási prioritás meghatározásával és biztonságos paraméterekkel, továbbá minden érzékeny adat titkosítása nyugalmi állapotban;
- naprakész és erős szabványos algoritmusok, protokollok és kulcsok alkalmazása, megfelelő kulcskezelés.[158]

[155] Transport Layer Security (TLS) – szállítási réteg biztonsága: egy titkosítási protokoll, amely az adatok hálózaton keresztüli átvitele során az adatok biztonságát védi.

[156] Hyper Text Transfer Protocol Secure (HTTPS) – biztonságos hiperszöveg-átviteli protokoll: titkosítást használ (például: TLS-t) a böngésző, illetve az alkalmazás és a webhelyek közötti biztonságos kapcsolat létrehozásához.

[157] Hyper Text Transfer Protocol (HTTP) – hiperszöveg-átviteli protokoll: egy kérdés-válasz alapú információátviteli protokoll kliens és szerver között, amely meghatározza, hogy milyen szabályok szerint kommunikáljon a weblapot kiszolgáló gép a böngészőprogrammal.

[158] Isha Kudkar: *OWASP: Sensitive Data Exposure Attacks,* 2021.

Ismert sebezhetőségű komponensek alkalmazása

Az infokommunikációs rendszerekben alkalmazott egyes komponensek könyvtárakból, keretrendszerekből és más szoftvermodulokból állnak. Gyakran a komponensek ugyanolyan jogosultságokkal futnak, mint maga az alkalmazás, amelyhez tartoznak. Ha egy komponens sebezhető, azt egy támadó nagyon könnyen kihasználhatja, ami komoly adatvesztést vagy esetlegesen a szerver/szerverek feletti irányítás átvételét okozhatja. Alapvető problémák lehetnek az alábbiak a komponensek sebezhetőségével kapcsolatban:

- az adminisztrátorok/fejlesztők nem tudnak lépést tartani a frissítések ütemével; elvégre a megfelelő frissítés időigényes;
- az adminisztrátorok félnek, hogy valami elromlik az általuk üzemeltetett weboldalon, alkalmazásban, szerveren;
- az adminisztrátorok félnek, hogy a régebbi kód nem fog működni a függőségek újabb verzióin;
- az adminisztrátoroknak nincs meg a frissítés megfelelő alkalmazásához szükséges szakértelmük.

A biztonsági gyengeség itt egyszerűen abból adódik, hogy a legtöbb fejlesztőcsapat nem biztosítja, hogy a komponensek/könyvtárak naprakészek legyenek. A megelőző mechanizmusok közé tartozik például, hogy az adminisztrátorok ismerik az általuk használt összes alkalmazást. Azokról naprakész dokumentációkkal rendelkeznek az összes komponens (operációs rendszer, webszerver, könyvtárak, hálózati komponensek stb.) és az alkalmazás által használt aktuális verziók vonatkozásában. Mindezekhez folyamatos felügyelet és biztonsági tesztelés társul, amelyek magukban foglalják a rendszeres sebezhetőségi felméréseket és behatolási tesztek elvégzését mind belső, mind külső szinten az alkalmazás biztonságának mélyreható megerősítése érdekében. Az adminisztrátoroknak az adatok és a rendszer védelme érdekében megfelelő patchkezelési rendszert kell működtetniük, és meg kell győződniük arról, hogy a frissítések és a biztonsági javítások csak megbízható szállítóktól származnak, valamint el kell távolítaniuk a nem szükséges vagy nem használt komponenseket az alkalmazás megbízhatóságának fokozása érdekében. A megfelelő védelem érdekében biztosítani kell, hogy ne csak az összetevők, hanem az alkomponensek is naprakészek legyenek, ezzel ne legyenek sebezhetők. A magasabb biztonsági szint eléréséhez célszerű webalkalmazás-tűzfalakat telepíteni a mélységi védelem biztosításához.

Mindezeket figyelembe véve az alábbi eljárásokat kell betartani az alkalmazott komponensek biztonságának fenntartása érdekében:

- minden felesleges függőség eltávolítása;
- kimutatás készítése az összes kliens- és szerveroldali komponensről;
- a komponensek sebezhetőségeiről készített releváns kimutatások folyamatos figyelése, reakció a felmerült új sérülékenységekre;
- csak hivatalos forrásból történő komponensbeszerzés;
- a nem aktívan karbantartott összetevők eltávolítása;
- virtuális javítások alkalmazása webhely-alkalmazás-tűzfalak segítségével.[159]

Cross-Site Scripting hibák

A Cross-Site Scripting (XSS) támadások a befecskendezéses támadásoknak egy olyan típusa, amely során rosszindulatú kódot juttat be a támadó az egyébként biztonságos webhelyekre. Ez történhet például a kliensoldali szkriptek webes alkalmazásokba történő bejuttatásával, ahol a támadó egy célzott webes alkalmazás hibáját használja ki arra, hogy rosszindulatú kódot küldjön a végfelhasználónak. Ezt általában a felhasználói bemenet hitelesítésének és helyes kódolásának hiánya teszi lehetővé. A rosszindulatú szkriptek a végfelhasználók böngészőjében kerülnek futtatásra, és számos támadást tesznek lehetővé a végfelhasználó munkamenetének ellopásától kezdve a végfelhasználó által az érintett weboldalon végzett összes művelet megfigyeléséig és megváltoztatásáig. Az XSS hibákról tehát elmondható, hogy webalkalmazásokra jellemző sérülékenységek, amelyeknek exploitjával a támadó kliensoldalon futtatható kódot juttat be az alkalmazásba, amelyet más felhasználó böngészője lefuttat. A futtatható kód az érintett felhasználó nevében fut, így az érintett felhasználó jogosultságával lehet a webalkalmazás funkcionalitását elérni általa. Egyéb célokra is felhasználható, mint például hamisított webhelyre történő átirányítás vagy adatgyűjtés. Legfejlettebb változatával az adott böngészőt regisztrálják be a háttérben egy menedzsmenteszközbe, amelyet ezt követően felhasználnak a böngésző viselkedésének befolyásolására. A böngésző beállításától függően az áldozat gépén különböző műveleteket tudnak végrehajtani (kommunikáció megfigyelése, üze-

[159] Siemba: *OWASP Top 10: Using Components with Known Vulnerabilities,* 2021.

netek küldése, e-mail-küldés, webkamera-vezérlés stb.). Alapvetően háromfajta XSS-típust különböztetünk meg, amelyek a következők:

- DOM-alapú (kliensoldali) XSS: A DOM (Dokumentum Objektum Modell[160]) a HTML-,[161] XML-, XHTML-[162] dokumentumok szerkezetének modellezésére használt, faszerkezetű objektum. Az egyes dokumentumok elemeinek változása a DOM szerkezetét is érinti. Kliensoldali szkriptekkel a DOM elemei elérhetők, a kapcsolódó események elfoghatók, vezérelhetők. A DOM-alapú XSS a DOM elemeihez, eseményeihez kapcsolódó támadások kivitelezésére használható, például egy weboldal tönkretételére, a tartalom összezavarására. A kliensoldali XSS némileg hasonlít a tükrözött XSS-hez, mivel gyakran egy kártékony szkriptet tartalmazó rosszindulatú URL-[163]címen keresztül kerül átadásra. Ahelyett azonban, hogy a hasznos terhet egy megbízható webhely HTTP-válaszába foglalná, a támadást teljes egészében a böngészőben hajtják végre a dokumentum objektum modell módosításával. Ez azt célozza, hogy a már az oldalon lévő legitim JavaScript nem képes megfelelően szanálni a felhasználói bemenetet.
- Visszatükrözéses (nem tartós) XSS: Akkor használható, amikor a szerveroldali program a kliens által szolgáltatott adatokat azonnal végrehajtja, és egy HTML választ ad vissza. Az ilyen típusú XSS kihasználásához a támadónak rá kell vennie a felhasználót, hogy adatokat küldjön a céloldalra, ami gyakran úgy történik, hogy a támadó a felhasználót egy rosszindulatúan szerkesztett linkre kattintásra buzdítja vagy kényszeríti. A visszatükrözéses XSS-támadások sok esetben adathalász e-mailekre vagy a célzott felhasználónak küldött rövidített vagy más módon eltitkolt URL-címekre támaszkodnak. Amikor az áldozat meglátogatja a linket, a szkript automatikusan elkezd lefutni a felhasználó böngészőjében.

[160] Angolul: Document Object Model.

[161] HyperText Markup Language (HTML) – hiperszöveges jelölőnyelv: A weboldalakat leíró jelnyelv, amit a weboldalak elkészítéséhez használnak. Egy HTML-kód egyértelműen meghatározza a weboldal felépítését, kinézetét.

[162] Extensible Hypertext Markup Language (XHTML) – bővíthető hiperszöveges jelölőnyelv: az XML jelölőnyelvek egy családja, amely a weboldalakhoz széleskörűen használt HTML-t tükrözi vagy kibővíti.

[163] Uniform Resource Locator (URL) – egységes erőforrás-helymeghatározó: az interneten megtalálható egyes erőforrások (például weboldalak, szövegek, képek, videók) szabványosított címe, más néven webcím.

– Tárolt (tartós) XSS: Akkor fordul elő, amikor a célkiszolgálón nem megbízható vagy nem ellenőrzött felhasználói bemenet kerül tárolásra. A tartós XSS gyakori célpontjai közé tartoznak az üzenetfórumok, a kommentmezők vagy a látogatói naplók – minden olyan funkció, ahol más hitelesített vagy nem hitelesített felhasználók láthatják a támadó rosszindulatú tartalmát. A támadó rosszindulatú szkripteket írhat be a profiljába vagy bármilyen kommentfelületre, és amikor más felhasználók meglátogatják a profilt vagy rámennek a kommentben elhelyezett URL-címre, a böngészőjük automatikusan lefuttatja a rosszindulatú kódot.[164]

Az XSS-sebezhetőségek megelőzhetők a biztonságos kódolási gyakorlatok következetes alkalmazásával, és olyan keretrendszerek használatával, amelyek eleve automatikusan elkerülik az XSS-t. A megelőzésnek a fejlesztési folyamat részét kell képeznie, és célszerű a gyártás minden egyes szakaszában folyamatos ellenőrzéseket végrehajtani, amelyekkel felismerhetők a potenciális sebezhetőségek és megelőzhetők a támadások.

Hibás autentikáció

Hibás autentikációról akkor beszélünk, ha a hitelesítést nem megfelelően hajtották végre, lehetővé téve ezzel a támadók számára, hogy engedély nélkül hozzáférjenek fiókokhoz, vagy egy másik felhasználó személyazonosságát vegyék fel. Egy hibás hitelesítési sebezhetőség lehetővé teheti a támadó számára, hogy kézi és/vagy automatikus módszerekkel megpróbálja megszerezni az irányítást a rendszer bármelyik fiókja felett – vagy ami még rosszabb, akár teljes irányítást szerezhet a teljes rendszer felett. A feltört hitelesítési sebezhetőséggel rendelkező weboldalak nagyon gyakoriak a világhálón. Ezek általában olyan logikai problémákra utalnak, amelyek az alkalmazás hitelesítési mechanizmusában fordulnak elő, mint például a rossz munkamenet-kezelés, amely hajlamos a felhasználónév-katalogizálásra, amikor egy rosszindulatú szereplő brute-force[165] technikával próbálja kitalálni az érvényes felhasználói adatokat a rendszerben. Az OWASP

[164] HUNCERT: *Cross Site Scripting (XSS),* 2021.

[165] Nyers erős támadás, egy olyan technika, amely próba- és hibaalapú felhasználói adatok begyűjtésére vagy adatok visszafejtésére szolgál.

Top 10 szerint ezek a sebezhetőségek számos formában jelentkezhetnek. Egy webes alkalmazás akkor tartalmaz sérült hitelesítési sebezhetőséget, ha:

- lehetővé teszi az olyan automatizált támadásokat, mint például a hitelesítő adatok folyamatos kitöltése, amikor a támadó rendelkezik az érvényes felhasználónevek és jelszavak listájával;
- lehetővé teszi a brute-force vagy más automatizált támadásokat;
- engedélyezi az alapértelmezett, gyenge vagy jól ismert jelszavakat, például „Password1" vagy „admin/admin";
- gyenge vagy nem hatékony hitelesítő adatokat helyreállító és elfelejtett jelszómechanizmusokat használ;
- hiányzik vagy nem hatékony a többfaktoros hitelesítés;
- munkamenet-azonosítókat tesz közzé az URL-ben (pl. URL átírása);
- nem változtatja meg a munkamenet-azonosítókat a sikeres bejelentkezés után;
- nem érvényteleníti megfelelően a munkamenet-azonosítókat. A felhasználói munkamenetek vagy hitelesítési tokenek (különösen az egyszeri bejelentkezési [single sign-on – SSO] tokenek) nem lesznek megfelelően érvénytelenítve kijelentkezés vagy inaktivitás esetén.

Ahol lehetséges, többfaktoros hitelesítést kell alkalmazni az olyan automatizált támadások megelőzése érdekében, amelyek pédául a brute-force támadással történő feltörés eredményei alapján megszerzett hitelesítő adatok újrafelhasználását célozzák meg. Feltétlenül el kell kerülni az alapértelmezett hitelesítő adatok alkalmazását, különösen az adminisztrátorok esetében. Ennek megfelelően a jelszavak hosszára, összetettségére és változtatásának ütemére a biztonsági követelményeknek megfelelő jelszóházirendet kell kialakítani. Biztosítani kell, hogy a regisztráció, a hitelesítő adatok helyreállítása és az API-útvonalak védettek legyenek az olyan támadásokkal szemben, amelyek katalogizálhatják az egyes fiókadatokat. Korlátozni kell a sikertelen bejelentkezési kísérletek számát, minden sikertelen bejelentkezést naplózni kell, és automatikus értesítést és riasztást kell küldeni a rendszergazdáknak, ha hitelesítő adatok kitöltésére, brute-force támadásra vagy egyéb káros tevékenységre utaló jelet észlel a rendszer.[166]

[166] Sucuri Guides: *OWASP Top 10 Security Risks & Vulnerabilities,* 2021.

Hibás hozzáférés-ellenőrzés

Egy megfelelően kialakított rendszerben minden egyes információ csak a felhasználók egy meghatározott csoportja számára érhető el a számukra biztosított hozzáférés alapján. Ez különösen fontos a digitális állam vonatkozásában, ahol számos érzékeny adat kerül feldolgozásra és tárolásra. A hozzáférés-szabályozás hibás működése olyan forgatókönyvekhez vezethet, amelyekben a felhasználók olyan információkhoz férhetnek hozzá, amelyekhez nincs jogosultságuk. A hozzáférés-szabályozás azt jelenti, hogy a felhasználók igényeiktől függően korlátozzák, hogy milyen fájlokhoz, mappákhoz, meghajtókhoz vagy weboldalakhoz férhetnek hozzá.

Néhány példa a hozzáférések típusaira:

- hozzáférés a tárhely vezérlő/adminisztrátori paneljéhez;
- hozzáférés egy szerverhez FTP[167]/SFTP[168]/SSH[169] segítségével;
- hozzáférés egy weboldal adminisztrációs paneljéhez;
- hozzáférés a szerveren lévő egyéb alkalmazásokhoz;
- hozzáférés egy adatbázishoz.

A jogosulatlan hozzáférések elkerülése érdekében kiemelten fontos, hogy csak a legszükségesebb jogosultságokat és csak a feladatuknak megfelelő szerepet kell megadni az egyes felhasználóknak, és csak annyi ideig, amennyi a feladat elvégzéséhez szükséges. Minden olyan fiókot el kell távolítani a rendszerből, amelyre nincs szükség, vagy amelyek felhasználójának már nincs szüksége rájuk, esetleg már nincs a szervezetnél. Folyamatosan ellenőrizni kell az üzemeltetett szervereket és webhelyeket, hogy ki, mit, mikor és miért csinált azokon. A kiszolgálókról célszerű a felesleges szolgáltatásokat eltávolítani. Ebben az esetben is javasolt többfaktoros hitelesítés alkalmazása az összes hozzáférési ponton, amelyeket érdemes kikapcsolni a hozzáférési felületek számának csökkentése érdekében, amíg nincs rájuk szükség.

[167] File Transfer Protocol (FTP) – fájlátviteli protokoll: a protokoll feladata a számítógépek közti fájlcsere biztosítása.

[168] SSH File Transfer Protocol (SFTP) – SSH fájlátviteli protokoll: használatával az adatok titkosítás segítségével biztonságosan továbbítódnak, és nem kerül sor tiszta szöveges fájladatok átvitelére.

[169] Secure Shell (SSH): egy olyan protokoll, amelyet egy helyi és egy távoli számítógép közötti biztonságos, titkosított csatorna kiépítésére használnak.

XML külső entitások

A kiterjeszthető jelölőnyelv (XML) egy népszerű adatformátum, amelyet webes szolgáltatásokban, dokumentumokban és képfájlokban használnak. Az XML-küldő entitásbefecskendezés, más néven XXE-támadás, a webes alkalmazások, API-ok és mikroszolgáltatások egyik leggyakoribb biztonsági sebezhetősége. Lehetővé teszi a hackerek számára, hogy egy alkalmazás XML-adatok feldolgozását kezeljék. Az XXE-befecskendezés végrehajtásával a támadók megtekinthetik az alkalmazáskiszolgálón lévő fájlokat, azokhoz hozzáférhetnek, azokat esetlegesen módosíthatják, vagy kapcsolatba léphetnek bármely olyan külső háttérrendszerrel, amelyhez maga az alkalmazás hozzáférhet. Bizonyos esetekben a támadók akár szolgáltatásmegtagadást (DoS) is okozhatnak, és XXE-támadással kompromittálhatják az alkalmazott kiszolgálókat vagy más infrastruktúrákat. Az OWASP Top 10 szerint az XXE fő támadási vektorai közé tartozik a következők kihasználása:

- sebezhető XML-processzorok, ha a rosszindulatú szereplők képesek XML-t feltölteni vagy ellenséges tartalmat beilleszteni egy XML-dokumentumba;
- sebezhető kódok;
- sebezhető függőségek;
- sebezhető integrációk.

Az XXE-támadások megelőzésének néhány módja a következő:

- amikor csak lehetséges, kevésbé összetett adatformátumok alkalmazása, az érzékeny adatok sorozatba rendezésének elkerülése;
- az alkalmazás által vagy az alapul szolgáló operációs rendszerben használt összes XML-processzor és -könyvtár folyamatos javítása vagy frissítése;
- függőség-ellenőrzők alkalmazása;
- szűrés alkalmazása az XML-dokumentumokon, fejléceken vagy csomópontokon belüli támadóadatok megállítása érdekében;
- alkalmazásbiztonsági tesztelőeszközök alkalmazása az XXE felismerésére a forráskódban.[170]

[170] Kudkar (2021): i. m.

Hibás biztonsági konfiguráció

Hibás biztonsági konfigurációról akkor beszélünk, ha a tervezés vagy a konfiguráció gyengeségei konfigurációs hibából vagy hiányosságból adódnak. Néhány példa a hibás biztonsági konfigurációkra: a nem biztonságos alapértelmezett konfigurációk, a hiányos vagy ad hoc konfigurációk, a nyílt felhőtárolók, a rosszul konfigurált HTTP-fejlécek, a szükségtelen HTTP-módszerek, a túlságosan megengedő erőforrás-megosztás. A webszerverek, az adatbázisok, a tárolók, az alkalmazások, a könyvtárak, az operációs rendszerek, a kódolási keretrendszerek, a platformok, a virtuális gépek, a tanúsítványok, a titkosítási beállítások és a felhők hibás konfigurációja a sebezhetőség jellegétől függően a CIA-triász különböző aspektusait érintheti. Ez jogosulatlan hozzáféréshez, fiókátvételhez, érzékeny adatok kiszolgáltatottságához, adatlopáshoz, a rendszer veszélyeztetéséhez, valamint jogi és pénzügyi következményekhez vezethet, amelyek mindegyike komoly hatással lehet a digitális állam működésére.

A biztonsági félrekonfigurálások megelőzése érdekében célszerű megfelelő alapkonfigurációs házirend kialakítása az egész szervezetre vonatkozóan (ami magában foglalja például a javításkezelést), és ennek alapján folyamatos képzés szervezése a teljes személyi állomány részére. Feltétlenül módosítani kell az alapértelmezett beállításokat, és célszerű statikus és automatizált biztonsági szkennereket alkalmazni a hibás konfigurációk kiszűrésére, a keretrendszerek, komponensek, könyvtárak, nem használt oldalak, kódok, egyedi kódok hibás konfigurációinak felderítésére. A konfigurációs hibákat folyamatosan ellenőrizni kell a fejlesztési, a termelési és a tesztkörnyezetben. Szintén kiemelten fontos az alkalmazott szoftverek naprakészen tartása és frissítése.[171]

Nem biztonságos deszerializáció

Azt a tevékenységet, amikor egy adatot, adatszerkezetet olyan formára alakítunk, amely külső adattárolóra lementhető vagy vezetékes hálózaton könnyen továbbítható és amelyből az eredeti állapot később helyreállítható, szerializálásnak (serialization – sorosítás) nevezzük. A szerializálás meghatározható úgy, hogy egy objektumot bájtfolyamokká alakítunk át, az objektum állapotát pedig megtartjuk egy fájl memóriájában, adatbázisában. A szerializálás fordítottja a deszerializáció,

[171] Reshmi Radhakrishnan: *OWASP Top 10: Security Misconfiguration,* 2021.

amely rekonstruálja az objektumot a bájtfolyamból. Más szavakkal, a deszerializáció egy sorosított objektum eredeti állapotba konvertálásának folyamata. A nem biztonságos deszerializáció egy jól ismert, de nem gyakran előforduló sebezhetőség, amelynek során a támadó rosszindulatú objektumokat juttat be egy webes alkalmazásba. Ez lehetővé teszi számukra, hogy szolgáltatásmegtagadási (DoS) támadásokat, távoli kódfuttatási támadásokat, kódbefecskendezéseket és hitelesítési megkerüléseket hajtsanak végre. Az ilyen típusú támadások komoly fenyegetést jelentenek, és súlyos következményekkel járhatnak a digitális állam egészére vagy az állami szervezetek és vállalkozások, valamint azok ügyfelei számára.

A nem biztonságos deszerializációs sebezhetőség legjellemzőbb példája, amikor a támadó egy nem megbízható kódot tölt be egy szerializált objektumba, amelyet aztán továbbít a célobjektum felé. Ha nincsenek megfelelő ellenőrzések, az alkalmazás visszaalakítja a rosszindulatú bemenetet, lehetővé téve, hogy még több részéhez férjen hozzá a káros kód a megtámadott alkalmazásban, eszközben, rendszerben. Így további támadásokat tesz lehetővé, amelyek végül komoly adatvédelmi sebezhetőséget okozhatnak az alkalmazás vagy eszköz felhasználói számára. A nem biztonságos deszerializációt ezért néha „objektumbefecskendezéses" sebezhetőségnek is nevezik.

A legjobb módja annak, hogy az alkalmazások védve legyenek az ilyen típusú kockázatoktól, az, ha a nem megbízható forrásból származó szerializált objektumok nem kerülnek elfogadásra az eszközök vagy a rendszer által. Abban az esetben, ha mégis szerializált objektumokat kell elfogadni, az alábbi lehetőségekkel lehet megállítani a nem biztonságos deszerializációt:

- digitális aláírások és egyéb integritás-ellenőrzések bevezetése a rosszindulatú objektumok létrehozásának vagy más adatok zavarásának megakadályozására;
- a deszerializációs kódok korlátozott jogosultságú környezetben történő futtatása;
- naplózási tevékenységek folytatása a deszerializációs kivételekről és hibákról;
- szigorú korlátozások bevezetése és végrehajtása a deszerializálási folyamatokra az objektum létrehozása előtt;
- a deszerializációs konténerek és kiszolgálók összes bejövő és kimenő hálózati tevékenységének korlátozása és ellenőrzése;
- a deszerializációs tevékenységek nyomon követése.[172]

[172] Borislav Kiprin: *What is Insecure Deserialization and How to Prevent It,* 2021.

Veszélyek és lehetséges támadási vektorok

Az információbiztonsági fenyegetések alapvetően három fő kategóriába sorolhatók, nevezetesen a hálózati fenyegetések, a kliensfenyegetések és a felhasználókra irányuló fenyegetések. Ebben a fejezetben az egyes kategóriákban megjelenő legjellemzőbb veszélyeket és esetleges támadási vektorokat ismertetjük.

A hálózatokat fenyegető veszélyek

A hálózati infrastruktúra alapvető összetevői az útválasztók, kapcsolók, elosztók, tűzfalak és végberendezések. Az útválasztási és egyéb hálózati műveletek elvégzése mellett ezek az eszközök felelősek a futó alkalmazások, eszközök és szerverek támadásoktól és behatolásoktól való védelméért is. Az eszközök rossz konfigurációja a támadók számára egy lehetséges útvonalat biztosít a rendszerünkbe való bejutáshoz. A kihasználáshoz vezető gyakori sebezhetőségek a nyílt hozzáférés-szabályozás, a gyenge titkosítás és jelszavak, az alapértelmezett telepítési beállításokat használó eszközök, valamint a legújabb biztonsági javítások nélküli eszközök. A digitális államban üzemeltetett információs és kommunikációs rendszereket veszélyeztető legjellemzőbb hálózati fenyegetések az alábbiak:

- forgalomfigyelés, szimatolás (sniffing);
- adatforgalom-lehallgatás (eavesdropping);
- munkamenet-eltérítés (session hijacking);
- IP-hamisítás (IP spoofing);
- ARP-mérgezés[173] (ARP Poisoning);
- DNS-mérgezés (DNS Poisoning).

