Magyar Sándor

A stratégiai gondolkodás szerepe a kiberbiztonságban

Bevezetés

Az élet egyre nagyobb részét támogatják már elektronikus információs rendszerek. Az elektronikus eszközök számának drasztikus növekedése, jelentősége a mindennapi élet során – legyen az a munkában vagy a magánéletben – folyamatosan növekvő tendenciát mutat. A civil szektor mellett a nemzetbiztonsági, honvédelmi és rendvédelmi szervek informatikai rendszerei is jelentős fejlődésen mennek át, reagálva a külvilág változásaira, fejlődésére annak érdekében, hogy a versenyképesség, az eredményesség, valamint a szervezeti célok és alaprendeltetési feladatok ellátásának követelményeit teljesíteni tudják.

A Covid–19-világjárvány is a digitalizáció egyfajta katalizátoraként működött, a *home office*[1] és a távmunka előmozdításával. A jelen és jövő technológiáinak – mint az ötödik generációs (5G) mobilhálózatok, a kvantum-számítástechnika, a mesterséges intelligencia, a gépi tanulás, a drónok, autonóm rendszerek stb. – felhasználása további kitettségeket generál az informatikai rendszerek területén. Az információs technológia folyamatos fejlesztésének, követésének jó példája a nemzeti laboratóriumok[2] létrehozása. A felforgató (diszruptív) technológiák – ahogy már eddig is – beavatkoznak a megszokott tevékenységeinkbe a magasabb szintű szolgáltatások biztosításával.

A szervezetek függősége az informatikai rendszerektől megemelte, átalakította a kibertérben elkövetett támadások, visszaélések számát, amelyeknek a kivitelezései komplexebbé, kifinomultabbá váltak, és ezzel párhuzamosan hatásaik is növekedtek. A magánszektor mellett a létfontosságú rendszerek ellen elkövetett kibertámadások száma szintén emelkedő tendenciát mutat. A támadások besorolása is változhat, erre jó példaként említhető Paul Nakasone[3] tábornok nyilatkozata, aki egy 2021-es interjújában azt mondta: „Hat hónappal ezelőtt a zsarolóvírusok alkalmazását valószínűleg még csak bűncselekménynek neveztük volna, azonban ha az egy egész nemzetre van hatással, mint láttuk, akkor nemzetbiztonsági kérdéssé válik."[4]

A kibertérből érkező fenyegetésekre történő reagálás nem valósulhat meg *ad hoc* módon a következmények kezelésével, hanem nagy figyelmet szükséges fordítani a meg-

[1] A. m. „otthoni iroda" – azaz a munkahely helyett az otthonban történő munkavégzési forma.
[2] A nemzeti laboratóriumokról részletesen lásd Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Nemzeti laboratóriumok bemutatása (2022. június 9.).
[3] Paul Miki Nakasone az Egyesült Államok hadseregének tábornoka, az Egyesült Államok Kiberparancsnokságának (United States Cyber Command) parancsnoka, egyidejűleg a Nemzetbiztonsági Ügynökség (National Security Agency) igazgatója és a Központi Biztonsági Szolgálat (Central Security Service) főnöke.
[4] Nomaan Merchant: General Promises US 'Surge' Against Foreign Cyberattacks. *AP News,* 2021. szeptember 14.

https://doi.org/10.36250/01098_05
https://orcid.org/0000-0002-6085-0598

előzésre is. Ezért a stratégiai gondolkodásnak rendkívül nagy jelentősége van minden szektorban az informatikai rendszerek üzemeltetése, fejlesztése és biztonsága tekintetében. A kiberbiztonság jogszabályi definíciója – „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása”[5] – is megmutatja, mennyi aspektusból lehet megközelíteni a területet, amelynek esetében nem lehet kikerülni az összehangolt, átgondolt lépéseket.

A kiberfenyegetések elleni sikeres fellépés egyik eszköze, hogy tisztában kell lenni stratégiai szinten az információs technológia területét körülvevő környezettel, a kibertér fenyegetéseivel, továbbá azokkal a képességekkel, amelyek esetében meg kell teremteni a feltételeket azok hatékony kezeléséhez.

