Jog-Állam-Politika, 2025/3.125
DOI: 10.58528/JAP.2025.17-3.125

GULYÁS KRISZTINA – FARKAS ÁDÁM – KELEMEN ROLAND

Az olasz kiberbiztonság egyes aspektusai 2023-ban

ABSTRACT

Cybersecurity is of paramount importance at the individual, corporate, and public levels. At the individual level, cybersecurity is essential to protect personal information online, preventing data and identity theft and financial loss. At the corporate level, cybersecurity plays a critical role in protecting confidential corporate information and intellectual property. Organizations must ensure the integrity of their systems to maintain customer confidence and remain competitive in the marketplace. Data leaks and cyber-attacks can have serious financial and legal consequences for companies. At the public level, cybersecurity is essential for national security and the protection of citizens. The state must be prepared to protect critical infrastructure, including energy networks, transportation systems, and communications networks. With a population of nearly 60 million people and serious demographic, educational, and economic challenges, Italy has a lot at stake in terms of cyber defense: the growth rate of detected cyber attacks is skyrocketing, with a +169% increase between 2021 and 2022, compared to an average global increase of 21%. According to the Italian police report on the extent of online fraud committed in the first half of 2023 (a period of only six months!), a total of 7,661 cases were reported in five categories (real estate, emotional fraud, online trading, e-commerce, other), with a total of €58,253,567 in material damage.

Keywords: cyberspace ■ cybersecurity ■ SMEs ■ Italy ■ vulnerability

I. BEVEZETÉS

A kiberbűnözési események száma 2023-ban tovább nőtt, és az elkövetkező évekre vonatkozó előrejelzések sem a legfényesebbek. A Cybersecurity Ventures – a világ vezető kibergazdasági kutatószervezete – szerint 2025-re a világot 10,5 billió dollár értékű kibertámadás éri majd, szemben a 2021-es 6 billió dollárral.

Éppen a zűrzavaros helyzet s az egyre komolyabb visszhangot kiváltó esetek (pl. a Westpool botrány 2023. december 08-án) miatt az olasz

média figyelme a témára exponenciálisan megnőtt, így a vállalatok és az állami szervezetek is egyre inkább tudatában vannak a kiberbiztonság stratégiai fontosságának Olaszországban is.

Egy Meltwater által készített „Digital 23" nemzetközi felmérés a kiberincidensek olasz vetületéről meglepő adatokat publikált. Olaszország kicsit kevesebb, mint 59 millió összlakosa (0–100+ évig!) 78,2 millió mobiltelefon-felhasználót (SIM-kártya-birtokost) tesz ki, vagyis a lakosság 132,6%-a rendelkezik mobiltelefon-előfizetéssel/SIM-kártyával. Ez a gyakorlatban jelentheti a magán és a céges mobiltelefonok miatti duplázódást, illetve a mobiltelefonban és a táblagépben vagy a mobilnethez szükséges „pen"-ben a SIM-kártyák miatti duplázódást. A lakosság 86,1%-a (vagyis észszerűen a nagyjából 12 év alatti és a 90 év feletti lakosokat leszámítva mindenki) 50,78 millió lakos internethasználó, és 43,9 millió fő, az összlakosság 74,5%-a rendelkezik aktív szociálismédia-fiókkal (Facebook, Instagram, Tik-Tok, Pinterest, WhatsApp, Messenger). A felhasználók (mint magánszemélyek) a nemzetközi felméréshez viszonyítva hasonló okokból lépnek fel a virtuális térbe: hogy tájékozódjanak, szeretteikkel/barátaikkal kapcsolatot tartsanak, szabadidejüket töltsék, inspirációt keressenek tennivalókhoz vagy megvásárolható termékekhez (inkluzíve online shopping), vagy konkrét tartalmat, pl. videót keressenek. Pénzügyeit az olasz felhasználók több mint egyharmada online intézi.

A felmérés szerint Olaszországban a leggyakrabban használt közösségi platformok rangsorát a WhatsApp vezeti, a 16–64 éves olasz lakosság 89%-a használja, míg a Facebook és az Instagram 78%-kal, illetve 73%-kal a dobogó második és harmadik fokát foglalják el, a Messengert és a Telegramot megelőzve. TikTokot a 16–64 évesek 38%-a használ.

A felmérés összefoglalójában „rémisztő" átlagos fogyasztási/felhasználási statisztika született: az olaszok továbbra is – a Covid-évek óta, melyek Olaszországban komoly fogyasztói ugrást generáltak a szigorú kijárási tilalmak miatt – sok időt töltenek az interneten, mind a keresőmotorokban, mind a közösségi médiában, fejenként átlagosan minden nap legalább napi 6 órát.[1]

Ez nem csupán az online értékesítésnek, de a kiberbűnözőknek is óriási potenciált jelent. Hiszen az elmúlt évek digitális robbanását egyáltalán nem követte, nem kísérte (s megelőzni végképpen nem előzte meg) egy digitális fogyasztói tudatosság kialakulása, kialakítása/nevelése Olaszországban sem. Az olasz belügyminisztérium jelentése szerint csak Milánó városában, 2022-ben a bűncselekmények miatti feljelentések közel 8%-a informatikai csalás kapcsán történt (4.504 esetben).

[1] Statistiche Meltwater, 2023.

II. BÉKE ÉS BIZTONSÁG A DIGITÁLIS TÉRBEN MINT A FENNTARTHATÓ FEJLŐDÉS EGYIK KIEMELT ZÁLOGA A KOMPLEX BIZTONSÁGI KIHÍVÁSOK KORÁBAN

A biztonság komplexitása ma már alapvetés[2] a nemzeti és nemzetközi közösségek működéséről való gondolkodásban. Lényegét tekintve a biztonság az élet minden területére értelmezhető egyes szektoraival. A hagyományos katonai biztonság és közbiztonság mellett, ha csak példákat mondunk az élelmezésbiztonsággal, gazdaságbiztonsággal, közlekedésbiztonsággal, energiabiztonsággal vagy információbiztonsággal, akkor magától érthető, hogy a biztonság társadalmaink működését mind horizontális, mind pedig vertikális értelemben áthatja.

Innen nézve a biztonság nemcsak komplex, hanem a 21. században totális jellegű is,[3] akárcsak az abban dinamikusan változó kihívások, hiszen az élet minden szegmensére hatni tudnak, ténylegesen globálisak és való idejűek, valamint a technológiafejlődés – különösen a kibertér – révén részint már el tudnak szakadni a térbeli kötöttségektől is. Ha úgy tetszik, a biztonsági közeg azért totális, mert abban horizontálisan – azaz a kihívások és fenyegetések típusainak sokasága szerint – és vertikálisan – azaz az egyes konkrét kihívások/fenyegetések hatóképessége szerint – is a szélsőértékek között mozgó és részint kiszámíthatatlan variabilitás van.

Ebből az is következik, hogy a fenntarthatóság alapvető biztonsági kapcsolódásokkal bír, hiszen a környezeti változások, a fogyasztói társadalom kitettsége a különféle ellátási rendszereknek, a gazdasági stabilitásnak és az erőforrásoknak[4] mind-mind magukkal hozzák azt a felismerést, hogy a fenntarthatóság hosszú távú stratégiai érdek, a biztonság megóvása kapcsán is. Ezt a felismerést az éghajlatváltozás és biztonság kapcsolatát vizsgáló munkák[5] vagy épp az erőforrások determinálta konfliktusok[6] mind-mind alátámasztják konkrét katonai, illetve tágabb geopolitikai kontextusban[7] is.

