Bányász Péter

# A kiberbiztonság az FMCG-szektorban és a kiskereskedelemben

## Bevezetés

Az új típusú koronavírus okozta globális járványügyi helyzet korábban nem tapasztalt kiberbiztonsági kihívások elé állította az állami és piaci szereplőket egyaránt. Sok szervezetnek szinte egyik napról a másikra kellett átállnia távoli munkavégzésre, illetve kialakítania azt a munkakörnyezetet, ahol a megváltozott körülmények között tudják biztosítani az üzletmenet-folytonosságot. A koronavírus az élet számos területén felgyorsította a digitális transzformációt, rengeteg kisvállalkozásnak kellett átgondolnia üzletpolitikáját. Éttermeknek, kávézóknak, de kocsmáknak is szinte egyik napról a másikra kellett átváltania házhoz szállításra, online rendelés biztosítására. Ez azonban gyakran komolyabb költségvonzattal jár, hiszen meg kell felelni az adatvédelmi és egyéb előírásoknak, ami ingyen nem valósítható meg.

A szervezetek jelentős része azonban nem készült fel megfelelően a digitális transzformációra, és ez természetszerűleg magával hozta a kiberbűncselekmények számának növekedését. A megfelelő és elvárt szintű adat- és kiberbiztonság kialakítása nem olcsó, a szervezetek szeretnek ezeken a kiadásokon spórolni, egészen addig, amíg jelentős kár nem éri őket egy-egy kibertámadás következtében. Mindez olyan nehéz gazdasági körülmények között, mint ami a koronavírus okozta kötelező leállásból fakad, különösen fontos. Jelen tanulmány azokat a kiberbiztonsági kockázatokat vizsgálja, amelyek a gyorsan forgó fogyasztási cikkek és kiskereskedelem viszonyában megjelennek, de nem kizárólagosan e szektor tekintetében fogalmazza meg a következtetéseket. A tanulmány célja, hogy a felhívja a figyelmet a kockázatokra, és olyan megoldási javaslatokat fogalmazzon meg, amelyek segítenek mérsékelni a szervezetek kibertérnek való kitettségét.

https://doi.org/10.36250/01053_11

https://orcid.org/0000-0002-7308-9304

## 1. A kiberbiztonság alapjai

Annak érdekében, hogy a bevezetőben megfogalmazott célokat elérhessem, szükséges a kiberbiztonsággal kapcsolatos főbb fogalmak bemutatása, ugyanis a köznyelvben gyakran tévesen használják a különböző *terminus technikusokat,* ami sokszor a kiberbiztonsággal kapcsolatos attitűdöt is befolyásolja. Laikusok részéről jellemző az a kijelentés, hogy ők nem értenek az informatikához, így a kiberbiztonsággal sem foglalkoznak, hiszen azok műszaki- informatikai kérdések. Megítélésem szerint ez roppant káros „mantra", hiszen, mint a fejezet során remélhetőleg bizonyítjuk, a kiberbiztonság inkább humán terület, mint műszaki-informatikai. Ha pedig ragaszkodunk ezekhez a káros beidegződésekhez, nem fogunk megfelelő szintű védelem kialakítására törekedni.

A fogalmak tisztázásakor az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.) hívjuk segítségül, amelynek bár az FMCG-szektor nem tartozik hatálya alá, a jogszabály mégis a magyarországi információbiztonsági szabályozás alapja, az értelmező rendelkezés résznél szereplő fogalmi meghatározások ily módon általánosnak tekinthetők. Terjedelmi korlátok okán az egyes fogalmakat nem magyarázzuk részletesen, azok az idézett jogszabály értelmező rendelkezéseinél megtalálhatóak – számos egyéb fontos fogalommal együtt.

A kiberbiztonság alapja minden esetben az adat. Gyakran szinonimaként jelenik meg az adat és az információ; nagyon leegyszerűsítve: az információ az értelmezett adat.

Az adatokat elektronikus információs rendszerekben tároljuk, amely meglehetősen tág fogalmat jelöl. Az elektronikus információs rendszer körébe soroljuk az adatok, információk kezelésére használt eszközöket (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárásokat (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

Mindezzel eljutunk az információbiztonsághoz, amely alapvetően egy követelményrendszert takar. Az Ibtv. az információbiztonságot az elektronikus információs rendszer biztonságaként nevesíti: „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása", függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel és milyen adathordozón jelenik meg. Ezt nevezzük CIA-triádnak, ami az adatok bizalmasságát *(C-onfidentiality),* sértetlenségét *(I-ntegrity),* rendelkezésre állását *(A-vailability)* jelenti.

Nem nehéz belátni, hogy a CIA-triád bármely sérülése komoly kockázattal van a szervezetek működésére, hiszen ha e három közül akár egyik is sérül, az megakadályozza a normál üzletmenetet. Ennek igazolására a zsarolóvírusok tekinthetők a legjobb példának. A zsarolóvírus alatt olyan kártékony kódot értünk, amely az elektronikus információs rendszerben tárolt adatokat titkosítja,[1] a feloldásért cserébe pedig meghatározott összegű kriptovalulát követelnek a kiberbűnözők. Azáltal, hogy a rendszerben tárolt adatokat titkosítja a vírus, mind a bizalmassága, mind a sértetlensége, mind a rendelkezésre állás sérül, hiszen a jogosultak nem használhatják fel az adatot, a tartalma nem ellenőrizhető, illetve a rendelkezésre állás sem valósul meg.

2021. március 30-án az Unix, Magyarország legnagyobb autóalkatrész-kereskedőjének informatikai rendszerét fertőzte meg egy zsarolóvírus,[2] amely napokra elérhetetlenné tette a szervezet weboldalát, lehetetlenné téve a megrendeléseket, komoly kiesést okozva a cég üzletmenet-folytonosságában.[3] Az ellátási láncok egymásrautaltságából következően azonban nemcsak az Unix szenvedett el károkat, hanem azok a szervizek is, amelyek vele álltak szerződéses viszonyban.[4]

Mindez elvezet bennünket egy másik káros, de sajnos nagyon élő, a kiberbiztonsággal kapcsolatos tévhithez: én nem vagyok érdekes/értékes, én miért lennék célpont? Az ellátási láncok összetettsége hamar beláttatta a kiberbűnözőkkel, hogy sokszor célszerűbb a gyengén védett beszállítót támadni, és rajta keresztül férni hozzá az egyébként jól védett célpont elektronikus információs rendszeréhez, ahogy ezt a közelmúltban az Apple is megtapasztalta.[5] 2021 áprilisában a tajvani Quanta cégtől loptak el hackerek olyan információkat, amelyek bizonyos Apple-szabadalmakat is tartalmaztak, és licitet hirdettek, hogy

[1] Bányász Péter – Krasznay Csaba: Kiberbiztonsági incidensek a magyar közigazgatásban. In *A Jó Állam mérhetősége III.* Budapest, Dialóg Campus Kiadó, 2019. 249–270.

