Rendező:

Hungarnet

Networkshop 2020 ONLINE

Házigazda:

PÉCSI TUDOMÁNYEGYETEM
UNIVERSITY OF PÉCS

„Esélyeink és kihívásaink a digitális transzformáció világában”

Országos Online Konferencia
2020. szeptember 2–4.

INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM

Szerkesztette: Tick József, Kokas Károly, Holl András

Tipográfia és tördelés: Vas Viktória

Networkshop
2020. szeptember 2-4. Pécsi Tudományegyetem, (On-line)
konferencia előadásainak közleményei

ISBN 978-615-01-0376-1
DOI: 10.31915/NWS.2020

Kiadja a HUNGARNET Egyesület
az MTA Könyvtár és Információs Központ közreműködésével
Budapest
2020

Borítókép: freepik.com

CC BY

DOI: 10.31915/NWS.2020.13

A humán faktor szerepe a kiberbiztonság megteremtésében

Legárd Ildikó
Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Doktori Iskola
ildiko.legard@gmail.com
ORCID: 0000-0002-1469-8679

The role of the human factor in cyber security
Technological advances in recent decades, the rapid increase in digitization, the tremendous development of ICT tools and services, the widespread use of the Internet, and rapid access have irreversibly changed the lives of people, the way businesses operate and the organization of public administration. In parallel with the incessant development the security awareness of the users of these systems did not keep pace with the pace of technical development. So it is not surprising that cybercriminals have begun using a recently very popular form of attack, so-called social engineering that builds on influencing, manipulating and exploitable properties of human factor. „Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19" – said Jürgen Stock, INTERPOL Secretary General.

Effective protection against threats can be ensured by the security awareness of the users, which can be achieved through a well-organized and successful security awareness program.

Keywords: information security, IT security, information security awareness, information security awareness programs

Bevezetés

Az elmúlt évtizedekben bekövetkező digitális fejlődés, az Internet és az infokommunikációs technológiák használatának elterjedése jelentősen megváltoztatta a mindennapi életünket, a vállalkozások működését, valamint a közigazgatás szervezését egyaránt. Az idei évben bekövetkező járvány azonban minden eddiginél erőteljesebb eltolódást eredményezett az online tér irányába az élet minden területén: a hagyományos iskolai oktatás helyett bevezetésre került a távoktatás, a munka világában soha nem látott mértékben terjedt el a home office intézménye, a kikapcsolódás, a barátokkal, szeretteinkkel való kapcsolattartás elsődlegesen az Internet és a különböző infokommunikációs eszközök segítségével valósul meg.

A koronavírus okozta járványhelyzet és a karantén alatt, az online tevékenységek körében tapasztalható ugrásszerű növekedés a kiberbűnözőknek is kiváló terepet nyújtott, ezért az év első felében az ártó szándékú kibertámadások számának szignifikáns emelkedése figyelhető meg.[1] Jürgen Stock, az INTERPOL főtitkára szerint a „számítógépes bűnözők riasztó ütemben fejlesztik és fokozzák támadásaikat, kihasználva a COVID-19 által létrehozott instabil társadalmi és gazdasági helyzet okozta félelmet

1 https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/digital_hu (Letöltés: 2020. 09. 25.)

és bizonytalanságot”[2]. Ursula von der Leyen, az Európai Bizottság elnöke március 24-i, Twitteren közzétett közleményében úgyszintén felhívja az európai lakosok figyelmét a kiberbűncselekmények számának emelkedésére.[3]

1. A kiberbűncselekmények száma a COVID-19 első hulláma alatt

Az Interpol 2020. augusztus 4-én megjelent, az év első négy hónapját vizsgáló jelentése, az alábbi kiberbűncselekmények számának növekedésére figyelmeztet[4]:

- Adathalászat (Phishing /Scam/ Fraud): A koronavírushoz kapcsolódó adathalászat, valamint a számítógépes és egyéb eszközzel elkövetett csalások száma növekedett meg a legnagyobb százalékban a jelzett időszakban (907.000 spam került azonosításra).
- A második leggyakoribb károkozók a malware-ek (rosszindulatú alkalmazások). A jelentés szerint a vizsgált időszakban 737 malware-hez kapcsolódó incidenst detektáltak, többek között zsarolóvírusok, trójai vírusok, férgek, illetve banki kártevők formájában.
- A virtuális dobogó harmadik helyén azok a rosszindulatú weboldalak állnak, amelyek valamilyen káros funkciót valósítanak meg. Április végéig több mint 48 000 olyan weboldalt regisztráltak, többnyire károkozási céllal, amelyek domain neve tartalmazza a „covid” vagy „corona” szavakat. Az Interpol szerint, naponta több ezer új oldalt regisztrálnak, amelyeket aztán például kártékony szoftverek (malware) terjesztésére, adathalászatra, vagy hamis egészségügyi termékek értékesítésére használnak fel.
- A negyedik helyen az álhírek kaptak helyet, azonban ezek jelentőségét sem szabad alábecsülni. Az Egészségügyi Világszervezet (WHO) szerint a valótlan történetek jelenleg „gyorsabban terjednek, mint a vírus”.[5]
- Tipikus elkövetési formává vált, amikor a támadó a megtévesztő, csaló üzenetet valamely egészségügyi hatóság nevében küldi, melyet jól példáz az alábbi adathalász üzenet is:

2 https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (Letöltés: 2020. 09. 25.)
3 https://twitter.com/vonderleyen/status/1242437934051135489?lang=en (Letöltés: 2020. 09. 25.)
4 https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (Letöltés: 2020. 09. 25.)
5 https://www.europarl.europa.eu/news/hu/headlines/society/20200326STO75917/felretajekoztatas-es-alhirek-virusszeruen-terjednek-a-covid-19-jarvany-idejen (Letöltés: 2020. 09. 25.)

P 2020. 06. 12. 9:12

Nemzeti Egészségügyi Központ Magyarország <Muller.Cecilia@nnk.gov.hu>

Message has been disinfected :A Covid-19 védőfelszerelés ingyenes forgalmazása (Nemzeti Egészségügyi Központ Magyarország)

Címzett undisclosed-recipients:

NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT

Állami Népegészségügyi és Tisztiorvosi Szolgálat

Kedves mindenkinek,
A magyar kormány által kiadott covid-19 válaszadási utasítások szerint mi, a Magyar Nemzeti Egészségügyi Központ a covid-19 védőeszközöket ingyenesen kívánjuk eljuttatni a magyarországi összes regisztrált vállalathoz és iparághoz. Kérjük, töltse ki egyértelműen a mellékelt űrlapot. győződjön meg arról, hogy az alkalmazottak száma és a cég címe egyértelműen meg van írva ebben a formában.

Töltse ki a mellékelt űrlapot, és a mai bezárás előtt küldje vissza nekünk a másolatot, várva a gyors választ.

Az összes kitöltött nyomtatványt erre az e-mailre kell küldeni: Müller.Cecília@nnk.gov.hu

Szia

- Dr. Müller Cecília
- osztályvezető
- Országos Tisztifőorvos
- NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT
- 1097 Budapest, Albert Flórián út 2-6.
- Müller.Cecília@nnk.gov.hu

1. ábra: Adathalász levél a Nemzeti Népegészségügyi Központ nevében Forrás: https://index.hu/tech/hoax/2020/06/12/muller_cecilia_adathalasz_email_csalas_visszaeles_atveres_virus/ (Letöltés: 2020. 09. 25.)

A levél látszólag a Nemzeti Népegészségügyi Központtól, Dr. Müller Cecília tisztifőorvos asszonytól érkezett, melyben ingyenes Covid-19 védőfelszerelést ígérnek minden magyar vállalatnak, amennyiben a mellékelt űrlapra rákattintanak, és kitöltik azt a cég adataival. Azonban a levél vírust terjeszt és egyértelműen adathalász célokat szolgál, melyre számos jelből lehet következtetni: pl. a helytelen megfogalmazás és helyesírás, a megszólítás, illetve az elköszönés, valamint a fejlécben olvasható, valójában nem létező „Nemzeti Egészségügyi Központ Magyarország” feladó.