A 27. táblázat szemlélteti az egyes fenyegetések legjellemzőbb tulajdonságait.

[173] ARP: Address Resolution Protocol – címfeloldási protokoll: a számítógépes hálózatokon használatos protokoll az IP-címek és fizikai címek egymáshoz rendeléséhez.

27. táblázat: A hálózati fenyegetések legfőbb tulajdonságai

Támadási vektorok	Jellemzők és tulajdonságok
Forgalomfigyelés, szimatolás	Adatok lehallgatása a hálózati forgalom rögzítésével.
Adatforgalom-lehallgatás	Behatolás, amikor a támadó megpróbálja ellopni a hálózaton keresztül továbbított érzékeny információkat.
Munkamenet-eltérítés	Érvényes munkamenet kihasználása.
IP-hamisítás	Internetes protokollok létrehozása hamis IP-címmel.
ARP-mérgezés	A támadó ARP-üzeneteket továbbít egy helyi hálózatra.
DNS-mérgezés	Hibás tartománynévrendszer-információk bejuttatása a feloldó gyorsítótárába.

Forrás: Sinha (2020): i. m.

Forgalomfigyelés, szimatolás

A szimatolás információszerzés a hálózati csomagok elfogásának segítségével. A lehallgatással szemben (ami általános hálózati forgalomra vonatkozik) a szimatolás kimondottan csomagkapcsolt hálózatokra értelmezhető. A szimatolás a hálózaton keresztül áramló összes adatcsomag megfigyelésére és lefoglalására szolgáló módszer. A szimatolást a támadó az érzékeny adatcsomagok, például számlainformációk, hitelkártyaadatok, jelszavak stb. elkapására használja. A digitális állam működése szempontjából számos olyan érzékeny információhoz juthatnak ezzel a módszerrel, amelyek befolyásolhatják az állam működését, illetve közvetve vagy közvetlenül veszélyeztethetik az állampolgárok életét. Egy rosszindulatú behatoló az összes hálózati forgalmat megfigyelheti, elkaphatja és elemezheti, amennyiben be tudja juttatni a szimatoló eszközét a hálózatba. A szimatolásnak két típusát különböztethetjük meg:

- Aktív szimatolás: A kapcsoló esetében a szimatolást aktív szimatolásnak nevezzük. A kapcsoló egy olyan unicast- (az információtovábbítás során egyetlen forrás és egyetlenegy célállomás kommunikál egymással) eszköz, amely a MAC-címek alapján működik az eszközök közötti adatáramlás szabályozásával és a csomagok legitim címzetthez történő továbbításával. A célpontok közötti csomag elfogásához a támadók a helyi hálózat forgalmába a szimatolóeszközöket (kapcsolókat) úgy illesztik be, hogy azok lehetővé tegyék a forgalom aktív megfigyelését/szimatolását.

– Passzív szimatolás: A hub esetében a szimatolást passzív szimatolásnak nevezzük. Minden csomag, amely nem kapcsolt hálózati szegmenseken keresztül halad, látható az adott hálózat összes gépe számára. Mivel a hub nem intelligens eszköz, ezért a helyi hálózatra átvitt adatokat az összes csatlakoztatott eszköznek elküldi. Ezt a folyamatot passzívnak nevezzük, mivel a támadók által elhelyezett szimatolók (hubok) passzívan várják az adatok átvitelét és rögzítik azokat.

Az adatforgalom-lehallgatás

A szimatoláshoz hasonlóan a lehallgatás is a hálózat adatforgalmának monitorozását jelenti abból a célból, hogy érzékeny adatok birtokába jusson a megfigyelő. A lehallgatás más célpontok kommunikációjának nem hitelesített letapogatásaként definiálható. Ez történhet e-maileken, üzeneteken vagy más internetes szolgáltatásokon keresztül. A lehallgatás során a kommunikáló felek nagy valószínűséggel nem veszik észre, hogy adataikat ellopták vagy megváltoztatták, mivel ez a folyamat ritkán befolyásolja a normál átviteli módszert. Az elektronikus lehallgatóeszköz tipikus példája egy otthon vagy irodában fizikailag elhelyezett rejtett poloska. Ezeket az eszközöket elrejthetik olyan nyilvánvaló helyeken, mint például egy szék alatt vagy az asztalon, illetve egy mikrofont elrejthetnek egy feltűnésmentes tárgyban, például egy tollban vagy táskában, de vannak kifinomultabb, nehezebben felderíthető megoldások, például mikrofonok elhelyezése mennyezeti lámpákban, könyvespolcon lévő könyvekben vagy a fali képkeretekben. A digitális lehallgatást egyre könnyebbé tevő technológiai fejlődés ellenére számos támadás még mindig a telefonok lehallgatására épül. Ennek oka, hogy a telefonok elektromos árammal, beépített mikrofonokkal, hangszórókkal és poloskák elrejtésére alkalmas helyekkel rendelkeznek, és könnyen és gyorsan telepíthetők. A lehallgatást végző támadók megfigyelhetik a beszélgetéseket abban a szobában, ahol a telefon van, és a telefonokra irányuló hívásokat bárhol máshol a világon. A modern számítógépes telefonrendszerek lehetővé teszik a telefonok elektronikus úton történő lehallgatását anélkül, hogy a készülékhez a közvetlen hozzáférés biztosított lenne. A támadók jeleket küldhetnek a telefonvonalon, és továbbíthatnak minden olyan beszélgetést, amely ugyanabban a szobában zajlik, még akkor is, ha a telefonkagyló nem aktív. Hasonlóképpen, a számítógépek is kifinomult kommunikációs eszközökkel rendelkeznek, amelyek lehetővé teszik a lehallgatást végző támadók számára, hogy lehallgassák

a kommunikációs tevékenységeket, a hangbeszélgetésektől kezdve az online csevegéseken át egészen a billentyűzetfigyelő megoldásokig, amelyekkel nyomon követhetik, hogy a felhasználók mit gépelnek. A számítógépek elektromágneses sugárzást is kibocsátanak, amelyet a kifinomult lehallgatók arra használhatnak, hogy rekonstruálják a számítógép képernyőjének tartalmát. Ezek a jelek akár néhány száz méteres távolságra is eljuthatnak, és továbbterjedhetnek az antennaként használható kábeleken és telefonvonalakon keresztül. A lehallgatás során alkalmazott legjellemzőbb módszerek:

- Felvevőeszközök: A támadók olyan eszközöket használhatnak, amelyek hangot vagy képet vesznek fel (például mikrofonokat és videókamerákat), és ezeket elektromos formátumra alakítják át, hogy lehallgassák a célpontokat. Ideális esetben olyan elektromos eszközről van szó, amely a célpont helyiségében található áramforrásokat használja, így a támadónak nem kell belépnie a helyiségbe, hogy feltöltse az eszközt vagy kicserélje az elemeit. A támadók használhatnak minierősítőket is, amelyek lehetővé teszik számukra a háttérzajok eltávolítását.
- Gyenge jelszavak: A gyenge jelszavak megkönnyítik a támadók számára, hogy jogosulatlanul hozzáférjenek a felhasználói fiókokhoz, és így bejuthassanak a vállalati rendszerekbe és hálózatokba. Ez magában foglalja azt is, hogy a hackerek veszélyeztethetik a bizalmas kommunikációs csatornákat, lehallgathatják a munkatársak közötti tevékenységeket és beszélgetéseket, és ellophatják az érzékeny vagy értékes üzleti adatokat.
- Nyílt hálózatok: Azok a felhasználók, akik olyan nyílt hálózatokhoz csatlakoznak, amelyek nem igényelnek jelszavakat és nem használnak titkosítást az adatok továbbításához, ideális helyzetet biztosítanak a támadók számára a lehallgatáshoz. A hackerek figyelemmel kísérhetik a felhasználói tevékenységeket, és megfigyelhetik a hálózaton zajló kommunikációt.[174]

A nagyon gyorsan fejlődő digitális világ egyre inkább megkönnyíti a támadók számára a vállalati információk és a felhasználói beszélgetések lehallgatását. Ugyanakkor lehetőséget is kínál a szervezetek számára, hogy megakadályozzák a támadók rosszindulatú szándékait. A lehallgatási támadások megelőzését elősegítő módszerek közül néhányat szemléltet a 28. táblázat:

[174] Fortinet: *Eavesdropping Definition: What Is An Eavesdropping Attack?* 2021.

28. táblázat: A lehallgatás elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Magas szintű titkosítás	A lehallgatási támadások megelőzésének egyik legjobb módja az adatátvitel és a magánbeszélgetések titkosítása. A titkosítás megakadályozza, hogy a támadók elolvashassák a két fél között kicserélt adatokat. A 256 bites titkosítás olyan védelmet jelent, ahol egy támadó számára a rejtjelezett üzenet visszafejtése szinte lehetetlen.
A tudatosság terjesztése	Annak biztosítása, hogy az alkalmazottak tisztában legyenek a kiberbiztonság kockázataival és veszélyeivel, kulcsfontosságú első lépés a szervezetek bármilyen kibertámadás elleni védelmében. Ez nagyon is igaz a lehallgatási támadásokra, ezért a szervezeteknek olyan képzéseket kell biztosítaniuk, amelyek tájékoztatják a felhasználókat arról, hogy a támadók hogyan, milyen módon indíthatják el ezeket a támadásokat. Az alkalmazottaknak meg kell érteniük a támadók által a beszélgetések lehallgatására használt módszereket, követniük kell a legjobb gyakorlatokat a kockázat csökkentése érdekében, és folyamatosan tudatában kell lenniük a támadás jeleinek. Kerülniük kell továbbá a nem biztonságos alkalmazások vagy szoftverek letöltését, és tisztában kell lenniük a gyenge vagy nyílt hálózatokhoz történő csatlakozás veszélyeivel.
Hálózati szegmentálás	A szervezetek a hálózatok elérhetőségének korlátozásával korlátozhatják a támadók lehallgatási lehetőségeit. A hálózat virtuális felosztása lehetővé teszi a szervezetek számára, hogy az erőforrásokat csak azokra az elemekre és felhasználókra korlátozzák, akiknek szükségük van a hozzáférésre. A hálózati szegmentálás felosztja a hálózatot, ami csökkenti a forgalmat, megakadályozza a nem kívánt tevékenységeket, és az illetéktelen hozzáférés megakadályozásával javítja a biztonságot.
A kétes linkek elkerülése	A tudatosság terjesztéséhez kapcsolódik a kétes vagy megbízhatatlan linkek elkerülésének szükségessége. A lehallgató támadók kétes linkeken keresztül terjeszthetnek lehallgató kártevőket tartalmazó rosszindulatú szoftvereket. A felhasználók csak hivatalos szoftvereket tölthetnek le megbízható forrásokból és szolgáltatóktól, és csak hivatalos alkalmazásboltokból tölthetnek le alkalmazásokat.
Szoftverfrissítés és -javítás	A támadók a szoftverek sebezhetőségeit is kihasználhatják, hogy szervezeteket és felhasználókat támadjanak meg. Ezért kulcsfontosságú az automatikus frissítések bekapcsolása és annak biztosítása, hogy minden szoftver azonnal javításra kerüljön, amint új kiadás vagy frissítés jelenik meg.
Fizikai biztonság	A szervezetek az adataikat és a felhasználóikat az irodahelyiségek fizikai biztonsági intézkedéseivel is megvédhetik. Ez kulcsfontosságú az irodák illetéktelen személyektől való védelme érdekében, akik fizikai vagy logikai lehallgató eszközöket, megoldásokat helyezhetnek el az irodában, telefonokban, a számítógépekben és más eszközökben.
Árnyékolás	A számítógépes sugárzáson keresztüli lehallgatás kockázata biztonsági intézkedésekkel és árnyékolással megelőzhető. A TEMPEST-védelemmel ellátott számítógépek például lehetővé teszik a szervezetek számára, hogy blokkolják a nem kívánt sugárzást, és biztonságban tartsák adataikat és felhasználóikat.

Forrás: Fortinet (2021): i. m.

A munkamenet-eltérítés

A munkamenet-eltérítés rendszerek vagy rendszerelemek közötti kapcsolatokban már létrehozott, megbízható és érvényes munkamenetek átvételének folyamata, amelynek célja a felhasználó bizalmas adatainak ellopása és veszélyeztetése. Ezt más néven közbeékelődéses (Man-in-The-Middle – MiTM) támadásnak is nevezzük. Amikor valaki bejelentkezik egy webes alkalmazásba, a háromirányú kézfogás segítségével megbízható munkamenetet hoz létre az ügyfél és a kiszolgáló között. Csak a megbízható és biztonságos kapcsolat létrehozása után kezdődik meg az igazi információcsere, -megosztás az ügyfél és a kiszolgáló között. A munkamenet-eltérítő támadásban a támadó átveszi az érvényes, megbízható kapcsolatot, csomagokat küld a kiszolgálónak mint valódi ügyfél, majd fogadja a csomagot a kiszolgálótól, és valódi kiszolgálóként továbbítja azt az ügyfélnek, ezzel azt mutatva mind a két félnek, hogy a valódi célállomással kommunikálnak. A támadás nagy előnye, hogy nem kell feltörnie, illetve áthatolnia semmilyen védelmen vagy biztonsági tűzfalon, csak folyamatosan figyelnie kell a hálózatot és átvenni valamely érvényes munkamenetet. Alapvetően háromféle, ugyanazt a tevékenységet különböző módon elvégző munkamenet-eltérítő támadás létezik, amelyek a következők:

- aktív munkamenet-eltérítés;
- passzív munkamenet-eltérítés;
- hibrid munkamenet-eltérítés.

Az aktív munkamenet-eltérítés során a támadó elhallgattatja az egyik gépet, általában az ügyfélszámítógépet, és átveszi az ügyfelek helyét a munkaállomás és a kiszolgáló közötti kommunikációban. Az aktív támadás azt is lehetővé teszi, hogy a támadó parancsokat adjon ki a hálózaton, ami lehetővé teszi új felhasználói fiókok létrehozását, amelyekkel később hozzáférhet a hálózathoz anélkül, hogy a munkamenet-eltérítő támadást újra végre kellene hajtania.

A passzív munkamenet-eltérítő támadás során a támadó figyeli a munkaállomás és a kiszolgáló közötti forgalmat. A passzív támadás elsődleges motivációja a hálózati forgalom figyelése és az értékes adatok vagy jelszavak esetleges felfedezése.

A hibrid munkamenet-eltérítés az aktív és a passzív munkamenet-eltérítés kombinációja. Ebben a támadó mindkét típusú munkamenet-eltérítési technikát használja a célja elérése érdekében.[175]

[175] Anuj Kumar Baitha – Smitha Vinod: Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology,* 7. (2018), 2.6. 193–198.

A 29. táblázatban látható lépések alkalmazásával megelőzhetők a munkamenet-eltérítések és növelhető az online biztonság.

29. táblázat: A munkamenet-eltérítés elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Nyilvános wifihálózatok elkerülése	A nyilvános wifihálózatok használatát minden esetben kerülni kell, különösen olyan fontos tranzakciókhoz, mint a munkahelyi levelezés, a céges tranzakciók indítása, a banki ügyintézés vagy az online vásárlás. Előfordulhat, hogy a szomszédos asztalnál kiberbűnözők ülnek, akik a csomagok kiszimatolásával próbálják megszerezni a munkamenetsütiket és egyéb információkat.
VPN[176] alkalmazása	A VPN elrejti az IP-címet, és az online tevékenységeket is titokban tartja azáltal, hogy egy „privát alagutat" hoz létre, amelyen keresztül az összes online tevékenység halad. A VPN titkosítja az összes küldött és fogadott adatot. A nyilvános wifi használatakor egy virtuális magánhálózat alkalmazásával távoltarthatók a munkamenet-eltérítők a munkamenetektől.
Biztonsági szoftverek alkalmazása	A munkamenetek biztonságban tartása érdekében célszerű jó hírű biztonsági szoftvereket alkalmazni, és emellett gondoskodni azok folyamatos naprakészen tartásáról és rendszeres frissítéséről. A biztonsági szoftverek képesek felismerni a vírusokat, és megvédik az eszközöket a kártékony programoktól, beleértve a támadók által a munkamenet eltérítéséhez használt rosszindulatú szoftvereket is.
Az átverések szűrése és elkerülése	Minden olyan esetben el kell kerülni az e-mailekben található linkekre való kattintást, amikor nem tudunk meggyőződni arról, hogy az a legális feladótól származik. A munkamenet-eltérítők küldhetnek olyan e-mailt, amely tartalmaz egy figyelemfelkeltő linket. A link rosszindulatú programot telepíthet az eszközre, vagy egy olyan bejelentkezési oldalra vezetheti a felhasználót, amely a támadó által előkészített munkamenet-azonosítóval jelentkezik be egy webhelyre.
A webhely biztonságával kapcsolatos tudatosság	A jó hírű bankok, e-mail-szolgáltatók, online kereskedők és közösségi oldalak rendelkeznek a munkamenet eltérítésének elkerülésére szolgáló biztonsági intézkedésekkel. A biztonságtudatos webhelytulajdonosok a HTTPS-t az egész webhelyre telepítik, nem csak a kezdőlapra, továbbá azonnal megtalálják és bezárják a biztonsági réseket. Ha egy felhasználó bizonytalan online áruházakat vagy más, nem feltétlenül a legjobb biztonsággal rendelkező szolgáltatók alkalmazásait veszi igénybe, akkor sebezhetővé válhat egy munkamenet-eltérítő támadással szemben.

Forrás: Amy Machnak: *Session Hijacking: What is a Session Hijacking and How Does It Work?* 2021

[176] Virtual Private Network (VPN) – virtuális magánhálózat: lehetővé teszi a vállalatok számára a belső intranet kiterjesztését a nyilvános hálózatok meglévő infrastruktúrájának felhasználásával. Virtuális magánhálózatokkal felügyelhető a hálózati forgalom, további biztonsági szolgáltatásokat is nyújtva, például a hitelesítést és az adatok bizalmasságát.

Az IP-hamisítás

A hamisító támadások a kibertámadások speciális típusai, amikor valaki megpróbál egy számítógépet, eszközt vagy hálózatot arra használni, hogy más számítógépes hálózatokat becsapjon úgy, hogy legitim entitásnak adja ki magát. A hamisító támadás során a behatoló üzeneteket küld egy számítógépnek, azt sugallva, hogy az üzenet egy megbízható rendszertől származik. A sikerhez a behatolónak először meg kell határoznia egy megbízható rendszer IP-címét, majd úgy kell módosítania a csomagcímeket, hogy úgy tűnjön, a csomagok a megbízható rendszerből érkeznek. Az IP-hamisítás célja, hogy a támadó jogosulatlan hozzáférést szerezzen egy távoli rendszerhez egy megbízható állomás IP-címének segítségével. Az ilyen támadások indításához a munkamenet-eltérítő vagy a rosszindulatú támadó megszerzi az ügyfelek IP-címét, és a TCP-munkamenetet saját IP-címével hamisított csomagokkal táplálja be. Az IP-hamisítást sikeresen alkalmazó támadásoknak több változata is létezik. Bár néhány viszonylag elavult, mások nagyon is relevánsak a jelenlegi biztonsági problémák szempontjából.

A vak hamisítás során a támadó több csomagot küld a célpontnak, azonban ebben az esetben a támadó gépe nem kap közvetlen választ a hálózatról, hiszen a válasz a hamisított címre érkezik. Általában ezek a támadók a helyi hálózat határain kívül helyezkednek el, és többnyire nincsenek tisztában azzal, hogy az átvitel hogyan történik az említett hálózaton. Ezért a támadás végrehajtása előtt először a csomagok olvasási sorrendjének megismerésével szokták azt felderíteni.

A nem vak hamisítás során a támadó és a célpont ugyanabban az alhálózatban tartózkodik. Ez megadja a támadónak azt a szabadságot, hogy a kommunikációt vizsgálva meghatározza a csomagok sorrendjét. Amint a szekvencia ismerete a rendelkezésére áll, a támadó egy másik megbízható és legitim gépnek kiadva magát megkerülheti a hitelesítést.[177]

Bár az IP-hamisító támadás korai felismerése komoly kihívást jelenthet, számos lépést lehet tenni annak érdekében, hogy a digitális állam működésében részt vevő szervezetek védve legyenek az IP-hamisítás veszélyeitől. A 30. táblázat ezek közül a megoldások közül szemlélteti a legjellemzőbbeket.

[177] Sharmin Rashid – Subhra Prosun Paul: Proposed Methods of IP Spoofing Detection & Prevention. *International Journal of Science and Research,* 2. (2013), 8. 438–444.

30. táblázat: Az IP-hamisítás elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Csomagszűrés	A csomagszűrés megvizsgálja az IP-csomagokat minden olyan eszköz vagy felhasználó esetében, amely megpróbál csatlakozni a hálózathoz (ez lehet a bejövő vagy a kimenő kommunikáció figyelése). Ez a gyakorlat különösen alaposan megvizsgálja az egyes IP-csomagok fejlécét, amely az IP-címet tartalmazza, hogy meggyőződjön arról, az megegyezik a forrás IP-címével, és minden úgy néz ki, ahogyan kell. Ha bármi hibásnak tűnik, a csomagot a szűrést végző eszköz eldobja (jellemzően tűzfal).
Hitelesítés nyilvános kulcsú infrastruktúrán keresztül	A nyilvános kulcsú infrastruktúra (Public Key Infrastructure – PKI) a felhasználók és az eszközök hitelesítésének elterjedt módszere, amely egy nyilvános és egy magánkulcspárra támaszkodik. A magánkulcs titkosítja a kommunikációt és ellenőrzi a felhasználó/eszköz hitelességét, míg a nyilvános kulcs visszafejti a kommunikációt. Ezek a hitelesítési módszerek aszimmetrikus titkosítást használnak, ami azt jelenti, hogy az egyes kulcsok páronként különböznek egymástól. Ez a módszer rendkívül megnehezíti a támadók számára a privát kulcs meghatározását, és rendkívül hatékonyan akadályozza meg az IP-hamisító támadások gyakori típusait, például a közbeékelődéses (MiTM) támadást.
Hálózatfelügyelet és tűzfalak	A hálózatfelügyelet olyan kritikus informatikai folyamat, amely nyomon követi a hálózati komponenseket és végpontokat, és biztosítja a hibák, a teljesítmény és a forgalom felügyeletét. Ez magában foglalja a kritikus hálózati problémák nyomon követését, a hibák észlelését és a különböző hálózati elemek állapotfigyelését az eszközszinttől a protokoll- és interfészszintekig. A hálózatfelügyeleti rendszerek olyan eszközöket tartalmaznak, amelyek nyomon követik a hálózati műveleteket. A forgalom, a sávszélesség-kihasználtság és más mérőszámok teljesítményszámlálók segítségével történő nyomon követése kritikus fontosságú lehet az IP-hamisítások egy másik nagyon jellemző támadási típusa esetén, a szolgáltatásmegtagadásos (DoS-) támadásoknál. Eközben a hálózati tűzfal beállítása egy másik módja az IP-címek hitelesítésének és a bizonytalannak tűnő és potenciálisan IP-hamisításnak kitett forgalom kiszűrésének.
Biztonsági képzések	Végezetül, a legitim hálózati felhasználók biztonsági képzése szintén segíthet az IP-eltérítésből eredő károk elleni védekezésben. Fontos azonban figyelembe venni, hogy nagyon sok esetben a támadók előrébb járnak, mint ezeknek a képzéseknek a sikeres beépülései a felhasználói tudatba, így gyakran előfordul, hogy egy hacker már sikeres IP-eltérítést hajtott végre, és hozzáférést szerzett bizonyos rendszerekhez.

Forrás: Sami VanVliet: *What It Is IP Spoofing, How to Protect Against It,* 2021

Az ARP-mérgezés

A címfeloldási protokoll (ARP) egy olyan protokoll, amely egy adott IP-cím és a hozzá tartozó MAC-cím[178] összekapcsolására szolgál. Az ARP-mérgezéses támadás egy olyan támadás, amelyet egy helyi hálózaton keresztül hajtanak végre, ami arra szolgál, hogy megváltoztassák az IP–MAC-címtábla párosításait, ami lehetővé teszi a támadó számára, hogy a hálózati forgalmat a támadó gép irányába irányítsa át. Ez a fajta támadás csak akkor lehetséges, ha a támadó és a célgépek is közvetlen kapcsolatban állnak ugyanazon a helyi hálózaton.