A kiberbiztonságot érintő nemzeti szintű stratégiák

Magyarország számos legfelsőbb szintű stratégiai dokumentumban szerepelteti a kiberbiztonság feladatait, meghatározza irányait, fejlesztési területeit. Teljes részletezésük meghaladja e fejezet kereteit, továbbá globális kontextusban Kovács László a *Kiberbiztonság és -stratégia* című könyvében részletesen foglalkozott a kérdéssel.[6] Itt csupán a legfontosabb, területtel összefüggő magyarországi stratégiákat emeljük ki, megjelenésük sorrendjében.

Az 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról[7] szól, és foglalkozik Magyarország kiberbiztonsági környezetén túl hazánk kiberbiztonsági értékrendjével, jövőképével, céljaival. A célok eléréséhez szükséges feladatok vonatkozásában számos területet határoz meg stratégiai irányvonalként. Ezeken a területeken az együttműködés, a kormányzati kommunikáció, a szakosított intézmények, a szabályozás, a tudatosítás és a gyermekvédelem is szerepet kap.

A Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról[8] szóló 1838/2018. (XII. 28.) Korm. határozat megállapítja a hálózati és információs rendszerek biztonságára vonatkozó stratégia megalkotásának indokoltságát. Célkitűzéseiként a digitális környezet iránti bizalom erősítését, a digitális infrastruktúra védelmét és a gazdasági szereplők támogatását jelöli meg, tartalmaz továbbá 56 intézkedést, valamint az akkor hatályos jogszabályok alapján a végrehajtásba bevont szereplők jegyzékét és a hozzájuk tartozó stratégiai feladatokat.

[5] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 26. pont.
[6] Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.
[7] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. 1. melléklet: Magyarország Nemzeti Kiberbiztonsági Stratégiája.
[8] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. A stratégia szövegét lásd: A hálózati és információs rendszerek biztonságára vonatkozó Stratégia.

Az 1163/2020. (IV. 21.) Korm. határozattal elfogadott Nemzeti Biztonsági Stratégia[9] a kiberbiztonság területén jelentősen bővült a 2012-es Nemzeti Biztonsági Stratégiához[10] képest, amelyben a kiberbiztonság egy külön pontként szerepel, azonosítva a legfontosabb feladatokat. A 2020-as Nemzeti Biztonsági Stratégia ezzel szemben már a kiemelt biztonsági kockázatok közé sorolja a kormányzati informatikai és létfontosságú rendszerek ellen végrehajtott, jelentős károkat okozó kibertámadásokat, továbbá Magyarország és a magyar állampolgárok kibertérbeli biztonságát alapvető értékként definiálja. Felismeri a felhasználók információbiztonsági tudatosságának alacsony szintjét mint a kiberincidensek kockázatának egyik kulcselemét. A kibertér itt már a szárazföld, a tengerek, a levegő és a világűr mellett külön műveleti térként szerepel, a jövőbeli konfliktusok valószínű helyszíneként említve. A Nemzeti Biztonsági Stratégia „a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges".[11] A kibertérrel kapcsolatban itt is megjelenik a nemzetközi együttműködés, a jogi szabályozások fejlesztése, a kutatás-fejlesztés.

Az 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról megállapítja, hogy a modern konfliktusok már a legtöbb esetben rendelkeznek kiberbiztonsági összetevővel is. Itt szerepel a kibertámadások potenciálja, amely anyagi kár okozásában és a közrend megzavarásában nem marad el a hagyományos fegyvereké-től. A stratégia a 2020-as Nemzeti Biztonsági Stratégiához hasonlóan deklarálja, hogy „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat pedig akár fegyveres támadásnak tekinti, amelyre adott esetben katonai válaszadás is lehetséges".[12]

A szervezeti stratégiaalkotás szerepe a kiberbiztonságban

Az előző fejezetben szereplő nemzeti stratégiák is erőteljesen rávilágítottak az információtechnológia rohamos fejlődésére és a vele együtt növekvő számú és hatású tendenciát mutató fenyegetések kockázataira. Míg korábban egy informatikai rendszernél az üzembiztonság, azon belül a magas rendelkezésre állás volt az elvárás, napjainkban már nem kérdés, hogy a biztonság előtérbe helyezése a cél, amelyet minden rendszerre – a már meglévőkre is – alkalmazni kell. A szervezetek mindennapi életét egyre jobban támogató elektronikus információs rendszerek növekvő kitettséget jelentenek az üzleti folyamatok, szervezeti célok teljesítése során.