[2] Dömös Zsuzsanna: Zsarolóvírussal támadták meg az egyik legnagyobb hazai autóalkatrész-kereskedőt. *24.hu,* 2021. április 1.

[3] A szervezet egyébként a kibertámadást követően példamutató kríziskommunikációról tett tanúbizonyságot.

[4] Az ellátási láncok kiberfenyegetettségével kapcsolatban bővebben lásd Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése.* Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673.

[5] Kevin Collier: Hackers Try to Extort Apple after Stealing Files from Manufacturer. *NBC News,* 2021. június 11.

a legtöbbet fizetőknek adják át a megszerzett adatokat.[6] Ez természetesen nem csak kiberbűnözök gyakori eljárása; az ipari kémkedésnek, üzleti hírszerzésnek fontos elemét képezi a behatolás a riválisszervezetek információs rendszereibe, és az azokból való információszerzés. Hírszerzés a kibertérben: misztikusnak tűnhet, és a laikusok rendkívül nagy felkészültséget feltételezhetnek a támadókról, ez azonban újabb mítosz. Számos olyan eszköz és eljárás létezik, amelynek segítségével a kevésbé képzettek is sikeresen hajthatják végre támadásaikat. Az informatikailag kevésbé képzett bűnöző például megvásárolhatja a dark neten azokat a *toolokat,* amelyek pár kattintással elvégzik a támadást, amely lehet például behatolás felhasználói fiókba vagy kártékony kód telepítése más informatikai rendszerbe. Ennél komplexebb alternatíva az úgynevezett *crime as a service,* vagyis a szolgáltatásszerű bűnözés, amely esetében a megrendelő lényegében felbéreli azokat a kiberbűnözőket, akik elvégzik a kívánt támadást. Ez esetben a bűnözők gyakran 0–24-ben működő *helpdesket* is biztosítanak a megrendelő számára.

A támadókat nagyban segíti a művelet előkészítésében az úgynevezett nyílt forrású információgyűjtés, vagyis, mint ahogy a neve is mutatja, minden nyilvánosan elérhető információ összegyűjtése, azok elemzése és értékelése. A szervezetek és az egyének is rengeteg olyan információt tesznek közzé, amelyek sokszor segítik a támadókat. A fogyasztóknak természetes igénye, hogy a vállalatok aktívan legyenek jelen a közösségi oldalakon, minél több információt tudjanak elolvasni a cégről, termékekről, szolgáltatásokról. Marketingszempontból a vállalatoknak is érdeke, hogy vásárlóközpontú, újabban környezetbarát, társadalmi felelősségvállalásra hajlamos szervezetként tekintsenek rájuk, így sokszor meggondolatlanul osztanak meg magukról, szervezetükről információkat, amelyek szisztematikus összegyűjtése aranyat érhet. Egy itt meg nem nevezett kisüzemi sörfőzde e fejezet írásakor kampányszerűen mutatja be munkatársait, fényképpel, érdeklődési körrel, esetleges családi állapotra vonatkozó információkkal, aminek a célja marketingszempontból teljesen legitim, azonban biztonsági megfontolásokból nem, a támadó név szerint, fényképpel ismeri meg azokat a munkatársakat, akik mondjuk a cég HR-es, pénzügyi vagy egyéb területen dolgozó alkalmazottai; az információkat adott esetben a szervezet

[6] Az eset előtt nem sokkal az Apple tőle szokatlan formában, mindenféle komoly showműsor nélkül, szinte rejtve jelentette be új fejlesztéseit. Értelemszerűen nincs bizonyíték rá, de többek véleménye, hogy erre azért került sor, mert így akarták elejét venni, hogy a konkurensek megvásárolják az ellopott adatokat, és előttük nyilvánosságra hozzák mint saját szellemi termékeket.

honlapjáról ilyen részletességgel nem tudná kideríteni. Ezek az információk egy *social engineering* támadás esetében kiemeltek, hiszen úgy lehet megtalálni a szervezet gyenge láncszemét, a kevésbé biztonságtudatos felhasználót, hogy őt befolyásolva/megzsarolva/lefizetve férhetnek hozzá a kívánt információkhoz a szervezetben.

Emellett természetesen sok olyan információ gyűjthető össze nyílt forrásból mind a munkavállalókról, mind a szervezetekről, amelyek tovább növelik a sikeres támadás esélyét. Szürke zónát jelent az okosmobil-készülékekre optimalizált alkalmazások engedélykérése. Sajnos a felhasználók nagy része úgy telepít készülékére mindenféle alkalmazást, hogy nem ellenőrzi, mihez adhat engedélyt. A támadóknak elég rávenni a célszemélyt, hogy telepítsen egy ilyen alkalmazást, és ha a felhasználó óvatlan, akkor a bűnöző gyakorlatilag minden információhoz hozzáférhet, amit a készüléken elér a munkatárs, legyen szó privát vagy munkahelyi e-mailekről, magánbeszélgetésekről, a telefonon tárolt file-okról.

Ennél is komolyabb lehet a kamera és mikrofon feletti irányítás megszerzése, hiszen a támadók ezeket bármikor aktiválhatják a tulajdonos tudta nélkül. Ez nem csupán abban jelent kockázatot, hogy a felhasználóról kompromittáló felvételek készülhetnek, amellyel akár zsarolhatóvá válik (például ha nem dug be egy fertőzött *pendrive-ot* munkahelyi eszközébe, hogy a versenytársak azon keresztül szerezzék meg a cég érzékeny adatait, akkor nyilvánosságra hozzák a kellemetlen felvételeket), hanem ugyanúgy lehallgathatják a belső céges megbeszéléseket, hozzáférve olyan fontos információkhoz, amelyek felhasználásával nemcsak versenyelőnyt szerezhetnek, hanem egyéb módon is komoly károkat okozhatnak a szervezetnek, például olyan hangfelvételek kiszivárogtatásával, amely a vásárlói bizalom megrendítésével járhat (rasszista, szexista stb. felvételek nyilvánosságra hozatalával).

Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) a személyes adatok védelmét kiemelten fontosnak tekinti,[7] komoly pénzbírsággal büntetve azokat a szervezeteket, amelyek megsértik a felhasználók személyes adatait, így nem nehéz belátni, hogy a szervezeteknek nagy hangsúlyt kell fektetni az általuk kezelt személyes adatok védelmére. Egy adatvédelmi bírság kiszabása nemcsak a vásárlók, partnerek bizalmát áshatja alá, de a szervezet további működését is

[7] 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 (általános adatvédelmi rendelet) (EGT vonatkozású szöveg).

nagyban befolyásolhatja, ha ezáltal likviditási problémák merülnek fel. Ennek elérése megvalósulhat a kevésbé erkölcsös vetélytársak részéről is, akiknek a támadás elkövetésével az a célja, hogy a szervezet komoly adatvédelmi bírságot kapjon.