Egy támadó számos okból végezhet ARP-mérgezéses támadást, a magas szintű kémkedéstől kezdve a hálózati káosz megteremtésének izgalmáig. Az egyik lehetséges forgatókönyv szerint a támadó hamisított ARP-üzenetekkel átveszi egy adott alhálózat alapértelmezett átjárójának szerepét, és így a helyi útválasztó helyett a támadó gépe irányítja a forgalmat. Ezután kémkedhet, módosíthatja vagy megszakíthatja a forgalmat. Ezek a támadások „zajosak" abban az értelemben, hogy bizonyítékot hagynak maguk után, de nem kell, hogy zavarják a hálózat tényleges működését. Ha a kémkedés a cél, a támadó gép egyszerűen továbbítja a forgalmat az eredeti célállomásra, és a végfelhasználónak nem ad jelzést arról, hogy bármi megváltozott.

Az ARP-támadások kivédésének lehetséges módjait szemlélteti a 31. táblázat.

31. táblázat: Az ARP-mérgezés elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Statikus ARP-táblák alkalmazása	Lehetőség van arra, hogy statikusan hozzárendeljük az összes MAC-címet a megfelelő IP-címekhez a hálózatban. Ez rendkívül hatékony az ARP-mérgezéses támadások megelőzésében, de óriási adminisztrációs terhet jelent. A hálózatban bekövetkező bármilyen változás esetén az ARP-táblák manuális frissítése szükséges az összes állomáson, ami a statikus ARP-táblákat a legtöbb nagyobb szervezet számára megvalósíthatatlanná teszi. Azokban a helyzetekben azonban, ahol a biztonság kulcsfontosságú, egy különálló hálózati szegmens kijelölése, ahol statikus ARP-táblákat használnak, segíthet a kritikus információk védelmében.

[178] Media Access Control (MAC) – közeghozzáférés-vezérlő: a MAC-cím egy egyedi azonosító, amelyet a hálózati hardver gyártója rendel az eszközhöz, és amely alapján azonosítható a hálózaton.

Megoldás	Jellemzők és tulajdonságok
Kapcsoló-biztonság	A legtöbb Ethernet-kapcsoló rendelkezik az ARP-mérgezéses támadások enyhítésére tervezett és kialakított megoldásokkal. Ezek a jellemzően dinamikus ARP-ellenőrzés (Dynamic ARP Inspection – DAI) néven ismert funkciók értékelik az egyes ARP-üzenetek érvényességét, és eldobják a gyanúsnak vagy rosszindulatúnak tűnő csomagokat. A DAI általában úgy is konfigurálható, hogy korlátozza az ARP-üzenetek átjutási sebességét a kapcsolón, így hatékonyan megakadályozza a DoS-támadásokat. A portbiztonság kapcsolón történő engedélyezése szintén segíthet az ilyen típusú támadások mérséklésében. A portbiztonság úgy konfigurálható, hogy csak egyetlen MAC-címet engedélyezzen egy switch porton, így a támadónak nincs lehetősége több hálózati identitást rosszindulatúan felvenni.
Fizikai biztonság	Az eszközök és rendszerek üzemeltetésének helyet adó helyiségekhez, valamint az irodákhoz vagy egyéb munkakörnyezetekhez való fizikai hozzáférés megfelelő ellenőrzése segíthet az ARP-mérgezéses támadások mérséklésében. Az ARP-üzenetek nem tudnak kintről bejutni a helyi hálózat határain belülre, így a potenciális támadóknak fizikailag kapcsolódniuk kell az áldozat hálózatához, vagy már kontrollal kell rendelkezniük egy gép felett a hálózaton. A vezeték nélküli hálózatok esetében a közelség nem feltétlenül jelenti azt, hogy a támadónak közvetlen fizikai hozzáférésre van szüksége; egy utcára vagy parkolóra kiterjedő jel is elegendő lehet.
Hálózati izolálás	Mint korábban említettük, az ARP-üzenetek nem jutnak túl a helyi alhálózaton. Ez azt jelenti, hogy egy jól szegmentált hálózat összességében kevésbé lehet érzékeny az ARP-mérgezésre, mivel az egyik alhálózatban végrehajtott támadás nincs hatással a másik alhálózat eszközeire. A különösen fontos erőforrások dedikált hálózati szegmensben való összpontosítása, ahol fokozott biztonság van jelen, nagymértékben csökkentheti az ARP-mérgezéses támadás lehetséges káros hatásait.
Titkosítás	A titkosítás ugyan nem akadályozza meg az ARP-támadást, de mérsékelheti a lehetséges károkat. Az MiTM-támadások egyik népszerű felhasználási módja a bejelentkezési hitelesítő adatok megszerzése volt, amelyeket korábban általában egyszerű szövegben továbbítottak. Az SSL[179]/TLS titkosítás széles körű elterjedésével a weben az ilyen típusú támadások nehezebbé váltak. A támadó továbbra is képes elfogni a forgalmat, de titkosított formában nem tud vele mit kezdeni.

Forrás: Robert Grimmick: *ARP Poisoning: What It Is & How to Prevent ARP Spoofing Attacks,* 2021

[179] Secure Socket Layer (SSL) – védett socketréteg: a kommunikáló felek közötti titkosítással és hitelesítéssel történő biztonságos kommunikációra szolgáló protokoll.

A DNS-mérgezés

A tartománynévrendszer (DNS) fordítást biztosít az olvasható tartománynevek és az IP-címek között. A DNS az internet kulcsfontosságú infrastrukturális eleme, és számos támadás elsődleges célpontja. A DNS működését veszélyeztető egyik legjelentősebb fenyegetés a DNS-mérgezéses támadás, amelynek során a DNS-válaszokat egy támadó rosszindulatúan kicseréli, vagyis megmérgezi. A DNS mérgezése akkor történik meg, amikor hamis információk kerülnek be a domainnév-kiszolgáló gyorsítótárába, aminek következtében a DNS-lekérdezések hibás választ adnak, és a felhasználókat rossz weboldalra küldik. Az ilyen jellegű támadásokat elsősorban a különböző válaszidők elemzésével azonosíthatjuk be.[180]

A DNS-mérgezés veszélye, hogy a támadó átirányíthatja a felhasználót egy adathalász webhelyre, amely összegyűjtheti a felhasználó személyes adatait. Amikor a felhasználó megadja a kért adatokat, azokat a webhely a támadónak küldi el, aki aztán felhasználhatja vagy eladhatja egy másik bűnözőnek. Az adathalászat mellett a kártékony weboldalak rosszindulatú szoftverekkel is megfertőzhetik a figyelmetlen felhasználó számítógépét. Ez történhet olyan módon, hogy a weboldalról automatikusan rosszindulatú programot juttatnak a felhasználó rendszerébe, vagy a webhelyen található rosszindulatú linkkel, amely rosszindulatú programot, például trójai vírust vagy botnetet[181] telepít. Szintén problémákat okozhat az eszközök és rendszerek biztonságában az a fajta megoldás, amikor egy támadó meghamisíthatja egy internetes biztonsági szolgáltató webhelyét. Így amikor a számítógép megpróbálja felkeresni az oldalt, hogy frissítsen, az rossz oldalra kerül. Ennek eredményeképpen nem kapja meg a szükséges biztonsági frissítést, így a számítógép vagy bármely más rendszerelem ki van téve a támadásoknak.

Az DNS-mérgezéses támadások kivédésének lehetséges módjait szemlélteti a 32. táblázat.

[180] Harel Berger – Amit Z. Dvir – Moti Geva: A Wrinkle in Time: A Case Study in DNS Poisoning. *International Journal of Information Security,* 20. (2021), 3. 313–329.

[181] A botnet zombi, azaz olyan számítógépek hálózata, amelyeket különböző vírusokkal és trójai szoftverekkel irányítása alá vett egy támadó.

32. táblázat: A DNS-mérgezés elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
DNS-mérgezést észlelő eszközök	Ezek az eszközök átvizsgálják a küldött DNS-adatokat, hogy megbizonyosodjanak azok pontosságáról, mielőtt továbbítanák a felhasználónak.
A tartománynév-rendszer biztonsági kiterjesztései	Ez egy olyan specifikációkészlet, amely a DNS-protokollt a hiteles DNS-kiszolgálóktól kapott válaszok kriptográfiai hitelesítésével bővíti. Célja, hogy megvédje az eszközöket és rendszereket az olyan támadásokkal szemben, amelyekkel a számítógépeket csaló webhelyekre és kiszolgálókra irányítják.
Végpontok közötti titkosítás	A végpontok közötti kommunikáció biztonságossá tétele fontos szerepet játszik a magánszféra, valamint a digitális állam egyes szereplőinek védelmében és a közbeékelődéses támadások bizonyos formáinak megelőzésében. A végponttól végpontig terjedő titkosítás lényege, hogy az üzeneteket titkosított formában küldik el, a feloldókulcsot pedig kizárólag a beszélgetésben részt vevő felek birtokolják.
Aktív felügyelet	Fontos a DNS-adatok figyelése és az új minták, például egy új külső állomás megjelenésének azonnali beazonosítása, amely egy támadó jelenlétére utalhat.
Patchelés	A DNS-kiszolgálók sebezhetők. A kiszolgálók naprakészen tartása (a legújabb verziók alkalmazása) védelmet nyújthat a támadókkal szemben, akik ezeket a jól ismert sebezhetőségeket próbálják kihasználni.
DNS-kiszolgálók megfelelő frissítése	A legújabb DNS-kiszolgálók az alkalmazott portok véletlenszerű változtatásának képességével és titkosított tranzakcióazonosítókkal vannak ellátva, amelyek segítenek a DNS-támadók elleni védekezésben. Ennek megfelelően kiemelten fontos, hogy az alkalmazott kiszolgálókra a legújabb frissítések a lehető leggyorsabban telepítésre kerüljenek.

Forrás: N-able: *How to Prevent DNS Poisoning,* 2019

A felhőalapú informatika biztonsági kihívásai

Az elmúlt évtizedben a felhőalapú informatika *(cloud computing)* a digitális infrastruktúra egyik meghatározó elemévé vált. Az üzleti vállalkozások, a kormányzati szervek és az egyéni felhasználók egyre inkább támaszkodnak a felhő nyújtotta rugalmasságra és skálázhatóságra. Ugyanakkor a technológia előnyeivel párhuzamosan komoly biztonsági kihívások is megjelentek, amelyek kezelése elengedhetetlen az információbiztonság és az adatvédelem szempontjából. A felhőalapú számítástechnika jelentős adatvédelmi aggályokat vet fel, mivel a felhasználók távoli adatközpontokban tárolt adatainak tulajdonjogát és tör-

vényeit nehéz meghatározni. Adatszuverenitási problémák merülnek fel, amikor egy európai vállalkozás adatait egy nem európai adatközpontban tárolják, amelyre eltérő adatvédelmi szabályok vonatkoznak. Emellett a felhőszolgáltatók gyakran hozzáférnek az ügyfelek adataihoz, ami visszaélésekhez vagy adatszivárgásokhoz vezethet. Ezek az adatszivárgások jelentős üzleti veszteségeket és hírnévkárosodást okozhatnak. Ilyen kockázatot jelenthetnek a helytelen konfigurációk, amelyek nyilvános hozzáférést eredményezhetnek az elérhető biztonsági beállítások nem megfelelő alkalmazása révén. Szintén problémát okozhatnak a célzott hackertámadások, amikor a támadó kihasználja a felhőalapú rendszerek ismert sérülékenységeit, és ezzel hozzáférhet a felhőben tárolt adatokhoz. Ilyen lehet például az API-ok nem megfelelő védelme. Ennek kihasználásánál a támadók jogosulatlan hozzáférést szerezhetnek, adatokat manipulálhatnak, vagy szolgáltatásokat tehetnek elérhetetlenné.

A felhőalapú rendszerek következő kritikus kihívása a megfelelő hozzáférés-kezelés biztosítása. Az adatokhoz és szolgáltatásokhoz való jogosulatlan hozzáférés jelentős kockázatot jelent. A leggyakoribb problémák közé tartoznak például a gyenge jelszavak, amikor a felhasználók egyszerű, könnyen kitalálható jelszavakat használnak. Szintén komoly probléma a többfaktoros hitelesítés hiánya és az elavult jogosultságok megléte. Ez azt az állapotot jelenti, amikor az alkalmazottak (volt alkalmazottak) vagy partnerek (volt partnerek) hozzáférési jogosultságait nem vonják vissza tőlük azután, hogy arra már nincs szükségük.

A megfelelésproblémák *(compliance)* szintén komoly gondot jelentenek. A vállalatoknak számos szabályozást és iparági szabványt kell betartaniuk, például a GDPR vagy az ISO 27001 előírásait. A felhőalapú rendszerek esetében a megfelelés biztosítása gyakran bonyolult, mivel nem egyértelműek a felelősségi körök. Nehéz meghatározni, hogy a szolgáltató vagy az ügyfél felelős bizonyos biztonsági intézkedésekért. Sok szolgáltató nem nyújt elegendő betekintést az adatkezelési gyakorlatába, ami hátráltatja az auditok lebonyolítását, ezzel megnehezítve többek között a biztonsági intézkedések bevezetését. Például a szolgáltató felel a fizikai infrastruktúra védelméért, míg az ügyfél az adatok titkosításáért és hozzáférés-kezeléséért. Ha az ügyfél nincs tisztában ezzel a felelősségi körrel, könnyen sérülékennyé válhat a rendszer. Hasonlóan komoly problémát jelent a *multitenant* környezet. A *multitenant* architektúra lehetővé teszi, hogy több ügyfél ossza meg ugyanazt a fizikai infrastruktúrát. Ez azonban adatizolációs problémákat eredményezhet. Ha egy ügyfél biztonsági réseit kihasználják, az hatással lehet más ügyfelek adataira is, így szintén felléphetnek a fenti problémák mind az illetéktelen hozzáférés és módosítás, mind a rendelkezésre állás területén.

33. táblázat: A DNS-mérgezés elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Biztonsági frissítések azonnali alkalmazása	A rendszerre vagy alkalmazásra vonatkozó legfrissebb biztonsági javításokat vagy hibajavításokat a lehető legrövidebb időn belül telepítik, amint azok elérhetővé válnak. Általuk bezárhatók a kritikus biztonsági rések, fenntartható az adatvédelem és a szolgáltatás folytonossága, valamint kivédhetők a kibertámadások.
Folyamatos monitorozás	A rendszer, alkalmazás vagy infrastruktúra állapotának és teljesítményének folyamatos figyelése és elemzése annak érdekében, hogy azonosíthatók legyenek a potenciális problémák, biztonsági fenyegetések vagy teljesítménybeli hiányosságok. Idetartozik többek között az infrastruktúra monitorozása, a biztonsági események figyelése, az adatforgalom ellenőrzése és a felhasználói viselkedés nyomon követése.
Automatikus konfiguráció-ellenőrző eszközök használata	Olyan szoftverek és megoldások alkalmazása, amelyek folyamatosan figyelik, elemzik és ellenőrzik a felhőalapú rendszerek és szolgáltatások konfigurációit. Ezek az eszközök segítenek biztosítani, hogy a rendszer beállításai megfeleljenek a biztonsági, szabályozási és teljesítménybeli követelményeknek, miközben csökkentik az emberi hibák kockázatát.
Erős titkosítási technológiák használata	Az adatok védelme korszerű és biztonságos titkosítási algoritmusokkal történik annak érdekében, hogy azokhoz illetéktelen személyek vagy rendszerek ne férjenek hozzá. Ez az adat minden állapotában kiemelten fontos, átvitel, tárolás és használat közben egyaránt. Kiemelten fontos még a megfelelő kulcskezelés is az adatok védelme szempontjából.
Szabványosított konfigurációs sablonok alkalmazása	Előre definiált, egységes és újra használható konfigurációs minták alkalmazása a felhőalapú erőforrások létrehozásához és kezeléséhez. Ezek a sablonok biztosítják, hogy az infrastruktúra minden eleme következetesen legyen beállítva, megfeleljen a vállalati irányelveknek, és elősegítsék az automatizációt azáltal, hogy növelik a biztonságot, szavatolják a konzisztenciát, a szabályozási megfelelést, valamint a könnyebb hibakeresést és karbantartást.
Folyamatos auditálás és biztonsági ellenőrzés	A rendszer és az infrastruktúra működésének, beállításainak, valamint az adatvédelmi és biztonsági gyakorlatoknak rendszeres és automatikus vizsgálata annak érdekében, hogy megfeleljenek a biztonsági, szabályozási és vállalati előírásoknak. Ez a megközelítés proaktív módon azonosítja és kezeli a biztonsági rések, szabályszegések vagy konfigurációs hibák kockázatát.
Többszintű védelem alkalmazása	Olyan védelmi megközelítés, amelyben több egymást kiegészítő biztonsági réteg védi az infrastruktúrát, az alkalmazásokat, az adatokat és a felhasználói hozzáféréseket. Ez a megoldás arra törekszik, hogy ha egy adott réteget sikerül is kompromittálni, a többi védelmi szint minimalizálja a sérülékenység hatását, és megakadályozza a további károkat. Idetartoznak többek között: fizikai biztonság, hálózati biztonság, alkalmazásbiztonság, adatvédelem és titkosítás, azonosítás és hozzáférés-kezelés, monitorozás és naplózás, végpontvédelem, felhasználói képzés és tudatosítás.

Forrás: Fargana Abdullayeva: *Cyber Resilience and Cyber Security Issues of Intelligent Cloud Computing Systems,* 2023

Az adatátvitel szintén egy kritikus pontja a felhőinformatikának. Az adatátvitel a felhőalapú informatika egyik legkritikusabb területe. Az adatokat gyakran kell mozgatni a helyi rendszerek és a felhő, illetve a felhőszolgáltatások között, ami számos támadási felületet teremt. Ilyen lehet például az adatok lehallgatása. Az adatátvitel során az adatok hálózati forgalmon keresztül közlekednek, ami lehetőséget adhat a lehallgatásra. A támadók például közbeékelődéses támadásokkal próbálhatják megszerezni az érzékeny adatokat. Ennek kihasználhatósága nagymértékben függ a megfelelő titkosítás alkalmazásától. Több esetben is előfordul, hogy a szervezetek alkalmaznak valamiféle titkosítást, de ez valamilyen gyenge titkosítási algoritmust használ, vagy a kulcskezelés nem megfelelően történik, így a támadók képesek a „védett" hálózatot sikeresen támadni, manipulálni.

A felhőinformatika esetében is megjelenhetnek többek között az olyan fentebb tárgyalt sérülékenységek, veszélyek, fenyegetések, mint például a nulladik napi sérülékenységek, a rosszul konfigurált virtuális környezetek és konténerek, továbbá számos webes sérülékenység, például a nem megfelelő konfigurációnak köszönhetően. Szintén problémát jelenthetnek a belső fenyegetések. Erről abban az esetben beszélhetünk, ha egy felhasználó, alkalmazott szándékosan vagy véletlenül problémát, kárt okoz a rendszerben, jelen esetben a felhő-infrastruktúrában vagy az adatokban.

A klienseket fenyegető veszélyek

Az egyre kifinomultabb kibertámadások, beleértve a rosszindulatú szoftvereket, az adathalászatot, a gépi tanulást és a mesterséges intelligenciát, a kriptopénzeket és még sok mást, állandó veszélynek teszik ki a vállalatok, kormányok és magánszemélyek adatait és eszközeit, különösen a digitális államban, ahol minden információcsere, -tárolás és -feldolgozás az online térben történik. Ezek a támadások nem csak a hálózatok ellen kerülhetnek végrehajtásra, számos esetben a rendszerekben működtetett állomások (kliensek) ellen irányulnak. A kliens kifejezés gyakran utal a vállalati végpontokra és a személyes eszközökre, például mobiltelefonokra, táblagépekre és hagyományos számítógépekre. Emellett azonban idesorolhatjuk

még a különböző hálózati elemeket, nyomtatókat vagy például az IoT-eszközöket[182] is. A kliensekre ható legjellemzőbb támadások a következők:

- túlterheléses támadások;
- célzott támadások;
- hátsó kapus támadások;
- közbeékelődéses támadások;
- kártékony programok;
- IoT-támadások.

A 34. táblázat szemlélteti az egyes támadási vektorok legjellemzőbb tulajdonságait.

34. táblázat: A klienseket érintő fenyegetések legfőbb tulajdonságai

Támadási vektorok	Jellemzők és tulajdonságok
Túlterheléses támadások	Az elkövető arra törekszik, hogy egy gépet vagy hálózati erőforrást elérhetetlenné tegyen a rendeltetésszerű felhasználók számára.
Célzott támadások	Olyan titkos és folyamatos támadófolyamatok sorozata, amelyeket jellemzően egy konkrét személy, személyek vagy szervezet ellen követnek el.
Hátsó kapus támadások	Megszünteti a rendszerhez való hozzáférés normál hitelesítési módszereit.
Közbeékelődéses támadások	A támadó titokban átveszi és megváltoztatja a kommunikáló felek közötti kapcsolatokat.
IoT-támadások	A támadó az IoT-eszközök sérülékenységét kihasználva átveszi felettük az irányítást, vagy zombihálózattá alakítja őket.

Forrás: Sinha–Rai–Bhushan (2020): i. m.

A túlterheléses támadások

A túlterheléses támadás egy rosszindulatú kísérlet a célzott hálózat vagy szerver normális működésének befolyásolására azáltal, hogy a környező infrastruktúrát vagy magát a céleszközt elárasztják az internetes forgalom megnövelésével a célpont irányába. A túlterheléses támadásoknak két fajtáját különböztetjük

[182] Internet of Things: A dolgok internete, ami különböző, egyértelműen azonosítható elektronikai eszközök egysége, amelyek egymással egy internetalapú hálózaton keresztül kommunikálnak. A gépek a bennük található szenzorok segítségével kapcsolódnak a hálózathoz, ilyen módon osztanak meg egymással minden lényegi információt.

meg, ezek a szolgáltatásmegtagadásos (DoS-) és az elosztott szolgáltatásmegtagadásos (DDoS-) támadások A DoS-támadások telítik a rendszer erőforrásait azzal a céllal, hogy megakadályozzák a szolgáltatási kérésekre adott válaszok küldését vagy fogadását. A DDoS-támadást több fertőzött állomásgépről indítják, azzal a céllal, hogy a szolgáltatásmegtagadást elérjék, és a rendszert offline állapotba hozzák, ezzel megnyitva az utat egy másik támadás előtt, amely bejuthat a hálózatba/környezetbe. Az ilyen típusú támadások alapvető célja, hogy a megtámadott alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, az eszközök, a rendszer vagy akár a teljes hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat, ezzel megakadályozza a szolgáltatások vagy eszközök elérését. A támadást jellemzően botnetek segítségével hajtják végre a támadók.[183]

A túlterheléses támadások kivédésének lehetséges módjait a 35. táblázat szemlélteti.

35. táblázat: A túlterheléses támadások elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Megfelelő hálózatfelügyeleti gyakorlatok bevezetése	A megfelelő hálózatfelügyeleti gyakorlatok bevezetése olyan technológiák alkalmazását jelenti, amelyek lehetővé teszik a hálózat vizuális és valós idejű felügyeletét. Ezek segítenek megismerni a rendszer, a hálózat vagy az eszközök által átlagosan használt sávszélesség mennyiségét. Ennek segítségével könnyedén kiszűrhetők az anomáliák annak alapján, hogy a túlterheléses támadások látható jeleket hagynak maguk után a rendszerben, és ha a hálózat normál viselkedése jól ismert, az megkönnyíti a támadások valós időben történő észlelését.
Alapvető biztonsági higiéniák gyakorlása	A kiberbiztonsági higiénia magában foglalja azokat az alapvető legjobb gyakorlatokat, amelyek segítenek megvédeni az eszközöket és rendszereket a különböző típusú támadások ellen. Ezek többek között lehetnek az aktuális szoftverfrissítésekkel rendelkező rendszerek, a naprakész vírusirtó programok alkalmazása vagy a használaton kívüli portok letiltása a tűzfalon. Idetartoznak az olyan jól bevált gyakorlatok is, mint például az összetett jelszavak használata, a jelszó néhány havonta történő módosításának előírása, valamint a jelszavak jegyzetekben való tárolásának vagy leírásának elkerülése/tiltása.

[183] Bányász Péter: *Közösségi média és közszolgálat.* Budapest, NKE Közigazgatási Továbbképzési Intézet, 2020.

