IT biztonságtudatosság fontossága

Fehér-Polgár Pál

tanársegéd, Óbudai Egyetem Keleti Károly Gazdasági Kar

feherpolgar.pal@uni-obuda.hu

Abstract: Az IT biztonságtudatosság kulcsfontosságú szerepet játszik az e-kereskedelemben, mivel a legtöbb adatvédelmi incidens és támadás gyakran az emberek, nem pedig a technológiai rendszerek hibáira vezethető vissza. Az e-kereskedelmi cégek számára a felhasználói és alkalmazotti biztonságtudatosság növelése alapvető a hatékony védekezés érdekében. Az emberek hajlamosak figyelmetlenül kezelni a jelszavaikat, megosztani érzékeny információkat, vagy nem frissíteni a szoftvereket, ami biztonsági résekhez vezethet. A leggyakoribb támadási módszerek, mint a phishing, social engineering és a zsarolóvírusok kifejezetten a felhasználók pszichológiai gyengeségeire építenek.
Az e-kereskedelmi cégeknek és a felhasználóknak szembe kell nézniük azzal a kihívással, hogy az alkalmazottak és vásárlók gyakran nem rendelkeznek a megfelelő biztonsági ismeretekkel és gyakorlati tudással a kibertámadások megelőzésére. Az alkalmazottak nem megfelelő biztonsági tudatossága a legnagyobb kockázatot jelenti, hiszen egy-egy figyelmetlen kattintás vagy gyenge jelszó használata komoly adatvédelmi incidenst eredményezhet. Ezért a folyamatos tréningek és a biztonsági szimulációk kulcsszerepet játszanak a tudatosság növelésében. Ezen túlmenően a cégek számára elengedhetetlen, hogy olyan biztonsági szabályzatokat alkalmazzanak, mint a többfaktoros hitelesítés és a rendszeres szoftverfrissítések, hogy minimalizálják a biztonsági fenyegetéseket.

Kulcsszavak: E-kereskedelem; IT-biztonságtudatosság

1 Biztonságtudatosság

A biztonságtudatosság, cybersecurity awareness, a szervezetek és egyének azon képességét jelenti, hogy felismerjék a digitális környezetben rejlő biztonsági fenyegetéseket és megfelelően reagáljanak rájuk. A biztonságtudatosság nem csupán a technológiai megoldások alkalmazását jelenti, hanem a felhasználói viselkedés és döntéshozatal formálására is kiterjed. A megfelelő biztonságtudatosság révén az egyének és szervezetek képesek minimalizálni a különböző kiberfenyegetések, például a phishing támadások, malware (rosszindulatú szoftverek), vagy ransomware (zsarolóvírusok) által okozott károkat (Horváth, 2021).

Hadnagy (2018) szerint a biztonságtudatosság fejlesztése kulcsfontosságú ahhoz, hogy a felhasználók képesek legyenek megérteni és felismerni a biztonsági fenyegetéseket, amelyek gyakran manipulálják az emberek pszichológiai gyengeségeit. Ezen felül a szerző hangsúlyozza, hogy a kiberfenyegetések megelőzése érdekében szükséges a rendszeres oktatás és a biztonságos online magatartásformák kialakítása. Peltier (2016) szerint a biztonságtudatosság nem csupán az egyes felhasználók, hanem az egész

szervezet biztonságának alapját képezi. A szerző szerint a munkavállalók tudatosítása és megfelelő képzése nélkül a legmodernebb technológiai megoldások is kevésnek bizonyulhatnak a kiberfenyegetések ellen.

A biztonságtudatosság fejlesztésében és fenntartásában a rendszeres tréningek és szimulációk kulcsszerepet játszanak. Cheng et al. (2020) kutatása szerint az interaktív és gyakorlati tréningek jelentősen javítják a munkavállalók reakcióidejét és döntéshozatalát valódi támadások esetén. A kutatás szerint az online támadásokkal szembeni felkészültség növelése érdekében elengedhetetlen a szervezetek számára, hogy ne csak elméleti tudást, hanem gyakorlati tapasztalatokat is biztosítsanak.

Cunningham et al. (2019) szerint a biztonságtudatosság kiterjed a személyes eszközökre is, mivel a felhasználók gyakran nem veszik figyelembe a mobil eszközök és az internetes alkalmazások biztonságát. A biztonságtudatosság növelésére irányuló programoknak tehát az összes digitális platformra és eszközre ki kell terjedniük, hogy a felhasználók képesek legyenek védekezni a különböző kiberfenyegetésekkel szemben.

Összességében a biztonságtudatosság fejlesztése nemcsak a felhasználói szintű biztonságot növeli, hanem segít abban is, hogy a szervezetek teljes körű védelmet biztosítsanak a kiberfenyegetésekkel szemben, így minimalizálva a potenciális adatvédelmi incidensek és a pénzügyi veszteségek kockázatát.

2 Biztonságtudatosság kihívásai

A felhasználók gyakran nem ismerik fel az online fenyegetéseket, például a phishing támadásokat, a rosszindulatú szoftvereket vagy az adathalászatot, mivel ezek egyre kifinomultabbá válnak. A phishing támadások során a támadók hamis e-maileket vagy weboldalakat hoznak létre, hogy személyes adatokat, például jelszavakat, bankkártya-információkat vagy más érzékeny adatokat szerezzenek. A statisztikák szerint az online felhasználók 30%-a nem képes megfelelően azonosítani egy tipikus phishing e-mailt, ami megnöveli a kiberbűnözők sikerének esélyeit (Hadnagy, 2018).

Ezen kívül az e-kereskedelem számos érzékeny adatot kezel, mint például banki információk, személyes adatok és tranzakciós történetek, amelyeket a támadók célba vesznek. A vásárlók és alkalmazottak tudatosságának növelése alapvető fontosságú a kiberbiztonsági támadások megelőzésében. A megfelelő tudatosság fejlesztése érdekében elengedhetetlen a rendszeres képzés és a biztonságos internethasználat iránti elköteleződés (Peltier, 2016). A többfaktoros hitelesítés (MFA) és a szoros ellenőrzésű hozzáférés-irányítási szabályok alkalmazása, például a jelszókezelés során, szintén kulcsszerepet játszanak a biztonság fenntartásában (Ali, 2017).

A tudatosság növelésére szolgáló tréningek és szimulációk segíthetnek a felhasználók és alkalmazottak felkészítésében a különböző online fenyegetések felismerésére. Cheng et al. (2020) kutatása szerint az interaktív, szimulált támadásokkal való tréningek eredményesebbek, mivel ezek elősegítik a gyakorlatban való alkalmazást és gyors reakcióképességet.

A felhasználók, akik nem tisztában vannak a fenyegetésekkel, könnyen célponttá válhatnak, ezért a tudatosság növelése az egyik legfontosabb lépés a kiberbiztonság megőrzésében, különösen az e-kereskedelemben, ahol az adatvédelmi incidensek súlyos pénzügyi és reputációs következményekkel járhatnak (Cunningham et al., 2019).

3 A biztonságtudatosság néhány kiemelt kérdése – primerkutatáson keresztül bemutatva

2024 tavaszán szakdolgozat konzulensként vettem részt Csatári Gábor gazdaságinformatikus hallgató Információbiztonsági tudatosság vizsgálata című dolgozatának elkészítésében. A szerző primerkutatása részeként egy kérdőíves kutatást végzett, melynek összeállításában és az eredmények feldolgozásában és értelmezésében segítettem munkáját. A következőkben az általa gyűjtött mintát elemzem, ehhez felhasználva az ő eredményeit.

A minta elemszáma 183 fő, a mintavételezés hólabda módszertant használva történt melynek során a szerző megosztotta ismerősei körében és több online felületen a kérdőívet, majd kérte a kitöltőket, hogy ők is küldjék tovább azt és kérjenek fel másokat is a kutatásban való részvételre. A mintavételezés tehát nem tekinthető irányítottnak. A kérdőívre adott válaszokat vizsgálva megállapítható, hogy a minta nem reprezentatív a magyar lakosságra, így e sokaságra nem általánosítható, arra azonban mégis alkalmas, hogy a mintára vonatkozva megállapításokat tehessünk s ezeket más kutatások eredményeivel is összevethessük.

A kérdőívre összesen 183 válasz érkezettbe, a kitöltők 72 %, azaz 131 fő nő, valamint 28%, azaz 51 fő férfi. 130-an a 19-29, fiatal felnőtt korcsoportba tarttak, így a válaszokat ennek megfelelően érdemes értelmezni.

A kitöltők 71% azaz 130 ember hallott már információbiztonsági tudatosságról, míg a megmaradt 29%, 53 ember nem, vagyis kicsit kevesebb, mint a megkérdezettek háromnegyede hallott már a témáról.

Szabadszavas kérdésként feltevésre került, hogy a válaszadók ismerik-e az információbiztonsági tudatosságot és ha igen, akkor hogyan definiálnák?

• *„Azt, hogy az adatainkra tudatosan vigyázunk”*

• *„Gondolom, hogy mennyire figyelsz a saját adataid biztonságos használatára, tárolására stb.”*

Azon kitöltők, akik a ’Nem’ választ jelölték be az előző kérdésnél, szintén nagyon jól megpróbálták összefoglalni a tudatosság fogalmát:

„Nem hallottam még róla, így nem tudom biztosan, de feltételezem, hogy valami olyasmiről van szó, hogy odafigyelünk adataink biztonságára, tudatosan teszünk azért, hogy mások ne tudjanak visszaélni velünk. (Leginkább talán az online térre vonatkozik.)”

Vajon tudatosan kezelik-e adataikat a válaszadók? Az eredmények szerint mindössze 6-an jelölték azt, hogy egyáltalán nem tudatosak, míg 45-en, hogy részben tudatosak. Összesen 113-an jelölték, hogy gyakran odafigyelnek rá és mindössze 19 fő jelölte be, hogy teljesen tudatosan kezeli adatait.

A megkérdezettek közül csupán 9 személy bízik teljes mértékben az online szolgáltatókban. A válaszadók többsége, összesen 74 fő, „kevésbé bízik”, míg 34 válaszadó „egyáltalán nem bízik” az online szolgáltatókban. Ez alapján úgy tűnik, hogy a kitöltők többsége inkább negatívan ítéli meg az online szolgáltatók adatvédelmét. Valószínű, hogy a Meta, mint a világ legnagyobb közösségi hálózataihoz tartozó cég (pl. Facebook, Instagram, WhatsApp), jelentős hatással van az emberek bizalmára. 2022-ben a Meta csaknem 2 milliárd eurós bírságot fizetett, mivel több ponton megszegte az európai GDPR előírásait.

A kitöltők közül csupán 50 ember ellenőrzi naponta a fiókjainak a gyanús tevékenységeit, annak ellenére, hogy mindenki számára fontos lenne, hogy figyelje az esetleges támadásokat az online térben. Ilyen lehet például egy gyanús, szokatlan bejelentkezési hely, olyan e-mail-ek, melyeket nem a felhasználó küldött, vagy esetleg olyan közösségi média aktivitás, posztolás, melyet nem a fiók gazdája kezdeményezett.

Csatári Gárbor e kérdések mellett még további kérdésekben is mélyen elemzi a kérdőívre kapott válaszokat. Kiemelten érdekes és vizsgálandó kérdés még a biztonságtudatosság fejlesztésére vonatkozó kérdések összegzése.

• Oktatás és képzések: Rendszeres oktatások és képzések szervezése az emberek számára a biztonságtudatosság terén.

• Applikációk: Biztonsági applikációk fejlesztése, amelyek segítenek az embereknek adataik védelmében.

• Gyakorlatias tréningek: Rendszeres és gyakorlatias tréningek szervezése, amelyek hatékonyan felhívják a figyelmet a biztonsági kérdésekre.

• Ingyenes programok: Ingyenes programok és események szervezése a biztonságtudatosság terjesztése érdekében.

• Figyelemfelkeltő előadások: Figyelemfelkeltő előadások tartása, amelyek rávilágítanak a biztonsági kockázatokra.

• Okos technológiai fejlesztések: Okos technológiai megoldások fejlesztése a biztonságtudatosság növelése érdekében, valamint állandó oktatás és felvilágosítás biztosítása.

• Iskolai oktatás: A biztonságtudatosság tananyagba való beépítése az általános és középiskolákban, valamint a szülők bevonása a témába.

• Kétlépcsős autentikáció: A kétlépcsős autentikáció bevezetése szélesebb körben a biztonsági intézkedések erősítése érdekében.

• Figyelemfelhívás közösségi média platformokon: A biztonsági kockázatokra való figyelemfelhívás a mindennapi használatban lévő platformokon.

• Jogi intézkedések: Jogszabályok módosítása a biztonságtudatosság növelése érdekében, valamint jogi könnyebbségek biztosítása az átlag állampolgárok számára.

• Média megjelenések: Több média megjelenés és influenszerek bevonása a biztonságtudatosság terjesztése érdekében.

• Kötelező kurzusok: Kötelező kurzusok vagy képzések bevezetése, hogy az emberek megértsék a biztonsági kockázatokat és annak fontosságát.

Összességében megállapítható, hogy a mintát alkotó válaszadók ismerik a biztonságtudatosság fogalmát, saját állításuk és válaszaik alapján. S arról is van elképzelésük, hogy hogyan fejleszthetnék saját és összességében is a társadalom biztonságtudatossága hogyan fejleszthető. Az is elmondható ugyan akkor, hogy az önbevalláson alapuló kérdőíves kutatás, bár kiváló információforrás, a biztonságtudatos viselkedés kutatása és vizsgálata további primerkutatási módszerek bevonását igényli.

Források

[1] Cheng, T., et al. (2020). Cybersecurity awareness training and its impact on reducing security breaches. Journal of Information Security, 25(1), 45-62.

[2] Cunningham, L., et al. (2019). Security awareness training: A comprehensive approach to risk reduction. Information Systems Management, 36(4), 295-305.

[3] Csatári Gábor (2024) Információbiztonsági tudatosság vizsgálata (szakdolgozat) Óbudai Egyetem Keleti Károly Gazdasági Kar

[4] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

[5] Peltier, T. R. (2016). Information Security Awareness and Training: Protecting Your Organization. Auerbach Publications.

[6] Ali, B., & Szikora, P. (2017). Információbiztonság az Y generáció körében. *Tanulmánykötet-Vállalkozásfejlesztés a XXI. században VII.*, 24-40.

[7] Horváth, Ádám Béla A magyarországi gazdálkodó szervezetek információbiztonsági jellemzőinek empirikus elemzése BIZTONSÁGTUDOMÁNYI SZEMLE 3 : 1 pp. 79-90. , 12 p. (2021)