Hajlamosak vagyunk azonban a biztonság megóvása kapcsán teljes hangsúllyal a materiális kapcsolódásokra: az infrastruktúrára, szolgáltatásokra, erőforrásokra fókuszálni. Az információs hadviselés, a dezinformáció és a post-truth jelenségei, hovatovább a hibrid fenyegetések[8] problémaköre azonban pontosan arra világított rá, hogy nemcsak materiális, hanem kognitív, egyéni és társadalmi-pszichológiai értelemben is fenntarthatóságra kell törekednünk ahhoz, hogy a biztonságunk is fenntartható legyen. Társadalmaink működése, sőt számos technikai rendszerünk biztonságos üzemeltetése kapcsán is alapvető kérdés az

[2] Dannreuther, 2013
[3] Farkas, 2018.
[4] Khanna, 2016.
[5] Moran, 2011.
[6] Isaszegi, 2015.
[7] Dalby, 2020.
[8] Giannopoulos – Smith – Theocharidou, 2021.

emberi tényező és ezen belül a kognitív és mentális ellenállóképesség, hiszen ezek nélkül téves információk kelthetnek olyan bizonytalanságot, aminek aztán már a materiális értelemben vett biztonságra nézve is jelentős hatásai lehetnek.

A komplex biztonságból továbbfejlődött totális biztonság korában a különféle védelmi mechanizmusok már nem tudnak kizárólag válságreagálásra, eseménykezelésre fókuszálni. Az állami működés tervezése, szervezés és irányítása során is érvényesíteni kell az egyre átfogóbb biztonsági érdekeket. Ez pedig jelentős kihívás, hiszen a különféle szektorok sajátosságaihoz kell transzformálni a biztonsági specialitásokat és viszont. Ez azt is jelenti, hogy a döntéshozatalnak, a különféle kutatás-fejlesztési tevékenységeknek és végső soron a szabályozásnak és állami működésnek is nyitottabbá kell válnia a biztonsági szemléletre. Ezzel párhuzamosan viszont a biztonsági szférák együttműködőképességét is növelni kell, és a különféle – például katonai, rendőri, hírszerzési, kiberbiztonsági, stb. – speciális szaktudásokra építve szükség van generalisták[9] felkészítésére és alkalmazására is a biztonságpolitikában.

A totális biztonság korában tehát a fenntarthatóság is komplex módon értelmezendő, és ebben a komplexitásban kiemelkedő szerepe van az információk megbízhatóságának, az információfeldolgozási és -ellenőrzési képességeinknek, valamint az egyéni és társadalmi kognitív rezilienciának. Ha úgy tetszik, a fenntarthatóság kulcskérdés az információs társadalom működése és kultúrája tekintetében is, és ebből következően az információbiztonság tágabb értelmezésében is. Ezek hiánya vagy működési zavarai ugyanis olyan biztonsági kitettséget eredményeznek, ami már politikai-legitimációs zavarokhoz, súlyos esetben pedig – például dezinformáción alapuló zavargások szítása esetén – a fizikai biztonság eróziójához vezethetnek. A totalitás korának fenntartható biztonságában ezért szükségszerű egy politikai dimenziót is megfelelően vizsgálni.

Nem véletlen, hogy az Internet Society elnevezésű szervezet által a fenntarthatósági célok elfogadásának évében kiadott dokumentuma rámutat arra, hogy a digitális ökoszisztéma egyes részei (például az IKT-termékek, a szélessávú internet) fontos láncszemei a fenntartható fejlődési célok megvalósíthatóságának. Így például az újonnan kialakuló digitális gazdaság és azon belül a termelés, az elosztás és a fogyasztás a szélessávú internetkapcsolattól függ, e gazdasági szegmensek pedig eszközöket biztosítanak többek között az egészségügy vagy az oktatás számára is. A szervezet pontosan emiatt rendkívül aggasztónak tartja, hogy nincs egy külön fenntartható fejlődési cél, amely az internettel vagy az IKT szektorral foglalkozna.[10] E szűk szegmensű fenntarthatósági cél nem volna elég kifejező, viszont egy ennél összetettebb, vagyis az egész kiber- vagy digitális ökoszisztémát magába foglaló fenntartási cél megfogalmazása mindenképpen átgondolandó és támogatandó.[11]

[9] Epstein, 2021.
[10] Internet Society, 2015.
[11] Clark et al., 2022.

Mindemellett a digitális ökoszisztéma egyes szegmenseit több fenntartható fejlődési cél, vagy azon belüli cél, illetve indikátor is megjelöli. Így például a minőségi oktatáson belül a 4. b cél kimondja, hogy fejlődő országok és kifejezetten az afrikai országok számára a felsőoktatásban való részvételt növelni kell, kifejezetten az információs technológia területén. A nemek közötti egyenlőséget megfogalmazó 5. cél b pontja rámutat arra, hogy a nők helyzetének javulását elősegítő technológiák, így különösen az információs technológiák használatának fokozása és e területeken a nők szerepvállalásának elmozdítása szükséges. A 9-es cél az ipar, innováció és infrastruktúra esetében a rugalmas, fejlődő és fenntartható iparosodás ma már elképzelhetetlen a digitális ökoszisztémához való hozzáférés, annak innovatív felhasználása és fejlesztése nélkül. Mindezek tetőpontjaként értelmezhetők a digitális ökoszisztéma szempontjából a 17-es fenntarthatósági célon belüli a 6-os és a 8-as alcélok, amelyek lényege, hogy fokozni kell a tudomány, a technológia és az innováció területén az együttműködést, valamint a technológiákhoz való hozzáférést és a tudásmegosztást.

Bár expressis verbis a 16-os SDG-cél nem emeli ki a digitális környezetet, azonban a totális biztonság korában, amikor is az állam első védelmi vonala a digitális környezetben már az egyén, akkor a 16-os cél, vagyis a béke, a stabil és átlátható államműködés és azon belül, alcélként megfogalmazott a jogállamiság előmozdítása, a korrupció minden formájának a csökkentése, a hatékony, elszámoltható és átlátható intézmények kialakítása, az információhoz való nyilvános hozzáférés biztosítása, valamint érintett nemzeti intézmények megerősítése az erőszak megelőzésére (a terrorizmus és a bűnözés elleni küzdelemre irányuló kapacitásépítés minden szintjén) mind olyan elvárások, amelyek a digitális ökoszisztémához erősen kötődő állam és társadalom esetében a digitális ökoszisztéma biztonsága nélkül nem tudja megvalósítani. Amihez – a hálózatbiztonságon túl – a kognitív oldal is hozzátartozik, amely egyfelől jelenti az infrastrukturális háttér fejlesztését és folyamatos fejlődését mind az állam, mind a gazdasági szervezetek oldaláról, másfelől pedig a társadalom digitális képességeinek egyre magasabb szintre juttatását.

III. PILLANATKÉPEK AZ OLASZ KIBERBIZTONSÁG JELENLEGI ÁLLAPOTAIRÓL[12]

A Milánói Egyetem informatikai tanszékén székelő Olasz Informatikai Biztonsági Egyesület 2023 végén egy komoly összefoglalót adott ki az olasz kiberbiztonságról. Gabriele Faggioli, az egyesület elnöke nyilatkozataiban elszomorítónak találja a lesújtó eredményeket, s két felvetéssel él, melyeket megfontolásra javasol. Elmondhatjuk, hogy a közel 60 millió lakosú, komoly demográfiai, oktatási és gazdasági kihívásokkal küzdő ország esetében a tét nem kevés. Alapvető kérdései a jelenlegi olasz helyzet elemzése után:

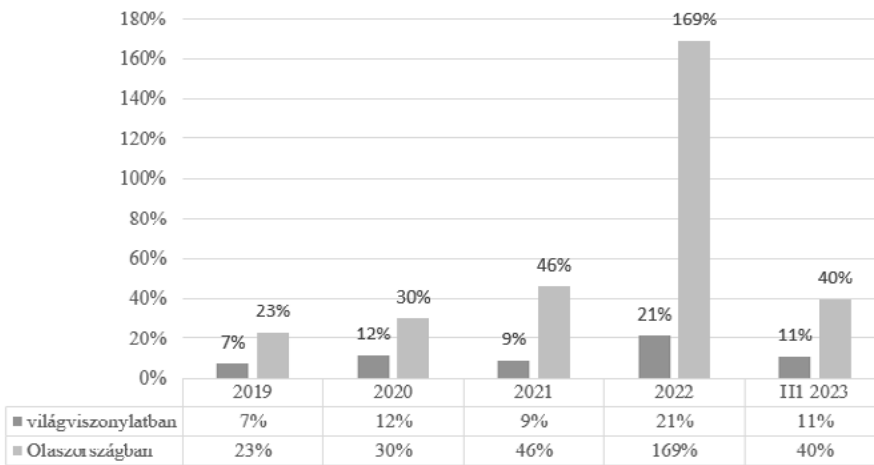
[12] Rapporto Clusit, 2023.