2. A támadás sikeressége – A humán faktor szerepe

A kibertámadások sikeressége alapvetően két tényezőn múlik: az informatikai eszközök és rendszerek sebezhetőségén (fizikai és logikai védelem), valamint a felhasználók biztonságtudatosságán. A felhasználók nem megfelelő szintű biztonságtudatosságához köthetők az ún. social engineering típusú támadási formák, amelyek az emberi hiszékenységre és együttműködési képességre épülnek. Aszerint, hogy a támadó milyen módszereket használ, humánalapú és számítógép-alapú technikákat különböztethetünk meg. [1]

2.1 Humán alapú social engineering [2] [3]

A **humánalapú technikák** alkalmazásához nem feltétlenül szükséges szaktudás, a támadó nem használ informatikai eszközöket, bárki által kivitelezhető, azonban előzetes megfigyelést és felkészülést igényel. A támadó és áldozata között közvetlen kontaktust feltételez, így a lebukás veszélye is nagyobb.

Típusai:

- segítség kérése;
- segítség nyújtása (fordított social engineering);
- megszemélyesítés, vagyis az identitás lopás;
- tombstone theft, azaz a sírkő lopás, mely a megszemélyesítés egy speciális fajtája;
- shoulder surfing (képernyő lelesése);
- az irodai hulladék átvizsgálása, azaz a dumpster diving;
- tailgating, vagyis a szoros követés módszere a bejáraton történő bejutáshoz;
- piggybacking: a támadó az áldozat segítségével és tudtával jut át a bejáraton.

2.2 Számítógép-alapú social engineering [3] [4]

A közvetett kapcsolattartást preferáló, számítógép-alapú támadások sokkal elterjedtebbek, mivel a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal, így kisebb a lebukás veszélye.

Típusai:

- adathalászat – phishing: olyan, jellemzően e-mail küldése az áldozatnak, amely megtéveszti őt és olyan hamis weboldalra „irányítja át", ahol kiadja személyes adatait, felhasználó nevét, jelszavát. Több válfaja ismert: hamisított e-mailek és hamisított weboldalak (scam); vishing (VOIP csalás); smishing (SMS); pharming, azaz az eltérítéses adathalászat; whailing, vagyis „bálnavadászat"; nyereményjátékokat, ajándékokat vagy ingyenes szolgáltatásokat hirdető áloldalak;
- kártékony programok: a támadás során olyan rosszindulatú kódok vannak elrejtve az eszközön vagy a file-on, amelyeknek segítségével megszerezhetik a célszemély vagy egy szervezet adatait, például: keylogger; baiting; javítás, frissítés felajánlása; trójai programok; veszélyes csatolmányok;
- Wi-Fi hálózat veszélyei: a hálózat üzemeltetője képes monitorozni a hálózaton zajló adatforgalmat, így elsősorban a nyílt hozzáférésű Wi-Fi hálózatok rejtenek magukban veszélyeket, hiszen gyakran adathalász célokat szolgálnak, bár előfordulhat jelszóval védett hálózatok esetében is;
- okostelefon alkalmazások általi hozzáférés – alkalmazásengedélyekből fakadó kockázatok: az okostelefonra telepített alkalmazások nem csak a készülék alapvető funkcióihoz, hanem használatukért cserébe egyéb adatokhoz és információkhoz is kérnek és általában kapnak hozzáférést, mint pl. a felhasználó személyes adataihoz, névjegyeihez, fényképeihez, üzeneteihez stb.