A köznyelvben gyakran szinonimaként használják az információbiztonságot az informatikai biztonsággal, azonban a két fogalom eltér egymástól. Az informatikai biztonság egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.[8] Célja, hogy az információ megőrizze és fenntartsa a biztonsági tulajdonságait, a korábban említett CIA-triádnak megfelelően.

Ennek érdekében különféle hardveres és szoftveres biztonságtechnikai eszközöket alkalmaznak az illetéktelen hozzáférések és károkozás megelőzésére (például tűzfalak, vírusirtók, hozzáférés-szabályozás), továbbá biztonsági szabályzatokat, előírásokat (jelszóhasználat, biztonsági mentés) is létrehoznak. Ilyen védelmi megoldások:

- az adminisztratív védelem;
- a fizikai védelem;
- a logikai védelem.

Mindezekből jutunk el a kiberbiztonság fogalmához, amely az Ibtv. alapján „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". Ebből következően a kibervédelem „a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését".

## 2. A koronavírus-járvány hatása a kiberbiztonságra

A 2019. év végén Kínából elindult, és globális pandémiát okozó új típusú koronavírus alapjaiban változtatta meg társadalmunk működését. Az egyik percről

[8] Munk Sándor: Információbiztonság vs. informatikai biztonság. *Hadmérnök,* 3. (2008), ksz. 1–21.

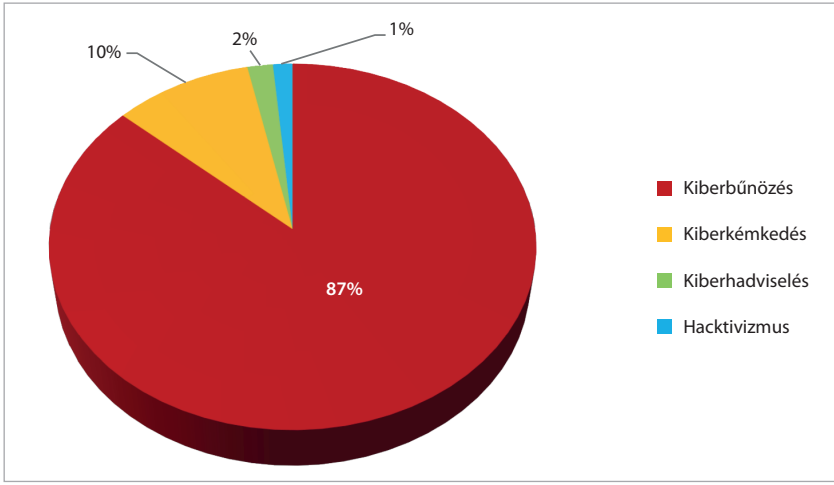
a másikra történő lezárások teljes szektorokat kényszerítettek leállásra, és helyezték át az emberi élet számos szegmensét a digitális térbe. A modern társadalmak évtizedek óta folyamatosan fejlesztették digitális ökoszisztémájukat, amelyek 2020 tavaszán vizsgára kényszerültek. A tudományos kutatások visszatérő toposza volt az elmúlt évtizedben, hogy az infokommunikációs eszközök elterjedése új típusú biztonsági fenyegetéseket eredményezett, és a digitalizáció magas fokából származó függőségünk óriási kockázatot jelent.

A szakértők a kibertér kockázatait számos különböző aspektusból vizsgálták, amiket a kritikus információs infrastruktúrák védelmétől kezdve a felhasználók alacsony szintű kiberhigiéniai képességeiken át az államok politikai döntéshozatalának befolyásolásáig bezárólag rendkívül széles skálán azonosítottak. Az elmúlt másfél évben a koronavírus következtében a kibertér jelentette kockázatok hatványozottan jelentkeztek.

A járványügyi korlátozások elhúzódása óriási feszültséget okozott a társadalmakban, amelyet a futótűzként terjedő álhírek tovább fokoztak. A lezárások nehézséget okoztak mind egyéni, mind csoportszinten, a megélhetés veszélye sokak számára jelentett súlyos egzisztenciális válságot, a vírustól való rettegés pedig tovább fokozta a pszichózist. A megterhelt idegrendszer, a számos, az otthoni munkavégzés során átélhető feszültség (például a felnőtt a gyermek digitális oktatása miatt korlátozott a saját munkavégzésében) tovább növeli a kibertérből érkező támadások elleni kitettséget: csökkenő figyelemmel sokkal hajlamosabbak vagyunk arra, hogy óvatlanul internetezzünk, rákattintsunk olyan oldalakra, amelyekre nem feltétlenül tennénk más esetben.

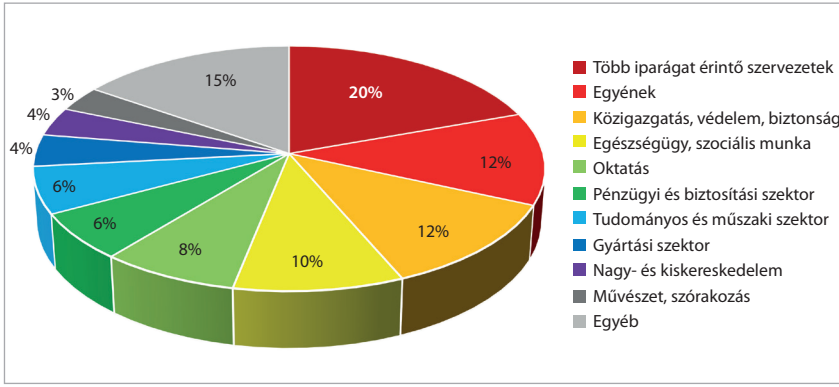
A hirtelen tömegessé vált távoli munkavégzés felkészületlenül érte az alacsony digitális kompetenciával rendelkezők tömegét, illetve a nem kidolgozott válságkezelési stratégiával rendelkező állami és piaci szervezeteket egyaránt, ami a kiberbűnözéshez köthető kibertámadások számának szignifikáns emelkedésével járt. Mindez érthető, ugyanis rendkívül „szerencsés" együttállás következett be: a munkavállalók jelentős tömegének alacsony fokú digitális írástudása találkozott a szintén alacsony fokú adat- és információbiztonsági tudatossággal, aminek hatását felerősítette a nem megfelelően védett informatikai eszközök sokasága, illetve a saját, szintén nem minden esetben megfelelően védett otthoni eszközök használta.

A 2020-as évre vizsgálva a kibertámadások statisztikáit, a Hackmageddon adataiból a kiberbűnözés dominanciája rajzolódik ki *(1. ábra),* az összes bejelentett[9] támadás 87%-a erre a típusra vezethető vissza.