„A) reálisan arra a valós lehetőségre kellene összpontosítania az olasz államnak, hogy a kiberkultúra minden korú és foglalkozású polgárban növekedjen, és hogy

B) olyan állami- és magánstruktúra jöjjön létre, amely a nagy központi és multinacionális államigazgatási szervektől a legkisebb vállalatokig és szakmai cégekig képes megfelelően karbantartott és védett technológiákkal rendelkezni, és képes a szükséges forrásokat befektetni."[13]

A jelentésben feldolgozott adatok szerint Olaszországban tavaly havonta körülbelül 22 komolyabb kibertámadást észleltek, ami 40%-kal több az előző évhez képest. 2018-tól 2023 júniusáig 505 különösen súlyos támadás történt olasz érdekeltségek ellen, és ebből nem kevesebb, mint 132 (26%) csak 2023 első hat hónapjában történt a Clusit felmérése szerint.

A jelentés szerint ez a növekedési ütem komoly aggodalomra ad okot, hiszen 2022-ben egész évben 188 támadást észleltek, ami már akkor negatív rekordot jelentett 169%-os növekedéssel 2021-hez képest, miközben világszerte átlagosan 21%-os növekedés volt tapasztalható.



	2019	2020	2021	2022	III 2023
világviszonylatban	7%	12%	9%	21%	11%
Olaszországban	23%	30%	46%	169%	40%

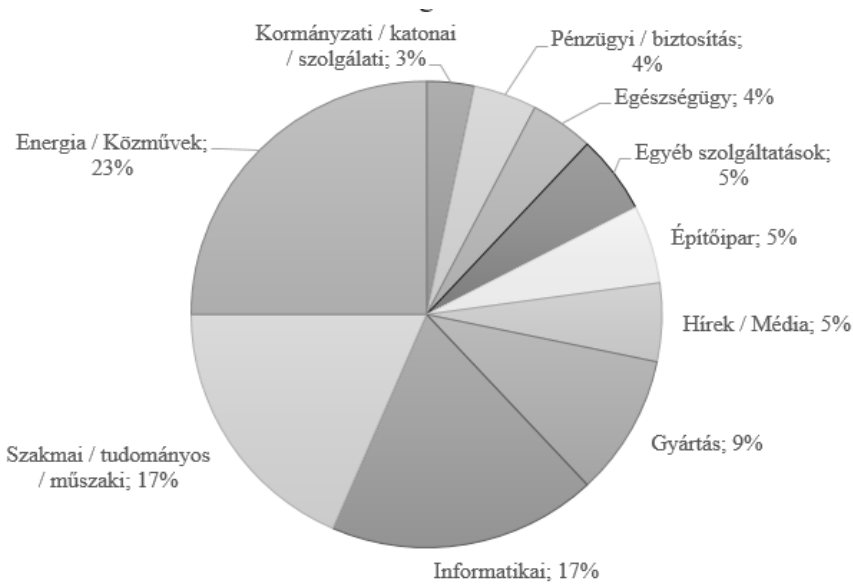
1. ábra: A kibertámadások növekedési ütemének összehasonlítása 2018-2023 H1 (Forrás: Rapporto Clusit, 2023)

Az olasz támadások besorolásában a hackertámadások száma 2023 első félévében elérte a 30%-ot (2022-ben ez csak 6,9% volt), 69%-uk a kiberbűnözésből eredt, míg 1% a kémkedés-szabotázs kategóriájába tartozott a szakértők szerint. A hackertámadások számának emelkedését az orosz–ukrán háborús konfliktus

[13] Rapporto Clusit, 2023.

folyományaként is lehet értelmezni, ezekre azonban semmilyen konkrét vagy egyértelmű bizonyíték nincs, ezt a tanulmány is kiemeli. A „kémkedés / szabotázs" kategóriába tartozó támadások 1%-os szeletét illetően megjegyezzük, hogy 2020 óta ez az első alkalom, hogy Olaszországban ebbe a kategóriába soroltak be incidenseket.

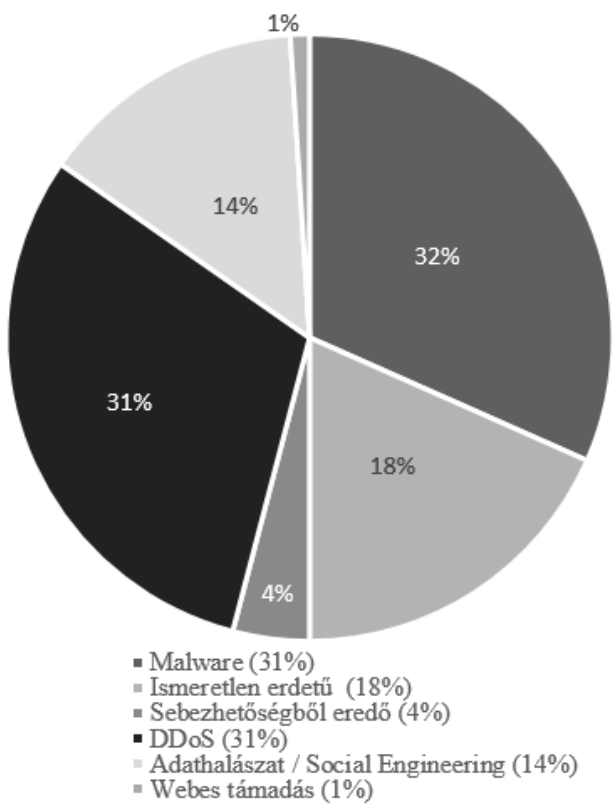
A Clusit kutatás eredményeiből az is egyértelműen kiderül, hogy a kormányzati szervek (23%) és a feldolgozóipar (17%) voltak az incidensekben leginkább érintett ágazatok 2023 első felében Olaszországban. Ez a megoszlás jelentősen eltér a világméretű mintától, ahol a két kategória a támadások 12%-át, illetve 5%-át teszi ki. Még szemléletesebb mutató, hogy az Olaszországban észlelt, „feldolgozóipar ellen elkövetett" incidensek az ezen ágazat ellen világszerte elkövetett támadások 34%-át teszik ki.



2. ábra: Az olasz áldozatok ágazat szerint besorolása, 2023 H1
(Forrás: Rapporto Clusit, 2023)

Az észlelt súlyos incidensek számának növekedése a „pénzügyi/biztosítási" ágazatban volt tapasztalható, mely a negyedik helyre ugrott a támadások 9%-ával (2022-ben az arányuk csupán 3,7% volt). A támadásokat elemezve a szakértők megállapították, hogy az egyik tényező, amely a legnagyobb hatással volt erre a negatív tendenciára, az egyre több szereplő (pl. az úgynevezett fintechek) megjelenése, valamint a banki és biztosítási folyamatok és szolgáltatások kiszervezésének egyre szélesebb körű alkalmazása, ami miatt ez a piac egyre inkább széttöredezetté és sebezhetővé vált az olyan támadásokkal szemben.