[9] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet: *Magyarország Nemzeti Biztonsági Stratégiája.*

[10] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet: *Magyarország Nemzeti Biztonsági Stratégiája.*

[11] 1163/2020. (IV. 21.) Korm. határozat. 1. melléklet, 101. pont.

[12] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról. 1. melléklet: *Magyarország Nemzeti Katonai Stratégiája,* 2/3. bek.

A nemzetbiztonsági, honvédelmi és rendvédelmi szervezetek is egyre több és nagyobb végpontszámú informatikai rendszert használnak a jogszabályokban meghatározott feladataik ellátásához. Az elektronikus ügyintézés, elektronikus irat- és dokumentumkezelés, a különféle adatbázisok használata, a feldolgozandó adatok nagy mennyisége, az adattudomány, a kormányzati célú hálózatok stb. mind-mind alátámasztják a nagymértékű fejlődés tényét és várható fokozódását. Az élet paradoxona, hogy ezen szervezetek esetében az informatika, az információbiztonság, a kiberbiztonság feladatrendszere a szervezet működése szempontjából a támogató szerepkörhöz társul. Ezért a szervezeti célok elérésében a közvetett funkció miatt előfordulhat, hogy a biztonság adott esetben másodlagos prioritást kap.

Az elektronikus közigazgatási projektek költség-haszon elemzése (*cost-benefit analysis,* CBA) is komplex feladat,[13] azonban a kiberbiztonság területén még nehezebbnek mondható. Mint sokan említik, 100%-ban biztonságos rendszer csak végtelen költségvetési forrás esetén lehetséges, azonban amennyiben nem biztosítjuk az erőforrásokat (pénzügyi, humán stb.), könnyen támadás áldozatává válhat a szervezet.

Már az információs technológiától történő ilyen mértékű függés előtt is fontos volt a közép- és hosszú távú előrelátás minden szervezet esetében, azonban az „ipar 4.0”[14] idején még hangsúlyosabbá vált a stratégiai gondolkodás. Ennek jelentőségét az informatikai rendszerek beszerzési és üzemeltetési költségei is jól mutatják.

Minden szervezet fennmaradásához, hatékonyságának növeléséhez szükséges szervezeti (vagy üzleti) stratégiával rendelkezni. Ezen dokumentum részét képezik, egészítik ki a funkcionális stratégiák, úgymint a humán stratégia, a pénzügyi stratégia vagy akár az informatikai stratégia területei. A stratégiák jelentősége, hogy felmérik az aktuális állapotot, meghatározzák az elérni kívánt célt, és hozzárendelik a szükséges lépéseket, feltételeket a célok eléréséhez. A tanulmány következő része egyes funkcionális stratégiákat vizsgál meg a kiberbiztonság oldaláról megközelítve.

A kiberbiztonság kapcsolata a humán stratégiával

A humán stratégia rendkívül fontos eleme a szervezeti stratégiának, és arra szolgál, hogy az emberi tényező megfelelően támogathassa a stratégiai célok elérését. A korábbiakban is említett emelkedő számú és végpontszámú, illetve komplexitású rendszerek kiszolgálásához emberi erőforrásra is szükség van. Ezen a területen stratégiai szinten egyrészt a létszámbővítés hozhat megfelelő eredményt, másrészt a pályamodellek, az oktatási tervek, elgondolások megvalósítása.

[13] A Közigazgatási Informatikai Bizottság 29. számú ajánlása: Az elektronikus közigazgatási projektek költség-haszon elemzéséről. *Magyarország.hu,* 2013. október 3.

[14] „Az ipar 4.0 a termelési folyamatok technológiai alapú szervezését jelenti, amelyben az eszközök önállóan kommunikálnak egymással az értéklánc mentén.” (Jan Smit – Stephan Kreutzer – Carolin Moeller – Malin Carlberg: Industry 4.0. *Study for the ITRE Committee. 2016.* (h. n.), Policy Department A: Economic and Scientific Policy, 2016. 20.