A social engineering típusú támadást jól példázza a közelmúltban a Tesla ellen tervezett, végül sikertelen „dollármilliós" zsarolóvírus támadás, melyet a vállalat az FBI közreműködésével sikeresen védett ki.[6]

6 https://computerworld.hu/biztonsag/dollarmillios-zsarolovirust-vedett-ki-a-tesla-es-az-fbi-283697.html (Letöltés: 2020. 09. 25.)

CC BY

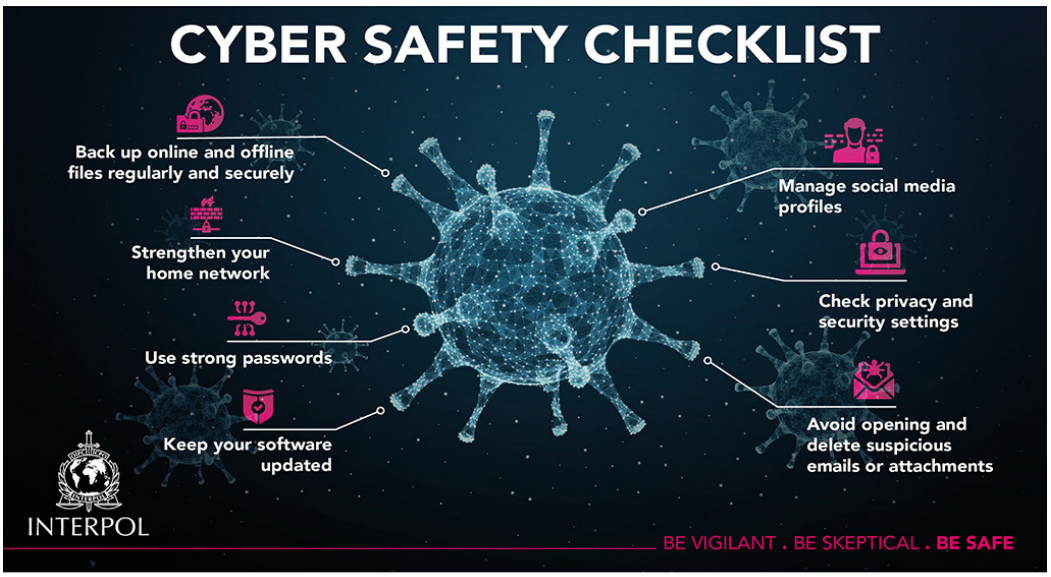
3. Védekezés: egyéni biztonságtudatosság, biztonságtudatos szervezeti kultúra

A social engineering ellen az egyetlen védekezési lehetőség a tudatosítás segítségével kialakított egyéni biztonságtudatosságon keresztül a biztonságtudatos szervezeti kultúra megvalósítása.

Az információbiztonság-tudatosság a tudás, a képességek és a viselkedés olyan hármasa, amely biztosítja az egyén számára a megfelelő szintű informatikai és információbiztonsági ismereteket, az ezekre épülő és alkalmazásukat biztosító képességeket, valamint e két elemnek megfelelő, belső igényként megjelenő, az információbiztonság jelentőségét elismerő viselkedést. [5] Az információbiztonság-tudatosság a szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a szervezetek alkalmazottai elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket. [6]

3.1 Egyéni biztonságtudatosság

Az Európai Bizottság a koronavírus-járvány elleni válaszintézkedések körében új iránymutatást tett közzé az európai polgárok digitális kompetenciájának fejlesztésére, melyben leírja a gyakorlati lépéseket, a fő teendőket, továbbá tanácsokkal és online segédanyagokkal szolgál a digitális felhasználóknak.[7] Figyelemfelhívó poszterek, videók[8] alkalmazásával az Interpol is tudatosító kampányt indított a felhasználók tudatossága növelése érdekében.[9]



2. ábra: Az Interpol biztonságtudatosító posztere
Forrás: https://www.interpol.int/How-we-work/COVID-19/COVID-19-Stay-Safe (Letöltés: 2020. 09. 25.)

7 https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/digital_hu (Letöltés: 2020. 09. 25.)
8 Covid-19 Cyber hygiene tips (Interpol): https://www.youtube.com/watch?v=TKB8rdYKcUE
9 https://www.interpol.int/How-we-work/COVID-19/COVID-19-Stay-Safe (Letöltés: 2020. 09. 25.)

3.2 Biztonságtudatos szervezeti kultúra

A biztonságtudatos szervezeti kultúra kialakításához szükség van egy hatékony tudatosítási programra, mely biztosítja a felhasználók megfelelő szintű biztonságtudatosságát.

A hatékony tudatosítási program 5 lépése [5] [7]:

I. A tervezéshez szükséges információk megszerzése:
- a szervezet jellemzői: köz-, vagy magánszféra, milyen típusú adatokat kezel, a szervezet stratégiája milyen hosszú- és rövidtávú célokat fogalmaz meg;
- az információbiztonság szempontjából a kulcsterületek beazonosítása, ahol a biztonsági problémák jelentkeztek, a fenyegetések, kockázatok és incidensek tipizálása és ezek gyökereinek elemzése, valamint a szükséges helyreállító intézkedések beazonosítása;
- a szervezet humán jellemzői: hány fős a szervezet, mekkora a fluktuáció; mely munkavállalói körnek szeretnénk a programot szervezni, az érintetti kör kor szerinti összetétele, munkaköreik és biztonságtudatosságuk szintjének meghatározása.

II. Felsővezetői támogatás biztosítása: kutatások igazolják, hogy a támogatás nélkülözhetetlen eleme a sikeres programnak.

III. A tudatosító program megtervezése:
- a célcsoportnak megfelelő tudatosító anyag összeállítása,
- a szervezeti és humánpolitikai jellemzőkhöz igazodó módszerek és kommunikációs csatornák kiválasztása, valamint
- az időzítés megtervezése.

IV. A tudatosító program megvalósítása.

V. A program megvalósítása közben és azt követően a visszacsatolások alapján a program korrekciója.

Ahhoz, hogy a program képes legyen pozitív irányban megváltoztatni a résztvevők tudását, attitűdjeit és viselkedését, szükséges, hogy a megfelelő embernek, a megfelelő információt, a megfelelő időben és formában adjuk át.

Mit? – Tananyag, „Érzékenyítés”

A felhasználók tekintetében az egyik leggyakoribb probléma a veszélyérzet hiánya, valamint a fenyegetettség fel nem ismerése. A program során ezért nagyon fontos felhívnunk a figyelmet arra, hogy bárki áldozattá válhat, ellenben ha ismerjük a kibertér felől érkező fenyegetéseket, az egyes támadási formákat, akkor nagyobb eséllyel azonosíthatjuk be időben és háríthatjuk el az ellenünk indított támadást, amely nagyban hozzájárul nem csak a munkahelyi, hanem a személyes és az otthoni biztonság megteremtéséhez is.

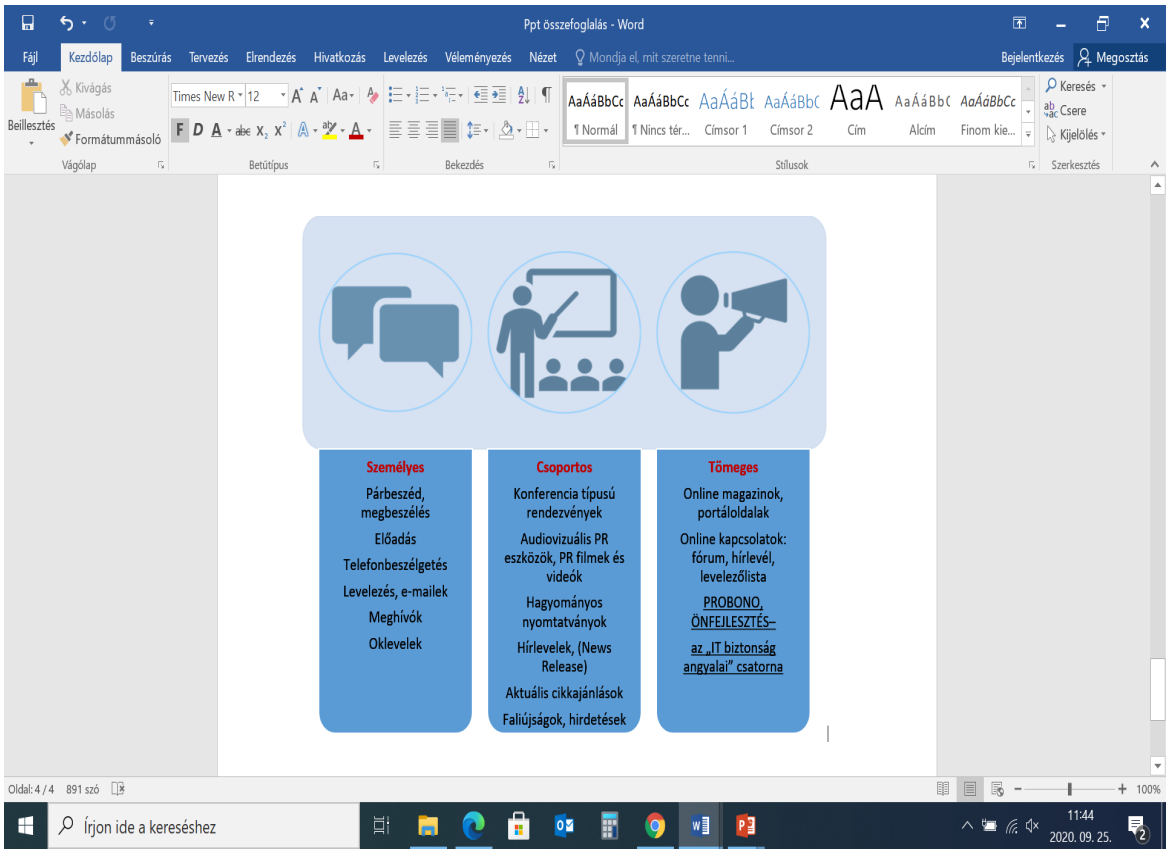
Mikor? – Időzítés

Az információbiztonság nem egy statikus állapot, amelyet ha egyszer elérünk minden erőfeszítés nélkül megmarad, így sajnos a biztonságtudatosság sem az. A támadók folyamatosan újabb és újabb támadási technikákat alkalmaznak, akár például a COVID-hoz kapcsolódó, megváltozott körülményekhez igazodva. Ezért elengedhetetlen, hogy folyamatosan pallérozzuk az elménket, ismerjük meg a legújabb támadási módszereket és időről időre frissítsük fel a korábbi ismereteinket.

CC BY

Hogyan? – IT eszközök, módszerek, kommunikációs csatornák

Az információbiztonsági tréningeknek számos formája ismert, mely különféle kommunikációs eszközökre épít. A rendelkezésre álló IT eszközök, oktatási módszerek, kommunikációs csatornák kiválasztásánál szem előtt kell tartanunk, hogy a célközönségnek megfelelő formát és nyelvezetet válasszunk a tudástranszfer megvalósítására. Az információbiztonság „eladására" és átadására kiválóan alkalmazhatók a marketingkommunikáció részeként a belső PR egyes eszközei: a személyes, a csoportos, illetve a tömegkommunikációs módszerek és formák [8].



3. ábra: A belső PR eszközeinek a biztonságtudatosító programban lehetséges alkalmazási területei (saját szerkesztés)

A cél elérése érdekében egyszerű, rövid, a napi gyakorlatban és a munkavégzés során jól alkalmazható tudást szükséges közvetíteni a résztvevők felé érdekes, újszerű, gyakorlatias formában.

A sikeres program kritikus tényezői [7]

- felsővezetés támogatásának, valamint a megfelelő erőforrások allokációjának biztosítása;
- szervezeti tényezők (struktúra, management, biztonsági politika, anyagi lehetőségek);
- a célközönséggel kapcsolatos tényezők: a szervezet összes felhasználójának bevonása; az ismeretek számukra érthető módon történő közvetítése; az eltérő igényű munkatársak eltérő képzése;

- szociális faktorok: a demográfiai jellemzők és a kulturális különbségek figyelembe vétele;
- egyéni tényezők: egyéni sajátosságok, különböző személyek eltérő reagálása egy esetleges támadásra;
- **üzleti környezet**: a szervezet által használt technológiák, a szervezeti kultúra, a munkatársak oktatása, a különböző üzleti/szervezeti politikák meghatározása, a fizikai biztonsági kontrollok rendszere, a távoli munkavégzéssel kapcsolatos biztonsági problémák kezelése;
- technológiai tényezők: IT biztonsági standardok használata és a technikai támogatás biztosítása;
- vonatkozó szabályozás.

Összegzés

A kiberbűnözés egyre nagyobb kihívások elé állítja mind a rendvédelmi szerveket, mind pedig a digitális eszközöket használó, bármikor célponttá váló vállalatokat, szervezeteket és az egyéni felhasználókat egyaránt. A humán tényező információbiztonságban betöltött kulcsfontosságú szerepe ma már megkérdőjelezhetetlen. Robert Mueller, az FBI egykori igazgatója azt nyilatkozta korábban: „Csak kétféle vállalat létezik: azok, amelyeket meghackeltek, és azok, amelyeket meg fognak hackelni". Mára szerinte ez az állítás inkább így hangzik: „Csak kétféle vállalat létezik: azok, amelyeket meghackeltek, és azok, amelyek még nem tudják, hogy meghackelték őket"[10]. Így tehát a kérdés nem az, hogy célponttá válhat-e bárki az online térben, hanem az, hogy az egyének és a szervezetek felismerik-e ennek jelentőségét és mennyire képesek előmozdítani saját, vagy munkatársaik biztonságtudatosságát.

Mi magunk is nagyon sokat tehetünk a biztonságos online jelenlétünk megteremtése érdekében, ha éberen, fokozott elővigyázatossággal, és egészséges gyanakvással „közlekedünk" a kibertérben, és nem utolsó sorban, figyelmemmel kísérjünk gyermekeink internethasználatát is.

Legyünk éberek! Legyünk tudatosak!

10 https://dynamicbusiness.com.au/topics/technology/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html (Letöltés: 2020. 09. 25.)

CC BY

Irodalomjegyzék

[1] MUHA L., KRASZNAY CS., Az elektronikus információs rendszerek biztonságának menedzselése, Budapest: NKE, Vezető- és Továbbképzési Intézet, 2014., p. 120.

[2] DEÁK V., „A social engineering humán alapú támadási technikái," Biztonságpolitika, p. 11, 2017. április 10.

[3] BÁNYÁSZ P., „Social engineering and social media," Nemzetbiztonsági Szemle 6. évf. 1. szám, pp. 59–77., 2018.

[4] DEÁK V., „A számítógép alapú social engineer támadási technikák," Biztonságpolitika, 2017. április.

[5] LEGÁRD I., „Célpont vagy! – a közszolgálat felkészítése a kiberfenyegetésekre", HADMÉRNÖK 15. évf. (2020) 1. szám: pp. 91.–105.

[6] NEMESLAKI A., SASVÁRI P., „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában," Háttér, pp. 169–177., 2014./4.

[7] LEGÁRD I., „Building An Effective Information Security Awareness Program", In: Thomas, Hemker; Robert, Müller-Török; Alexander, Prosser; Dona, Scola; Tamás, Szádeczky; Nicolae, Urs (szerk.) Central and Eastern European e|Dem and e|Gov Days 2020, Österreichische Computer Gesellschaft (ÖCG) (2020) pp. 189-200.

[8] LENDVAI E., GÁL J., Marketingkommunikáció 1., Keszthely, 2011, p. 160.