A kutatók a kiberbűnözők által használt fő támadási technikákat is elemezték. A rosszindulatú szoftverek továbbra is a bűnözők által használt fő támadási technika (31%) volt, de sokkal kevésbé következetesen, mint egy évvel korábban (2022-ben 53% volt az arány). Abszolútértékben a malware-támadások száma nem csökkent jelentősen, de az alacsonyabb százalékos arány azt jelzi, hogy a zsarolóprogram jelenség kirobbanása óta először figyelhettek meg Olaszországban jelentős változást a támadók céljai elérésének módjában, akik nyilvánvalóan más technikák alkalmazásával hatékonyabban érik el céljaikat. Ezt a tényt a kutatók szerint azt bizonyítja, hogy a DDoS-támadások száma jelentősen növekszik, ahogy a fenti ábrán is látható, a 2022-es 4%-ról 2023 első felére ijesztő 30%-ra emelkedett az arányuk, ami ötszörös növekedést jelent. Az ilyen típusú támadások előfordulása Olaszországban kirívó mértékben magas.



3. ábra: Kibertámadások típus szerint – Olaszország, 2023 H1
(Forrás: Rapporto Clusit, 2023)

A DDoS-támadások a hackerek által céljaik eléréséhez leggyakrabban alkalmazott technikák közé tartoznak, melyek célja egy online szolgáltatás elérhetetlenné/használhatatlanná tétele annak erőforrásainak (hálózat, feldolgozás, tárolás...) túlterhelésével.

A hackerek ezt a technikát előszeretettel használhatják egy vállalat vagy intézmény tevékenységének megzavarására, azzal a céllal, hogy a média figyelmét egy politikai vagy társadalmi ügyre irányítsák, ezáltal nyomást gyakorolva az áldozatra és rávilágítva annak védekezési képességeinek hiányára.

A kutatás eredményei rávilágítanak, hogy az adathalász és social engineering támadások is egyre gyakoribbak Olaszországban, amelyek – a 2022-es évtől eltérően – már egy félév alatt nagyobb arányban fordultak elő 2023 H1-ben, mint a világ többi részén (14% Olaszországban vs. 8,6% globálisan), ami azt jelzi, hogy az információs rendszerekkel napi szinten foglalkozó felhasználók részéről nagy szükség lenne a tudatosságra és a kiberfenyegetésekkel kapcsolatos tudatosság növelésére.

A 2023 első félévben elkövetett online csalások mértékéről az Olasz Posta- és Kommunikáció Rendőrség kimutatást készített, melyben kimutatták, hogy az öt kategóriában (ingatlanszektorral kapcsolatos esetek, érzelmi vonalra alapozó csalások, átverés, online trading, e-commerce, egyéb) összesen 7.661 feljelentés született 2023 első hat hónapjában, melyek összesen 58.253.567 Euró kárt tettek ki, és összesen 1853 gyanúsított meghallgatásával jártak az ügyek felderítése során.

Ez annyit tesz, mintha 2023 első hat hónapjában Olaszország minden lakója átlagosan – a 0-99+ évesek is –, fejenként 1 eurónyi kárt szenvedtek volna online csalások okán.

4. ábra: Online csalások ügyében tett feljelentések statisztikája Olaszországban, a 2023. január 1. és június 30. közötti időszakban (Forrás: Rapporto Clusit, 2023)

A Clusit tanulmányában van egy kkv-król szóló rész. A Lombardia régió Varese és Como tartományaiban végzett kiberbiztonsági kérdőíves felmérés 2022 novembere és 2023 júliusa között zajlott, a Reti S.p.A. közreműködésével, amelynek keretében 150 vállalat – legnagyobb arányban kkv-k – válaszolt a feltett kérdésekre. Az adatok heterogén helyzetet mutatnak a felmérésben részt vevő vállalatok között a méret és a forgalom tekintetében. A részt vevő vállalatok méretét illetően széles skálán mozognak a különbségek, egyes vállalatok jelentős számú alkalmazottat foglalkoztatnak, míg mások a létszámot tekintve jóval kisebbek.

A részt vevő vállalatok mérete túlnyomórészt kicsi volt, 37%-ban 10 főnél kevesebb alkalmazottat foglalkoztatnak; a felmérésben részt vevő összes cég átlagos dolgozói létszáma 18 fő volt. Az árbevétel is nagyon változatos képet mutatott, de a méret és az árbevétel közötti összefüggés eredménye reálisnak tűnik. A válaszadók 97%-a rendelkezik saját honlappal, de csak 18%-uk üzemeltet webshopot. Tekintettel azonban a minta kis méretére, ez nem tekinthető különösebben a széleskörű valóságot jelző adatnak, és keresztelemzést sem végeztek. Ami az e-maileket illeti, ma már a felhőalapú rendszerek vannak túlsúlyban, de összesen a megkérdezett csupán 31%-a állította, hogy dedikált, belső céges rendszerben használja az e-maileket. Némi aggodalomra ad okot a „fogyasztói" szintű szolgáltatásokkal (ingyenes levelezőrendszerek, mint a „gmail.com", stb.) beérő számos kkv, ami nem szól e vállalatok erős technológiai érettsége mellett, még akkor sem, ha sok esetben kis vagy nagyon kis cégekről van szó. Nem lehet elégszer hangsúlyozni, ha kkv-ról van szó, milyen fontos lenne a professzionális szintű levelezőszolgáltatás használata, mivel általában olyan biztonsági funkciókkal van felszerelve, amelyekkel a magánfelhasználóknak szánt (sokszor ingyenes) levelezőrendszer nem rendelkezik.

A megkérdezett vállalatok informatikai és kiberbiztonsági felépítése egyértelműen mutatja a vállalatok eltérő érettségi szintjét a kérdéssel kapcsolatban. Az IT-feladatokat a legtöbb esetben belső munkatárs végzi részben vagy egészben, és csak a vállalatok körülbelül ötöde támaszkodik kizárólag külső szolgáltatókra. Mely érthető, tekintve a mintában szereplő vállalatok átlagosan kis méretét.

Ami viszont a kiberbiztonságot illeti, csak alig több mint 20 százalékban dedikálnak a cégek belső személyeket, míg a minta több mint egyharmadában nincs azonosított személy, még külsős sem. Ezekben az esetekben azt kell feltételeznünk, hogy szükség esetén más feladatoktól elvont emberek gondoskodnak kiberbiztonsági feladatokról; hogy milyen készségekkel és milyen felkészültséggel, azt nem lehet tudni. A válaszadó cégek 22%-ánál belső csapat foglalkozik a kiberbiztonsággal, 27%-nál egy vegyes belsős és külsős emberekből álló csapat, 16%-ban külsős beszállító, míg 35%-ban senki. Jellemző, hogy ezekben az esetekben még külső csapatra sem utalnak a kutatók szerint, azaz kénytelenek vagyunk azt gondolni, hogy a vállalat még csak nem is azonosított előre egy olyan potenciális beszállítót, akihez szükség esetén fordulhat, holott triviális tény, hogy a például egy adatvédelmi incidens felfedezését követő nehéz pillanatok

nem a legalkalmasabbak arra, hogy egy ilyen kényes kérdésben higgadtan és körültekintően válasszunk beszállítót.

A válaszadók közül a 20 főnél kevesebbet foglalkoztató olasz kkv-k kevesebb, mint 30%-a rendelkezik írott IT-eszköz-szabályzattal, míg az összes válaszadó 150 cég közül – tehát mérettől függetlenül – 75 cégnél nem létezik ilyen írásos szabályzat. Ez egy komoly veszélyforrás lehet, hiszen a céges laptop vagy okostelefon kiberbiztonsági szempontból nem megfelelő használata óriási veszélyeket hordoz magában. Biztonsági kérdés, hogy van-e vagy nincs a vállalat által átadott informatikai eszközök használatára vonatkozó szabályozás a dolgozók számára. Ez a szabályozás részét képezi az olasz adatvédelmi hatóság által is erősen ajánlott intézkedéseknek, és ezért általában a „minimális védelmi felkészültség" részét képezi az adatvédelem területén is. Minden olyan vállalatnak, még a kicsiknek is, amely alkalmazottait (akár csak egyet is) informatikai eszközökkel látja el, rendelkeznie kellene írásos szabályozással, melyet az alkalmazottakkal megfelelően ismertetni is ajánlott, elmagyarázva a veszélyeket, a miérteket és a lehetséges következményeket.