Megoldás	Jellemzők és tulajdonságok
Alapvető forgalmi küszöbértékek beállítása	A túlterheléses támadásokat részben enyhíteni lehet olyan biztonsági intézkedéssel, mint a forgalmi küszöbértékek és korlátok beállítása, például a sebességkorlátozás az útválasztón és a gyanús forrásból származó csomagok szűrése. A küszöbértékek beállítása mellett a feketelistás IP-címek alkalmazása, a földrajzi blokkolás és az aláírás-azonosítás további technikák, amelyeket a védelem első szintjeként alkalmazhatnak.
A biztonsági infrastruktúra naprakészen tartása	A hálózat annyira erős, amennyire a leggyengébb láncszeme erős. Ezért fontos, hogy tisztában kell lenni az infrastruktúrában lévő régi és elavult rendszerekkel, mivel ezek, ha kompromittálódnak, nagyon könnyen a támadók belépési pontjai lehetnek a rendszerbe. Ennek megfelelően az adatközpontok és rendszerek naprakészen tartása, valamint a webes alkalmazások tűzfalainak és más hálózati biztonsági programoknak a folyamatos javítása elengedhetetlen a DoS-támadások elkerülése érdekében.
DDoS-reagálási terv készítése	A DDoS-támadás bekövetkezését követően már nem lesz idő kitalálni a megfelelő válaszlépéseket, ezért célszerű előre elkészíteni egy tervet, hogy a támadás hatása minimalizálható legyen. A reagálási tervnek ideális esetben a következőket minimum tartalmaznia kell: A rendelkezésre álló eszközök nyilvántartása – a bevezetésre és alkalmazásra került eszközök listája, beleértve a fejlett fenyegetésérzékelést, -értékelést, -szűrést, valamint a szoftvereket és hardvereket. A reagáló erők adatait, képességeit – a támadás észlelése után a végrehajtásban részt vevő, egyértelműen meghatározott szerepkörrel és felelősséggel rendelkező személyek köre és szerepe. Eszkalációs protokollok – világosan meghatározott szabályok arra vonatkozóan, hogy kit kell értesíteni és bevonni a feladat-végrehajtásba támadás esetén. Kommunikációs terv – stratégia a belső és külső érdekelt felekkel való kapcsolattartásra, beleértve az internetszolgáltatót, a beszállítókat és az ügyfeleket, illetve minden olyan szervezetet, akiket egy bekövetkezett támadás esetén értesíteni kell, vagy akikkel együtt kell működni.
Elegendő szerverkapacitás biztosítása	Mivel a DDoS-támadások a hálózati sávszélesség túlterhelésével működnek, a sávszélesség túlbiztosításával lehet ellenük védekezni. Ha tehát sávszélesség hozzáadásával biztosított, hogy az alkalmazott kiszolgálók kapacitásai képesek legyenek kezelni a nagy forgalmi csúcsokat, azzal fel lehet készülni a DDoS-támadások okozta hirtelen és váratlan forgalmi megugrásokra.
Felhőalapú DDoS védelmi megoldások alkalmazása	A felhő több sávszélességet és erőforrást biztosít a magánhálózatokhoz képest. A felhőadatközpontok képesek elnyelni a rosszindulatú forgalmat, más területekre szétszórni, és megakadályozni, hogy elérjék a kívánt célpontokat.

Megoldás	Jellemzők és tulajdonságok
Tartalomszolgáltató hálózat használata	A tartalomszolgáltató hálózat (Content Delivery Network – CDN) drasztikusan csökkentheti a weboldalak betöltési idejét, miközben csökkenti a sávszélességet és növeli a megbízhatóságot. A DDoS-támadások esetében a CDN-ek segíthetnek azáltal, hogy a terhelést egyenlően osztják meg több földrajzilag elosztott szerver között. Így ha egy szerver leáll, a többi még rendelkezésre áll, ezáltal a munkamenet nem feltétlenül szakad meg. A CDN-ek tanúsítványkezelést és automatikus tanúsítványgenerálást és -megújítást is biztosíthatnak.

Forrás: CDNetworks: *How to Stop a DDoS Attack & Protect Your Business,* 2020

A célzott támadások

A célzott támadások mögött általában egy adott konkrét indíték áll, amely lehet információszerzés, károkozás, zsarolás, hátráltatás, pénzszerzés és még számos más ok. Ezekre a támadásokra alapvetően az jellemző, hogy a támadónak elegendő idő és erőforrás áll rendelkezésére, ezért nem az a kérdés, hogy sikerrel jár-e, hanem hogy mennyi idő alatt tudja végrehajtani a célját. A célzott támadások egyik jellemző módszere a fejlett, folyamatos fenyegetést biztosító APT-támadások. Ezalatt legtöbbször olyan rejtőzködő állami vagy nem állami bűnözői csoportokat értünk, amelyek magas szintű szervezettség mellett rendkívül kifinomult módszerekkel szereznek hozzáférést informatikai rendszerekhez, és képesek hosszabb időtartamon keresztül észrevétlenek maradni.[184] Az APT-támadások többnyire magánszervezetek, vállalkozások, szolgáltatók vagy állami szereplők ellen irányulnak, és üzleti vagy politikai motivációk vezérlik az elkövetőket.

Az advanced jelző arra utal, hogy a támadók kifinomult technikák és rosszindulatú szoftverek segítségével, általában a rendszerek nulladik napi sebezhetőségeinek kihasználásával jutnak be a rendszerbe és maradnak hosszú ideig ott. Jellemzően nem egyetlen támadási formát alkalmaznak, hanem tipikusan két-három vagy több részlépésből, külön technikai megoldásokból építik fel támadásukat.

A persistent kifejezés kettős jelentéssel bír. Az első, hogy a támadók több különböző forrásból gyűjtik az információkat, amelyeket a tervezési szakaszban

[184] Selján Péter – Selján Gábor: Kiberbiztonsági kitekintés. *Nemzet és Biztonság – Biztonságpolitikai Szemle,* 14. (2021), 1. 29.

használnak fel. Ezt mindaddig végzik, amíg elegendő információt nem gyűjtöttek a következő lépés kivitelezéséhez. A második jelentés lényege, hogy a támadók a célrendszerbe bejutva hosszú ideig észrevétlenül maradnak jelen, valamint folyamatosan figyelik és szivárogtatják az adatokat onnan.

A threat magának a támadásnak a veszélyességére utal, hiszen a támadók célirányosan, meghatározott háttérrel végzik el az információ-, adat- és személyiséglopásokat, amivel hatalmas károkat okozhatnak az áldozatoknak.[185]

A célzott támadások kivédésének lehetséges módjait a 36. táblázat szemlélteti.

36. táblázat: A célzott támadások elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Behatolás-vizsgálat	A behatolásvizsgálat segít az ismeretlen sebezhetőségek feltárásában és a telepített eszközök hatékonyságának tesztelésében. Lehetővé teszi, hogy utánozza a támadók által esetlegesen alkalmazott műveleteket és módszereket, és azonnali visszajelzést adhat arról, hogyan szükséges javítani a rendszereket.
Fenyegetés-elhárítási szolgáltatások	A fenyegetéselhárítás olyan szolgáltatás, amely figyeli, gyűjti és elemzi azokat az eseményeket, amelyek fenyegetést jelenthetnek egy szervezet számára. A szolgáltatott információk lehetővé teszik a védelmi és megelőzési intézkedések kialakítását. Az új generációs szoftverekkel és végpontvédelemmel kombinálva ezek az információk lehetővé teszik a szervezetek számára, hogy gyorsabban fedezzék fel a fenyegetéseket, és hamarabb megfékezzék a károkat.
A munkavállalók oktatása és tudatosítása	A rendszerhez való hozzáférés megszerzésének egyik leggyakoribb módja a kompromittált hitelesítő adatok használata. Ezeket a hitelesítő adatokat ellophatják adathalász akciókkal, hamis bejelentkezési portálok vagy brute-force alkalmazásával. Az APT-csoportok gyakran phishing e-mailek vagy social engineering technikák segítségével szerzik meg a szükséges adatokat. Ez azt jelenti, hogy a szervezet tagjainak kiberbiztonsági képzése kritikus fontosságú.
A rendszerek naprakészen tartása	Az APT-támadások során a hozzáférés megszerzésére vagy kiterjesztésére használt gyakori taktika a meglévő sebezhetőségek kihasználása, különösen az olyan ismert sebezhetőségek kihasználása, amelyeket nem javítottak ki. Ehhez folyamatosan figyelni kell az alkalmazott szoftverek és eszközök verzióit, és amint lehetséges, azonnal frissíteni kell azokat.

[185] Bodó Attila Pál et al.: *Célzott kibertámadások.* Budapest, NKE, 2018. 159.

Megoldás	Jellemzők és tulajdonságok
A rendszerhez való hozzáférés korlátozása	A rendszerhez való hozzáférés korlátozásának leghatékonyabb módja a mélységi védelem (Defense-in-Depth – DiD) és a legkisebb kiváltság elve. A mélységi védelem magában foglalja a rendszerek teljes körű védelmét, szemben a csak a periférián történő védelemmel. Ez magában foglalja a belső tűzfalak és a belső forgalomszűrés használatát. A legkisebb jogosultság elve kiegészíti a mélységi védelmet azzal, hogy a felhasználók és alkalmazások számára csak a minimálisan szükséges hozzáférést biztosítják. Ezek a stratégiák együttesen segíthetnek korlátozni a támadók azon képességét, hogy áthatoljanak a hálózaton. A kombináció jelentősen lelassíthatja a hozzáférést, így több idő áll rendelkezésre a támadás észlelésére és megállítására.
Incidenskezelési terv	Az incidenskezelési terv azokat a lépéseket tartalmazza, amelyeket incidens során kell a szervezetnek megtennie. Az incidenskezelési terv kialakításakor figyelembe kell venni a rendelkezésre álló erőforrásokat, az elvárt szolgáltatásokat, illetve hogy milyen típusú, fajtájú és súlyosságú fenyegetésekkel néz szembe az adott szervezet. Rendkívül fontos, hogy a szervezetnek legyen egy terve arra, hogyan reagáljon az APT- és más támadásokra, beleértve a forensics[186] tevékenységeket is. A szervezeteknek pontosan meg kell határozniuk, hogy ki a felelős a károk minimalizálása és a megismétlődés megelőzése érdekében teendő lépésekért.
Felhőalapú DDoS védelmi megoldások alkalmazása	A felhő több sávszélességet és erőforrást biztosít a magánhálózatokhoz képest. A felhőadatközpontok képesek elnyelni a rosszindulatú forgalmat, más területekre szétszórni és megakadályozni, hogy elérjék a kívánt célpontokat.
Tartalomszolgáltató hálózat használata	A tartalomszolgáltató hálózat (Content Delivery Network – CDN) drasztikusan csökkentheti a weboldalak betöltési idejét, miközben csökkenti a sávszélességet és növeli a megbízhatóságot. A DDoS-támadások esetében a CDN-ek segíthetnek azáltal, hogy a terhelést egyenlően osztják meg több, földrajzilag elosztott szerver között. Így ha egy szerver leáll, a többi még rendelkezésre áll, ezáltal a munkamenet nem feltétlenül szakad meg. A CDN-ek tanúsítványkezelést és automatikus tanúsítványgenerálást és -megújítást is biztosíthatnak.

Forrás: Gilad David Maayan: *How to Prevent and Detect APT Attacks,* 2020

[186] A forensics célja, hogy egy informatikai rendszerben vagy számítógépen bekövetkezett káros eseményeket hiteles módon, az időrendiség betartása mellett rekonstruáljon, felderítsen. Mindezeken túl releváns bizonyítékokat szolgáltat a bekövetkezett eseményekről, amelyek a későbbiekben akár nyomozati és igazságszolgáltatási tevékenységek során is felhasználhatóvá válhatnak.

A hátsó kapus támadások

A hátsó kapu egy eszköz vagy rendszer olyan része, amely bizonyos kiválasztott személyek részére illetéktelen hozzáférést enged a programhoz, a géphez vagy az azokon kezelt adatokhoz. A hátsó kapuk egy részét tudatosan, szervizcélokkal építik be, míg kisebb részük programozási hiba következtében teszi lehetővé a szabályok kikerülését. Ezenkívül léteznek kifejezetten a hátsó kapuk nyitásának céljával létrehozott programok is, amelyek általában vírusok, illetve kémszoftverek részeként kerülnek terjesztésre.[187] Mindezeknek megfelelően a hátsó kapu egy számítógépes rendszer olyan rejtett bejárata, amely a biztonsági irányelvek megkerülésére használható, ezzel az azt kihasználó személy dokumentálatlan módon hozzáférhet a számítógépes rendszerhez vagy a benne lévő adatokhoz, például jelszó használata nélkül.

Ahhoz, hogy egy támadó sikeresen telepíthessen hátsó kaput a céleszközre, először is hozzáférést kell szereznie az eszközhöz, akár fizikai hozzáféréssel, akár rosszindulatú támadással, akár a rendszer sebezhetőségének kihasználásával, úgymint nyitott portok, gyenge jelszavak, elavult szoftverek, hiszékeny felhasználók vagy gyenge tűzfalak. Néhány példa a különféle, gyakran használt hátsó kapukra:

- Trójai programok: A trójaiak olyan rosszindulatú programok, amelyek legitim fájloknak adják ki magukat, hogy hozzáférjenek egy eszközhöz, rendszerhez. Alapvető működési elvük, hogy mást csinálnak, mint aminek valójában mutatják magukat. Jellemzően valamilyen kártékony weboldal meglátogatása révén vagy e-mail-csatolmányra történő kattintással kerülhetnek az áldozat eszközére. Funkciójukat tekintve megkülönböztethetünk billentyűzetleütést naplózó, jelszavakat gyűjtő, felhasználói adatokat begyűjtő és a témánk szempontjából legrelevánsabb trójai programokat, amelyek hátsó kaput nyitnak a támadónak az áldozat eszközén, rendszerén.
- Rootkitek: A rootkitek olyan fejlett rosszindulatú eszközök, amelyek képesek elrejteni tevékenységüket az operációs rendszer vagy a felhasználó elől. Egy telepített rootkit olyan funkciókat használ, amelylyel nemcsak saját magát és működését képes elrejteni, hanem további kártékony kódokat is észrevehetetlenné tud tenni. Ezáltal a rootkitek

[187] Erdősi Péter Máté – Solymos Ákos: *IT biztonság közérthetően.* Budapest, Neumann János Számítógép-tudományi Társaság, 2019. 25–26.

lehetővé teszik a támadók számára, hogy távolról hozzáférjen egy eszközhöz vagy rendszerhez, fájlokat változtassanak meg, megfigyeljék a hálózati tevékenységeket vagy működésképtelenné tegyék a rendszert. A rootkitet rendkívül nehéz kimutatni, mivel aktívan próbálja elrejteni magát a felhasználó, az operációs rendszer és az antivírusprogramok elől. Számos módon települhet a rendszerre, beleértve az operációs rendszer biztonsági réseinek kihasználását vagy adminisztrátori jogok szerzését a számítógépen.[188]

- Hardveres hátsó kapuk: A hardveres hátsó kapuk olyan módosított számítógépes chipek vagy más firmware-ek/hardverek, amelyek hozzáférést biztosítanak egy eszközhöz a támadónak. Ezek közé az eszközök közé tartozhatnak a telefonok, az IoT-eszközök, például termosztátok és otthoni biztonsági rendszerek, a routerek és a számítógépek. A hardveres hátsó kapuk felhasználói adatokat közölhetnek, távoli hozzáférést biztosíthatnak vagy megfigyelésre használhatók. A hardveres hátsó kapuk már a gyártása során rákerülhetnek az eszközre (akár jóindulatú céllal is), de fizikailag is telepíthetik őket abban az esetben, ha egy eszközt ellopnak.
- Titkosítási hátsó kapuk: A titkosítási hátsó kapuk lényegében egy „mesterkulcsot" jelentenek, amelyek képesek feloldani minden olyan titkosított adatot, amely egy adott titkosítási protokollt használ. Az AES-hez[189] hasonló titkosítási szabványok végponttól végpontig tartó titkosítást alkalmaznak, így csak a véletlenszerűen generált titkosítási kulcsot cserélő felek képesek visszafejteni a megosztott információt. A hátsó kapukkal meg lehet törni ezt a biztonságos beszélgetést, és a titkosítási protokoll manipulálásával a támadó hozzáfér a felek között megosztott összes titkosított adathoz.

A hátsó kapukat nehéz felderíteni, azonban néhány egyszerű lépést, amellyel megvédhetők a készülékek és a rendszerek a hátsó kapus támadásoktól, a 37. táblázat ismertet.

[188] Bányász (2020): i. m. 32.

[189] Advanced Encryption Standard (AES) – fejlett titkosítási szabvány: egy szimmetrikus kulcsú titkosítás, ami azt jelenti, hogy az adatok titkosításához ugyanazt a kulcsot használják, mint az adatok visszafejtéséhez.

37. táblázat: A hátsó kapus támadások elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Megbízható anti-malware[190] szoftverek használata	Olyan fejlett vírusirtó szoftver alkalmazása, amely képes felismerni és megelőzni a rosszindulatú programok széles körét, beleértve a trójaiakat, kémprogramokat és rootkiteket. A vírusirtó felismeri a hátsó kapus vírusokat, és kiiktatja őket, mielőtt megfertőzhetnék a számítógépet.
Tűzfalak alkalmazása	A tűzfalak elengedhetetlenek a hátsó kapuk elleni védelem kialakításához és fenntartásához. Ha valaki a hálózaton kívülről próbál bejutni az eszközre, a tűzfal blokkolja a kapcsolatot, és ha egy alkalmazás ismeretlen hálózati helyre próbál adatokat küldeni, a tűzfal blokkolja az alkalmazást.
Jelszókezelők használata	A jelszókezelők segítenek létrehozni és tárolni a felhasználói fiókok bejelentkezési adatait, sőt segítenek az automatikus bejelentkezésben is. Mindezeket az információkat 256 bites AES titkosítással biztonságosan titkosítják, és egy fő jelszó mögé zárják. Mivel véletlenszerű, összetett jelszavakat generálnak, a jelszókezelők sokkal nehezebbé teszik a támadók számára, hogy bejussanak a hálózatába vagy terjeszkedjenek a hálózaton, ha hátsó kaput telepítettek a rendszerre.
A biztonsági frissítések/ javítások kezelése	A szoftverfejlesztők gyakran tesznek közzé új javításokat a szoftvereikben lévő sebezhetőségek kijavítására. Az általános javításkezelési stratégia több folyamatot foglal magában: a hálózati eszközök vizsgálata a hiányzó szoftverfrissítések után, a javítások letöltése, amikor azok elérhetővé válnak, a javítások telepítése a szükséges eszközökre és a megfelelő telepítés biztosítása.
Tudatos felhasználói viselkedés	A hátsó kapus programokat gyakran törvényesnek tűnő ingyenes szoftverekbe, fájlokba vagy alkalmazásokba csomagolják be. Számos e-mail-küldő platform az általa alkalmazott erős biztonsági algoritmusnak köszönhetően könnyen felismeri a káros tartalmú e-maileket. Sok ilyen e-mail a spam mappába kerül, amint megérkezik. Azonban több olyan levél is átjuthat a szűrőn, amely káros tartalmakat vagy kártékony webhelyre irányító linkeket tartalmaz. A felhasználóknak éppen ezért tisztában kell lenniük, hogy csak megbízható forrásból származó levelek tartalmát nyissák meg.

Forrás: Finidi Lawson: *How to Protect Your PC and Data Against Backdoor Attacks?* 2021

[190] A malware kifejezés magába foglal mindenféle rosszindulatú szoftvert, beleértve ezek legismertebb fajtáit, mint a trójaiak, zsarolóvírusok, vírusok és férgek.

A közbeékelődéses támadások

A közbeékelődéses támadások (MiTM) során a támadó beékelődik az egyes kliensek (például két eszköz vagy egy eszköz és az általa elérni kívánt szerver) közé azzal a céllal, hogy hozzáférjen a köztük végbemenő kommunikációkhoz, ezzel például érzékeny információkat szerezzen meg. Ez a beékelődés azt jelenti, hogy a kliens által közölt adatokat a támadó szervere fogadja és továbbítja a legitim szerver felé, majd az onnan érkező válaszokat mint kliens fogadja, és továbbítja a felhasználó felé. Normál http-alapú oldalak esetében a felhasználó sok esetben nem is veheti észre, hogy nem direkt az általa meglátogatott weboldal kiszolgáló szerverével kommunikál.[191]

Az MiTM-technikákat általában a kibertámadási lánc elején alkalmazzák, jellemzően a felderítés, a behatolás és a kihasználás során. A támadók gyakran használják az MiTM-technikákat a hitelesítő adatok megszerzésére és a célpontokról való információgyűjtésre. Az MiTM-támadás jellemzői:

- a munkamenet-eltérítés egy fajtája;
- a támadók közvetítőként vagy proxyként kapcsolódnak be egy folyamatban lévő, legitim beszélgetésbe vagy adatátvitelbe;
- a támadók kihasználják a beszélgetések és adatátvitelek valós idejű jellegét, hogy észrevétlenek maradjanak;
- lehetővé teszi a támadók számára a bizalmas adatok lehallgatását;
- lehetővé teszi a támadók számára, hogy rosszindulatú adatokat és hivatkozásokat illesszenek be a legitim adatoktól megkülönböztethetetlen módon.

A közbeékelődéses támadások kivédésének lehetséges módjait a 38. táblázat szemlélteti.

38. táblázat: A közbeékelődéses támadások elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Erős titkosítás a hozzáférési pontokon	A vezeték nélküli hozzáférési pontok erős titkosítási mechanizmusa megakadályozza, hogy a nem kívánt felhasználók a közelben tartózkodva csatlakozhassanak a hálózathoz. Egy gyenge titkosítási mechanizmus lehetővé teheti egy támadó számára, hogy brute-force technika segítségével megszerezze a hitelesítő adatokat, majd bejusson a hálózatba és MiTM-támadást indítson. Minél erősebb a titkosítás megvalósítása, annál biztonságosabb.

[191] Bodó et al. (2018): i. m. 239.

Megoldás	Jellemzők és tulajdonságok
Biztonságos kapcsolatok alkalmazása	A biztonságos internetkapcsolat az első védelmi vonal. A HTTPS nyilvános-magán kulcscsere segítségével a kommunikáció biztonságossá tehető az interneten. Ennek érdekében csak SSL-technológiát használó, biztonságos HTTP-kapcsolattal rendelkező weboldalak látogatása javasolt. Léteznek különböző böngészőbővítmények, amelyek kikényszerítik, hogy a kéréseknél mindig HTTPS-t használjanak az egyes weboldalak.
Virtuális magán-hálózatok használata	A VPN-ek arra használhatók, hogy biztonságos környezetet hozzanak létre az érzékeny információk számára egy helyi hálózaton belül. Kulcsalapú titkosítást használnak a biztonságos kommunikációhoz szükséges alhálózat létrehozásához. Ez a titkosítás megakadályozza, hogy az MiTM-támadó beszivárogjon a hálózati forgalomba. Még ha egy bűnözőnek sikerül is hozzáférnie a hálózatához, a titkosított adatok megakadályozzák, hogy elolvassa az üzeneteket, vagy megtudja, hogy milyen webhelyeket látogat meg a kliens.
Végpont-védelmi megoldások	Az erős végpontvédelmi szoftverek alkalmazásával szintén megelőzhetők az MiTM-támadások. A legjobb védelmi szoftverek ellenőrzik a potenciálisan veszélyes webhelyeket és e-maileket, hogy segítsenek a felhasználóknak elkerülni, hogy kibertámadás áldozatává váljanak. Ezek a szoftverek védelmet nyújtanak például a rosszindulatú programok ellen is, elhárítják az adathalászattal összefüggő támadásokat, megvédik a tárolt adatokat az eszköz elvesztése vagy eltulajdonítása esetén, valamint alkalmazásfelügyeletet is biztosítanak. A védelmi tevékenységük mellett jellemzően információt is szolgáltatnak a védett rendszerelemekről a központi felügyeleti rendszer, illetve a naplógyűjtő rendszer számára.
Többfaktoros hitelesítés alkalmazása	A többfaktoros hitelesítés egy olyan biztonsági fejlesztés, amelynél nemcsak a felhasználónévre és a jelszóra van szükség a fiókba való bejelentkezéshez, hanem az ellenőrzés egy másik formáját is használja. Ilyen például egy PIN-kód vagy egy mobiltelefonra küldött speciális kód megadása. Azzal, hogy a könnyen ellopható bejelentkezési adatokon túl többféleképpen kell igazolnia egy felhasználónak a jogosultságát az alkalmazáshoz, az eszközhöz vagy a hálózathoz való hozzáféréshez, megakadályozható, hogy a bűnözők hozzáférjenek a felhasználó adataihoz, érzékeny információihoz vagy pénzéhez.
Tudatosítás és képzés	A kibertámadások, úgymint például az MiTM-támadások, nagy százalékáért valamilyen emberi figyelmetlenség vagy mulasztás a felelős. Az emberek tudtukon kívül rákattintanak egy rossz linkre, vagy bejelentkezési adataikat használják egy veszélyeztetett webhelyen, így a hackerek hozzáférhetnek az összes adatukhoz. Ennek elkerülése érdekében az oktatás kritikus fontosságú, különösen az állami szférában és az üzleti életben. Amennyiben az alkalmazottakban megfelelő oktatás és tudatosítás során kialakítják a kibertámadások megelőzésének alapelveit, például az MiTM-támadások kapcsán, sok időt, pénzt és energiát takaríthat meg a szervezet, amely elkerülhet egy potenciális támadást. Az olyan egyszerű dolgokkal, mint például az alkalmazottak utasítása, hogy kerüljék a nyilvános wifihálózatokat, vagy annak megtanítása, hogyan néz ki egy adathalász e-mail, sokat segíthet az ilyen támadások megelőzésében.