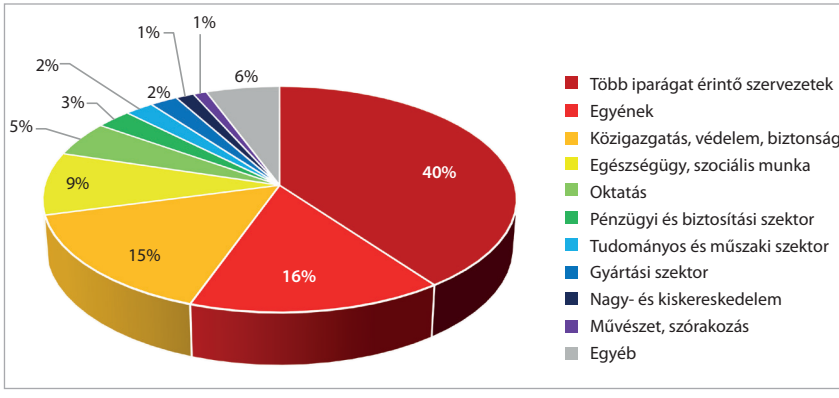

*1. ábra: A kibertámadások motivációjuk szerint 2020-ban*
*Forrás:* a Hackmageddon.com alapján a szerző szerkesztése

[9] A *bejelentett* kifejezés több szempontból hangsúlyos. Egyrészt sok esetben az áldozatok nem konstatálják, hogy támadások áldozatai. Ennek oka lehet, hogy valamilyen rendkívül szofisztikált kibertámadást hajtanak végre ellenük, például APT (folyamatosan fennálló fejlett támadás) áldozatai. Jellemző azonban az is, hogy a már említett alacsony fokú kiberhigiéniai képességek okán nem ismerik fel, hogy valamilyen biztonsági esemény következett be, például a jelentősen lecsökkent számítási kapacitással üzemelő informatikai eszköz esetében nem kártékony kódok jelenlétével magyarázzák a működést, hanem az eszköz elévülésével. A másik ok, hogy az áldozatok nem jelentik a biztonsági eseményt. A bejelentés hiánya elmaradhat, mert a kárvallottak nem tudják, kik azok az érintett szervezetek, akik részére az őket ért kibertámadásokat be kell jelentsék, de szerepet játszhat az a sokszor téves meggyőződés is, hogy az illetékes hatóságok úgysem tudják felderíteni az elkövetőket. Nem szabad elfelejteni azt a tényezőt sem, hogy a támadást elszenvedett szervezetek tartanak attól, hogy megrendül a felhasználói bizalom, és emiatt inkább elhallgatják a történteket. Az Európai Unióban ez azonban komoly hatósági bírsággal járhat a GDPR értelmében, hiszen a személyes adatokat érintő biztonsági események bekövetkezésekor 72 órája van a szervezeteknek, hogy az incidenst jelentsék az érintett tagállami hatóság részére.




*2. ábra: A kibertámadások megoszlása célpontok szerint 2020-ban*
*Forrás:* a Hackmageddon.com alapján a szerző szerkesztése

A *3. ábra* az egyes támadástípusok megoszlását mutatja, amelyek közül legnagyobb arányban a kártékony kódok, közismert nevükön a *malware*-ek szerepelnek.




*3. ábra: A kibertámadások megoszlása típusok szerint 2020-ban*
*Forrás:* a Hackmageddon.com alapján a szerző szerkesztése

Amennyiben megvizsgáljuk a különböző jelentéseket, amelyeket kifejezetten a koronavírus-járványra vonatkozóan készítettek el a kibertámadásokat elemezve, szintén a malware-ek számának jelentős növekedését tapasztaljuk.

A továbbiakban vizsgált statisztikai adatok, amelyek a különböző kibertámadásokat elemzik, az FMCG-szektor minden szereplője esetében relevánsak, ahogy 2. ábrán is láthattuk. Terjedelmi korlátok miatt nem vehetjük végig az ellátási lánc érintett szereplőit, csupán arra hívhatjuk fel a figyelmet, hogy ugyanúgy érvényesek a leírtak kiskereskedőkre, mint a logisztikai vállalatokra stb.

Az Interpol által 2020 augusztusában publikált jelentés szerint,[10] amelyben 194 tagállam, illetve partnerszervezetek által kapott adatokat értékeltek 2020. április és május között, riasztó kép rajzolódik ki. A támadások volumenével kapcsolatban figyelemreméltó, hogy csupán a TrendMicro, az Interpol magánszektorbeli partnere e kéthónapos időszak alatt több mint 900 ezer spam üzenetet kapott, 737 malware-hez köthető biztonsági esemény következett be nála, és 48 ezer fertőzött URL-lel kapcsolatos támadás érte.

A kiberbűnözők szokásukhoz híven rendkívül adaptív tulajdonságról tettek tanúbizonyságot, roppant gyorsan alkalmazkodtak a megváltozott körülményekhez; korábbi módszereiket adaptálták a pandémiához köthető forgatókönyvekkel, gyakran kormányzatok, egészségügyi szervezetek nevében indították leggyakrabban adathalászatra vonatkozó támadásaikat.[11] A leggyakoribb malware-ek az Emotet, TrickBot és Cerberus voltak, amelyeket gyakran .pdf, .mp4 és .docx csatolmányokba rejtve küldtek a címzetteknek. Az adathalászat sokszor az online bankolás kifürkészésére irányult, ahogy ez sokak számára Magyarországon is ismertté vált 2021 tavaszán a FluBot kampány során.[12] A FluBot malware rendkívül kreatív adathalászkampány volt, amely nagyban alapozott a felhasználók alacsony szintű adat- és információbiztonsági tudatosságára – mint kiderült, sikeresen –, hiszen olyan emberek tömegét szedte rá, akik nem rendeltek semmilyen csomagot, mégis rákattintottak az erről küldött SMS-ben szereplő gyanús hivatkozásra, majd feltelepítették a benne szereplő alkalmazást mobil készülékükre.

Szintén jelentősen nőtt az úgynevezett Business Email Compromise-támadások száma, amely során üzleti tranzakciók teljesítésére veszik rá az áldozatot, ezek gyakran célzott formában valósultak meg.

[10] Interpol: *Report Shows Alarming Rate of Cyberattacks during COVID-19* (2021. június 12.).

[11] E mondat a laikusok számára ellentmondásosnak tűnhet: korábban a malware-ek számának jelentős megugrását fogalmaztuk meg, ezért fontos tisztázni: a malware-eket számos tevékenységre használják, lehetnek kémprogramok, zsarolóvírusok, trójai programok, de ugyanúgy adathalászatra is gyakran alkalmazzák őket.

[12] Koi Tamás: Példátlan krízist okozott itthon a FluBot androidos kártevő. *HWSW,* 2021. március 26.

A leggyakoribb adathalászathoz és online csalásokhoz kapcsolódó támadások az Interpol jelentése alapján az alábbiak voltak:

- nemzeti vagy globális egészségügyi hatóság nevében küldött e-mail;
- kormányzatok nevében kezdeményezett támogatás;
- hamis fizetési kérések és pénzvisszatérítés;
- oltóanyaghoz és orvosi ellátmányhoz kapcsolódó ajánlatok;
- Covid–19-hez köthető mobilalkalmazások;
- befektetésekhez és részvényekhez kapcsolódó ajánlatok;
- Covid–19-hez kapcsolódó adományok kérése.