A válaszadókat a közelmúltban érintő kiberbiztonsági incidensek kapcsán az érintett cégek aránya 37% volt (18%-nál egy éven belül, 9%-uknál 1 és 2 év között, míg 10%-uknál 2 évnél régebben történt). 63%-uk nem szenvedett kibertámadást, vagy legalábbis a válaszadó személy nem tudott róla. A megkérdezett vállalatok 2%-a nem tudja, mi (lenne) a teendő kibertámadás / IT havária esetén. 26%-uknál van írásbeli utasítás, 19%-uknál informális eljárás ismeretes, míg a válaszadók 53%-a „felhívna valakit ebben az esetben"".

Ugyanezt az incidensekre való felkészültségre vonatkozó adatsort összefüggésbe hozva az incidensek időbeli távolságával, azt várhatnánk, hogy minden, korábban incidensben már érintett vállalat elhivatott lesz hivatalos eljárást elfogadni, s az írásbeli eljárási utasítások számának növekedését várnánk az idő múlásával. A szomorú valóság az az, hogy csupán kis különbséget látunk azon vállalatok hozzáállása között, akiket soha nem érintettek kibereesemények és azok között, akiket érintettek, de nincs jelentős korreláció az eseményt következő időszakokban tanúsított tudatos viselkedés és az azóta eltelt idő kapcsolatában.

A kérdésekre adott válaszok alapján a kiberbiztonsági képzési helyzet meglehetősen komor képet fest, s talán csak az adatvédelem terén kevésbé elkeserítő. Ez utóbbinak véleményünk szerint az oka, hogy a GDPR már 2018 óta napirenden van, így az eltelt idő hosszúsága és a GDPR kötelező, kikényszerített és büntetésekkel szankcionálható mivolta „motiválták" a vállalatokat. Míg a kiberbiztonság témaköre új, a NIS2 még nem fejtette ki hatását, s az első érintettségig sokan azt hiszik, vállalatvezetők és tulajdonosok is (ahogy a magánszemélyeknél is jellemző), hogy „ez velük sohasem történhet meg". A válaszadók 9%-ánál csupán adatvédelmi, 4%-ánál csak cybersecurity-ről van belső céges IT-oktatás, 56%-uknál egyik sincs, és csak 29%-uknál van mindkét témára oktatás. A válaszadók 2%-a nem tudja, van-e egyáltalán bármilyen IT-oktatás a cégénél. Pedig a munkavállalók IT-oktatása kulcsfontosságú, hiszen ők jelentik az első és sokszor utolsó

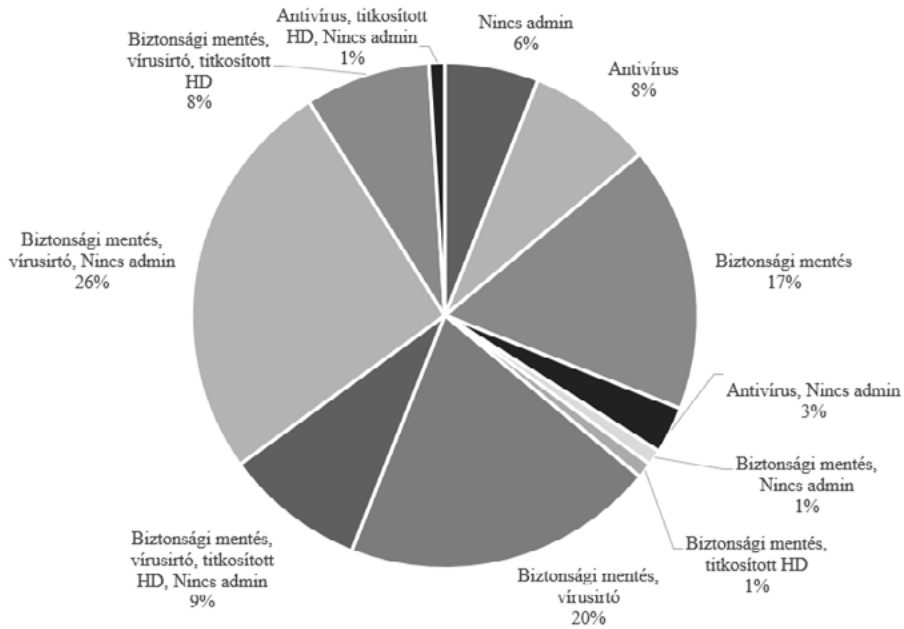
„védelmi vonalat" egy kis cég esetében. Egyetlen munkavállaló figyelmetlensége (pl. adathalász linkre kattintás), illetve nem megfelelő, szabálykövető magatartása, egyetlen hibás lépése (például tiltás ellenére külső, fertőzésgyanús meghajtót csatlakoztat a vállalati rendszer egy gépéhez) a teljes vállalatot veszélybe sodorhatja. S ha egy ilyen, balszerencsés esetben nincs azonnal reagálni tudó, képzett szakember a cégnél (belső vagy külső munkatárs), akkor a reakcióidő hosszúra nyúlása és a kár mértéke egyenesen arányosan nőnek majd.

A megkérdezett vállalkozások 87%-a rendelkezik tűzfallal a vállalati belső hálózat védelmére, 1%-uk egyáltalán nem, 12%-uk pedig nem tudja, használnak-e egyáltalán ilyet a cégénél.

Ellentmondásosabbak azonban az ellenőrizetlen eszközök hálózathoz való hozzáférésére vonatkozó adatok: míg a kívülről (pl interneten keresztül) történő külső hozzáférés a belső vállalati rendszerhez a vállalatok nagy többségénél lehetetlen vagy legalábbis nagyon ritka, ugyanakkor a személyes eszközök engedélyezésének gyakorlata a hálózaton belül a vállalatok 38%-ánál lehetséges és gyakori szokás. Határozottan kijelenthetjük, hogy ez nagyrészt semmissé teszi az első ellenintézkedés hatékonyságát. Valójában egy ellenőrizetlen eszköz használata a hálózaton belül ugyanolyan bizonytalan, ha nem rosszabb, mint az interneten keresztül történő hozzáférés. Csupán a vállalkozások 31%-ánál nem lehetséges személyes eszközt hálózatra csatlakoztatni. Ami a hitelesítést illeti, szintén jelentős probléma a kiberbiztonsági szempontból történő alulértékelése. Ez nem lenne indokolt, hiszen számos erős hitelesítési mechanizmus áll rendelkezésre, például az okostelefonok alkalmazásain keresztül az egyszer használatos jelszavak, a biometrikus autentikáció mellett számos lehetőség kínálkozik, ingyen vagy bagatell áron. A 150 kkv csupán 9%-ánál kötelező a többfaktoros/többlépcsős beléptetés a vállalati rendszerbe; 22%-uknál többlépcsős és lejárathoz kötött jelszóval kombinált azonosítás működik; 3%-uknál általános jelszavakkal kombinált; 1%-uknál többlépcsős általános jelszóval kombinált; 45%-uknál lejárati időhöz kötött jelszavak; míg 21%-uknál általános jelszavak jelentik a hitelesítést.

A vállalatok kiberbiztonsági felkészültségének és viselkedésének témakörében négy olyan biztonságtechnológiai intézkedés jelenlétét is felmérték a vállalatoknál, amelyek nagyon kiforrottak és elterjedtek, és amelyek költsége ma már elenyésző vagy akár nulla:

- központosított biztonsági mentés („Backup")
- irányított vírusirtó a vállalati eszközökön („Antivirus");
- a személyes mobileszközök (laptopok, okostelefonok stb.) konfigurálása úgy, hogy a felhasználó nem rendelkezik adminisztrációs jogosultságokkal („No admin");
- a laptopokon tárolt adatok védelme titkosítással („Encrypted HD").