A humán stratégia kialakítását számos sajátosság nehezíti az informatika, az információbiztonság és a kiberbiztonság területén, az alábbi körülmények miatt:

- A munkaerő piaci értéke – éppen az elektronikus információs rendszereknek a szervezetek eredményességéhez hozzájáruló hozzáadott értéke révén – rendkívül megemelkedett. A nemzetbiztonsági, honvédelmi és rendvédelmi szervezetek esetében nem érdek az, hogy az alkalmazott a munkaerőpiacon fizetett magasabb bérköltségért elhagyja a munkahelyét, egyrészt mivel a feladatrendszerének ellátását pótolni kell, másrészt azon kockázat miatt, amelyet az elektronikus információs rendszerekkel, a szervezettel kapcsolatos ismeretei jelentenek.
- Az életkori, generációs sajátosságok tovább nehezítik – különösen a Z generáció esetében[15] – a munkahelyváltás gyakoriságának kérdéskörét, mivel a nagyobb kihívások, gyorsabb előmenetel más szervezetnél csábítóbb lehet, nem beszélve ezek bérköltségekkel kapcsolatos összefüggéséről.
- Míg egyes szakmai területeken a főiskolákon és egyetemeken elvégzett alap- és mesterképzés, továbbá a belső szakmai tanfolyamok és a munkahelyi tapasztalat elégségesek lehetnek, az informatikai, információbiztonsági területeken mindezek mellett rendkívül magas képzési költségekkel is számolni kell (akár egy ötnapos tanfolyam költsége is meghaladhatja egy főiskolai alapképzés árát).
- Az informatikai, információbiztonsági és kiberbiztonsági munkaerő magas piaci értéke miatti kompenzálás és a támogató területi elhelyezkedés a fizetésben belső feszültségeket okozhat.
- Az információtechnológia területén sok esetben a munkaerőpiacon keresett tudás az alacsonyabb beosztású pozíciókhoz kötődik. Így a vezetővé válással – ami nagyobb fizetést eredményezhet – az eszközöktől való „távolodás" más kompetenciajegyek irányába tolja a munkaerőt, veszítve annak értékességéből.

A képzett, megfelelő képességekkel rendelkező szakemberek szükséges létszámát optimálisan stratégia lefektetésével lehet elérni.

A kiberbiztonság kapcsolata az innovációs stratégiával

Mint a nemzeti stratégiákból kiolvasható, a kibertérből érkező fenyegetések a jövő háborúinak színterét az informatikai rendszerek területére fogják áthelyezni, ezért a szemléletváltás elkerülhetetlen.

Magyarország kutatási, fejlesztési és innovációs stratégiája (2021–2030)[16] a helyzet- és jövőkép mellett a tudástermelés, tudásáramlás és tudásfelhasználás meghatározó

[15] Lukovszki Lívia: Generációk és vállalkozók. *Marketing és Menedzsment,* 49. (2015), 4. 52–63.

[16] Innovációs és Technológiai Minisztérium – Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Magyarország kutatási, fejlesztési és innovációs stratégiája, 2021–2030 (2021. szeptember 3.). Elfogadva az 1456/2021. (VII. 13.) Korm. határozattal.

kérdéseit tisztázza, amelyeket a szervezeteknek eredményességük fenntartása érdekében szükséges átültetniük saját szervezeti stratégiájukba.

A kutatás, a fejlesztés és az innováció a szervezetek jövőbeli fejlődésének hatékony előmozdítója. A korábban említett információtechnológiai fejlődést – beleértve a felforgató technológiákat is – a szervezeteknek követniük kell. Reagálni kell a külső és belső környezet változásaira, adaptálni kell az új eredményeket, proaktívan, szükség szerint „előremenekülve" kell megteremteni a feltételeket a versenyképesség fenntartásához, eléréséhez.

Számos alkalommal fordulhat elő, hogy az informatikai, információbiztonsági, kiberbiztonsági területen nem valamely adott piaci eszközt, rendszert szereznek be – amelynek általában az egyszeri és a folyamatos támogatási költsége rendkívül magas –, hanem a szervezetnél folyó kutatás, fejlesztési munka eredményeként kidolgozott megoldást.

Az informatikai biztonsághoz tartozó tudás felértékelődik, sok esetben paradigmaváltás szükséges a teljesen új fenyegetések kezeléséhez, előtérbe kerülhet a projektszemléletű gondolkodás.

Az innovációs stratégiának – mint funkcionális stratégiának – az informatikai rendszerek esetében illeszkedni kell az információbiztonsági stratégiához.

A kiberbiztonság kapcsolata az informatikai stratégiával

Az informatikai stratégia is a szervezeti stratégia egyik funkcionális eleme, azonban igen szervesen kapcsolódik a kiberbiztonsághoz. Az informatikai stratégia meghatározza a szervezeti célok eléréséhez szükséges fejlesztéseket az IT területén.