Ahogy fentebb a Trend Micro példája is jelezte, a kiberbűnözők rengeteg kártékony kódot tartalmazó weboldalt hoztak létre, kihasználva az orvosi ellátás és a Covid–19 iránti megnövekedett információéhséget, jelentősen megnőtt az olyan domainnevek bejegyzése, amelyek megadott keresőkifejezéseket tartalmaztak, mint például „koronavírus" vagy „Covid". A csaló weboldalakhoz számos kiberbűncselekmény volt köthető, mint az említett kártékony kódok telepítése, illetve adathalászat. 2020. március végéig több mint 100 ezer újonnan regisztrált a Covid–19-hez köthető domaint azonosítottak az Interpol szakértői. Ezek közül 2022-t rosszindulatúnak, több mint 40 ezret „magas kockázatúnak" azonosítottak. 2020 júniusában a Számítógépes Bűnözés Elleni Igazgatóság globális rosszindulatú domain-munkacsoportja 200 000 kártékony kódot tartalmazó domaint azonosított és elemzett, amelyek több mint 80 tagországot érintenek. Az Interpol partnere, a Palo Alto Networks a 2020. február és március közötti vizsgálata alapján azt mutatta ki, hogy 569%-kal nőtt meg a kártékony kódot tartalmazó weboldalak száma, amelyek malware-ekre és adathalászatra specializálódtak. 788%-kal nőtt a magas kockázatú oldalak regisztrációja, ide sorolva a spamküldésre, kriptovaluta-bányászatra optimalizált oldalakat. Az ilyen típusú csalások számának megugrása kimutatható volt a Google Trend keresésekben is, miután a felhasználók sokszor szembesültek kiberbiztonsági incidensekkel.

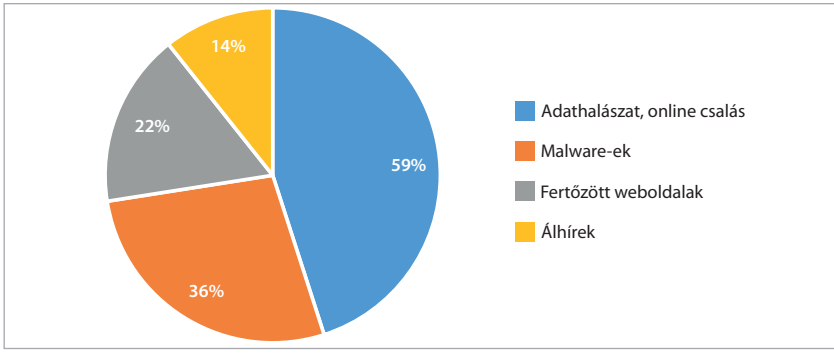
Az Interpol jelentésének regionális vizsgálatából megállapíthatjuk, hogy

- *Afrikában* a megnövekedett online fizetések száma az ezekkel kapcsolatos csalások számát növelte meg, amelyet a távmunkavégzésre történő átállásból fakadó kockázatok egészítettek ki, ideértve a jótékonysági csalásokat, sextortiont, valamint az adathalászatot. A világ többi részéhez hasonlóan magas volt a Covid–19-hez kapcsolódó álhírek száma.
- Az *amerikai régióban* a már említett adathalászkampányok voltak a dominánsak, de jellemző volt a távmunkavégzés okán a vállalati hálózatok

kompromittálása és érzékeny adatok ellopása. A LockBit ransomware volt a legelterjedtebb, amely jellemzően a középvállalatokat célozta.

– Az *ázsiai és csendes-óceániai régió* esetében a Covid–19-hez köthető adathalász-tartalmak megugrása volt tapasztalható, illetve a hamis orvosi cikkek, gyógyszerek és egyéni védőeszközök illegális online értékesítése, a videókonferenciák biztonsági sérülékenységeinek kihasználása, továbbá a dezinformáció növekedése. A régió fő kihívásaként az alacsony kiberhigiéniai képességeket azonosították.
– Az *európai tagállamok* kétharmada számolt be a rosszindulatú weboldalak számának jelentős növekedéséről a Covid kapcsán, széles körű adathalászkampányok zajlottak hivatalos kormányzati szereplők nevében, amelyek nem csupán adathalászat, de későbbi kibertámadás megalapozását is szolgálhatják. Gyakori volt a zsarolóvírusok számának növekedése a kritikus infrastruktúrákkal szemben, különösen egészségügyi intézmények tekintetében.
– A *Közel-Keleten és Észak-Afrikában* jelentős számban nőtt a Covid–19-kapcsolódású álhírek száma, a hamis gyógyszerek árusítása a közösségi oldalakon. Megfigyelhető volt a kártékony weboldalak számának növekedése, amelyek jellemzően járványstatisztikákat szolgáltatnak, illetve a Covid–19-kapcsolódású adathalász-tartalmak terjedése.

A tagállamok visszajelzése alapján (lásd *4. ábra*) a leggyakoribb támadástípusok visszaigazolják az egyes régiókban jellemző bűncselekményeket.




*4. ábra: A Covid–19-hez köthető leggyakoribb kibertámadások típusaik szerint*

*Forrás:* az Interpol adatai alapján a szerző szerkesztése (Lásd: (www.europol.europa.eu/cms/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf.)

Az Interpolhoz hasonló eredményeket fogalmazott meg az Europol témában készített jelentése.[13] Általánosságban megállapítható, hogy a Covid–19 kapcsán a kiberbűncselekmények száma drasztikusan megnőtt más típusú bűncselekményekhez képest. A kiberbűnözők gyorsan alkalmazkodtak a pandémia jelentette változásokhoz, és hatékonyan alapoztak az áldozatok járvánnyal kapcsolatos szorongásaira, félelmeire. A megugrott zsarolóvírus- és adathalász-kampányok várhatóan még jobban fel fognak erősödni a jövőben.

A jelentést erősíti az Europol által minden évben közreadott a Szervezett bűnözés internetes jelenlétét vizsgáló kiadványa,[14] amely szintén vizsgálja a kiberbűnözés koronavírussal kapcsolatos trendjeit.

## 3. Hogyan védekezzünk a kibertérből érkező fenyegetésekkel szemben?

A kiberbiztonság fogalmi kérdéseinél már volt szó a kockázatokkal arányos védelemről. Ez kiemelten fontos minden szervezet esetében, hiszen a védekezés költségei jelentősen magasabbak, mint a támadók költségei. Rengeteg pénzt lehet elkölteni magas szintű védelmi megoldásokra, amelyek a szervezet fizikai, logikai védelmét erősítik, de ez nem jelenti, hogy biztonságban leszünk, ugyanis 100%-os védelem nem létezik, sosem valósítható meg. Védelmi képességeinket úgy kell kialakítanunk, hogy azok arányosak legyenek a szervezetet érintő kockázatokkal.[15] Ebben különösen hasznos lehet a Magyar Nemzeti Bank által kiadott 12/2020. (XI. 6.) számú ajánlás a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről, ami az érintett pénzügyi szervezetek számára természetesen kötelező, azonban a benne megfogalmazottak az FMCG-szektor szereplői számára is tartalmaznak jó gyakorlatokat.

A koronavírus következtében rengeteg vállalkozás állt át házhoz szállításra, illetve alakított ki webshopot. Ez együtt jár a személyes adatok magas szintű védelmének kötelezettségével, amit a GDPR ír elő. A GDPR mellett egyes szervezetek esetében releváns lehet az Európai Unió Hálózati és Információbiz-

[13] Europol: *Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic* (2021. június 12.).

[14] Europol: *Internet Organised Crime Threat Assessment (IOCTA) 2020* (2021. június 12.).

[15] Az állami és önkormányzati szervek esetében ezt a szervezet által kezelt adatok fényében egytől ötig terjedő skálán biztonsági szintbe, a szervezet információs rendszerét pedig szintén egytől ötig terjedő skálán biztonsági osztályba kell sorolni. A biztonsági osztály és biztonsági szint előírja azokat a védelmi eljárásokat, amelyeket a szervezetnek ki kell alakítania.

tonsági Irányelve (NISD),[16] illetve a 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ekertv.)[17] is. A NISD meghatározza az úgynevezett bejelentésköteles szolgáltatások[18] fogalmát. Ahogy a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete fogalmazza,[19] amely egyúttal az érintett szervezetek esetében a hatósági jogkört is gyakorolja,

„célja, hogy a bejelentés-köteles szolgáltatást nyújtók az általuk használt hálózati és információs rendszerek biztonságát növeljék, az azokat érő biztonsági eseményeket megelőzzék, illetve hatásukat csökkentsék, ezáltal emelve az általuk nyújtott szolgáltatások biztonságát. A bejelentés-köteles szolgáltatások elterjedtsége, illetve más fontos szolgáltatásokba történő beépülése miatt a megbízható, folyamatos működésükre alapvető gazdasági és társadalmi tevékenységek támaszkodhatnak. Az erre épülő célokat, illetve a kibertérbeli működés biztonságát és üzemfolytonosságát támogatja az eseménykezelő központ és a hatóság. A kiberbiztonság érdekében az EU rendelet előírja a hálózati és információs rendszerek kockázatokkal arányos védelmét és az alkalmazandó biztonsági elemeket. Az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet[20] bejelentés-köteles szolgáltatást nyújtó szereplők számára előírja a hatóságnál történő regisztrációt, valamint a hálózati és információs rendszereikben bekövetkezett jelentős biztonsági események bejelentését az eseménykezelő központ számára."

Bejelentésköteles szolgáltatást nyújtónak minősül az a magyarországi székhelyű gazdasági társaság, amely a következő szolgáltatások valamelyikét nyújtja:

- az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi és szolgáltatási szerződések megkötését teszi lehetővé fogyasztók és kereskedők között (online piactér);

[16] Az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelve.

[17] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

[18] A fogalom a NISD-ben digitális szolgáltatásként szerepel, a hazai terminológia sajnos félrefordította.

[19] Nemzeti Kibervédelmi Intézet honlapja. 2021. június 12.

[20] 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről.

- információk megtalálását elősegítő segédeszközöket biztosít az igénybevevő számára, amelyek lehetővé teszik, hogy adott kulcsszó, lekérdezés alapján elvben minden webhelyen keresést hajtsanak végre bármely témában (keresőszolgáltatás);
- távoli hozzáférést tesz lehetővé a többek között hálózati funkciókat, adattárolást, alkalmazások, szolgáltatások futtatását biztosító számítástechnikai megoldásokhoz (felhőalapú számítástechnikai szolgáltatás).

Nem tartoznak a fenti jogszabályok hatálya alá azok a bejelentésköteles szolgáltatások, amelyeket a szolgáltatók mikro- és kisvállalkozásként nyújtanak.[21]

Fontos látni, hogy a GDPR nem határoz meg a szervezetek számára konkrét előírásokat a védelmi megoldásokat illetően, csupán előírja a személyes adatok biztonságát garantáló megoldások alkalmazását a szervezetek számára. Ezek között „szervezeti megoldások" (például a szervezeten belül a személyes adatokhoz hozzáférő személyek számának korlátozása) és „technikai megoldások" (például az adatok titkosítása) egyaránt szerepel. A GDPR előírásainak megfelelően az adatkezelő, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, intézkedéseket hajt végre, ilyenek például:

- a személyes adatok álnevesítése és titkosítása;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítása;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A biztonság kialakításakor ökölszabályként meghatározhatjuk, hogy a védelemnek egyenszilárdságúnak kell lennie, illetve nem szabad többet költeni, mint amekkora kárt az információ valamilyen kompromittálódása okozhat.

A biztonsági mechanizmusok kialakításakor az úgynevezett PreDeCo-elv kialakítására kell törekedni. A rövidítés a predektív, detektív és korrektív szavakból áll össze, vagyis a megelőzés (a fenyegetés hatása bekövetkeztének elke-

[21] A szervezetek kötelezettségeiről bővebben lásd a Nemzeti Kibervédelmi Intézet honlapját.

rülése), észlelés (a biztonsági esemény bekövetkezésének felismerése), illetve a reagálás (a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés) hármasát fogja egybe. A biztonsági mechanizmusok negyedik lépése a már bekövetkezett biztonsági események kezelése.

Az információbiztonság esetében három kérdést kell megválaszolnunk. Mit kell megvédenünk? Az adatokat. Mi ellen kell megvédeni őket? Azon támadások ellen, amelyek a CIA-triád tulajdonságokat – és ezen keresztül a szabályzatok betartását – veszélyeztetik. Milyen módon kívánjuk megvédeni? Azokkal a védelmi mechanizmusokkal, amelyek a PreDeCo-elvet teljesítik.

Az információbiztonságot folyamatként szükséges értelmezni, amely öt lépésből áll:

1. információvagyon felmérése, értékelése;
2. fenyegetések számbavétele, kockázatok meghatározása;
3. kockázatok kezelése;
4. védelmi intézkedések nyomon követése;
5. ugrás az elsőre.

A kockázatok kezelésére számos módszertan áll rendelkezésünkre, mint például a *consultative, objective & bifunctional risk analysis* (COBRA), *cost-of-risk analysis* (CORA), *Central Computer and Telecommunications Agency* (CCTA), *risk analysis and management methodology* (CRAMM), *information security risk analysis method* (ISRAM), ISO 3100 stb.[22]

A kockázatelemzés eredményeképpen meghatározzuk azokat a területeket, amelyek beavatkozást igényelnek, és kidolgozzuk azokat a kockázatkezelési eljárásokat, amelyekkel csökkentjük a kockázat bekövetkezésének valószínűségét. A kockázatelemzés fontos részét képezi (egyéb tevékenységekkel kiegészülve, mint például üzleti hatáselemzés) az üzletmenet-folytonossági terv (BCP) elkészítésének, amelynek relevanciájára az első hullám hangsúlyosan felhívta a figyelmet. Az üzletmenetfolytonosság-terv célja, hogy az esetlegesen bekövetkező rendkívüli eseményeket, amelyek szervezetünket fenyegetik, hogyan, milyen módon kezeljük. Azok a szervezetek, amelyek rendelkeztek BCP-vel, óriási helyzetelőnybe kerültek az első hullám idején versenytársaikkal szemben.

[22] Ming-Chang Lee: Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. *International Journal of Computer Science and Information Technology,* 6. (2014). 29–45.

A fejezet terjedelmi korlátai nem teszik lehetővé, hogy részletes és mindenre kiterjedő tanácsokat fogalmazzunk meg a szervezetek kiberbiztonsági kockázatainak csökkentésére (elsősorban a távoli munkavégzésre vonatkozóan), így csupán néhány területet említünk:

- használjunk többfaktoros azonosítást;
- használjunk jelszómenedzser-alkalmazást, hogy biztonságos jelszavakat használjunk az egyes fiókjainknál;
- csak megbízható WiFi-hálózatot használjunk;
- változtassuk meg a routerünk alapértelmezett felhasználó nevét és jelszavát;
- tisztázandó, hogy a munkavégzés saját vagy a munkáltató által biztosított eszközzel történik-e, illetve ebből következően milyen biztonsági eljárásokat szükséges követni. A saját eszközök gyakran más védelmi megoldásokat alkalmaznak, hiszen míg a munkáltató által biztosított eszközön korlátozva lehet például a külső adathordozók csatlakoztatása, a biztonsági frissítések automatizáltan történhetnek, addig saját eszközön ezek nem feltétlenül valósulnak meg;
- amennyiben a felhasználó a saját eszközét nem védi megfelelően, és a munkavégzés ezen keresztül történik, magában hordozza annak a veszélyét, hogy rajta keresztül a szervezet elektronikus információs rendszeréhez is hozzáférhetnek a támadók. Éppen ezért létfontosságú, hogy a használt eszközökön (legyen szó számítógépről, okosmobil eszközről) a legfrissebb szoftverfrissítések legyenek telepítve;
- csak jogtiszta szoftvereket használjunk, ugyanis az illegális csatornákról letöltött, tört szoftverek tartalmazhatnak kártékony kódokat (például kémprogramokat, zsaroló vírusokat);
- használjunk vírusirtót;
- telepítsünk a böngészőnkbe különböző privát szférát erősítő technológiákat, amelyek csökkentik az internetezés kockázatait, például azáltal, hogy jelzik a nem biztonságos oldalakat, letiltják az oldalak által esetlegesen futtatott kémprogramokat vagy egyéb kártékony kódokat;[23]
- a korábban említett kockázatelemzésnek értelemszerűen a munkavállaló által kezelt adatokra is ki kell térnie, hiszen az adatok esetleges kiszivárgása szervezetenként eltérő kockázatot jelent, így olyan korlátozó

[23] Ezzel kapcsolatban a www.maganelet.hu oldal számos hasznos tanácsot nyújt.

megoldások alkalmazása is szükséges lehet, amelyek például a file-ok titkosítását követelheti meg;
- figyeljünk a jogosultságkezelésre, különösen saját eszközről való hozzáférés esetében;
- képezzük folyamatosan a munkavállalókat az adat- és információbiztonsággal kapcsolatban, ugyanis folyamatosan új típusú kihívások jelennek meg, amelyek felülírhatják adott esetben a korábbi tudásunkat.

Természetesen a felsoroltokon felül rengeteg egyéb védelmi megoldásra kell tekintettel lennünk, amihez a kockázatkezeléshez hasonlóan számos módszertant vehetünk alapul. Ilyen például az Australian Cyber Security Centre által kidolgozott ajánlás,[24] amely enyhítési stratégiákkal szolgál a távoli munkavégzés kiberbiztonsági kockázataival kapcsolatban. Az ajánlás az egyes stratégiákat három szempont alapján értékeli:
- felhasználói ellenállás a stratégiával szemben;
- előzetes költségek mértéke (személyzet, szoftver és hardver);
- folyamatos karbantartási költség mértéke.

Végezetül öt olyan területet vizsgálok, amely létfontosságú a hatékony digitális átállás megvalósításában, de egyúttal komoly adat- és kiberbiztonsági kockázatot is jelent, ha nem szentelünk rá kellő figyelmet. A Covid alatt számos kisvállalat, étterem, kocsma stb. állt át az online szolgáltatásra, komoly növekedés következett be a házhoz szállítást végző cégek esetében. Az online vásárlás ilyen mértékű növekedése, mint a fent vizsgált statisztikákból is kiderült, megnövelte a kiberbűnözéshez kapcsolódó támadásokat, hiszen rengeteg pénzügyi tranzakció zajlott le ezeken a nem feltétlenül megfelelő védelemmel ellátott oldalakon. Ahogy fentebb már utaltam rá, amennyiben a szervezet weboldala ügyféladatokat tárol, online fizetést lehet kezdeményezni rajta, webshopot üzemeltet, úgy ezen adatok kompromittálódása nem csupán a fogyasztói bizalom sérülésével járhat, hanem komoly bírsággal is. Fontos megjegyezni, hogy az egyes részeknél javasolt intézkedések nem teljesek, csupán példázó jelleggel szerepelnek, ezeken kívül egyéb megoldások is léteznek.

Az első terület a hibás weboldal-beállításokkal függ össze. Főszabályként kijelenthető, hogy bizonyos szakspecifikus feladatokat kizárólag hozzáértőkre

[24] Australian Cyber Security Centre: Strategies to Mitigate Cyber Security Incidents. *Cyber.gov.au,* 2021. június 12.

szabad bízni. Mint a fentiekből is látható, nem szabad félvállról venni a szervezet weboldalának megfelelő üzemeltetését. A leggyakoribb támadástípusok, amelyek a személyes adatok, fizetési adatokkal összefüggő incidensekhez vezethetnek:

- SQL-injekció;[25]
- Cross site scripting (XSS);[26]
- útkeresztezési támadások.[27]

Megfelelő beállításokkal ezek kockázatát csökkenteni lehet, de ez szakértelmet igényel.

A második terület az e-kereskedelem kockázata: ha a weboldalon lehetőségük van a felhasználóknak terméket, szolgáltatást rendelni, és azon keresztül fizetési lehetőség is biztosított, az alábbi beállítások alkalmazása indokolt, hogy a különböző személyes adatokkal, fizetési információkkal kapcsolatos incidenseket megelőzzük:

- véletlenszerű vásárlói azonosítás;
- biztonságos bejelentkezés;
- automatikus kijelentkeztetés megadott idő után;
- SSL-tanúsítvány alkalmazása, hogy titkosított adatkapcsolaton keresztül valósuljon meg többek között a fizetési tranzakció;
- meghatározott jelszószabályok elvárása (x karakter, speciális karakterek elvárása stb.);
- biztonsági tokenek alkalmazása.

Harmadik terület a zsarolóvírusokkal szembeni védekezés. Ahogy fentebb már volt szó róla, a kiberbiztonsági fenyegetések kapcsán az egyik leggyakoribb támadástípusként a kártékony kódokat azonosíthatjuk, amelyeknek egyik legelterjedtebb módja az úgynevezett ransomware-ek, vagyis zsarolóvírusok. Ez a fajta támadás szervezettől függően nem csupán anyagi károkat okozhat, hanem adott esetben a szolgáltatás leállásával a létfontosságú rendszerelemek sérülését is okozhatja (ahogy például 2017-ben a NotPetya nevű ransomware a logisztikai rendszerekben okozott globális kiesést). A támadók célja jellemzően anyagi haszonszerzés, az adatok feloldásáért cserébe általában kriptovalutában köve-

[25] A védekezési lehetőségekről a támadást illetően bővebben lásd Fleiner Rita Dominka: SQL inkejcióra épülő támadások és védekezési lehetőségek. *Hadmérnök,* 3. (2008), 4. 117–128.

[26] Bővebben lásd Hun-CERT: *Cross Site Scripting (XSS)* (2012. május 9.).

[27] Bővebben lásd Ficsor et al.: Szoftvertesztelés. *Digitális Tankönyvtár,* 2021. június 12.

telnek váltságdíjat. A fizetés azonban nem garantálja, hogy valóban visszakapjuk az adatainkat (hiszen sok esetben dark neten elérhető zsarolóvírust használhatnak a támadók, amelyhez ők sem ismerik a feloldáshoz szükséges titkosító kulcsot), így ennek tudatában érdemes meghoznunk a döntésünket. A legfontosabb ez esetben is a megelőzés, ami az alábbi intézkedéseket foglalja magában:

- rendszeres biztonsági mentés adatainkról;
- a szoftverek rendszeres biztonsági frissítése, ami azokat a sebezhetőségeket javítja, amiken keresztül a zsarolóvírusokkal megfertőződhetünk;
- felhőszolgáltatások használata.

Negyedik terület az adathalászattal szembeni védekezés. A koronavírussal összefüggésben a Gmail naponta körülbelül 100 millió adathalászlevelet blokkol, de így is több százmillió ilyen témájú levél esik be a spamszűrőn. Hogyan védekezhetünk ellene? Az egyik legfontosabb a munkatársak oktatása, hogy kiszűrhessék az ilyen típusú leveleket. De fontos a megfelelő műszaki védelem is, mint például:

- a VPN-használat esetében eltérő jogosultságkezelés,
- az IP-cím-tartomány felülvizsgálata.

Az utolsó, ötödik terület a videókonferenciák kockázata. A távoli munkavégzés kapcsán gyakran kényszerültek a szervezetek online értekezletek megtartására, amelyek önmagukban is kockázatot hordozhatnak. A kockázatok azonban jellemzően a biztonságtudatosság hiányából fakadnak, és rendkívül könnyű ellenük védekezni. Tipikus veszély, amikor az értekezlethez való csatlakozás információit nyilvános helyeken megosztják, és ily módon bárki „beeshet az utcáról". Ezt elkerülendő fontos, hogy jelszóval lássuk el a csatlakozást, csak azoknak a személyeknek küldjük el, akiknek részt kell vennie. Amennyiben van lehetőség, állítsunk várótermet is, hogy a jelentkezőket az értekezlet szervezője engedje be, és elutasíthassa az illetéktelenek csatlakozását. Korlátozzuk a résztvevők jogosultságát, mint például a képernyő megosztása, az értekezlet rögzítése stb. Adatvédelmi és biztonsági szempontból hasznos a virtuális háttér alkalmazása, hogy a résztvevők ne lássák a mögöttünk levő környezetet, és ne vonhassanak le belőle következtetéseket.

## Felhasznált irodalom


270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

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

Australian Cyber Security Centre: Strategies to Mitigate Cyber Security Incidents. *Cyber.gov.au,* 2021. június 12. Online: www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

Az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelve

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 (általános adatvédelmi rendelet) (EGT vonatkozású szöveg)

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése*. Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673. Online: 2016.http://real.mtak.hu/94339/1/Az_ellatasi_lanc_kiberfenyegetettsege_ku.pdf

Bányász Péter – Krasznay Csaba: Kiberbiztonsági incidensek a magyar közigazgatásban. In *A Jó Állam mérhetősége III.* Budapest, Dialóg Campus Kiadó, 2019. 249–270. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13172/A_Jo_Allam_merhetosege_III_2019.pdf?sequence=1#page=250

Collier, Kevin: Hackers Try to Extort Apple after Stealing Files from Manufacturer. *NBC News,* 2021. június 11. Online: www.nbcnews.com/tech/apple/hackers-try-extort-apple-stealing-files-company-makes-products-rcna750

Dömös Zsuzsanna: Zsarolóvírussal támadták meg az egyik legnagyobb hazai autóalkatrész-kereskedőt. *24.hu*, 2021. április 1. Online: https://24.hu/tech/2021/04/01/zsarolovirus-ransomware-unix/

Europol: *Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic* (2021. június 12.). Online: www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-COVID-19-pandemic

Europol: *Internet Organised Crime Threat Assessment (IOCTA) 2020* (2021. június 12.). Online: www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Fleiner Rita Dominika: SQL inkejcióra épülő támadások és védekezési lehetőségek. *Hadmérnök,* 3. (2008), 4. 117–128. Online: http://hadmernok.hu/archivum/2008/4/2008_4_fleiner.pdf

Ficsor Lajos – Kovács László – Krizsán Zoltán – Kusper Gábor: *Szoftvertesztelés.* (H. n.), Kelet-Magyarországi Informatika Tananyag Tárháza, (é. n.). Online: https://dtk.tankonyvtar.hu/bitstream/handle/123456789/13039/0046_szoftverteszteles.pdf?sequence=2&isAllowed=y

Hackmageddon. Online: www.hackmagaddeon.com

Hun-CERT: *Cross Site Scripting (XSS)* (2012. május 9.). Online: www.cert.hu/cross-site-scripting-xss

Interpol: *Report Shows Alarming Rate of Cyberattacks during COVID-19* (2021. június 12.). Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Koi Tamás: Példátlan krízist okozott itthon a FluBot androidos kártevő. *HWSW,* 2021. március 26. Online: www.hwsw.hu/hirek/63075/flubot-android-kartevo-malware-sms-phishing-adathalasz-tamadas.html

Lee, Ming-Chang: Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. *International Journal of Computer Science and Information Technology,* 6. (2014). 29–45. Online: https://doi.org/10.5121/ijcsit.2014.6103

Munk Sándor: Információbiztonság vs. informatikai biztonság. *Hadmérnök,* 3. (2008), ksz. 1–21.