5. ábra: Biztonsági intézkedések típusai
(Forrás: Rapporto Clusit, 2023)

A fenti grafikon az intézkedések különböző kombinációinak elterjedtségét mutatja, amelyből látható, hogy a mintának csak 9%-a alkalmazza mind a négy intézkedést, és a vállalatok kevesebb mint fele alkalmaz legalább hármat. Nagyon elgondolkodtató, rémisztő adat, hogy a válaszadó 150 vállalat 17%-ánál csak Backup van; 8%-uknál csak Antivírus, de összesen 19 %-uknál Backup egyáltalán nincs. Vagyis egy adatvesztés, egy zsarolóvírus vagy bármilyen kiberbiztonsági incidens után a 150 cégből 28,5 cég semmilyen módon nem tudna semmilyen céges dokumentumból egy mentett biztonsági másolatot elővenni, sem vevői adatokat, sem pénzügyi dokumentumokat, szerződéseket, semmit.

Megállapítható, hogy a legkevésbé elfogadott intézkedés a merevlemez titkosítása, annak ellenére, hogy ez szinte ingyenes (szinte minden operációs rendszer és vírusirtó szoftver árában benne van), és az egyetlen, védelmet nyújtó megoldás az eszköz lopása vagy elvesztés esetén.

Végezetül a „felhőmegosztási" technológiák elterjedését illetően, amelyek kiváló módját jelenthetik az adatok védelmének egy ellenőrzött környezetben (feltéve természetesen, hogy az ember megbízik a szolgáltatóban, minőségi beszállítót választva), és – ha jól használják – védvonalat jelenthetnek a különböző rosszindulatú szoftverekkel szemben. Ezeknek a technológiáknak az az előnye is megvan, hogy szinte mindig ingyenesek, egy kezdeti időszakban és/vagy bizonyos szolgáltatások árában foglalt adatmennyiség esetén, mely kkv-k esetén vagy induló vállalkozásoknál mindenképp jó érv ezeknek a biztonsági megoldásoknak a használatra.

IV. DE MIT IS TESZ MINDEKÖZBEN AZ OLASZ ÁLLAM?

Olaszországnak is megvan a maga nemzeti kiberbiztonsági stratégiája, amióta a Mario Draghi volt miniszterelnök által elnökölt kiberbiztonsági tárcaközi bizottság (CIC – Comitato Interministeriale sulla Cybersecurity) 2021. május 18-án jóváhagyta a Nemzeti Kiberbiztonsági Ügynökség (ACN – Agenzia per la Cybersicurezza Nazionale) által kidolgozott kiberstratégiát.

Olaszországban a sajtóban szinte napi szinten kiemelik, hogy a hibrid háború keretében az országot, az olasz gazdasági érdekeket is sújtó kibertámadások – amelyeket az ukrán–orosz invázió súlyosbított – bizonyítékul szolgálnak a vállalkozásoknak okozott gazdasági és hírnévbeli károkról, az energetikai infrastruktúrák működésének blokkolásáról, a kórházak és az egészségügyi vállalatok által használt információs rendszerek meghibásodásáról, sőt közszereplők, újságírók és politikai aktivisták személyes adatainak terjesztéséről.

A 2022-től 2026-ig tartó időszakra szóló olasz nemzeti programstratégia (PNRR – Piano Nazionale di Ripresa e Resilienza per il digitale e la sicurezza informatica) egy komoly és részletesen kidolgozott szakmai csomagból áll. A kiberstratégia meghatározásával és a végrehajtási tervvel az olasz kormány a kibertér artikulált dimenziójára jellemző kihívások sokaságát kívánta/kívánja kezelni. Az ACN-jelentésekből kiderül, hogy az olasz kiberbiztonsági nemzeti startégiában négy fő területre összpontosítanak:

1. „az ellenálló képesség erősítése az ország rendszerének digitális átállásában (kiberbiztonság).
2. a stratégiai autonómia elérése a kiberdimenzióban – a kiberbűnözés megelőzése;
3. a kiberfenyegetettség alakulásának előrejelzése – az ország védelmi és katonai biztonsága;
4. a kiberválságok kezelése - kutatás és információfeldolgozás."[14]

Az olasz felelős szakmai vezetők megfogalmazták, hogy az olasz állam feladatai közé tartozik, hogy megfelelő kiberbiztonsági stratégiákat határozzon meg, amelyek célja olyan intézkedések tervezése, koordinálása és végrehajtása, amelyek az országot a digitális térben is biztonságossá és ellenállóvá teszik, miközben biztosítják az állampolgárok bizalmát a versenyelőnyök kihasználásának lehetőségében, az alapvető jogok és szabadságok teljes körű védelmében. Kiemelték, hogy a kiberbiztonságnak – amely stratégiai jelentőségű kérdéssé vált – a digitális átalakulás nélkülözhetetlen elemeként támogatnia kell az ország digitalizációs folyamatát, ebben az ágazatban a stratégiai nemzeti autonómia elérése érdekében is, s ezt nem költségként, hanem beruházásként és a nemzeti gazdaság és ipar fejlődését elősegítő tényezőként kell felfogni, hogy az ország versenyképessége globális szinten növekedjen.

[14] PNRR, 2024.

Célul tűzik ki, hogy az infrastruktúrák, a közigazgatási/adminisztratív rendszerek és információk technikai szempontból történő biztosítását a társadalom minden szintjén kulturális fejlődésnek kell kísérnie a „biztonságorientált" megközelítés felé, amely elengedhetetlen építőköveként az emberek, a vállalatok értékrendjébe kell, hogy beépüljön a nemzet- és közbiztonság, valamint a demokrácia védelme érdekében.

Elismerik, hogy a gyors technológiai változások mindig új kiberbiztonsági kockázatokat hoznak magukkal, és az olasz nemzeti kiberbiztonsági stratégia a következő kihívások kezelésére törekszik:

- „A közigazgatás és a termelési struktúra kibernetikai szempontból ellenálló digitális átállásának biztosítása: A digitális szolgáltatások kiberbiztonsága alapvető fontosságú ahhoz, hogy javuljon azok használhatósága a polgárok számára, akiknek bízniuk kell abban, hogy adataik védve vannak.
- A kiberfenyegetettség alakulásának előrejelzése: A támadó kibertevékenységek hatásait előre kell jelezni, meg kell előzni és a lehető legnagyobb mértékben enyhíteni kell.
- Az online dezinformáció elleni küzdelem az úgynevezett hibrid fenyegetés tágabb kontextusában: Az alapvető szabadságjogok gyakorlásának biztosítása, például választások idején vagy nemzetközi válsághelyzetekben.
- Kiberválságkezelés: A rendszerszintű kibernetikai események esetén azonnali reagáláshoz az összes köz- és magánérdekelt fél közötti koordinációra van szükség.
- Nemzeti és európai stratégiai autonómia a digitális területen: Közvetlen ellenőrzés a modern technológiákon keresztül tárolt, feldolgozott és továbbított adatok felett."[15]

Olaszország kibervédelmi kihívásainak legjobb kezelése érdekében a nemzeti kiberbiztonsági stratégia három fő célkitűzést határozott meg:

- „Védelem: A nemzeti stratégiai eszközök védelme kockázatkezelésre és kockázatcsökkentésre irányuló megközelítéssel, amelyet egyrészt szabályozási keret, másrészt az ország rugalmas digitális átállását lehetővé tevő intézkedések, eszközök és ellenőrzések alkotnak.
- Reagálás: A nemzeti kiberfenyegetésekre, incidensekre és válsághelyzetekre való reagálás a teljes nemzeti kiberbiztonsági ökoszisztémát magában foglaló folyamatok megfigyelésére, észlelésére, elemzésére és aktiválására szolgáló rendszerek révén.
- Fejlesztés: A digitális technológiák biztonságos fejlesztése a piaci igények kielégítése érdekében, a kiválósági központok, kutatási tevékenységek és vállalkozások támogatását célzó eszközök és kezdeményezések révén."[16]

[15] PNRR, 2024.
[16] PNRR, 2024.