Az informatikai stratégia feladata meghatározni azokat a lépéseket, amelyek által a szervezet céljai az informatikai erőforrások felhasználásával minél hatékonyabban elérhetők. Az információs technológia, a felforgató technológiák fejlődési üteme miatt öt évnél hosszabb időre nehéz tervezni. Gondoljunk bele, hogy ennél hosszabb távra történő tervezés esetében miként mutatna a stratégiában a „kor színvonalának megfelelő informatikai eszközök" kifejezés.

A szervezeti stratégiák eléréséhez szükséges az üzleti hatáselemzés, azonosítani kell a kritikus szolgáltatásokat, tisztában kell lenni az ezek leállása nyomán felmerülő károkkal.

Az informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló legjobb gyakorlatokon alapuló *(best practice)* módszertan az ITIL,[17] amely a teljes szolgáltatási életciklus menedzselésében segít, a szolgáltatásstratégia, a szolgáltatástervezés, a szolgáltatáslétesítés és -változtatás, a szolgáltatásüzemeltetés és az állandó szolgáltatásfejlesztés területén.

[17] Information Technology Infrastructure Library – IT-infrastruktúra-könyvtár.

A legjobb gyakorlatokon alapuló módszertan mellett az IT-folyamatok optimalizálásában segíthetnek még a nemzetközi ajánlások is, mint például az ISACA[18] Cobit-ajánlása.[19]

Az informatikai stratégia kialakítása során az elérendő cél esetében az „érettségi" szintnek megfelelően figyelembe kell venni a szervezeti stratégiában meghatározott célokat. A kialakítás során biztosítani kell az állami és önkormányzati szervek elektronikus információbiztonságáról[20] szóló 2013. évi L. törvény (Ibtv.) és végrehajtási rendeleteinek érvényesülését – különös tekintettel az Ibtv.-ben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló BM-rendelet[21] előírásaira.

Az informatikai stratégia megvalósítása során kiemelt jelentősége van a szabályozottságnak, a fejlesztések meghatározott pontjain a biztonsági teszteléseknek és a sérülékenységvizsgálatoknak, amelyeknek meg kell történniük.

Az eszközök, szoftverek fejlesztési problémáinak való kitettség, a folyamatosan megjelenő sérülékenységek mind gyakoribb frissítést igényelnek a fenyegetettségek kiiktatására, ezért az eljárásrendek kialakítása ebben az esetben is nagy hangsúlyt kap.

A fejlesztés során a rendszereket úgy kell kialakítani, hogy – megfelelő naplógyűjtéssel – képesek legyenek támogatni a kiberbiztonsági területet. Ebből a célból az eseménykezelésekhez ki kell alakítani eljárásrendeket a naplóadatok átadására, mivel ezekből a *log*okból lehet meghatározni a fontosabb támadási vektorokat, a kártékony tevékenységhez tartozó indikátorokat (IoC[22]). Ezek az indikátorok lehetnek: vírusszignatúrák, minták, támadó IP-címek, a rosszindulatú fájlok fájlnevei, az elérési útja, mérete, a róluk készült *hash*ek (lenyomatok) stb.

Kiberbiztonsági stratégia

A kiberbiztonsági stratégiák szempontjából rendkívül fontos a PreDeCo-elv[23] területeinek érvényesítése. Ezeket szabályozza az Ibtv. és végrehajtási rendeletei, míg a 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szól, a 271/2018. (XII. 20.) Korm. rendelet pedig az eseménykezelő központok

[18] Information Systems Audit and Control Association – informatikai auditorok nemzetközi szervezete.
[19] Control Objectives for Information and Related Technology – információs és kapcsolódó technológiai kontrollcélkitűzések.
[20] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[21] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
[22] Indicator of Compromise – kompromittálódási mutató, amely egyértelműen azonosítja a kártékony tevékenységet.
[23] *Preventive, detective, corrective* – megelőző, észlelő, korrigáló.

feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól.