Forrás: Robert Izquierdo: *5 Ways to Prevent a Man-in-the-Middle Cyberattack,* 2021

A kártékony programok

A digitális állam vonatkozásában is komoly kihívást jelentenek az egyre szofisztikáltabb kártékony programokkal végrehajtott támadások. A fentiekben esett már szó pár kártékony programról, de az egyre inkább elterjedt és jellemző elektronikus ügyintézés és a digitális alkalmazások használatának széles körű elterjedése sokkal több fajta és lényegesen veszélyesebb kártékony kódokkal való támadás lehetőségét biztosítják a támadóknak. A rosszindulatú programok számos módszert használnak arra, hogy a kezdeti támadási vektoron túl más számítógépes rendszerekre is átterjedjenek. Alapvető jellemzőik, hogy általában ártó szándékkal készülnek, a felhasználó tudta nélkül jutnak be a rendszerbe, és ott rejtetten működnek. Egyre fejlettebb intelligenciával rendelkeznek, például változtathatják saját kódjukat és aktivitásukat, és gyakran időzítve tesznek tönkre rendszereket, eszközöket vagy fájlokat. A rosszindulatú támadások közé tartozhatnak a következők:

- A rosszindulatú kódot tartalmazó e-mail-mellékleteket a gyanútlan felhasználók megnyitják, és ezáltal a kód le tud futni, a támadás végre lesz hajtva. Amennyiben ezeket az e-maileket továbbítják, a rosszindulatú szoftverek még mélyebben elterjedhetnek a szervezetben, tovább veszélyeztetve a hálózatot.
- A fájlkiszolgálók alkalmazása lehetővé teheti a rosszindulatú programok gyors terjedését, mivel a legitim felhasználók hozzáférnek a kiszolgálón található fertőzött fájlokhoz, és letöltik azokat.
- A fájlmegosztó szoftverek lehetővé tehetik, hogy a rosszindulatú szoftverek átmásolják magukat a cserélhető adathordozókra, majd a számítógépes rendszerekre és hálózatokra.
- Az egyenrangú (Peer-to-Peer – P2P[192]) fájlmegosztás olyan látszólag ártalmatlan fájlok megosztása révén is képes rosszindulatú szoftverek bejuttatására, mint a zene vagy a képek.
- A távolról kihasználható sebezhetőségek lehetővé teszik a hackerek számára, hogy földrajzi helytől függetlenül hozzáférjenek a rendszerekhez.

A malware a rosszindulatú szoftverek minden típusát magában foglaló kifejezés. A rosszindulatú szoftverek típusait és jellemzőit a 39. táblázat tartalmazza.

[192] A Peer-to-Peer vagy P2P paradigma lényege, hogy az informatikai hálózat végpontjai közvetlenül egymással kommunikálnak, központi kitüntetett csomópont nélkül.

39. táblázat: A rosszindulatú programok típusai

Típus	Jellemzők
Férgek (worm)	Önszaporodó vírusok, amelyek a biztonsági réseket kihasználva automatikusan terjednek a számítógépeken és hálózatokon. A féreg az eszköz fizikai erőforrásait felhasználva másolatokat hoz létre saját magáról, majd elküldi ezeket más eszközöknek, amelyeket el tud érni. Nagy mennyiségű féregmásolat küldése esetén az eszköz teljesítménye romolhat, vagy a hálózati kapcsolat is megszakadhat. Abban különbözik a vírustól, hogy önmagában is működik és életképes, nem kapcsolódik egyéb szoftverekhez.
Kémszoftverek (spyware)	A felhasználó tudta és engedélye nélkül valamely adatot a támadónak továbbító rejtett programok. Elrejtőzhetnek bármilyen alkalmazáscsomag részeként, ahol futtatható programok vannak. A kémszoftverek akár a billentyűzet leütéseit is naplózhatják, például jelszavak ellopása céljából, vagy a kamerán vagy mikrofonon keresztül egyéb információkat lophatnak vagy gyűjthetnek be a felelőtlen felhasználóról.
Kéretlen reklám (adware)	Olyan szoftver, amely automatikusan reklámokat jelenít meg. Míg a reklámprogramok egyes formái legitimnek tekinthetők, mások jogosulatlan hozzáférést biztosítanak a számítógépes rendszerekhez, és nagymértékben megzavarják a felhasználókat.
Kriptovaluta-bányász kártevők (cryptojacking)	Rosszindulatú kriptobányász tevékenységet támogató programok, amelyek az általánosan elérhető kriptobányászszoftvereket használják, így kihasználhatják más felhasználók számítástechnikai erőforrásait anélkül, hogy erről a felhasználóknak tudásuk lenne, vagy ehhez beleegyezésüket adták volna (pl. kriptoeltérítés).
Távfelügyeleti eszközök (Remote Administration Tool – RAT)	Szoftver, amely lehetővé teszi egy távoli kezelő számára a rendszer irányítását. Ezeket az eszközöket eredetileg törvényes használatra fejlesztették ki, de ma már a fenyegető szereplők is használják őket. A RAT-ok lehetővé teszik a rendszergazdai irányítást, így a támadó szinte bármit megtehet a fertőzött számítógépeken. Nehéz felismerni őket, mivel jellemzően nem jelennek meg a futó programok vagy feladatok listáján, és a működésük könnyen összetéveszthető a legális programok működésével.
Vírusok (virus)	Olyan programok, amelyek másolják magukat egy számítógépen vagy hálózaton belül. A rosszindulatú vírusok a meglévő programokra épülnek, és csak akkor aktiválódnak, ha a felhasználó megnyitja a programot. A legrosszabb esetben a vírusok megrongálhatják vagy törölhetik az adatokat, a felhasználó e-mail-címét használhatják a terjedéshez, vagy mindent kitörölhetnek a merevlemezről.

Típus	Jellemzők
Zombihálózat (botnet)	A botnet a robot és a hálózat (robot és network) szó összekapcsolásából ered, és vírussal fertőzött számítógépek hálózatára utal, amelyeket az elkövető(k) távolról küldött utasítások sorozatán keresztül képes(ek) irányítani, ezáltal tömegesen felhasználni bűncselekmények elkövetéséhez. A botnettámadások jelentősége abban áll, hogy tipikusan nem az egyéni felhasználók, hanem kritikus infrastruktúrák, nagyvállalati rendszerek ellen irányulnak, és komoly károkat tudnak okozni.
Zsarolóprogramok (ransomware)	A támadó olyan programot juttat be a felhasználó gépére vagy bármilyen számítógép-alapú rendszerére, amely a fertőzött eszközöket zárolja, vagy titkosítja az értékes állományokat, és ezáltal használhatatlanná teszi azokat.

Forrás: Sorbán Kinga: Vírusok és zombik a büntetőjogban: Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res,* 7. (2018), 2. 376–377.

A rosszindulatú szoftverek támadásait nem lehet megakadályozni, de vannak megbízható módszerek a támadások észlelésére és blokkolására, így védve meg a rendszereket a rosszindulatú szoftverek által okozott fertőzésektől. A rosszindulatú szoftverek támadásainak megállítása kritikus fontosságú a szervezet biztonsága és az érzékeny adatok védelme szempontjából. A rosszindulatú szoftverek elleni támadások megelőzése a folyamatok, irányelvek és informatikai biztonsági eszközök meglétét jelenti, amelyek megakadályozzák a támadások bekövetkeztét. A malware-ek elleni védelem legjobb megoldásait a 40. táblázat tartalmazza.

40. táblázat: A kártékony programokkal végrehajtott támadások elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Hálózati és végpontvédelmi eszközök használata	A kártékony szoftverek elleni védelem során minden lehetséges útvonalat meg kell vizsgálni, amelyen keresztül egy bűnöző rosszindulatú szoftveres támadásokat intézhet a szervezet eszközei és hálózata ellen. A végpont- és hálózati biztonsági védelmi eszközök kombinációjának használata a válasz a rosszindulatú szoftverekkel kapcsolatos számos biztonsági probléma megelőzésére.

Megoldás	Jellemzők és tulajdonságok
Vírusirtó és rosszindulatú szoftverek elleni eszközök alkalmazása	A vírusirtó és rosszindulatú szoftverek elleni eszközök segíthetik megvédeni a végponti eszközöket számos hagyományos és új, rosszindulatú szoftverrel kapcsolatos fenyegetés ellen. A különböző vírusirtó és anti-malware eszközök különböző szintű védelmet nyújtanak: – Böngészőszintű védelem: Egyes böngészők (például a Chrome) beépített rosszindulatú programok elleni védelmi funkciókkal rendelkeznek, amelyek segítenek megvédeni az eszközöket az ilyen online fenyegetésektől. Ez segít megakadályozni, hogy a rosszindulatú programok a böngészőn keresztül elérjék a készüléket, de nem vizsgálja át a készüléket a meglévő fenyegetések után. – Eszközszintű védelem: Ez az alkalmazás megvizsgálja az eszközöket, és beazonosítja az esetleg már meglévő rosszindulatú szoftvereket vagy vírusokat. Amennyiben észlel egyet, értesíti a felhasználót, aki eldöntheti, hogy karanténba helyezi vagy eltávolítja a fertőzött elemet. – Hálózati szintű védelem: Ez a fajta hálózati eszköz védelmet nyújt a rosszindulatú szoftverek és egyéb fenyegetések ellen, amelyek a hálózat forgalmán keresztül érkeznek. – Kiszolgálói szintű védelem: Ez a szoftver kiválóan alkalmas a szerverek védelmére a vírusok és más rosszindulatú szoftverekkel kapcsolatos fenyegetések ellen.
Tűzfalak alkalmazása	A tűzfal egy újabb védelmi réteg, amely biztosítja az eszközök és a hálózat hatékonyabb védelmét. A tűzfal egy akadályként működik az internet és az alkalmazott informatikai infrastruktúra között, és számos típusú rosszindulatú támadást és egyéb rosszindulatú tevékenységet blokkol (mind bejövő, mind kimenő). A hálózathoz való jogosulatlan hozzáférést azonosítja, és ha a tűzfal rosszindulatúnak találja a forgalmat, leállítja.
A felhasználók és alkalmazottak oktatása a közös kiberfenyegetések és átverési taktikák felismerésére	A kibertudatossági képzés a valós fenyegetésekről és átverésekről, valamint az ezekre való reagálásról oktatja a felhasználókat. Ennek a képzésnek ki kell terjednie: – a szervezet biztonsági szabályzóira, házirendjére, eljárásmódjaira; – az általános kiberbiztonsági legjobb gyakorlatokra; – a kibertámadások és online fenyegetések gyakori típusaira (valós példákon keresztül: adathalász e-mailek, rosszindulatú webhelyek és hirdetések stb.); – a kiberbűnözők általánosan alkalmazott taktikáira (például social engineering,[193] e-mail-hamisítás, rosszindulatú URL-ek vagy e-mail-mellékletek stb.); – hogyan kell reagálniuk vagy válaszolniuk a gyanús/potenciálisan rosszindulatú üzenetekre és helyzetekre; – kihez tudnak fordulni, és hogyan kell jelenteniük, ha valami rendellenességet észlelnek.

[193] A social engineering egy olyan támadásforma, amely során a támadó az emberi tényező kihasználható tulajdonságait használja fel, hogy ily módon férjen hozzá megtévesztéssel, zsarolással

Megoldás	Jellemzők és tulajdonságok
Az informatikai rendszerek és annak bővítményeinek és szoftvereinek rendszeres frissítése	A támadók a javítatlan sebezhetőségeket használhatják fel jellemzően arra, hogy megtámadják azokat a szervezeteket, amelyek nem frissítették a szoftvereiket. Ezért kulcsfontosságú, hogy a frissítéseket a lehető leghamarabb telepíteni kell minden eszközre. Ez a szoftveralkalmazásoktól kezdve az informatikai infrastruktúra firmware-éig és az operációs rendszerekig mindenre vonatkozik. Ezenkívül a malware- vagy vírusirtó szoftvereket is rendszeresen frissíteni kell. Ez védelmet nyújt a legújabb ismert fenyegetések többségével szemben.
Biztonságos hitelesítési módszerek használata	Egy szervezet vagy vállalkozás erős hitelesítési módszerek alkalmazásával biztosíthatja hálózata megfelelő védelmét. Ahelyett, hogy csak jelszavakat használnának, a szervezeteknek olyan házirendeket kell kialakítaniuk, amelyek erősebb hitelesítési módszereket alkalmaznak, többek között a következőket: – többfaktoros hitelesítés; – jelszavak helyett erős jelmondatok használata; – jelszó nélküli hitelesítési módszerek használata (egyszeri PIN-kódok [One-time PIN, OTP], fizikai hardverek, például tokenek vagy azonosító kártyák, vagy ügyfél-hitelesítési tanúsítványok).
Identitáskezelés és hozzáférés-ellenőrzés bevezetése	Az identitás- és hozzáférés-kezelés (Identity and Access Management – IAM) az engedélyezés és a hitelesítés keretrendszere. Ez az egész a felhasználó személyazonosságának és jogosultságainak ellenőrzéséről szól, mielőtt hozzáférést kapna egy adott rendszerhez. A szervezet alkalmazottainak korlátozott hozzáféréssel kell rendelkezniük az érzékeny adatokhoz, még akkor is, ha megbízhatóak. Jó gyakorlatnak számít, hogy mindenki csak a munkája elvégzéséhez szükséges jogokat kap. A rendszergazdai jogok számának növelésével a szervezet támadási felületei és kockázatai is növekednek. A rendszergazdai jogosultságokkal rendelkezők számára külön fiókot kell létrehozni például a böngészésére és a nem rendszergazdai feladatok elvégzésére. A rendszergazdai fiók csak akkor használható, ha adminisztrátori feladatokat kell végrehajtani.
Fájlok és szoftverek letöltése csak hivatalos forrásból	A szoftverek vagy fájlok letöltése kétes webhelyekről és áruházakból gyakran rosszindulatú programok forrása. Ha a fertőzött eszköz csatlakozik egy hálózathoz, akkor az a támadóknak lehetőséget ad arra, hogy hozzáférjenek a hálózathoz. Ott aztán oldalirányban mozogva megpróbálhatnak más sebezhető eszközöket megfertőzni vagy érzékeny információkat ellopni.

a védett információkhoz, rendszerekhez.

Megoldás	Jellemzők és tulajdonságok
Rendszeres (titkosított) biztonsági mentések készítése és karbantartása az adatokról	Bár a rendszeres biztonsági mentések készítése nem egy olyan módszer, amely biztosítja a hálózatot a rosszindulatú szoftverek támadásaitól, mindenképpen nagy segítség lehet a támadás bekövetkezését követően. A 3-2-1 adatmentési szabály követése nagyszerű módja annak, hogy vészhelyzetekben (például zsarolóvírusos támadás esetén) a szükséges adatok rendelkezésre álljanak. A technika a következőket foglalja magában: – 3 másolat készítése minden fontos fájlról: ez magában foglal egy elsődleges és két biztonsági másolatot; – 2 különböző adathordozó-típus használata a fájlok és adatok tárolására: ez a megközelítés további védelmet nyújt többféle veszély ellen; – 1 példány külső helyszínen történő biztonságos tárolása: néha még az is ajánlott, hogy a természeti katasztrófák okozta károk ellen egy másolat egy másik földrajzi területen legyen elhelyezve.

Forrás: Savvy Security: *How to Prevent Malware Attacks,* 2021

Az IoT-támadások

A tárgyak internete (IoT) kifejezés alatt olyan eszközök (például okostelefonok, okostévék, hűtők, nyomtatók, kamerák, szenzorok) hálózatát értjük, amelyek különböző beágyazott érzékelőkkel, szoftverekkel és egyéb technológiákkal vannak felszerelve abból a célból, hogy az interneten keresztül kapcsolatba lépjenek és adatot cseréljenek egymással és más eszközökkel.[194]

Az IoT-támadások során a támadók kihasználják, hogy az IoT-eszközök és hálózati infrastruktúrák jellemzően nem rendelkeznek megfelelő védelemmel. Ennek egyik alapvető oka, hogy a gyártók úgy készítik az eszközöket, hogy abba komoly biztonsági hibák kerülnek bele. Ilyenek lehetnek például a nem megváltoztatható jelszavak, a beépített hátsó kapuk, a titkosítás kialakításának teljes hiánya. A sérülékeny IoT-eszközöket a támadók könnyedén megfertőzhetik, és nagyszabású DDoS indításához használhatják fel őket.

A digitális állam esetében is számos olyan terület van (okosvárosok, okos energiaellátás, okos egészségügyi rendszerek, intelligens közlekedés, okos gyárak és okos mezőgazdaság), ahol az IoT-eszközök megjelennek, így komoly problémát jelenthet annak teljes működése szempontjából egy kiterjedt IoT-támadás. Az OWASP IoT-sérülékenységek Projektje[195] (IoT Vulnerabilities Project)

[194] Selján–Selján (2021): i. m. 28.

[195] Az OWASP IoT-projekt célja, hogy segítse a gyártókat, a fejlesztőket és a felhasználókat abban, hogy jobban megértsék a dolgok internetével kapcsolatos biztonsági kérdéseket, valamint hogy

folyamatosan értékeli a tárgyak internete területén megjelenő biztonsági kihívásokat és sérülékenységeket. Ezek közül a legfontosabbakat és a legtöbbször előforduló sérülékenységeket egy adatbázisba rendezve, a támadási felületek alapján is kategorizálva nyilvánossá is teszi. Ezeket a digitális állam egyes területeire potenciális veszélyt jelentő, azok zavartalan működését veszélyeztető sérülékenységeket szemlélteti a 41. táblázat.

41. táblázat: IoT-sérülékenységek az OWASP alapján

Sérülékenység	Támadási felület	Összegzés
Felhasználó-név-számlálás	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	Valós felhasználónevek gyűjtésének képessége a hitelesítési mechanizmussal való kölcsönhatása kihasználásával.
Gyenge jelszavak	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	A fiók jelszavait például „1234”-re vagy „123456”-ra állíthatja. Előre programozott alapértelmezett jelszavak használata.
Fiók kizárása	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	Lehetőség a hitelesítési kísérletek továbbküldésére 3−5 bejelentkezési kísérlet után.
Titkosítatlan szolgáltatások	Eszközhálózati szolgáltatások	A hálózati szolgáltatások nem megfelelően vannak titkosítva, így nem akadályozzák meg, hogy a támadók lehallgassák vagy manipulálják a hálózatot/adatokat.
Kétfaktoros hitelesítés	Felügyeleti interfész Cloud webes felület Mobilalkalmazás	Kétszeres hitelesítési mechanizmusok hiánya, például token- vagy ujjlenyomatszkenner
Gyenge titkosítás	Eszközhálózati szolgáltatások	A titkosítás végrehajtása helytelenül van beállítva vagy nem megfelelően frissül, például az SSL v2 használatával.

a felhasználók, legyen szó bármilyen környezetről is, biztonsági szempontból jobb döntéseket hozhassanak az IoT-technológiák építése, telepítése és értékelése során.

Sérülékenység	Támadási felület	Összegzés
A frissítés titkosítás nélkül	Frissítési mechanizmus	A frissítések TLS használata vagy a frissítési fájl titkosítása nélkül kerülnek továbbításra.
Frissítés írható helyre	Frissítési mechanizmus	A frissítési fájlok tárolási helye bárhonnan írható, ami lehetővé teszi a firmware módosítását és az összes felhasználó számára terjesztését.
DoS	Eszközhálózati szolgáltatások	A szolgáltatás megtámadható túlterheléses támadással.
A tárolóeszköz eltávolítása	Készülékfizikai interfészek	Az adathordozó fizikailag eltávolítható az eszközből.
Nincs kézi frissítési mechanizmus	Frissítési mechanizmus	Nincs lehetőség az eszköz frissítésének kézi ellenőrzésére.
Hiányzó frissítési mechanizmus	Frissítési mechanizmus	Az eszköz frissítésére nincs lehetőség.
Firmware verzió megjelenítése és/vagy utolsó frissítés dátuma	Eszközfirmware	A jelenlegi firmware-verzió nem jelenik meg, és/vagy az utolsó frissítési dátum nem jelenik meg.
Firmware és tároló extrakció	Szervizinterfész Labormérés OTA-frissítés lehallgatása Letöltés a gyártó weboldaláról eMMC-lehallgatás Az SPI Flash/eMMC chip törése és adapterben való olvasása	A firmware sok hasznos információt tartalmaz, például a forráskódot és a futó szolgáltatások bináris kódjait, előre beállított jelszavakat, SSH-kulcsokat stb.
A készülék kódvégrehajtási folyamatának manipulálása	Szervizinterfész Oldalsócsatorna-támadások	Különböző csatlakozásokon keresztül módosíthatjuk a készülék firmware-ének végrehajtását, és szinte az összes szoftveralapú biztonsági vezérlőt megkerülhetjük. Az oldalcsatornás támadások módosíthatják a végrehajtási folyamatot is, vagy információkat szerezhetnek meg az eszközről.

Sérülékenység	Támadási felület	Összegzés
A konzol elérése	Soros interfészek	Soros interfészhez való csatlakozás esetén teljes konzolhozzáférés szerezhető egy eszközhöz. Általában a biztonsági intézkedések magukban foglalják az egyéni rendszerindító eszközöket, amelyek megakadályozzák a támadó egyetlen felhasználói módba való belépését, de így azt is megkerülhetik.
Nem biztonságos külső gyártók	Szoftverek	Elavult Open SSL, SSH, webszerverek stb.

Forrás: Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus Kiadó, 2018. 94–96.

A fenti sérülékenységeket, valamint a digitális állam egyes elemeire gyakorolt lehetséges hatásaikat figyelembe véve megállapítható, hogy az IoT-eszközök védelme szempontjából alapkövetelmény a megbízható gyártótól és beszállítótól származó eszközök alkalmazása. Fontos komoly figyelmet fordítani az eszközök szoftvereinek, firmware-einek frissítési lehetőségeire, amelyek hiánya komoly támadói potenciált jelenthet. Amennyiben az alkalmazott IoT-eszközök sérülékenysége nem javítható, mivel a gyártó nem nyújt hozzá megfelelő támogatást, a firmware-ek nem frissíthetők, az máris adataink védelmének megsértéséhez, a hálózati kommunikáció megszakadásához vagy szolgáltatásmegtagadáshoz vezethet. Szintén fontos a hálózat kiépítésénél olyan forgalomirányítók alkalmazása, amelyek már összetett feladatrendszerek ellátására is alkalmasak, ennek megfelelően a hálózati biztonság szavatolása mellett megfelelő szolgáltatásminőséggel rendelkeznek, hálózati címfordításra képesek, továbbá alkalmasak a virtuális magánhálózatok irányítására. Az IoT-támadások kivédésének lehetséges módjait a 42. táblázat szemlélteti.

42. táblázat: Az IoT-támadások elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Alapértelmezett routerbeállítások módosítása	Az IoT-eszközök védelme érdekében a hálózat és a wifi az első védelem a hackerekkel szemben, mivel sok IoT-eszköz wifihez kapcsolódik. Éppen ezért minden esetben meg kell változtatni az alapértelmezett adatvédelmi és biztonsági beállításokat minden ilyen eszközön.

Megoldás	Jellemzők és tulajdonságok
Biztonsági elemző szoftverek alkalmazása	Az IoT-biztonsági elemzések magukban foglalják a különböző adatforrásokból származó adatok gyűjtését, korrelációját és elemzését. Ezeket az információkat ezután az IoT-tevékenységek vizualizálására, a gyanús események azonosítására és a lehetséges fenyegetésekre való reagálásra lehet felhasználni. A biztonsági elemzéshez szükséges információk gyűjtése során fontos az IoT-átjárók, valamint az érzékelők CPU-tevékenységének és a memórián belüli folyamatoknak a megfigyelése. Ezeknek az adatoknak az elemzésével érhető el, hogy csak a valós események kerüljenek végrehajtásra a rendszeren.
Kontextuális sebezhetőségi értékelés	A sebezhetőségek kihasználása az IoT-eszközök egyik fő behatolási pontja. Ilyen lehet egy kódbefecskendezést lehetővé tevő könyvtár, amelyet nem foltoztak be, fixen bedrótozott (hardcoded) hitelesítő adatok vagy egy gyenge titkosítási kulcs egy protokollban. Az eszköz biztonsági helyzetének folyamatos nyomon követése kulcsfontosságú, és ez kontextuális sebezhetőségi elemzésekkel érhető el.
Láthatóság kialakítása	Az IoT-eszközök alkalmazása során nagyon fontos a láthatósági eszközök és megoldások alkalmazása. Ilyen például a hálózati hozzáférés-ellenőrzés és a hálózaton lévő összes lehetséges végpont részletes nyilvántartása. Ezeknek a nyilvántartásoknak automatikusan frissülniük kell, amikor új eszközöket adunk hozzá a rendszerhez vagy törlünk onnan, és meg kell őrizniük az inaktív eszközök előzményeit. Emellett a hozzáférési ellenőrzéseknek automatikusan le kell futniuk a rendszeren, amikor ahhoz egy új csatlakozás történik, hogy a biztonságot a működés akadályozása nélkül lehessen garantálni.
Szegmentálás	A szegmentálás magában foglalja a rendszerelemek elkülönítését és a biztonsági intézkedések rétegzését annak érdekében, hogy az érzékeny adatok és rendszerek védettek maradjanak. A hálózat szegmentálásával csökkenthetők a támadók lehetőségei arra, hogy oldalirányban áthaladjanak a komponenseken, és a sebezhetőségeket az egyes eszközökre korlátozhatja. Az IoT-eszközök szegmentálásakor hasznos lehet a kategóriák szerinti szegmentálás, mint például infrastrukturális, adatgyűjtő vagy felhasználói végpontok. Az egyes végpontok követelményei vagy célja alapján olyan hálózati házirendeket lehet a kliensekhez rendelni, amelyek megakadályozzák a jogosulatlan hozzáférést.
Védett kommunikáció alkalmazása	A védett kapcsolatok segítenek biztosítani, hogy az adatokat ne tudják elfogni vagy módosítani a támadók, éppen ezért elengedhetetlen az IoT-rendszerek esetében is az eszközök és a felhasználók közötti minden kommunikáció védelme. E védelem biztosítása érdekében a lehető legerősebb titkosítást kell alkalmazni, biztosítani kell továbbá, hogy a titkosítókulcsokat rendszeresen cseréljék.

Megoldás	Jellemzők és tulajdonságok
Eszközhitelesítés alkalmazása	Az eszközhitelesítési intézkedések szintén segíthetnek az IoT-végpontok védelmében. Ezek az intézkedések magukban foglalhatják a biometrikus vagy a többfaktoros hitelesítést, illetve a digitális tanúsítványokat. A hitelesítéssel biztosítható, hogy a támadók akkor sem férhetnek hozzá az eszköz adataihoz, ha maga az eszköz fizikailag elérhető.
A szoftverek és firmware-ek naprakészen tartása	Az IoT-gyártók többsége rendszeresen küld frissítéseket az eszközeire, vagy új frissítéseket és biztonsági javításokat tesz elérhetővé a weboldalán. Mivel az IoT-eszközök nem rendelkeznek más védelmi réteggel, a rendszeres frissítés kulcsfontosságú a biztonságuk szempontjából. Az IoT-eszközök szoftverének és firmware-ének frissítése biztosítja, hogy az eszköz a legújabb kártevőirtó és vírusirtó ellenintézkedésekkel rendelkezzen. Ezenkívül segít a rendszernek a régebbi szoftververziók biztonsági hibáinak kijavításában.

Forrás: Dmitry Raidman: *Top IoT Threats and How to Avoid the Next Big Breach,* 2020

A felhasználókat fenyegető veszélyek

Alapvető információbiztonsági mondás, hogy a szervezetben, a rendszerben a leggyengébb láncszem az ember. Ennek egyik legkézenfekvőbb oka, hogy csak az tud hibázni, aki dolgozik, tehát a rendszerben tevékenykedő bármely személy képes akarva vagy akaratlanul olyan hibákat generálni, amelyek befolyásolhatják annak zavartalan működését vagy akár a teljes összeomlásához is vezethetnek. A digitális államban különösen nagy felelősség hárul a felhasználókra az általuk kezelt érzékeny adatok megfelelő kezelésének vonatkozásában. Számos külső vagy belső fenyegetettség érheti őket és/vagy az általuk kezelt adatokat, rendszereket, ezekről korábban már esett szó. Emellett azonban léteznek még olyan módszerek, amelyek kifejezetten a felhasználói jóhiszeműségre vagy éppen a figyelmetlenségre alapoznak. A felhasználókat érintő támadások közül a legjellemzőbbek, a fentieken felül, amelyek közül számos irányulhat szintén a felhasználók ellen (MiTM, különböző malware, brute-force támadások):

- social engineering támadások;
- a deepfake és az álhírek.

A social engineering támadások

A social engineering fogalomnak, talán annak komplexitásából is fakadóan, jelenleg nincs egy általánosan elfogadott magyar megfelelője. Nagyon sokszor pszichológiai manipulációként jelenik meg az irodalmakban, amely leginkább a fogalom társadalomtudományi eredetére utal. A social engineering egy olyan támadásforma, amely során a támadó a kihasználható emberi tulajdonságokkal él vissza, hogy ily módon például megtévesztéssel, zsarolással férjen hozzá az áldozat által kezelt érzékeny adatokhoz, illetve rendszerekhez. A téma egyik elismert szakértője, Kevin D. Mitnick megfogalmazása szerint a social engineering a befolyásolás és rábeszélés eszközével téveszti meg az embereket, manipulálja vagy meggyőzi őket, hogy a támadó (social engineer) tényleg az, akinek mondja magát. Ennek eredményeként a támadó, különböző technológia megoldások alkalmazásával vagy anélkül, képes a felhasználókat információszerzés érdekében kihasználni.[196]

Bányász Péter gyűjtötte össze a *Social Engineering and Social Media* című cikkében a legjellemzőbb social engineering típusú támadásokat, amelyeket humánalapú és technikai megoldásalapú támadások alapján határozott meg alapvetően. A humánalapú támadások alatt alapvetően a 43. táblázatban szemléltetett módszereket értjük.

43. táblázat: A humánalapú social engineering támadások

Fenyegetettség	Jellemzők
Felhatalmazás	A támadó egy harmadik félre hivatkozva kér valamilyen információt, például egy szabadságon levő munkatárs kérte meg, hogy határidőre készítsen el egy jelentést, amihez nincs meg minden információja, így ahhoz kér adatokat.
Identitáslopás	A támadó egy szervezeten belüli (például karbantartónak, rendszergazdának, új munkatársnak) vagy szervezeten kívüli személynek (például futárnak, hivatalos személynek, auditornak[197]) adhatja ki magát, kihasználva a nagyvállalati környezeteknek azt az előnyét, hogy az ott dolgozók nem ismernek mindenkit.

[196] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37.

[197] Az auditor az a személy, akinek megvan a felkészültsége, hogy elvégezze egy szervezet vagy vállalat auditálását, amely az auditbizonyítékok nyerésére és ezek objektív kiértékelésére irányuló módszeres, független és dokumentált folyamat. Az auditálás az a minőségirányítási folyamat, amellyel meghatározható a minőségirányítási rendszer követelményeinek való megfelelés mértéke.

Fenyegetettség	Jellemzők
Kukabúvárkodás (dumpster diving)	Ezt a módszert a támadók nagyon gyakran használják, főleg a valódi támadást előkészítő időszakban Alapvetően a szemetesben talált hulladék átvizsgálását jelenti, de ide érthető az irodákban különböző módon tárolt információk megszerzése, lemásolása is (kallódó dokumentumok, külső adathordozók, cetlik a monitoron stb.).
Más jogosultságának felhasználása (piggybacking)	A támadó egy szervezeten belüli munkatársnak adja ki magát, aki otthon felejtette a belépőkártyáját, kulcsait, vagy megpróbálja rávenni a célszemélyt, hogy a saját jogosultságával, például a belépőkártyáját kétszer lehúzva engedje be őt az épületbe.
Quid pro quo	Sok social engineering támadás során elhitetik az áldozatokkal, hogy kapnak valamit cserébe az általuk megadott adatokért vagy hozzáférésért. Ebben az esetben az emberek naivitását használják ki a támadók.
Segítségkérés	Segítségkéréssel a támadók konkrét végcélja érhető el, de sokszor nagyon jó alapot ad a további információgyűjtéshez. A támadók jellemzően sikerrel járnak, ha valamilyen elsőre érdektelennek tűnő információt vagy segítséget kérnek például az ügyfélszolgálatoktól, titkárságoktól vagy a recepciók munkatársaitól.
Segítség nyújtása (fordított social engineering)	A támadó első lépésként valamilyen problémát okoz (például egy olyan kártevőt küld az áldozat számítógépére, ami akkor fejti ki a hatását, amikor a támadó is jelen van), amelynek a megoldásában segédkezik, ezzel kiépítve a bizalmat a célpont és közte, majd ezt használja ki a továbbiakban.
Szoros követés (tailgating)	Lényege, hogy a támadó úgy tesz, mintha egy látogató, munkás vagy vendég csoport tagja lenne, és a bejáratnál hozzájuk csatlakozva jut be az épületbe, ahol aztán már szabadon mozoghat.
Vállszörfölés (shoulder surfing)	Ennek a módszernek a végrehajtásához a támadónak már az áldozat közvetlen közelébe kellett férkőznie, hogy őt a tevékenységeiben meg tudja figyelni. A támadó úgy helyezkedik el a célszemély körül, hogy hasznos információkat tudjon leolvasni a monitorról, vagy lássa, hogy mit gépel be a billentyűzeten (például hitelesítő adatokat).

Forrás: Bányász Péter: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

A humánalapú támadások mellett megjelennek olyan módszerek is, amelyek technikai eszközök alkalmazásával próbálják befolyásolni, rávenni az áldozatot, hogy információkat osszon meg a támadóval, akár tudtán kívül is. A legjellemzőbb technikai alapú social engineering támadási módszereket és jellemzőiket a 44. táblázat szemlélteti.

44. táblázat: A technikai alapú social engineering támadások

Fenyegetettség	Jellemzők
Adathalászat (phishing)	A támadás lényege, hogy a támadók valamilyen elektronikus csatornán keresztül próbálnak információt szerezni az áldozattól. Ez lehet például egy olyan e-mail, amely tartalmaz egy weboldalra irányító linket, ahol az oldal bizalmas adatok, például jelszavak megadására kéri a célszemélyt. A levelek és weboldalak többségére jellemző, hogy valamilyen internetes fordító-program segítségével fordították le a bennük/rajtuk található szöveget, ami magyartalan mondatokat eredményez, ezért könnyen kételyt ébreszthetnek egy éber felhasználóban (ennek ellenére még mindig nagyon sikeres meg-oldásnak mondható az ilyen típusú információszerzés). A támadásnak több válfaját különböztetjük meg: – Adathalászat telefonon keresztül (vishing): például a Voice over IP (VoIP-) technológia segítségével végrehajtott támadás, amelynek jellemzője, hogy a támadó valamilyen IP-alapú hangátviteli technológiát használ. Mivel az emberek többsége bízik a telefonos hálózatokban, nem feltételezi, hogy a hangüzenet nem hiteles helyről érkezett, és a támadó így tud tőlük infor-mációkat megszerezni. – „Bálnavadászat" (whaling): cégvezetőkre („bálnákra") irányuló táma-dás. Olyan átverés, amelyben az adathalászok megtalálják a társaság legfontosabb ügyvezetőjének vagy vezetőjének nevét és e-mail-címét (ezek az információk legtöbb esetben szabadon hozzáférhetők a cég weboldalán), és a társaságban betöltött szerepükre vonatkozó e-mailt állítanak össze. Az e-mail megpróbálja rávenni az alsóbb vezetőket, hogy kattintsanak egy linkre, amely olyan webhelyre irányítja őket, ahonnan rosszindulatú szoftverek töltődnek le a gépükre. De az e-mail szövegének hatására érzékeny információkat vagy vállalati titkokat is közzétehetnek a hiszékeny vezetők. – Pharming: a támadó a megtévesztett felhasználót tudta nélkül egy hamis, de a megbízhatóhoz nagyon hasonlító weblapra irányítja. Az átirányítás valamilyen rosszindulatú szoftver vagy kémszoftver segítségével történik, és a támadó az általa létrehozott kártékony weboldalon kérdéseket tesz fel, a felhasználó válaszai pedig lehetőséget adnak neki bizalmas, fontos információk megszerzésére és azok rögzítésére. – Smishing: rövidüzenet-szolgáltatás (Short Message Service – SMS-) alapú adathalászat, amely során a támadó a mobiltelefonokra küldött szöveges üzenetekkel próbálja meg rávenni az áldozatát, hogy elárulja személyes adatait. Az üzenet tartalmazhat például az áldozatot kártékony weboldalakra irányító linkeket. – Szigonyozás (spear phishing): a támadó ebben az esetben nem több száz vagy sok ezer véletlenszerű címre küldi el a leveleit, hanem egy jól definiált célcsoportot választ ki.

Fenyegetettség	Jellemzők
Baiting	A baiting az emberek kíváncsiságán és segítőkészségén alapszik. A támadó valamilyen adathordozót (DVD, pendrive, memóriakártya) vagy akár veszélyes tartalommal ellátott mobiltelefont (ezek a „csalik") valahol látható helyen otthagy (célszerűen egy számítógép közelében). A figyelemfelkeltés érdekében az ilyen tárgyakon gyakran érdekes szöveg található, például „szexi képek", „bizalmas" stb. A talált tárgyon azonban rosszindulatú szoftverek rejlenek, és amikor a gyanútlan áldozat az eszközt csatlakoztatja a számítógéphez, hogy megtudja, kié lehet (hogy vissza tudja azt adni) vagy mi annak a tartalma, akkor a kártékony program automatikusan lefuttatja magát, és megtörténik a fertőzés.
Pretexting	Olyan támadási forma, amellyel a támadók nyílt forrásból vagy adathalászattal előzetesen információkat gyűjtenek az áldozatról, és ezekből felkészülve és ezeket alkalmazva próbálnak meg az áldozattól még több információt megszerezni, általában telefonon.
Szándékos elírással történő megtévesztés (typosquatting)	Az ilyen típusú támadások azért működnek, mert az emberek nem fordítanak akkora figyelmet az URL-címekre, mint kellene, különösen, ha azok ránézésre jól néznek ki. Typosquattingról akkor beszélünk, amikor a támadók például egy nagy bank URL-jéhez hasonló, de kissé másképp írt URL-t regisztrálnak.

Forrás: Pšenáková Ildikó: Ne hagyd magad becsapni! *Lélektan és hadviselés,* 2. (2020), 1. 55–65.

A social engineering támadásokat különösen nehéz kivédeni, mivel kifejezetten úgy tervezték őket, hogy a természetes emberi tulajdonságokra játszanak, mint például a kíváncsiság, a tekintély tisztelete és a barátok segítésének vágya. Bár a social engineering biztonsági fenyegetések soha nem fognak eltűnni, nagymértékben kezelhetők a social engineering támadások elleni megelőző módszerekkel. Az ilyen megelőző módszereket és jellemzőiket szemlélteti a 45. táblázat.

45. táblázat: A social engineering fenyegetések elleni védelmi megoldások legfőbb jellemzői

Megoldás	Jellemzők és tulajdonságok
Biztonságtudatossági képzések	Az „egészséges" kiberbiztonsági környezet leggyakrabban az emberi viselkedésen alapul. A social engineering a viselkedés manipulálásáról szól, ezért a legjobb védekezés ellene az lehet, ha minden munkatárs megérti a kiberbűnözők különböző trükkjeit, eljárásmódjait. A felhasználók, az alkalmazottak megfelelő képzésével megakadályozható, hogy a social engineering fenyegetésből biztonsági incidens váljon.

Megoldás	Jellemzők és tulajdonságok
Adathalász-szimulációk alkalmazása	Az adathalász-szimulációk használata népszerű módszer a felhasználók felkészítésére az adathalász e-mailek felismerésére. A szimulációs szoftver általában felhőalapú, és egy erre szakosodott szállító biztosítja. A szimulációs gyakorlatok így távolról is elvégezhetők, és gyakran a szervezet egyedi igényeihez igazodnak.
Csaló e-mailek szűrése átjárók alkalmazásával	A támadók előszeretettel használják az e-maileket social engineering típusú átverések kivitelezésének eszközeként; az e-mail-átjárókat a spam e-mailek kiszűrésére használják. Az e-mail-átjárók lehetnek helyi vagy felhőalapúak. Az e-mail-átjárók helyes konfiguráció esetén bizonyítottan akár 99,9%-kal csökkentik a spamek számát.
Megfelelő biztonsági folyamatok bevezetése	A social engineering célja az emberek becsapása. A technológiai folyamatok azonban csak korlátozott mértékben segíthetnek az ilyen típusú támadások megelőzésében. Bár az olyan technológiák, mint a rosszindulatú programok elleni védelem és a tűzfalak fontosak, nem tudják megakadályozni a social engineering alapú támadásokat. A vezérigazgatói csalás és az üzleti e-mail-kompromittálás esetében hasznos, ha ezekre az eljárásokra vonatkozó biztonsági folyamatok vannak érvényben. Például a pénzátutalások esetében rendelkezni kell egy ellenőrzési és mérlegelési folyamattal, például bizonyos összeg feletti átutalások esetén meg kell követelni az átutalás személyes megerősítését.
Megfelelő közösségimédia-szabályzat az adatvédelemről és a közzétételről	A social engineering támadások megelőzése érdekében olyan vállalati biztonsági házirendet kell kialakítani, amely egyértelműen szabályozza a közösségi média kezelését. A túlzott megosztás valós probléma, és a social engineering támadások elősegítője. A támadók a közösségi médiából könnyen juthatnak olyan információkhoz, amelyekkel aztán könnyedén befolyásolhatják vagy zsarolhatják az áldozatot. Ezt a biztonsági házirendet azonban nehéz érvényre juttatni, ha a közösségi médiát magánjellegű környezetben használják az alkalmazottak.
Biztonságos mobileszköz-használat	Az emberek hajlamosak megnyitni a telefonos szöveges üzeneteket (SMS-eket), amit az összes szöveg 98%-os megnyitási aránya is bizonyít. Ennek eredményeképpen a kiberbűnözők mobilszövegeket használnak rosszindulatú szoftverek, például mobilbanki trójaiak terjesztésére, amelyeknek a száma jelentősen megnőtt az elmúlt időszakban. Annak érdekében, hogy a mobiltelefonok ne váljanak fenyegetéssé, gondoskodni kell arról, hogy az alkalmazottak megértsék ezeket a típusú veszélyeket. Emellett olyan struktúrákat, például irányelveket kell bevezetni, amelyek megakadályozzák, hogy a munkahelyi mobiltelefonokra illetéktelen mobilalkalmazásokat telepítsenek.

Megoldás	Jellemzők és tulajdonságok
Privilegizált hozzáférés és 2FA[198] beállítása	A social engineering gyakran a jogosultságok kiterjesztésére támaszkodik a hálózati erőforrásokhoz való hozzáférés engedélyezéséhez. Egy további hitelesítési réteg hozzáadásával a social engineering támadások eredményessége csökkenthető. A kétfaktoros hitelesítés rendszerint egy másik tényező használatát is megköveteli a felhasználónév és a jelszó mellett, mielőtt a hozzáférés engedélyezésre kerülne. Ez lehet olyan egyszerű kód, mint például egy mobil szöveges kód, de akár biometrikus is. Ez az extra hitelesítő adat nehezíti az adathalászatot, hiszen a csaló esetleg könnyen megszerezheti a jelszót, de a második tényezőhöz már lényegesen nehezebben fér hozzá.
Rendszeres kiberbiztonsági helyzetértékelés végzése	A kiberbűnözők mindig igyekeznek növelni a siker esélyeit. Ennek érdekében frissítik és módosítják az általuk használt social engineering technikákat. Ahogy az olyan új technológiák is megjelennek, mint például a deepfake, amely már mesterséges intelligenciát használ a hang vagy az arc manipulálására, a social engineeringben használt technikák is megváltozhatnak. Éppen ezért létfontosságú, hogy a szervezetek biztonsági csapata naprakészen tartsa magát a kiberbűnözők által alkalmazott legújabb taktikákkal és technikákkal kapcsolatban. Ezután meggyőződhetnek arról, hogy a legmegfelelőbb védelmet alkalmazzák a csalások bármely típusa ellen. A kiberbiztonsági helyzetfelmérés tanulságos és hasznos eredményekkel szolgál a szervezetek számára azzal kapcsolatosan, hogy jelenleg hol tartanak, mi hiányzik, és mit kell tenniük a kiberbiztonsági fejlettségi szintjük növelése érdekében. A kiberbiztonsági helyzetértékelés célja, hogy átfogó kiberbiztonsági ütemterv kidolgozásával segítse a szervezeteket kiberbiztonsági védelmük megerősítésében.
24/7 felügyeleti gyakorlat bevezetése	A hálózatok és rendszerek biztonsága fokozható és kiegészíthető olyan szolgáltatásokkal, amelyek 24/7 felügyeletet biztosítanak. A felügyelet általában olyan eszközök használatát jelenti, amelyek segítenek a hálózati problémák észlelésében. Ezek közé tartozhat a viselkedéselemzés és az intelligens eszközök, amelyek segítenek az anomáliák észlelésében. A felügyelet javítja az általános biztonságot is, mivel biztosítja a szoftverek naprakészségét, valamint a szerverek stb. hibás konfigurációinak kezelését.

Forrás: Hitachi Systems Security: *10 Ways Businesses Can Prevent Social Engineering Attacks,* 2019

[198] Two-factor Authentication (2FA): kétfaktoros hitelesítés.

Az álhírek

Az álhír fogalmát szó szerint vizsgálva arra a megállapításra jutnunk, hogy az álhír valójában nem hír. Azonban a nem szó szerinti vizsgálatnál már teljesen más következtetéseket vonhatunk le. Az álhírek esetében azok terjesztőjének minden esetben kettős szándéka van. Egyrészt a hamis információk közlése (maga az álhír), másrészt az olvasók félrevezetése, megtévesztése. Ebből a megállapításból jól látszik, hogy függőség van a két szándék között, az előbbi az utóbbit szolgálja, a közlés a félrevezetés eszköze. Az álhír tehát olyan hír, amelynek nincs tényszerű alapja (azaz hamis), és a közlő tudja ezt, mégis hírként jeleníti meg azt, ezzel megtévesztve az olvasókat.

Az álhír szorosan kapcsolódik az új digitalizált világunkhoz, éppen ezért jelent komoly kihívást a digitális államban is. A fogalom a 2016-os amerikai elnökválasztás, valamint a brexit melletti kampány révén vált hírhedtté, amikor is a folyamatok végkifejletét döntő mértékben befolyásolták a tömegesen gyártott és terjesztett álhírek.[199]

Az álhírek lehetnek teljes egészében kitalációk, vagy csak bizonyos részletei hamisak. Többféle céllal hozhatják őket létre a politikai haszonszerzéstől a termékek vagy szolgáltatások értékesítésén keresztül egészen a humorig (ez azonban nem számít valódi álhírnek, mivel a célja nem a megtévesztés). Az álhírgyártók alapvetően az olvasók felületességére, hiszékenységére építenek, azokból próbálnak hasznot húzni.

Az álhírek terjedéséhez nagyon nagy mértékben hozzájárultak az egyre szélesebb körben elterjedt közösségimédia-platformok, azok hírmegjelenítési módjai, illetve a felhasználók olvasási szokásaiban végbement változások. A legnagyobb közösségi oldalak a cikkeket már csak egy címmel, egy nagy méretű képpel és párosoros leírással jelenítik meg. A címről az esetek többségében elmondható, hogy figyelemfelkeltő (főleg az álhírek és a lájkvadász oldalak esetében), a kép többnyire izgalmas (de nagyon sok esetben nincs köze a szöveghez), a leírás pedig sejtelmes, hogy felkeltse az olvasó figyelmét. Sok felhasználónak ez a három elem már elegendő ahhoz, hogy megossza ezeket a tartalmakat, anélkül hogy elolvasná magát a cikket. Ez az újfajta „olvasási" szokása a felhasználóknak nagymértékben hozzájárul az álhírek, illetve a csaló oldalak elterjedéséhez. Mindezek

[199] András Ferenc: A fakenews igazságértéke és megértése. In Garaczi Imre (szerk.): *Az életminőség-fejlesztés új paradigmái a 21. században.* Veszprém, Veszprémi Humán Tudományokért Alapítvány, 2020. 164–174.

alapján megállapítható, hogy a közösségi médián tájékozódókat az objektív tények egyre kevésbé érik el, a közvéleményt már nem a valós tények alakítják. Helyettük hangsúlyozottan kerülnek előtérbe az érzelmek és a hiedelmek, amelyekre remekül hatnak a különböző álhírek. Különösen a napjainkban egyre jellemzőbb olyan hírek, amelyek valósághű, gépi tanulással létrehozott hamis képeket, videókat tartalmaznak.

A deepfake

A „mélytanulás" (deep learning) és az „ál-" (fake) szavak kombinációjából született a deepfake kifejezés, amely olyan digitálisan manipulált, rendkívül valósághű képeket és videókat jelent, amelyek olyan (valós vagy nem létező) embereket ábrázolnak, akik olyan dolgokat mondanak és tesznek, amelyek valójában soha nem történtek meg. A deepfake a gépi tanulás és a mesterséges intelligencia technológiáit használja a hang- és videofájlok manipulálására, hogy nagy megtévesztési potenciállal rendelkező hamis médiatartalmakat hozzon létre. Olyan neurális hálózatokra támaszkodik, amelyek nagy mennyiségű adatmintát elemeznek, hogy megtanulják utánozni egy személy arckifejezését, gesztusait, hangját és hanglejtését. A kiberbűnözők a deepfake segítségével próbálják befolyásolni érzelmi előítéleteinket, hogy megváltoztassák gondolkodásmódunkat. A deepfake jellemzően a közösségimédia-platformokat célozza meg, ahol az összeesküvések, pletykák és félinformációk könnyen terjednek, mivel a felhasználók hajlamosak a tömeggel tartani. A technológia innovációja során már számos durva visszaélés történt, többször előfordult már, hogy egy személynek a jó hírét igyekeztek besározni, politikai befolyásolásra alkalmazták, illetve a stabilitás és a demokrácia globális veszélyeztetésére, továbbá álhírek terjesztésére a közösségimédia-platformokon keresztül. A deepfake komoly veszélyt jelenthet a társadalmakra, a politikai rendszerekre és az üzleti életre, mivel a bűnözök olyan mennyiségű és olyan minőségű álhírt képesek a technológia által generálni, amelyet még a jól felkészített mesterséges intelligenciákkal is nagyon nehéz szűrni. Éppen ezért komoly humán erőforrást igényelnek az egyes médiaplatformoktól, hogy a lehető legkevesebb álhír kerüljön ki a világhálóra, amelyek a lakosság gondolkodását, véleményét egy témával kapcsolatban befolyásolják. Ilyen lehet például a hamis propaganda terjesztése és a választásokba való beavatkozás, amelyekkel veszélyeztetik például a nemzetbiztonságot, és csökkentik a polgárok bizalmát a hatóságok tájékoztatásával szemben. Egy

vírusként terjedő videóban valakinek a szájába adni a szavakat erős fegyver a mai dezinformációs háborúkban, mivel az ilyen módosított videók könnyen elferdíthetik az állampolgárok vagy a szövetségesek véleményét. A technológia segítségével a bűnözők készíthetnek videót például egy politikusról, aki raszszista jelzőt használ vagy kenőpénzt fogad el, egy elnökjelöltről, aki bevallja bűnrészességét egy bűncselekményben, egy kormánytisztviselőt egy látszólag kompromittáló helyzetben, vagy katonákat, akik háborús bűncselekményeket követnek el a műveletek közben. Ezeknek a videóknak komoly hatásuk lehet az állam működésére, a nemzetbiztonság fenntartására.[200]

A fentiekből kiválóan látszik, hogy mind az álhírek, mind a deepfake technológia komoly hatással lehet a digitális állam megfelelő működésére, valamint az állampolgárok, a nemzet biztonságára. Éppen ezért minden egyes szereplőnek komoly figyelmet kell fordítani az álhírek terjedésének megállítására, valamint a deepfake technológiával előállított médiatartalmak kiszűrésére. Az álhírek és a deepfake elleni megoldásokat az egyes szereplők vonatkozásában a 46. táblázat tartalmazza.

46. táblázat: A digitális állam egyes szereplőinek feladata az álhírek és a deepfake technológia ellen

Szereplők	Tevékenységek
Kormányzatok	Az egyik legfontosabb dolog, amit a kormányok világszerte tehetnek, hogy ösztönzik a független, professzionális újságírást. A közvéleménynek szüksége van olyan riporterekre, akik segítenek értelmezni a bonyolult fejleményeket és kezelni a társadalmi, gazdasági és politikai események állandóan változó természetét.
	A kormányoknak el kell kerülniük a médiumok tudósítási képességének korlátozását. Ezek a tevékenységek korlátozzák a véleménynyilvánítás szabadságát, és akadályozzák az újságírókat abban, hogy a politikai fejleményekről tudósítsanak.
	A kormányoknak el kell kerülniük a tartalom cenzúrázását és az online platformok felelősségre vonását az általuk vélt félretájékoztatásért. Ez korlátozhatja a szabad véleménynyilvánítást, és az emberek haboznak megosztani politikai véleményüket, mert attól tartanak, hogy azt álhírként cenzúrázzák, vagy felelősségre vonják őket.

[200] Mika Westerlund: The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review,* 9. (2019), 11. 40–53.

Szereplők	Tevékenységek
Hírügynökségek	A híriparnak továbbra is a magas színvonalú újságírásra kell összpontosítania, amely bizalmat épít, és nagyobb közönséget vonz.
	Fontos, hogy a hírügynökségek az álhíreket és a dezinformációt anélkül nevezzék meg, hogy legitimálnák azokat.
Technológiai cégek	A technológiai cégeknek olyan technológiába kellene befektetniük, amely algoritmusok és a tömeges adatgyűjtés segítségével megtalálja és azonosítja az álhíreket a felhasználók számára.
	Ezeknek a vállalatoknak nem szabadna pénzt szerezniük az álhírgyártókból, és meg kellene nehezíteniük a megtévesztések pénzzé tételét.
	Az online elszámoltathatóság megerősítése a valós nevekre vonatkozó szigorúbb irányelvek kialakítása és a hamis fiókok elleni fellépés révén.
Oktatási intézmények	A felhasználóknak alapvetően nehéz megkülönböztetniük a hamis és a valódi híreket, ezért meg kell tanulniuk azt, hogyan értékeljék a hírforrásokat, továbbá hogy nem szabad mindent, amit a közösségi médiában vagy a digitális híroldalakon látnak, készpénznek venniük.
	A lehető legfiatalabb korban meg kell kezdeni a tudatosítást, ami hozzájárul ahhoz, hogy a fiatalok felismerjék azokat a jeleket, amelyek arra utalnak, hogy egy hír nem legitim.
Polgárok	Az egyének alapvetően úgy védekezhetnek az álhírek és a dezinformáció ellen, ha sokféle embert és nézőpontot követnek. A kisszámú, hasonlóan gondolkodó hírforrásra való támaszkodás korlátozza az emberek számára elérhető anyagok körét, és növeli annak esélyét, hogy átverések vagy hamis pletykák áldozatává váljanak.
	Az online világban az olvasóknak és a nézőknek szkeptikusnak kell lenniük a hírforrásokkal szemben. A kattintások ösztönzésére irányuló hajszában sok online hírportál félrevezető vagy szenzációhajhász címekhez folyamodik.
	A digitális korban kiemelt fontosságú, hogy megtanuljuk, hogyan ítéljük meg a híroldalakat, és hogyan védekezzünk a hamis információk ellen.

Forrás: Darrell M. West: *How to Combat Fake News and Disinformation,* 2017

A mesterséges intelligencia alkalmazásának biztonsági kérdései

A mesterséges intelligencia alkalmazása a digitális államban is jelentős technológiai, gazdasági és társadalmi előnyökkel járhat, azonban ezzel párhuzamosan

számos biztonsági kihívást is felszínre hoz. Több kutatás kimutatta már, hogy a mesterséges intelligencia alkalmazása nemcsak előnyökkel, hanem jelentős kockázatokkal is járhat, amelyek veszélyeztethetik a magánszemélyek, a szervezetek és akár a nemzetek biztonságát is. Az egyik legjelentősebb kihívás az adatokkal való visszaélés lehetősége. Az MI-rendszerek hatékonyságuk érdekében hatalmas mennyiségű adatot használnak fel, amely gyakran érzékeny személyes, vállalati információkat is tartalmaz. Ezeket az adatokat ellophatják, módosíthatják vagy jogosulatlanul felhasználhatják. Az adatvédelmi incidensek különösen súlyosak lehetnek, ha kritikus rendszereket, például egészségügyi vagy pénzügyi adatbázisokat érintenek, ami komoly társadalmi bizalomvesztéshez vezethet.

Egy másik kulcsfontosságú kérdés a manipuláció és a dezinformáció. Az MI által létrehozott tartalmak, például a fentebb tárgyalt deepfake videók vagy az automatikusan generált hamis hírek, veszélyeztethetik a közvéleményben az állam, az állami szereplők, a kormányzat hitelességét és a demokratikus intézmények stabilitását. Az ilyen technológiák segítségével könnyen lehet manipulálni az emberek véleményét, ami különösen kritikus lehet választási időszakokban vagy politikai konfliktusok során.

A kiberbiztonsági fenyegetések szintén az MI-vel kapcsolatos legégetőbb problémák közé tartoznak. Az MI-t alkalmazhatják támadások automatizálására, például számítógépes rendszerek sebezhetőségeinek gyors azonosítására és kihasználására. A fejlett algoritmusok és a gépi tanulási technikák segítségével a mesterséges intelligencia hatalmas mennyiségű adatot képes elemezni, hogy a hagyományos módszereknél hatékonyabban azonosítsa a rendszerek és hálózatok biztonsági réseit, gyenge pontjait. Amint ezeket a sebezhetőségeket azonosította, a mesterséges intelligencia képes automatizált támadásokat összehangolni, lehetővé téve a rosszindulatú szereplők számára, hogy azokat precízen és gyorsan kihasználják. A védelmi oldalon szintén megjelennek az MI-alapú rendszerek, amelyek noha fejlettek, nem tévedhetetlenek. Előfordulhatnak hibák, különösen akkor, ha a támadók kihasználják a tanulási algoritmusok sebezhetőségeit. Ha például egy támadó megzavarja az adatbevitelt vagy manipulálja a környezetet, amelyben a rendszer tanul, az pontatlan előrejelzésekhez és reagálásokhoz vezethet. A támadók emellett olyan módszereket is alkalmazhatnak, mint a félrevezető adatok vagy megtévesztő példák bevitele a modell összezavarására, ami csökkenti a modell hatékonyságát.

A kiberbiztonság területén az autonóm rendszerek biztonsága külön figyelmet érdemel. Az önvezető autók, drónok vagy más intelligens eszközök működése során technikai hibák, emberi szabotázs vagy rosszindulatú hackerek támadásai

komoly veszélyeket rejthetnek. Ha ezek a rendszerek hibásan működnek, akár emberéletek is veszélybe kerülhetnek, különösen kritikus környezetekben, például közlekedési vagy egészségügyi alkalmazások esetén.

47. táblázat: A mesterséges intelligencia alkalmazásának veszélyei, kihívásai

Veszély, sérülékenység	Jellemző
MI-vezérelt kibertámadások	A mesterséges intelligencia által vezérelt kibertámadások fejlett technológiákat használnak a rosszindulatú tevékenységek automatizálására és optimalizálására, jelentősen növelve azok hatékonyságát. Az adathalászkampányok például pontosabban az egyénekre szabhatók, így meggyőzőbbé és nehezebben felderíthetővé válnak. Hasonlóképpen, a mesterséges intelligencia felhasználható olyan kifinomult rosszindulatú programok létrehozására, amelyek valós időben tudnak igazodni a biztonsági intézkedések változásaihoz. A gépi tanulási algoritmusok alkalmazásával a támadók folyamatosan finomíthatják módszereiket, növelve ezzel esélyeiket a rendszerek sikeres feltörésére, továbbá könnyebben és jobban el tudják rejteni tevékenységeiket a megtámadott rendszerekben, hálózatokban.
Ellenséges támadások	Az ellenséges támadások olyan technikákat jelentenek, amelyekkel a bemeneti adatokat manipulálják, ami azt eredményezi, hogy az MI-modellek téves előrejelzéseket vagy döntéseket hoznak. Ezek a támadások jelentős kockázatot jelenthetnek a különböző, mesterséges intelligenciára épülő alkalmazásokra, például az arcfelismerő rendszerekre, amelyek tévesen azonosíthatnak személyeket, vagy az autonóm járművekre, amelyek félreértelmezhetik a környezetüket, ami potenciálisan veszélyes helyzetekhez vezethet. A támadók az adatok finom megváltoztatásával – például zaj hozzáadásával egy képhez vagy bizonyos jellemzők módosításával – igyekeznek kihasználni az MI-algoritmusok sebezhetőségeit, ezzel elérve a modellek félrevezetését.
Adatmanipuláció és adatmérgezés	Az adatmanipuláció és az adatmérgezés jelentős veszélyt jelent a mesterséges-intelligencia-rendszerek sértetlenségére, különösen az olyan kritikus ágazatokban, mint az egészségügy és a pénzügy. Ezek a támadások a gépi tanulási modellek fejlesztéséhez használt tanítási adatok szándékos megváltoztatását foglalják magukban. Azáltal, hogy pontatlanságokat és félrevezető információkat visznek be ezekbe az adatokba, a támadók ronthatják a modell teljesítményét és döntéshozatali képességeit. Ez hibás előrejelzésekhez vagy osztályozásokhoz vezethet, ami különösen veszélyes az olyan környezetekben, ahol a pontosság kulcsfontosságú. Az egészségügyben például a sérült modellek hibás diagnózisokat vagy nem megfelelő kezelési ajánlásokat eredményezhetnek, míg a pénzügyekben hibás kockázatértékeléshez vagy csalásfelismerési hibákhoz vezethetnek.

Veszély, sérülékenység	Jellemző
Modell-lopás és az ellátási lánc sebezhetőségei	A mesterségesintelligencia-modellek ellopása jelentős fenyegetést jelent, mivel a támadók lemásolják a védett modelleket, ezáltal veszélyeztetve a szellemi tulajdont és csökkentve a versenyelőnyöket. Továbbá az ellátási láncon belüli sebezhetőségek – különösen a bonyolult mesterségesintelligencia-fejlesztési folyamatokban – hátsó kapus támadásokat eredményezhetnek vagy manipulálhatják az adatokat, ami elfogult döntésekhez és pontatlan előrejelzésekhez vezethet.
Elfogultság és átláthatóság	A mesterséges intelligenciában az előítéletesség jellemzően a modellek képzéséhez használt adathalmazokból ered, amelyek akaratlanul is fenntarthatják vagy súlyosbíthatják a meglévő társadalmi előítéleteket. Például bizonyos kiválasztási algoritmusok aránytalanul előnyben részesíthetik a férfi jelölteket, így erősítve a rendszerszintű egyenlőtlenségeket. Ezen túlmenően számos mesterségesintelligencia-rendszer, különösen a mélytanulási modellek „fekete doboz" jellege tovább súlyosbítja ezt a problémát. Ezek a modellek gyakran egyértelmű magyarázat nélkül működnek, ami aláássa a bizalmat, és súlyos következményekkel járhat olyan kritikus területeken, mint az orvosi diagnosztika és a büntető igazságszolgáltatás. Az értelmezhetőség hiánya tovább ronthatja az AI-technológiák megbízhatóságába és hatékonyságába vetett bizalmat.
A mesterséges intelligenciára való túlzott támaszkodás	A mesterséges intelligenciával működő információbiztonsági rendszerekre való túlzott támaszkodás jelentős kockázatokkal járhat. A mesterséges intelligencia előrejelző képességeit természetüknél fogva korlátozzák azok az adatok, amelyeken betanítják őket; következésképpen ezek a rendszerek nehezen tudják azonosítani a nulladik napi támadásokat vagy a nem hagyományos fenyegetéseket, így a szervezetek sebezhetővé válnak. Ez a függőség a biztonság illúzióját is keltheti, ami a kritikus elemző és problémamegoldó készségek elvesztéséhez vezethet.
Automatizált rosszindulatú programok létrehozása és a mesterséges intelligencia által vezérelt rosszindulatú programok	A generatív mesterségesintelligencia-eszközök megjelenése jelentősen átalakította a szoftverfejlesztést. Ezek az innovációk azonban potenciális kockázatokat is rejtenek magukban, többek között a rosszindulatú programok létrehozásának automatizálását. Emellett a mesterséges intelligencia által vezérelt rosszindulatú szoftverek gépi tanulási algoritmusokat vehetnek igénybe a felderítési mechanizmusokhoz való alkalmazkodásra és azok megkerülésére, olyan technikákat használva, mint a generatív ellenséges hálózatok és a természetes nyelvi feldolgozás. Ez a képesség lehetővé teszi a támadók számára, hogy pontosan célzott támadásokat hajtsanak végre, elemezzék áldozataik viselkedését és szimulálják a legitim felhasználói műveleteket, ezzel megnehezítve a felderítési erőfeszítéseket.

Veszély, sérülékenység	Jellemző
Nem biztonságos API-végpontok a mesterséges-intelligencia-rendszerekben	A mesterségesintelligencia-rendszerekben a nem biztonságos API-végpontok komoly biztonsági kihívást jelentenek. A támadók kihasználhatják ezeket a sebezhetőségeket, hogy jogosulatlan hozzáférést szerezzenek, rosszindulatú bemeneteket vezessenek be, vagy megzavarják az üzemeltetési folyamatokat. A nem megfelelően védett API-ok akadálytalan hozzáférést biztosíthatnak a támadóknak, lehetővé téve számukra, hogy káros bemeneteket juttassanak be, vagy megkerüljék a hitelesítési mechanizmusokat, ezáltal érzékeny információkhoz jussanak. Az ilyen kihasználások személyes adatokhoz való jogosulatlan hozzáférést, szolgáltatásmegtagadási támadásokat vagy a mesterséges intelligencia kimeneteinek szándékos manipulálását eredményezhetik rosszindulatú célok érdekében.
Titkosítás hiánya az adatátvitel során	A mesterségesintelligencia-rendszerekben az adatátvitel során a titkosítás hiánya hatalmas kockázatot jelent az adatbiztonságra nézve, mivel megkönnyíti a támadásokat és aláássa a bizalmasságot. Titkosítás hiányában az adatok az adatátvitel során lehallgatásra, manipulációra és jogosulatlan hozzáférésre válnak fogékonnyá. A támadók támadásai kihasználják ezt a sebezhetőséget, és a titkosítatlan átviteleket lehallgatva jogtalanul szereznek meg érzékeny információkat. A rosszindulatú szereplők manipulálhatják a lehallgatott adatokat, kártékony utasításokat adhatnak, vagy megváltoztathatják a válaszokat, ezáltal veszélyeztetve az MI-rendszerek sértetlenségét.

Forrás: gov.uk: *Cyber Security Risks to Artificial Intelligence,* 2024

A mesterséges intelligenciára vonatkozó veszélyek és sérülékenységek kezelése összetett feladat, amely multidiszciplináris megközelítést igényel. A veszélyek kezelése több szinten történhet, ideértve a technológiai fejlesztéseket, a szabályozási intézkedéseket és a szervezeti stratégiákat. Technológiai szinten kiemelt jelentősége van az adatok titkosításának, amely megakadályozza az információkhoz való illetéktelen hozzáférést és azok manipulációját. A biztonságos API-végpontok kialakítása és az erős hitelesítési mechanizmusok alkalmazása szintén alapvető fontosságú a rendszerek védelme érdekében. Az MI-modellek robusztusságának növelése érdekében olyan algoritmusokat kell fejleszteni, amelyek ellenállnak a bemeneti adatok manipulációjának, például az ellenséges támadásoknak. A szabályozási intézkedések között szerepel az MI-rendszerek globális szabványosítása, amely meghatározza a biztonsági követelményeket és az adatok kezelésére vonatkozó irányelveket. Az átláthatóság növelése érdekében az MI fejlesztőinek biztosítaniuk kell, hogy a modellek működése érthető és értelmezhető legyen. Az adatvédelmi szabályozások szigorítása szintén elengedhetetlen az érzékeny adatok védelméhez. Szervezeti szinten a munkavállalók képzése és a kiberbiztonsági tudatosság növelése kiemelt fontosságú. Emellett

a rendszeres biztonsági auditok és kockázatelemzések lehetővé teszik a gyenge pontok azonosítását és a védekezési intézkedések hatékonyságának javítását.

Az MI-rendszerek védelmében a megelőzés is kiemelt szerepet játszik, amelylyel növelhető a biztonsági intézkedések hatékonysága. A támadások kivédése érdekében az MI-rendszereket proaktívan kell fejleszteni, hogy előre lássák és azonosítsák a potenciális fenyegetéseket. A multifaktoros hitelesítés szigorúbb ellenőrzési mechanizmusokat kínál az MI-rendszerekhez való hozzáférés szabályozására. Az ellátási lánc védelme szintén elengedhetetlen a rendszerek integritásának megőrzése érdekében. Emellett a folyamatos kutatás és fejlesztés hozzájárulhat az új fenyegetések gyors azonosításához és kezeléséhez.

Összefoglalás

A fejezet részletesen vizsgálja a digitális államot érintő biztonsági kihívásokat, valamint azokat az intézkedéseket, amelyek nélkülözhetetlenek a kiberbiztonság és az információbiztonság megőrzéséhez. Fontos megjegyezni, hogy noha ez a két fogalom gyakran összemosódik, eltérő célokat és tevékenységeket takar. Az információbiztonság a bizalmas jellegre, a sértetlenségre és az adatok rendelkezésre biztosítására összpontosít különböző formákban és környezetekben, míg a kiberbiztonság kifejezetten a digitális térben található rendszerek és adatok védelmét célozza, különös tekintettel az internetalapú fenyegetésekre. A fejezet továbbá vizsgálja a szabályozási keretrendszert Magyarországon és nemzetközi szinten. Magyarországon a 2013. évi L. törvény határozza meg a kibervédelem és a kiberbiztonság fogalmát. Az előbbi a fenyegetésekkel szembeni védelemre vonatkozik, míg az utóbbi a politikai, jogi, gazdasági és technikai intézkedések folyamatos végrehajtását jelenti a kockázatok csökkentése érdekében. Az Európai Unió eltérő megközelítést alkalmaz, mivel a kiberbiztonságot olyan tevékenységként értelmezi, amely a polgári és a katonai alkalmazásokat egyaránt érinti. A digitális állam fenntartható működéséhez elengedhetetlen az információbiztonság három alapelvének – a bizalmasság, a sértetlenség és a rendelkezésre állás, azaz a CIA-elv – fenntartása. A bizalmasság biztosítja, hogy az adatok kizárólag arra jogosult személyek számára legyenek elérhetők, míg a sértetlenség az adatok pontosságát és következetességét garantálja. A rendelkezésre állás szavatolja, hogy a rendszerek és az adatok a jogosult felhasználók számára szükség esetén hozzáférhetők legyenek. A fejezet példákat mutat be az ezen célokat fenyegető

támadásokra, mint például jelszólopás, adatmanipuláció, szolgáltatásmegtagadásos támadások és az infrastruktúra túlterhelése.

A rendszerek sérülékenysége különösen nagy kockázatot jelent mind az információbiztonság, mind a kiberbiztonság szempontjából, mivel a támadók gyakran ezeket használják ki információk megszerzésére, rendszerek manipulálására vagy működésük megzavarására. A hálózati, szoftver- és hardvergyengeségeken túl kiemelt figyelmet kapnak a „nulladik napi" támadások, amelyek korábban nem ismert hibákat céloznak meg. Az Open Web Application Security Project (OWASP) Top 10-es listája a webalkalmazások legkritikusabb sérülékenységeit sorolja fel, például az elégtelen naplózást, a kódinjektálást, az érzékeny adatok védelmének hiányát és a gyenge hitelesítési mechanizmusokat. A fejezet továbbá hangsúlyozza a megelőző és védekező intézkedések fontosságát. Az adatok titkosítása, a többfaktoros hitelesítés, a hozzáférési jogosultságok szigorú kezelése, valamint a rendszeres tesztelés és frissítés kulcsfontosságú a digitális állam biztonságának fenntartásához. Ezenkívül az oktatás és a tudatosság szintén kritikus elemek, amelyek lehetővé teszik a szervezetek tagjai számára a kiberbiztonsági fenyegetések felismerését és kezelését. A rendszeres adatmentések és folyamatos frissítések további biztosítékként szolgálnak a rendszerek és az adatok helyreállításához egy támadás esetén.

Összefoglalva, a fejezet megállapítja, hogy a digitális állam biztonságának szavatolása nem csupán technikai kérdés, hanem jelentős jogi és etikai kötelezettség is. Az állami vezetőknek, vállalatoknak és intézményeknek felelősséget kell vállalniuk az általuk kezelt rendszerek és adatok védelméért. A kiberbiztonság folyamatos fejlesztése és a fenyegetésekkel szembeni proaktív védekezés elengedhetetlen a digitális állam hatékony működéséhez, ezáltal biztosítva a polgárok, a gazdaság és a társadalom jólétét.

Felhasznált irodalom

Törvények, rendeletek, egyéb kormányzati és uniós dokumentumok

346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról

1404/2017. (VI. 28.) Korm. határozat a Digitális Nemzet Fejlesztési Program megvalósítása során elkészült Közgyűjteményi Digitalizálási Stratégiáról

1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről

1486/2015. (VII. 21.) Korm. határozat a Digitális Nemzet Fejlesztési Program megvalósításával kapcsolatos aktuális feladatokról, valamint egyes kapcsolódó kormányhatározatok módosításáról

1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról

1491/2016. (IX. 15.) Korm. határozat a digitális termékek és szolgáltatások exportjának növeléséről, Magyarország Digitális Exportfejlesztési Stratégiájáról

1536/2016. (X. 13.) Korm. határozat a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról

1858/2016. (XII. 27.) Korm. határozat a hazai innovatív vállalkozói környezet fejlesztéséről, a feltörekvő digitális vállalkozások versenyképességének javításáról és Magyarország Digitális Startup Stratégiájáról

2001. évi LXIV. törvény a kulturális örökség védelméről

2009. évi CLV. törvény a minősített adat védelméről

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai digitális egységes piaci

stratégia, COM/2015/0192 végleges (2015. május 6.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52015DC0192
COM (2020) 712: Javaslat: Az Európai Parlament és a Tanács rendelete a határokon átnyúló polgári és büntetőeljárásokban történő kommunikációra szolgáló számítógépes rendszerről (e-CODEX rendszer) és az (EU) 2018/1726 rendelet módosításáról
Digitális Jólét Program 2.0 stratégiai tanulmány (2017). Online: https://digitalisjoletprogram.hu/files/58/f4/58f45e44c4ebd9e53f82f56d5f44c824.pdf
Digitális Jólét Program: *DAS – Magyarország Digitális Agrár Stratégiája* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/das-magyarorszag-digitalis-agrar-strategiaja
Digitális Jólét Program: *Digitális adócsökkentés* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-adocsokkentes
Digitális Jólét Program: *Digitális Fogalomtár* (2019. december 10.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-fogalomtar
Digitális Jólét Program: *Digitális Jólét Hitelprogram* (2018. szeptember 8.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-jolet-hitelprogram
Digitális Jólét Program: *Digitális Jólét Pénzügyi Védjegy* (2020. november 24.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-jolet-penzugyi-vedjegy
Digitális Jólét Program: *Digitális Jólét Tőkeprogram* (2019. december 10.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-jolet-tokeprogram
Digitális Jólét Program: *Digitális Jólét WiFi* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-jolet-wifi
Digitális Jólét Program: *Digitális közigazgatás* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-kozigazgatas
Digitális Jólét Program: *Digitális Sport Tudásközpont* (2021. augusztus 15.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-sport-tudaskozpont
Digitális Jólét Program: *Digitális tudásfejlesztés* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digitalis-tudasfejlesztes
Digitális Jólét Program: *DigKomp, Digitáliskompetencia-keretrendszer* (2019. december 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/digkomp
Digitális Jólét Program: *DJP Lab* (2019. december 10.). Online: https://digitalisjoletprogram.hu/hu/tartalom/djp-lab
Digitális Jólét Program: *DMP – Digitális Munkaerő Program* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/dmp-digitalis-munkaero-program
Digitális Jólét Program: *Fintech Stratégia* (2020. október 28.). Online: https://digitalisjoletprogram.hu/hu/tartalom/fintech-strategia

Digitális Jólét Program: *Ipar 4.0.* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/ipar-40

Digitális Jólét Program: *Mesterséges Intelligencia Koalíció* (2019. július 14.). Online: https://digitalisjoletprogram.hu/hu/tartalom/mesterseges-intelligencia-koalicio

Digitális Jólét Program: *Mobilinternet Hálózatfejlesztés* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/mobilinternet-halozatfejlesztes

Digitális Jólét Program: *Okos Város – Smart City* (2019. január 19.). Online: https://digitalisjoletprogram.hu/hu/tartalom/okos-varos-smart-city

Digitális Magyarország Ügynökség: *Nemzeti Digitális Állampolgárság Program* (2024. december). Online: https://www.dmu.gov.hu/documents/prod/DMU_nemzeti_digitalis_allampolgarsag_program_2022.pdf

Digitális Munkaerő Program stratégiai dokumentum (2018). Online: https://digitalisjoletprogram.hu/files/2e/86/2e865bc650f57539da2dbccf7b169eda.pdf

Az Európai Parlament és a Tanács 1301/2013/EU rendelete (2013. december 17.) az Európai Regionális Fejlesztési Alapról és a „Beruházás a növekedésbe és munkahelyteremtésbe" célkitűzésről szóló egyedi rendelkezésekről, valamint az 1080/2006/EK rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács 1303/2013/EU rendelete (2013. december 17.) az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alapra, a Kohéziós Alapra, az Európai Mezőgazdasági Vidékfejlesztési Alapra és az Európai Tengerügyi és Halászati Alapra vonatkozó közös rendelkezések megállapításáról, az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alapra és a Kohéziós Alapra és az Európai Tengerügyi és Halászati Alapra vonatkozó általános rendelkezések megállapításáról és az 1083/2006/EK tanácsi rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács 1304/2013/EU rendelete (2013. december 17.) az Európai Szociális Alapról és az 1081/2006/EK tanácsi rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)

Az Európai Parlament és a Tanács (EU) 2021/523 rendelete (2021. március 24.) az InvestEU program létrehozásáról és az (EU) 2015/1017 rendelet módosításáról

Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2021/695 rendelete (2021. április 28.) a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról, továbbá az 1290/2013/EU és az 1291/2013/EU rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács Rendelete (2021. június 1.) az Európai Hálózatfinanszírozási Eszköz létrehozásáról, valamint az 1316/2013/EU és a 283/2014/EU rendelet hatályon kívül helyezéséről (COM/2018/438 végleges)

Kormányzati Informatikai Fejlesztési Ügynökség: *Szupergyors Internet Program (SZIP)* (2019. október 11.) Online: https://kifu.gov.hu/szip

Közgyűjteményi Digitalizálási Stratégia (2017–2025), 2017

Magyarország Digitális Agrár Stratégiája 2019–2022 (2019). Online: https://digitalisjoletprogram.hu/files/24/2e/242e263bd2b441f6f30cf400e06e1e4a.pdf

Magyarország Digitális Exportfejlesztési Stratégiája (2016). Online: https://digitalisjoletprogram.hu/files/a2/da/a2da4ddf80fe2c173c7a8d22d833e5cc.pdf

Magyarország Digitális Gyermekvédelmi Stratégiája (2016). Online: https://digitalisjoletprogram.hu/files/b9/55/b955b52770e659680b4e537e84df906b.pdf

Magyarország Digitális Oktatási Stratégiája (2016). Online: https://digitalisjoletprogram.hu/files/55/8c/558c2bb47626ccb966050debb69f600e.pdf

Magyarország Digitális Startup Stratégiája (2016). Online: https://digitalisjoletprogram.hu/files/51/80/518082ba18acf5b5d4e582f2969d4501.pdf

Magyarország Mesterséges Intelligencia Stratégiája 2020–2030 (2020). Online: https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf

MSZ ISO 27001:2014, Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

Nemzeti Digitalizációs Stratégia 2021–2030 (2020). Budapest, Innovációs és Technológiai Minisztérium – Belügyminisztérium, 2020. Online: https://2015-2019.kormany.hu/download/f/58/d1000/NDS.pdf

Nemzeti Infokommunikációs Stratégia 2014–2020 (2014). Online: https://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf

A Tanács (EU) 2018/1488 rendelete (2018. szeptember 28.) az európai nagy teljesítményű számítástechnika közös vállalkozás létrehozásáról

Nyomtatott és internetes források

Abdullayeva, Fargana: Cyber Resilience and Cyber Security Issues of Intelligent Cloud Computing Systems. *Results in Control and Optimization,* 12. (2023). Online: https://doi.org/10.1016/j.rico.2023.100268

András Ferenc: A fakenews igazságértéke és megértése. In Garaczi Imre (szerk.): *Az életminőség-fejlesztés új paradigmái a 21. században.* Veszprém, Veszprémi Humán Tudományokért Alapítvány, 2020. 164–174. Online: https://tab.mta.hu/files/5116/1113/9431/Eletminoseg_kotet.pdf

Baitha, Anuj Kumar – Smitha Vinod: Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology,* 7. (2018), 2.6. 193–198. Online: http://dx.doi.org/10.14419/ijet.v7i2.6.10566

Bányász Péter: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77. Online: http://real.mtak.hu/94335/1/EPA02538_nemzetbiztonsagi_szemle_2018_01_059-077.pdf

Bányász Péter: *Közösségi média és közszolgálat.* Budapest, NKE Közigazgatási Továbbképzési Intézet, 2020. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16210/Kozossegi%20media%20es%20kozszolgalat.pdf?sequence=1

Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37. Online: http://real.mtak.hu/105878/1/01_Banyasz_Bota_Csaba_A_social_engineering.pdfsequence22

Beláz Annamária: A digitális állam információbiztonsága: kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban. *Bánki Közlemények,* 1. (2018), 3. 56–60. Online: http://real.mtak.hu/86861/1/bel%C3%A1z-digit%C3%A1lis%20%C3%A1llam%20inform%C3%A1ci%C3%B3biztons%C3%A1ga-kock%C3%A1zatmenedzsment.pdf

Berger, Harel – Amit Z. Dvir – Moti Geva: A Wrinkle in Time: A Case Study in DNS Poisoning. *International Journal of Information Security,* 20. (2021), 3. 313–329. Online: https://doi.org/10.1007/s10207-020-00502-x

Bodó Attila Pál – Cser Orsolya Anikó – Gyaraki Réka Eszter – Kaczur Gábor – Lattmann Tamás – Solymos Ákos – Szabó Zsolt Mihály – Tikos Anita – Váczi Dániel – Zámbó Nóra: *Célzott kibertámadások.* Budapest, NKE, 2018. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11181/EIB2018_50_C%C3%A9lzott%20kibert%C3%A1mad%C3%A1sok_imprim%C3%A1lt.pdf?sequence=1&isAllowed=y

CDNetworks: *How to Stop a DDoS Attack & Protect Your Business* (2020. november 30.). Online: www.cdnetworks.com/cloud-security-blog/tips-to-protect-your-business-from-ddos-attacks/

Cirlig, Carmen-Cristina: *Cyber Defence in the EU: Preparing for Cyber Warfare?* EPRS_BRI(2014)542143, European Parliamentary Research Service, 2014. Online: www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

Dezső Mária – Fűrész Klára – Kukorelli István – Papp Imre – Sári János – Somody Bernadette – Szegvári Péter – Takács Imre: *Alkotmánytan I. Alapfogalmak, alkotmányos intézmények*. Budapest, Osiris Kiadó, 2007.

Erdősi Péter Máté – Solymos Ákos: *IT biztonság közérthetően*. Budapest, Neumann János Számítógép-tudományi Társaság, 2019.

Európai Bizottság: *Kiválóság és bizalom a mesterséges intelligencia terén* (é. n.). Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_hu#a-mestersges-intelligencia-s-az-eu-szmokban

European Commission: Hungary 2024 Digital Decade Country Report (2024). Online: https://digital-strategy.ec.europa.eu/en/factpages/hungary-2024-digital-decade-country-report

European Commission: *Digital Public Services for Businesses in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=e_gov_ebus_new&indicatorGroup=egovernment&breakdown=e_gov_scope_2_new&period=2023&unit=egov_score&country=EU,HU

European Commission: *Doing an Online Course in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_iuolc&indicatorGroup=internet-services&breakdown=ind_total&period=2023&unit=pc_ind&country=EU,HU

European Commission: *Enterprise Provided Training to Their Personnel to Develop/Upgrade Their ICT Skills in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=e_itt2&indicatorGroup=ict-specialist&breakdown=ent_all_xfin&period=2022&unit=pc_ent&country=EU,HU

European Commission: *Enterprises Employing ICT Specialists in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=e_itsp2&indicatorGroup=ict-specialist&breakdown=ent_all_xfin&period=2022&unit=pc_ent&country=EU,HU

European Commission: *Households with Access to the Internet at Home in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=h_iacc&indicatorGroup=internet-usage&breakdown=hh_total&period=2023&unit=pc_hh&country=EU,HU

European Commission: *Individuals Interacting Online with Public Authorities in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_iugov12&indicatorGroup=egovernment&breakdown=ind_total&period=2021&unit=pc_ind_ilt12&country=EU,HU

European Commission: *Individuals Submitting Completed Forms to Public Authorities in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_igov12rt&indicatorGroup=egovernment&breakdown=ind_total&period=2021&unit=pc_ind&country=EU,HU

European Commission: *Individuals Who Have Never Used the Internet in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_iux&indicatorGroup=internet-usage&breakdown=cc_for&period=2023&unit=pc_ind&country=EU,HU

European Commission: *Key Indicators of the European Information Society* (2024. november 20.). Online: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_ indicators/indicators

European Commission: *Looking for Information about Goods and Services Online in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_iuif&indicatorGroup=internet-services&breakdown=y16_24&period=2023&unit=pc_ind&country=EU,HU

European Commission: *Next Generation Access (NGA) Broadband Coverage/Availability* (as a % of Households) (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=bb_ngacov&indicatorGroup=broadband&breakdown=total_pophh&period=2022&unit=pc_hh_all&country=EU,HU

European Commission: *Persons Employed Using Computers with Access to the Web at Work (Business Sector) in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=p_iuse&indicatorG-

roup=ict-specialist&breakdown=ent_all_xfin&period=2022&unit=pc_emp&country=EU,HU

European Commission: *Rural Fixed Very High Capacity Network (VHCN) Coverage in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=rid_c_vhcnc&indicatorGroup=rid&breakdown=hh_deg3&period=2021&unit=pc_hh_all&country=EU,HU

European Commission: *Telephoning or Video Calls (via Webcam) over the Internet in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_iuph1&indicatorGroup=internet-services&breakdown=ind_total&period=2023&unit=pc_ind&country=EU,HU

European Commission: *Using Online Banking in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=i_iubk&indicatorGroup=internet-services&breakdown=ind_total&period=2023&unit=pc_ind&country=EU,HU

European Commission: *Digital Government Benchmark. Study on Digital Government Transformation.* European Union, 2018. Online: https://joinup.ec.europa.eu/sites/default/files/document/2018-10/330046042JRC_DigitalGovernmentBenchmark_FinalReport%20v2.0_DigGovSection.pdf

European Commission: *The 2019 EU Justice Scoreboard.* European Union, 2019. Online: https://ec.europa.eu/info/sites/info/files/justice_scoreboard_2019_en.pdf

European Commission: *Persons Employed with ICT Specialist Skills (Broad Measure) in the European Union and Hungary* (2024. november 20.). Online: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=ict_spec3_broad&indicatorGroup=ict-specialist&breakdown=total&period=2023&unit=th_ind&country=EU,HU

Fortinet: *Eavesdropping Definition: What Is An Eavesdropping Attack?* (2021. május 7.). Online: www.fortinet.com/resources/cyberglossary/eavesdropping

Gadget-info: *Difference Between E-government* (2019). Online: https://gadget-info.com/difference-between-e-government

Gál András Levente: *A polgárokra fókuszáló patrióta közadat-politikára van szükség* (2020. március 12.). Online: https://digitalisjoletprogram.hu/hu/hirek/a-polgarokra-fokuszalo-patriota-kozadat-politikara-van-szukseg

Gov.uk: *Cyber Security Risks to Artificial Intelligence* (2024. május 15.). Online: https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence

Grimmick, Robert: *ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks* (2021. április 27.). Online: www.varonis.com/blog/arp-poisoning/

Hírközlési és Informatikai Tudományos Egyesület: *Fogalomtár* (é. n.). Online: www.fogalomtar.hte.hu/

Hitachi Systems Security: *10 Ways Businesses Can Prevent Social Engineering Attacks* (2019. október 3.). Online: https://hitachi-systems-security.com/10-ways-businesses-can-prevent-social-engineering-attacks/

Horváth Gábor: A Digitális Európa Program és a BME VIK. *Híradástechnika,* 75. (2020), 1. 2–5.

HUNCERT: *Cross Site Scripting (XSS)* (2021. április 18.). Online: www.cert.hu/cross-site-scripting-xss#tip

I4.0 NTP: *Az Ipar 4.0 Nemzeti Technológiai Platform Szövetség* (2021. április 15.). Online: www.i40platform.hu/hu/szervezet

IFKA: *Ipar 4.0 fogalomtár* (2020. október 22.). Online: www.ipar4.hu/page/tudasbazis-ipar-4-0-fogalomtar

ISO/IEC 27032:2012 Information Technology – Security Techniques – Guidelines for Cybersecurity

ITU-T X.1205: *Overview of Cybersecurity* (2008). Online: www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Izquierdo, Robert: *5 Ways to Prevent a Man-in-the-Middle Cyberattack* (2021. február 9.). Online: www.fool.com/the-blueprint/mitm/

Kiprin, Borislav: *What is Insecure Deserialization and How to Prevent It* (2021. április 2.). Online: https://crashtest-security.com/insecure-deserialization/

Kofod, Andy: *OWASP Top 10 for Developers: Insufficient Logging and Monitoring* (2021. március 15.). Online: https://dev.to/leading-edje/owasp-top-10-for-developers-insufficient-logging-and-monitoring-41oa

Kormányzati Informatikai Fejlesztési Ügynökség: *A KIFÜ lett a jogutódja a Nemzeti Információs Infrastruktúra Fejlesztési Intézetnek* (2020. szeptember 19.). Online: https://kifu.gov.hu/content/kif%C3%BC-lett-jogut%C3%B3dja-nemzeti-inform%C3%A-1ci%C3%B3s-infrastrukt%C3%Bara-fejleszt%C3%A9si-int%C3%A9zetnek%C2%A0

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus Kiadó, 2018. Online: www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf

Kudkar, Isha: *OWASP: Sensitive Data Exposure Attacks* (2021. január 24.). Online: https://medium.com/shallvhack/owasp-sensitive-data-exposure-attacks-7ef41e6b4a59

Kudkar, Isha: *OWASP: XML External Entities Attacks* (2021. február 13.). Online: https://medium.com/shallvhack/owasp-xml-external-entities-attacks-741432591ad1

László Gábor: *Kockázatértékelés, kockázatmenedzsment.* Budapest, NKE, 2014. Online: https://lipusz.hu/pedagogia_tanulas/nke_eiv/kockazatertekeles-kockazatmenedzsment.original.pdf

Lawson, Finidi: *How to Protect Your PC and Data Against Backdoor Attacks?* (2021. április 13.). Online: www.auslogics.com/en/articles/how-to-avoid-backdoor-attacks/

Lexiq: *Backdoor* (2020. április 23.). Online: https://lexiq.hu/backdoor

Lexiq: *Deepfake* (2020. szeptember 21.). Online: https://lexiq.hu/deepfake

Maayan, Gilad David: *How to Prevent and Detect APT Attacks* (2020. április 9.). Online: https://hakin9.org/how-to-prevent-and-detect-apt-attacks/

Machnak, Amy: *Session Hijacking: What Is a Session Hijacking and How Does It Work?* (2021. május 6.). Online: https://us.norton.com/internetsecurity-id-theft-session-hijacking.html

Maydon, Thomas: *The 4 Types of Data Analytics* (2017. július 4.). Online: www.kdnuggets.com/2017/07/4-types-data-analytics.html

McAfee: *Mik azok a kártevő programok?* (2021. szeptember 1.). Online: www.mcafee.com/hu-hu/antivirus/malware.html

MeH ITB 12. számú ajánlás. Informatikai Rendszerek Biztonsági Követelményei

Misuraca, Gianluca – Egidijus Barcevičius – Cristiano Codagnone: *Exploring Digital Government Transformation in the EU – Understanding Public Sector Innovation in a Data-Driven Society.* EUR 30333 EN. Luxembourg, Publications Office of the European Union, 2020. Online: http://dx.doi.org/10.2760/480377

Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, NKE, 2014. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y

Munk Sándor: Kiberbiztonsági szervezetek közötti interoperábilis információcsere-megoldások. *Hadmérnök,* 13. (2018), 4. 315–328. Online: http://hadmernok.hu/183_32_munk.pdf

N-able: *How to Prevent DNS Poisoning* (2019. június 10.). Online: www.n-able.com/blog/what-is-dns-poisoning

NATO Security Policy, C-M(2002)49, Security Within the North Atlantic Treaty Organization (NATO), Enclosure "F", INFOSEC (NU), 2020. Online: www.nbf.hu/docs/C-M(2002)49-REV1.pdf

Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete: *Fehér Könyv a nemzeti adatpolitikáról.* Budapest, Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, 2016. Online: www.magyary.hu/wp-content/uploads/2019/09/Adatpolitikai_feher_konyv_201608.pdf

OECD: *Digital Security and Resilience in Critical Infrastructure and Essential Services.* OECD Digital Economy Papers, No. 281. Paris, OECD Publishing, 2019. Online: https://doi.org/10.1787/a7097901-en

OECD: *Going Digital Integrated Policy Framework.* OECD Digital Economy Papers, No. 292. Paris, OECD Publishing, 2020. Online: https://doi.org/10.1787/dc930adc-en

OECD: *OECD Digital Economy Outlook 2020.* Paris, OECD Publishing, 2020. Online: https://doi.org/10.1787/bb167041-en

OECD: *Recommendation of the Council on Digital Government Strategies, OECD/LEGAL/0406.* 2014. Online: www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

OECD: *The Path to Becoming a Data-Driven Public Sector.* Paris, OECD Digital Government Studies, OECD Publishing, 2019. Online: https://doi.org/10.1787/059814a7-en

Oracle: *What is Data Analytics?* (2021. október 11.). Online: www.oracle.com/business-analytics/data-analytics/

ORFK Kommunikációs Szolgálat: *Digitális kártevők és biztonsági mentés* (2021. február 6.). Online: www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag/digitalis-kartevok-es-biztonsagi-mentes

Pšenáková Ildikó: Ne hagyd magad becsapni! *Lélektan és Hadviselés,* 2. (2020), 1. 55–65. Online: http://dx.doi.org/10.35404/LH.2020.1.55

Radhakrishnan, Reshmi: *OWASP Top 10: Security Misconfiguration* (2021. május 12.). Online: www.siemba.io/post/owasp-top-10-security-misconfiguration

Raidman, Dmitry: *Top IoT Threats and How to Avoid the Next Big Breach* (2020. július 19.). Online: www.cybeats.com/blog/top-iot-threats-and-how-to-avoid-the-next-big-breach

Rashid, Sharmin – Subhra Prosun Paul: Proposed Methods of IP Spoofing Detection & Prevention. *International Journal of Science and Research (IJSR), India Online,* 2. (2013), 8. 438–444. Online: www.ijsr.net/archive/v2i8/MTIwMTMxMzA%3D.pdf

Rehrl, Jocken: *Handbook on Cyber Security.* EU publications. Luxembourg, Luxembourg Publications Office of the European Union, 2018. Online: https://op.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1/language-en/format-PDF/source-80572134?fbclid=IwAR2AS5dw8pbwu1OStIg-tMk2immKL-R_0e_LddMU3ejewHLhCuCV6cAYSSw

Savvy Security: *How to Prevent Malware Attacks* (2021. május 28.). Online: https://cheapsslsecurity.com/blog/how-to-prevent-malware-attacks/

Selján Péter – Selján Gábor: Kiberbiztonsági kitekintés. *Nemzet és Biztonság – Biztonságpolitikai Szemle,* 14. (2021), 1. 24–27. Online: https://doi.org/10.32576/nb.2021.1.3

Siemba: *OWASP Top 10: Using Components with Known Vulnerabilities* (2021. május 12.). Online: www.siemba.io/post/owasp-top-10-using-components-with-known-vulnerabilities

Sinha, Preeti – Amit Kumar Rai – Bharat Bhushan: *Information Security Threats and Attacks with Conceivable Counteraction.* Conference: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2020. 1208–1213. Online: https://doi.org/10.1109/ICICICT46008.2019.8993384

Sorbán Kinga: Vírusok és zombik a büntetőjogban: Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res,* 7. (2018), 2. 369–386. Online: http://real.mtak.hu/105339/1/imr-2018-02-08.pdf

Sucuri Guides: *OWASP Top 10 Security Risks & Vulnerabilities* (2021. április 27.). Online: https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2021/

Szádeczky Tamás: *Az IT biztonság szabályozása.* Berlin, GlobeEdit, 2018.

Van Ooijen, Charlotte – Barbara Ubaldi – Benjamin Welby: *A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance.* OECD Working Papers on Public Governance, No. 33. Paris, OECD Publishing, 2019. Online: https://doi.org/10.1787/09ab162c-en

VanVliet, Sami: *What it is IP Spoofing, How to Protect Against It* (2021. február 11.). Online: www.keyfactor.com/blog/what-it-is-ip-spoofing-how-to-protect-against-it/

Von Solms, Basie – Rossouw von Solms: Cybersecurity and Information Security – What Goes Where? *Information and Computer Security,* 26. (2018), 1. 2–9. Online: https://doi.org/10.1108/ICS-04-2017-0025

Welby, Benjamin: *The Impact of Digital Government on Citizen Well-Being.* OECD Working Papers on Public Governance, No. 32. Paris, OECD Publishing, 2019. Online: https://dx.doi.org/10.1787/24bac82f-en

West, Darrell M.: *How to Combat Fake News and Disinformation* (2017. december 18.). Online: www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

Westerlund, Mika: The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review,* 9. (2019), 11. 40–53. Online: http://doi.org/10.22215/timreview/1282

Zsom Brigitta: Az elektronikus közigazgatás és a területi kutatások kapcsolatáról. *Tér és Társadalom,* 28. (2014), 3. 18–31. Online: https://tet.rkk.hu/index.php/TeT/article/download/2598/4750/

Az internetes alkalmazások és szolgáltatások exponenciális növekedésének, a széles körben elterjedt és rohamosan fejlődő okos megoldásoknak, valamint az új típusú e-kormányzatoknak és az ezzel járó digitalizációs eljárásoknak köszönhetően kiemelt figyelmet kell fordítanunk digitális rendszereink védelmére a potenciális veszélyekkel és támadásokkal szemben. A felhasználók és üzemeltetők számára hatalmas kihívást jelent a megfelelő biztonság szavatolása a kibertérben káros tevékenységeket folytató egyénekkel, hacktivistákkal, terroristákkal, továbbá egyéb szervezetekkel szemben.

Jelen kötet célja átfogó képet adni a digitálisállam-koncepció kialakításához és működtetéséhez szükséges eszközök és rendszerek létrejöttének, fejlődésének, továbbá biztonsági kihívásainak és lehetséges megoldásainak területeiről.