A többszáz, konkrétan meghatározott intézkedési pontból kiemelkedik a 12. intézkedés, mely a következőket irányozza elő: „Feladatunk a nemzeti védelem, az ellenálló képesség, a bűnözés elleni küzdelem és a kibernetikai hírszerzés képességének további fokozása a helyzetfelismerés további erősítése révén, a fenyegetések, sebezhetőségek és támadások folyamatos figyelemmel kísérése és elemzése révén, a konkrét felelősségi köröknek megfelelően."[17]

A 33. intézkedés pedig éppen a közigazgatás és a teljes olasz termelési rendszer számára egy támogatási rendszer kiépítését célozza meg: „A kiberválságok utáni reagálási és helyreállítási képességek növelése az integrált ágazati hálózatának, valamint egy nemzeti válságkezelési tervnek a megvalósításával, amely meghatározza az állami és magánszereplőkkel összehangoltan alkalmazandó eljárásokat, folyamatokat és eszközöket, a hálózatok, információs rendszerek és IT-szolgáltatások működési folyamatosságának biztosítása céljából."[18]

Az olasz kormány kiberstratégiájának 49. intézkedésében megfogalmazott célja, hogy megvalósítson egy úgynevezett „nemzeti kiberbiztonsági parkot", amely a kiberbiztonság és a digitális technológiák területén végzett kutatási és fejlesztési tevékenységekhez szükséges infrastruktúráknak ad otthont, kiterjedt struktúrával, az ország egész területén elosztott telephelyekkel.

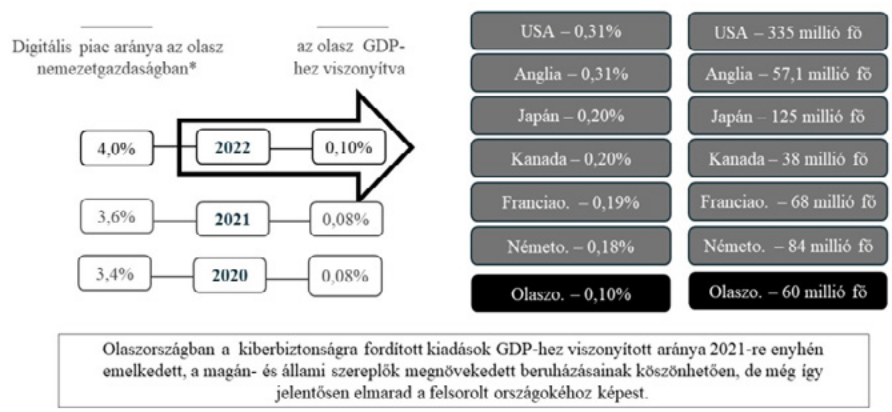
Végül érdemes megemlíteni a kiberstratégia „A technológiai innováció és a digitalizáció ösztönzése" című szakaszában szereplő intézkedéseket, amelyek az új technológiák kutatásának és fejlesztésének fontosságát hangsúlyozzák. Különösen az 53. intézkedés célja kiemelendő; „minden olyan hasznos kezdeményezés előmozdítása feladat, amely Olaszország ipari- és technológiai autonómiájának megerősítését célozza a stratégiai jelentőségű IT-termékek és -folyamatok tekintetében, valamint a nemzeti érdekek védelmét szolgálja az ágazatban, a saját fejlesztésű algoritmusok fejlesztésének, valamint a kutatásnak és az új nemzeti kriptográfiai képességek elérésének fokozásával is", míg az 54. intézkedés célja „a kutatás és fejlesztés támogatása, különösen az új technológiák terén, a kiberbiztonsági elvek beépítésének előmozdítása, valamint a magánszektor – különös tekintettel az induló vállalkozásokra és az innovatív kkv-kra – és a nemzeti területen működő kompetencia- és kutatóközpontok kiberbiztonsági projektjeinek támogatása, többek között finanszírozás, állami és magánbefektetések és egyszerűsítési mechanizmusok révén."[19]

Az olasz kormány 2023 év elején úgy döntött, hogy a bruttó nemzeti beruházások 1,2 százalékát különíti el a digitális szférában a technológiai autonómiát garantáló, konkrét projektek finanszírozására és a nemzeti információs rendszerek kiberbiztonsági szintjének emelésére. A kormány által kidolgozott nemzeti stratégia emellett jelentős támogatást irányoz elő a kiberbűnözés által szintén célzottan érintett magáncégek számára is: számukra adókedvezményeket biztosítanak. Ezek a beruházások hozzáadódnak ahhoz a 623 millió euróhoz,

[17] PNRR, 2024.
[18] PNRR, 2024.
[19] PNRR, 2024.

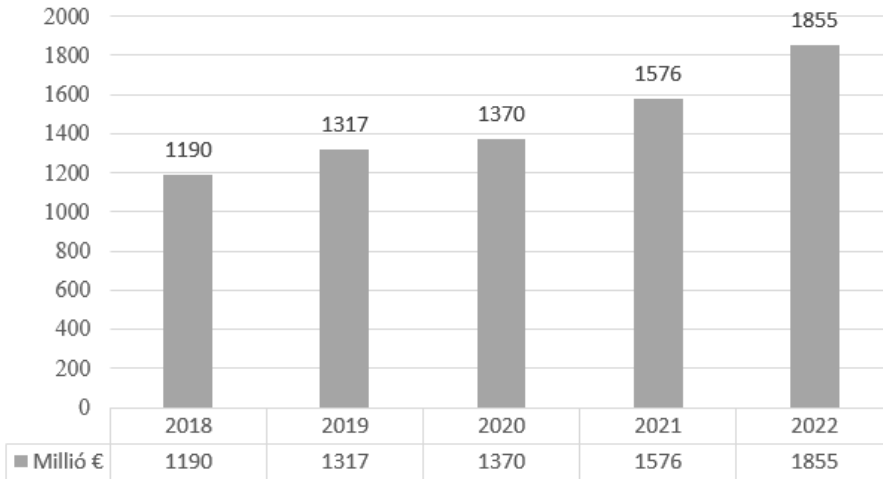
amelyet a PNRR már előirányzott, és amelyet a kiberügynökséghez mint a nemzeti helyreállítási és ellenálló képességi terv végrehajtójához rendeltek.

Az egyre növekvő veszélyhelyzettel szembesülve Európában – de világszinten is – egyre inkább terjednek a holisztikus kiberfenyegetés-kezelést támogató megközelítések a fejlett kockázatkezelési stratégiákon belül. A beruházások Európában azonban továbbra is (nevetségesen) alacsonyak, és sok vállalat még mindig nem tudja számszerűsíteni egy kedvezőtlen esemény gazdasági hatásait. A kiberbiztonság továbbra is határozottan a digitális beruházási prioritások élén áll Olaszországban, mind a nagyvállalatok, mind a kkv-k esetében. A PNRR által közvetített gyorsulás, valamint az európai adatvédelmi joggal (GDPR) kapcsolatos adatvédelmi kérdések egyre nagyobb hangsúlya a kiberbiztonsági kiadások GDP-hez (bruttó hazai termék) viszonyított arányát a 2021-es 0,08%-ról 0,10%-ra emelték 2022-ben. Ez sajnos még mindig messze elmaradt a többi G7-ország átlagától, ahol az Egyesült Államok és az Egyesült Királyság vezeti az adatvédelemre leginkább odafigyelő nemzetek rangsorát 0,31%-os aránnyal, őket követi Franciaország (0,19%) és Németország (0,18%).



6.ábra: Nemzetközi kitekintés a 2022. évre – Kiberbiztonságra fordított kiadások arányai a GDP és a lakosság viszonylatában
(Forrás: Rapporto Clusit, 2023)

Összességében az olasz kiberbiztonsági piac értéke 2022-ben 1,86 milliárd euró volt, ami 18%-os növekedést jelentett a 2021-es évhez képest.



7. ábra: Olasz kibervédelmi beruházások, kiadások értéke 2018-2022
(Forrás: Rapporto Clusit, 2023)

„Ma a fő kihívás egy strukturált hosszú távú stratégia meghatározása, a fenyegetésekkel szembeni közös front kialakítása – mondta sajtónyilatkozatában decemberben Alessandro Piva, a Kiberbiztonsági és Adatvédelmi Megfigyelőközpont igazgatója – Ehhez a célhoz a vállalati prioritásokra összpontosított pénzeszközökkel történő beruházásokra, kiberbiztonsági ismeretekkel rendelkező szakképzett személyekre és strukturált képzési tervekre van szükség minden vállalati szint számára, valamint kiforrott megközelítésű kiberkockázat-kezelésre, egy integrált kockázatkezelési folyamat keretében, amely a vállalati vezetőség számára könnyen érthető pénzügyi számszerűsítési mérőszámokon alapul."[20]

V. KONKLÚZIÓ

Az olasz vállalkozások, főként a kkv-k még mindig inkább „kezdőként" viselkednek a főbb kiberbiztonsági kérdésekben, s ezt a kiberbiztonsági éretlenséget a kiberkockázati kultúra előmozdításával lehetne leküzdeni. Olaszországban ugyanúgy, ahogy Magyarországon is. Olyan helyzetbe kellene hozni a vállalkozókat, hogy tudják, hogyan kezeljék a kiberincidensekből eredő kockázatokat. Ehhez jön még hozzá az a kihívás, amelyet az olyan bomlasztó technológiák meg-

[20] PNRR, 2024.

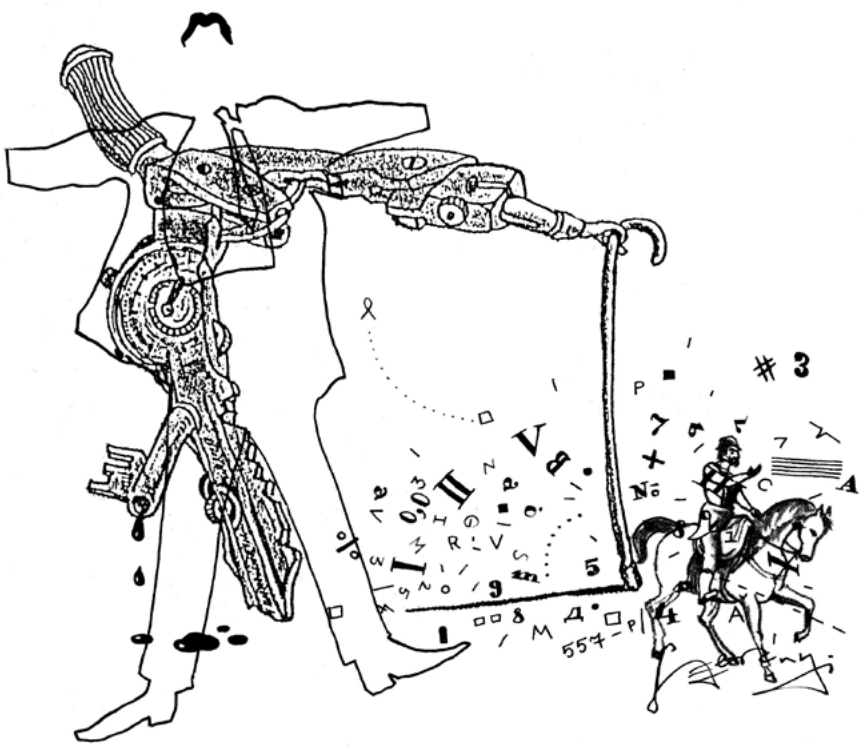
jelenése jelent, mint a mesterséges intelligencia és a kvantumszámítástechnika, az ezzel járó összes lehetőséggel és kockázattal együtt. Egy másik fenyegetés a távmunkásokat érinti, akik továbbra is a hackerek egyik fő célpontjai. A kibertámadások e típusának növekedése világszerte megfigyelhető, az RDP-n (Remote Desktop Protocol, távoli asztali protokoll) keresztüli brute force támadások 300 százalékos növekedésével. El kell felejteni a mítoszt, nincsenek olyan vállalatok, amelyek nem vonzóak a hackerek számára, és ezért immunisak a kiberbűnözéssel szemben.

A kiberbiztonság kultúrája az egyének szintjén is nagyon fontos, hiszen a felhasználók nagyon széles életkor-intervallumból kerülnek ki: a 6 évestől a 90+-ig, szélsőségesen szemlélve. Az életkorból eredően elvárható technológiai ismeretek és gyakorlat mellett a képzettség is árnyaló tényező. Ezért a kiberbűnözők egy jó része éppen a kkv-kat és a magánszemélyeket veszik célba, azért, mert ők általában nem rendelkeznek elegendő információval az adatbetörés közvetlen következményeiről és felkészületlenek. A magánszemélyek a szociális hálókon és az online terekben könnyen áldozatokká válnak. Bár az utóbbi hetekben történtek kapcsán az olasz polgárok még inkább rettegnek a digitális közigazgatásban és ügyintézések során használt érzékeny adataik biztonságáért, s valljuk be: nem ok nélkül.

IRODALOM

- Clark, Selena – MacLachlan, Malcolm – Marshall, Kevin – Morahan, Niall – Carroll, Claire – Hand, Karen – Boyle, Neasa – O'Sullivan, Katriona (2022): Including Digital Connection in the United Nations Sustainable Development Goals: A Systems Thinking Approach for Achieving the SDGs. In: *Sustainability.* Vol. 3/2022.
DOI: https://doi.org/10.3390/su14031883.
- Dalby, Simon (2020): *Anthropocene Geopolitics: Globalization, Security, Sustainability*. University of Ottawa Press, Ottawa, Kanada.
- Dannreuther, Roland (2013): *International Security: The Contemporary Agenda*. Polity Press, Cambridge.
- Epstein, David (2021): *Range: Why Generalists Triumph in a Specialized World*. Riverhead Books, New York.
- Farkas Ádám (2018): *A totalitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete*. Magyar Katonai Jogi és Hadijogi Társaság, Budapest.
- Giannopoulos, Georgios – Smith, Hanna – Theocharidou, Marianthi (szerk.) (2021): *The Landscape of Hybrid Threats. A Conceptual Model.* European Union and Hybrid CoE, Luxembourg.
- Internet Society: The Internet and Sustainable Development An Internet Society contribution to the United Nations discussion on the Sustainable Development Goals and on the 10-year Review of the World Summit on the Information Society, 2015. (Elérhető: https://www.internetsociety.org/wp-content/uploads/2015/06/ISOC-ICTs-SDGs-201506-Final.pdf. Letöltés ideje: 2024.04.02.).

- Isaszegi János (2015): *A 21. század élettérháború a földért, a vízért, az élelemért, a… létezésért!* Gondolat kiadó, Budapest.
- Khanna, Parag (2016): *Connectography: Mapping the Future of Global Civilization*. Random House, New York.
- Moran, Daniel (szerk.) (2011): *Climate Change and National Security: A Country-Level Analysis*. Georgetown University Press, Washington.
- Piva A. sajtónyilatkozata – Cybersecurity in Italia: cresce il mercato raggiunge 1,86 miliardi di euro (Elérhető: ttps://www.osservatori.net/comunicato/cybersecurity-data-protection/cybersecurity-italia-mercato-crescita-2022/e il mercato raggiunge 1,86 miliardi di euro, 2023. Letöltés ideje: 2024. április 2.).
- PNRR: Piano Nazionale di Ripresa e Resilienza per il digitale e la sicurezza informatica. (Elérhető: www.acn.gov.it. Letöltés ideje: 2024. március 18.).
- Rapporto Clusit, 2023. (Elérhető: Pubblicazioni – Clusit. Letöltés ideje: 2024. március 15.).
- Statistiche Meltwater: Statistiche su uso Internet e social network in Italia 2023, 2023. (Elérhető: motivonetwork.it. Letöltés ideje: 2024. január 18.).



Szerényi Gábor grafikája