Kiberbiztonsági stratégia esetében lényeges a kockázatelemzés oldaláról történő megközelítés, még a stratégia kidolgozásának megkezdése előtt a terület erős és gyenge oldalainak feltérképezése, amihez jó alapot adhat a SWOT-elemzés.[24]

Mint a nemzeti stratégiákban is láthattuk, jelentős szerepet kap a kiberbiztonság területén az együttműködés. A különböző szektorok elektronikus információs rendszereinek nagy hatása lehet más szegmensekre, ezért az együttműködési megállapodások jelentősége felértékelődik. Ezeknek az együttműködéseknek nemzetközi szinten egységesnek kell lenniük, például a jogi fellépések érdekében is.

A kiberbiztonsági stratégia megalkotása elvezethet a szervezetek sajátosságainak újraértékeléséhez. Üzletmenet, üzemeltetés és biztonság egyensúlya, rendszeres újraértékelése, még hangsúlyosabb közös munka lehet szükséges a szakterületeken.

A kibertér fenyegetéseinek elemzése támasztja alá, látja el szükséges információval a kiberbiztonsági területek munkáját, így az elemzések fejlesztésére kiemelt hangsúlyt kell fektetni.

Stratégiai szinten a biztonsági műveleti központ (*security operations center,* SOC) kialakítása kiemelt jelentőségű a kiberbiztonsági eseményekre való időbeni reagálás, illetve ezek megelőzése érdekében. Az észlelést erősíthetik a korai előrejelző és a csapdarendszerek is.

A kibervédelmi gyakorlatok segítenek a résztvevőknek abban, hogy megértsék a súlyos kibertámadások társadalomra gyakorolt hatását, a szövetségesekkel való együttműködésben való jártasság pedig elengedhetetlen egy összetett kibertámadás során. A területen szerepet vállalóknak meg kell érteniük, hogy tudásmegosztással hosszú távon el lehet érni a hátrányos „reaktív" helyzetből a következetesen „proaktív" helyzetbe való elmozdulást.

Összegzés

Minden szervezet számára kiemelten fontos a stratégiai gondolkodás, a szükséges stratégiák lefektetése, mivel azok által lehet a kitűzött célokat hatékonyan megvalósítani. A stratégiaalkotás közben a célok kitűzése, a környezet felmérése, a bejárandó út meghatározása rendkívül fontos, amelyeket a stratégia elfogadása után a hétköznapi tevékenységek közé is szükséges beépíteni.

A stratégiaalkotás szerepe az információtechnológia és a kapcsolódó szakterületek esetében nélkülözhetetlen, amelynek során fontos szerepe van az elérendő célok megvalósíthatóságának, a stratégia érintettekkel történő megismertetésének, a vezetői akaratnak és a környezeti, szervezeti változások követésének, továbbá a stratégia felülvizsgálatának.

A kiberbiztonság a stratégiai gondolkodás szintjén szorosan összefügg más területekkel, amelyekkel a szoros együttműködés nélkülözhetetlen.

[24] *Strengths, weaknesses, opportunities, threats* – erősségek, gyengeségek, lehetőségek, fenyegetések.

Felhasznált irodalom

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet: *Magyarország Nemzeti Biztonsági Stratégiája*

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet: *Magyarország Nemzeti Biztonsági Stratégiája*

1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról. 1. melléklet: *Magyarország Nemzeti Katonai Stratégiája*

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

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

A hálózati és információs rendszerek biztonságára vonatkozó Stratégia [a Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján]

A Közigazgatási Informatikai Bizottság 29. számú ajánlása: Az elektronikus közigazgatási projektek költség-haszon elemzéséről. *Magyarország.hu,* 2013. október 3. Online: https://regi.ugyintezes.magyarorszag.hu/dokumentumok/kib29.pdf

Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Lukovszki Lívia: Generációk és vállalkozók. *Marketing és Menedzsment,* 49. (2015), 4. 52–63. Online: https://journals.lib.pte.hu/index.php/mm/article/view/911/782

Magyarország kutatási, fejlesztési és innovációs stratégiája (2021–2030) [Elfogadva az 1456/2021. (VII. 13.) Korm. határozattal]

Merchant, Nomaan: General Promises US 'Surge' Against Foreign Cyberattacks. *AP News,* 2021. szeptember 14. Online: https://apnews.com/article/technology-europe-national-security-c4c8dace4708035d059be0fcd10e9e18

Smit, Jan – Stephan Kreutzer – Carolin Moeller – Malin Carlberg: *Industry 4.0. Study for the ITRE Committee.* (h. n.), Policy Department A: Economic and Scientific Policy, 2016. Online: www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf