Bottyán László

laszlo@bottyan.com

Információbiztonsági tudatosság az iskolákban

Bevezetés

2020-ban a koronavírus elleni védekezés keretében a köznevelési és szakképzési intézményekben új munkarend bevezetéséről született döntés Magyarországon. A Kormány 1102/2020. (III. 14.) Korm. határozata értelmében 2020. március 16. napjától valamennyi köznevelési és szakképző intézményben a nevelés-oktatás tantermen kívüli, digitális munkarendben került megszervezésre. (1102/2020. (III. 14.) Korm. határozat)

A digitális oktatásra való átállás a hagyományos tantermi oktató-nevelő munkát a tanév végéig gyakorlatilag a kibertérbe helyezte át. A tanórák megtartása és a kapcsolódó feladatok elvégzése azonban a kibertérben számos kockazzal is jár, a tantermi, iskolai védett közeggel szemben. Az interneten sajnos nem csak a segítőkész, de az ártani akaró résztvevők is jelen vannak, akik az információkat különböző motivációból szeretnék megszerezni, és saját hasznukra felhasználni.

A kibertér értelmezése

A kibertér értelmezéséhez először a görög „kübernétész” (jelentése: kormányos) szóból eredő kibernetika eredetét célszerű tisztázni. A kibernetika a Magyar nyelv értelmező szótára szerint „olyan komplex tudományág, amely a természettudományok egzakt módszereivel bonyolult rendszerek működési elveit tanulmányozza, és ennek gyakorlati alkalmazásával foglalkozik” (Bárczi, 1959). A kibernetika alapítójának az amerikai matematikus Norbert Wienert tartják, aki a második világháború alatt a légvédelmi rendszerek matematikai problémáival foglalkozva 1940-ben fogalmazta meg a korszerű számítógépekkel szemben támasztott alapkövetelményeket. A kibernetika szóval először az 1946-ban megjelent könyvében találkozhatunk, amelyben az állatokban és a gépekben zajló információáramlás, hírközlés, vezérlés és ellenőrzés kérdéseivel foglalkozik. (Gémes, 2018) A ki-

• Az internetes hivatkozások letöltési és ellenőrzési dátuma 2021. január 30.

bertér kifejezést William Gibson használta először 1982-ben megjelent Izzó króm (*Burning Chrom*) című, majd 1984-ben megjelenő „Neuromancer” című regényiben. A kifejezést a fizikai valóságtól elkülönülő környezetként írja le. A számítógép-hálózatok gyors fejlődésével és az internet megjelenésével létrejövő virtuális teret egyre többen azonosították Gibson sci-fi leírásával, így került át a fogalom hétköznapi szóhasználatba.

Habár számtalan meghatározás létezik a kibertérre, mi most a magyar jogban definiált verziót használjuk, mely szerint a kibertér a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese. (2013. évi L. törvény)

Biztonság a kibertérben

Nagyon sok helyen találkozunk a biztonság kifejezéssel, pl. közbiztonság. Mít is jelent a biztonság? Hétköznapi értelemben a biztonság valakinek, vagy valaminek veszélytől, kártól, jogtalan beavatkozástól, bántódástól való védett állapotát, helyzetét jelenti. (*Bárczi, 1959*) Vegyünk egy példát. Napjainkban akkor beszélhetünk például jó közbiztonságról, ha mondjuk az utcán nincsenek rablások, nem törik fel az autókat, nem törnek az ember életére. A kibertérben a legfontosabb feladat, és egyben napjaink legnagyobb kihívása az adatok, információk biztonságát megvalósítani.

Három adatbiztonsági követelmény létezik:

- Bizalmasság: valami, amit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerésre jogosultak köre
- Sértetlenség vagy integritás: valami, ami az eredeti állapotának megfelel és teljes
- Rendelkezésre állás: a szükséges infrastruktúrák, valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van. (*Erdősi, Sólymos, 2018*)

Vegyünk például egy kórházi beteglapot. A beteglapon szereplő információkat nem kívánjuk idegen emberek tudomására hozni, például azt, hogy milyen betegséget diagnosztizáltak, és mivel kezelnek minket. Ezt nevezzük bizalmasságnak. Az is nagy probléma lenne, ha valaki módosítaná a beteglapon szereplő adatokat, mivel akár félre is kezelhetnek minket. Ez a sértetlenség, vagy integritás. Végül nem

szeretnénk, ha valaki letörölné, vagy bármilyen módon elérhetetlenné tenné a beteglapunkat, amire a kezelőorvosnak igen nagy szüksége van, hogy a megfelelő kezelésben részesítsen minket. Ezt hívjuk rendelkezésre állásnak.

Fenyegetettség és támadási trendek

A kibertérben számos veszély fenyegeti a biztonságot. Fenyegetésnek nevezünk minden olyan lehetséges eseményt, vagy műveletet, amely sértheti az elektronikus információs rendszer, és ezáltal az adatok biztonságát. Fenyegetés például az, hogy egy rosszindulatú támadó lehallgatja a kommunikációt két fél között, vagy például az, hogy illetéktelenül szeretne megismerni rólunk érzékeny adatokat. Itt szükséges tisztáznunk még a sérülékenységi fogalmát. A sérülékenység az elektronikus információs rendszer, vagy környezetének olyan tulajdonsága, amely segítségével a fenyegetés megvalósulhat. Az előbbi példánál maradva, a kommunikációt nem védett csatornán végezzük, vagy ha érzékeny adatainkat nem védjük megfelelően, akkor ez a sérülékenység a fenyegetés által kihasználhatóvá válik. Mivel biztonság csak akkor létezhet, ha a fenyegetettség minimális, ezért mindnyájunk közös feladata, hogy igyekezzünk felismerni és megelőzni a fenyegetettségeket, erősítsük a sérülékenységeinkkel szembeni védelmet.

Figure 11: Number of breaches per economic sector, reported in 2019

Figure 14: Types of data lost by third party breaches, reported in 2019

Forrás: 2019 Year End Report Data Breach QuickView

Számtalan fenyegetettségi jelentés készül napjainkban, melyek bemutatják az adott időszak alatt bekövetkezett incidensek statisztikáit. Az alábbi részlet az egyik vezető nemzetközi kockázatfelmérő cég, a Risk Based Security (RBS) által publikált adatbiztonsági incidens-jelentésből, amely megmutatja, hogy az oktatás a 7. legjobban érintett szektor volt 2019-ben.

Megmutatja továbbá azt is, hogy leginkább a nevek, címek, születési adatok és e-mail címek voltak a leginkább érintett adattípusok, amelyek adatbiztonsági incidens áldozatául estek.

A támadások mögött különböző motivációk állhatnak, de leginkább pénzügyi haszonszerzés, vagy szándékos károkozás, rombolás céljából indítanak támadásokat.

Felmerül a kérdés, hogy mit tehet a támadó például egy név és egy cím, vagy e-mail cím párossal? A különböző támadások mögött különböző motivációk állhatnak, hírnév rontástól kezdve pénzügyi, vagy egyéb materiális károkozás. A támadások megértéséhez bele kell képzelniünk magunkat a támadó helyzetébe és motivációiba.

E-mail címek például arra használhatók, hogy az áldozat nevében a támadó e-mailt küldjön, melyhez nem szükséges az e-mail címhez tartozó jelszó sem, csupán a támadó úgy jelenti meg magát, mintha az áldozat lenne a valódi feladó. Ebben a levélben bármit el lehet helyezni, akár vírust, vagy egyéb károkozót. Értelemszerűen még nagyobb a kockázat, ha a fogadó fél „ismeri” az áldozatot, hiszen nagyobb eséllyel nyit meg egy rosszindulatú csatolmányt, vagy kattint a levélbe illesztett linkre.

Egy név és e-mail cím párossal könnyedén keresheti meg a támadó az áldozatot a közösségi oldalakon is, amelyen keresztül többféle információhoz juthat, pl. lakóhely, anyagi viszonyok, munkahely stb. Ezen információkat további támadásokra lehet használni pszichológiai manipuláció (social engineering) segítségével.

Az e-mail cím önmagában is kincs a támadónak, hiszen az email fiókjához tartozó információ fele már a birtokában van. Innen már csak a jelszóra van szüksége, amely köszönhetően a még mindig nagyon gyenge jelszókezelésünknek. Egy 2019-es Google felmérés szerint az Amerikai Egyesült Államokban a válaszolók negyede olyan jelszavakat használ, mint pl. abc123, Password, 123456 stb. (Poll, 2019)

A hanyag jelszavak nagyon könnyen feltörhetők egy erre a célra készített szoftver segítségével, melynek kezeléséhez még számítástechnikai szaktudás sem szükséges! Könnyen belátható tehát, hogy csupán egy e-mail címmel is milyen károkat lehet okozni, nagyon kevés idő alatt, csekély energia ráfordítással.

A támadások mechanizmusa tehát röviden az, hogy a támadó keres egy sebezhetőséget, ebben az esetben egy email címet, amelynek segítségével megtámadja a kiszemelt rendszert, esetünkben az e-mail fiókot. A rendszer, azaz az e-mail fiók tulajdonosa a kockázatot csökkentheti, esetünkben például egy helyesen megválasztott, bonyolult jelszó használatával.

Fenyegetettségek a digitális tanrendhez kapcsolódóan

Nézzük meg, hogy a kibertérben, a digitális oktatás során milyen fenyegetettségek merülhetnek fel. Vegyünk például egy tanórát, melynek során különböző tanári-tanulói tevékenységek zajlanak. Az alábbi táblázatban megtalálható néhány tanári-tanulói tevékenység és a felmerülő lehetséges fenyegetettség.

	Tanári–tanulói tevékenység	Lehetséges fenyegetettségek
1	Kapcsolódás az Internetre a számítógépen	Nyílt wi-fi kapcsolódás esetén engedély nélküli csatlakozás, lehallgatás. Vírusirtó, tűzfalprogram hiánya esetén a vírus továbbítása, illetve a tárolt oktatási anyag kompromittálódása
2	Elektronikus oktatási környezet, digitális oktatásra használt szoftver elindítása, bejelentkezés	Felhasználónév, vagy jelszó kompromittálódása, engedély nélküli-, vagy más nevében történő bejelentkezés. Az oktatási környezet, vagy digitális oktatásra használt szoftver nem működik, szándékosan vagy technikai hiba miatt nem elérhető.
3	Az oktatási anyag feltöltése / letöltése az elektronikus oktatási környezetben vagy külső weboldalra/-ről, vagy egyéb online helyre/-ről. Az oktatási anyag elküldése / fogadása e-mailben	Az oktatási anyag kompromittálása, engedély nélküli letöltése, megismerése, módosítása. Más nevében történő e-mail küldése, fogadása.
4	Online kommunikáció a tanóra alatt tanár és diák között	Nem védett kommunikáció alatt engedély nélküli-, vagy más nevében történő bejelentkezés
5	Számonkérés	A számonkérés során engedély nélküli segítség használata. A számonkérés során a tanuló másnak adja ki magát, és más nevében teljesíti a számonkérést. A számonkéréshez használt elektronikus anyag kompromittálódik
6	A számonkérés eredményeinek megjelenítése az elektronikus tanulási környezetben	Az értékelési osztályzatok engedély nélküli módosítása

Információbiztonsági tudatosítás és intézményi elkötelezettség

Az előzőekben már tárgyaltuk, hogy a biztonság megőrzésének érdekében igyekeznünk kell felismerni és megelőzni a fenyegetettségeket, erősítsük a sérülékenységeinkkel szembeni védelmet. Ehhez szükség van egyrészt az intézmény elkötelezettségére, másrészt az egyén, azaz a tanárok megfelelő szintű tudatosságának fenntartására. A digitális világ szinte napról napra változik, a Moore törvény alapján a tranzistorok száma az integrált áramkörökben 2 évente megduplázódik a világon, amely felismerés kiválóan mutatja a technológiai fejlődés mértékét. (Moore, 1965)

Ebben a gyorsan változó technológiai környezetben a tudatosság fenntartásához tehát szükség van az iskolák elkötelezettségére. Az elkötelezettség többféle módon nyilvánulhat meg. Néhány példa az elkötelezettségre:

- Az intézményben rendszeresen kommunikálják az információbiztonság fontosságát
- A tanárok rendszeres időközönként kapnak információbiztonsági tudatosító oktatást

2020. október 21 – 2020. november 15 között országosan, kb. 557 általános és közép fokú oktatási intézményt kerestem meg egy online kérdőív segítségével, melyből összesen 75-en vettek részt a kitöltésben. A válaszolók 88%-a azt mondta, hogy az információbiztonság fontosságát rendszeresen kommunikálják az intézményükben, de mindössze 29%-a mondta azt, hogy rendszeresen kap információbiztonsági tudatosító oktatást.

(1) Az információbiztonság fontosságát rendszeresen kommunikálják az intézményben; (2) A kollégáimmal együtt rendszeresen veszünk részt információbiztonsági oktatáson

Konklúzióink, hogy amennyiben a tanárok kétharmada nem kap megfelelő, naprakész ismereteket az aktuális támadási trendekről és védekezési mechanizmusokról, úgy a fenyegetettség felismerése, és a sérülékenységeinkkel szembeni védelem lehetősége arányosan csökken, tehát a biztonság megőrzése forog kockán.

Információbiztonsági tárgyi ismeretek

A digitális oktatás során számtalan eszközt és programot használunk. A sérülékenységekkel szembeni védelmet erősíteni úgy lehetséges, ha tisztában vagyunk az egyes digitális eszközök, programok alapvető biztonsági beállításával. A biztonsági tudatosság növelésére szolgáló oktatások részben ezt a célt is szolgálják. Vegyünk néhány példát arra, hogy a tanítási-tanulási folyamat során milyen biztonsági szempontokat kell figyelembe vennünk:

- Az internetre való kapcsolódás biztonsága: amikor kapcsolódunk az internetre, számtalan veszély leselkedik ránk. Publikus internet hozzáférést például nem célszerű oktatási csatornaként használni, de a saját otthoni vezeték nélküli hálózatunk védelme is fontos az illetéktelen lehallgatás ellen.
- A számítógép biztonsága: a számítógépünk naprakészen tartása alapvető fontosságú, ide lehet sorolni példaként a víruskezelő szoftver frissítését, a felhasználói fiókok jelszavas védelmét, vagy az adataink rendszeres mentését.
- Az elektronikus levelezés biztonsága: e-mail használata közben különösen óvakodnunk kell például a kéréslen levelek, csatolmányok, linkek megnyitásától, főleg ismeretlen feladó esetén, illetve mellőzni kell az érzékeny adatok titkosítatlan küldését.
- A böngészőprogramok biztonsága: weboldalak látogatásánál figyelni érdemes például a cookie-k (sütik) kezelésére, a kapcsolat titkosítására (https) és a felugró ablakokra.
- Az elektronikus tanulási környezet biztonsága: az egyes tanulási keretrendszerek használata (pl. Moodle) vagy más tanításra használt környezet (pl. Google Classroom) biztonsági beállításainak a tanulmányozása erősen javasolt a használat megkezdése előtt.

Az előző fejezetben említett kutatásra adott válaszok alapján a válaszolók 52%-a egyáltalán, vagy csak részben van tisztában a böngészőprogramok biztonságával. Hasonló 48% az arány az elektronikus ta-

nulási környezet biztonságánál és az internetre kapcsolódás biztonságánál is 47%-os aránnyal.

Az információbiztonsági tárgyi ismeretek témakörönként

Érdemes megfigyelni, hogy az e-mail biztonságra adott válaszok szerint a válaszolók 69%-a elég jól, vagy teljesen tisztában van az elektronikus levelezés biztonsági beállításával, közel egyharmaduk nincs, vagy csak részben. Visszaautalnék a fenyegetettségek és támadási trendek c. fejezetre, ahol jól látszik, hogy a 3. fél által bejelentett adatvesztések egyötödénél az e-mail is érintett. Ha ehhez hozzáadjuk azt az eredményt, amely a kutatásomból ered, hogy a tanárok kb. egyharmada nincs, vagy csak részben ismeri az e-mailezés biztonsági követelményeit, akkor világosan látszik az összefüggés, milyen potenciális veszélynek van kitéve a tanárok egy jelentős része. Vegyük azt is figyelembe, hogy ez az összefüggés csak az e-mail használatról szól, a fentebb tárgyalt egyéb tárgyi ismeretek, például a böngésző programok, elektronikus tanulási környezet biztonsága, még ennél is rosszabb arányt képviselhet.

Információbiztonsági ismeretek gyakorlati alkalmazása

Ahhoz, hogy felismerjük a fenyegetettségeket és sikeresen védekezzünk ellene, az információbiztonsági ismereteinket a gyakorlatban is tudnunk kell alkalmazni. Hiába tudjuk, hogy milyen fenyegetettségek vannak egy digitális tanórán, például az, hogy illetéktelen személyek is bekapcsolódhatnak, ha nem teszünk ellene semmit. Természetesen ez nem csupán a szándék hiányából eredhet, de abból is adódik, hogy nincs, vagy nem megfelelőek a tárgyi ismereteink.

Az előző fejezetben említett kutatásomra adott válaszok alapján a válaszolók 35%-a már legalább egyszer találkozott biztonsági incidenssel a digitális oktatás során. Ez a válasz is azt mutatja, hogy van létjogosultsága az információbiztonsági tudatossági szint növelésnek, hiszen előfordulnak incidensek a hazai gyakorlatban is.

Az információbiztonsági ismeretek gyakorlati alkalmazásának másik aspektusa, hogy a tanárok beépítik-e ismereteiket a gyakorlatba? Vegyünk például egy digitális tanórát, használnak-e bármilyen védelmi, ellenőrzési mechanizmust, amelynek célja kifejezetten az információbiztonság megóvása? (pl. bejelentkezett tanulók azonosítása, számonkérés hitelességének ellenőrzése stb.)

Kutatásomban a válaszolók 39%-a soha nem használ ilyet, 48%-ánál előfordul, mindössze 12% válaszolta, hogy rendszeresen, illetve 1% aki mindig.

75 válasz

Szoktam olyan ellenőrzést végezni a tanítás-tanulási folyamat során, amelynek célja kifejezetten az információbiztonság megóvása (pl. Bejelentkezett tanulók azonosítása, biztonságos kommunikációs csatornák használata, számonkérés hitelessége stb.)

A gyakorlatban tehát a tanárok többsége egyáltalán nem, vagy a rendszeresség teljes hiánya nélkül épít be védelmi mechanizmusokat a digitális tanórák menetébe. Könnyen belátható, hogy a gyakorlati alkalmazás hiánya rendkívül sérülékennyé tesz egy digitális tanórát a fenyegetettségekkel szemben.

Összefoglalás

A kibertérben a legfontosabb az adatok biztonságát megvalósítani, azaz a bizalmasságot, sértetlenséget, vagy integritást és a rendelkezésre állást megóvni. A támadások mögött különböző motivációk áll-

hatnak, de leginkább pénzügyi haszonszerzés, vagy szándékos károkozás céljából indítanak támadásokat. Biztonság csak akkor lehetséges, ha a fenyegetettségeket lecsökkentjük, ezért fel kell ismerni őket és erősíteni a védelmi intézkedéseket. Számtalan adattípus közül napjainkban leginkább a nevek, címek, születési információk és e-mail címek voltak a leginkább érintettek azok közül, amelyek adatbiztonsági incidens áldozatául estek. Ezeket az adatokat a sötét weben pénzzé lehet tenni, vagy további támadások alapjául szolgálhatnak.

A sérülékenységekkel szembeni védelemhez egyrészt az intézmény elkötelezettségére, illetve a tanárok megfelelő szintű információbiztonsági tudatosságának fenntartására van szükség. 2020. őszén végzett kutatásomra adott válaszok alapján a tanárok többsége nem kap rendszeres információbiztonsági oktatást, ezzel a fenyegetettség felismerése, és a sérülékenységeinkkel szembeni védelem lehetősége arányosan csökken. Másrészt szükség van arra is, hogy a tanárok tisztában legyenek az egyes digitális eszközök, programok alapvető biztonsági beállításaival. A biztonsági tudatosság növelésére szolgáló oktatások részben ezt a célt is szolgálják.

Az említett kutatásra adott válaszok alapján a válaszolók kb. fele egyáltalán, vagy csak részben van tisztában bizonyos digitális eszközök és programok biztonságával, pl. a böngésző programok, az elektronikus tanulási környezet és az internetre kapcsolódás tekintetében is. Szintén aggodalomra ad okot, hogy egyharmaduk nem, vagy csak részben ismeri az elektronikus levelezés biztonsági követelményeit, annak ellenére, hogy az adatlopások ötödénél az e-mail cím szerepel az eltulajdonított adatok között.

Az információbiztonsági ismeretek gyakorlati alkalmazása még lesújtóbb eredményt mutat, hiszen a tanárok jelentős többsége egyáltalán nem, vagy a rendszeresség teljes hiánya nélkül épít be védelmi mechanizmusokat a digitális oktatás menetébe.

Megoldási lehetőség egyrészt az információbiztonsági tudatosító oktatások rendszeresítése, melyen belül fontos az egyes biztonsági témakörök átfogó lefedettsége, a napi munka során előforduló kérdések megbeszélése, a támadási trendek bemutatása és a naprakész tárgyi ismeretek átadása. Másrészt fontos az ismeretek napi gyakorlatba való beépítése, preventív kontrollok kialakítása a biztonságos digitális oktatási környezet megteremtéséhez. Ha a tanárok és a diákok is biztonság tudatos környezetben tanítanak, illetve tanulnak, akkor jobban számonkérhetőnek érzik magukat a tetteikért. Mindez egy olyan iskolai kultúrát hoz létre, amelyben az adatbiztonsági incidensek valószínűsége csökkenthető.

A biztonságtudatosság növelése pénzben és időben is kifejezhető előnyt adhat. Önmagában a biztonságtudatosság nem zárja ki egy esemény bekövetkezését, de ha mégis bekövetkezik, akkor hatása jelentősen csökken. Mindez pedig csökkenti a jó hírnév, a jogi következmények, vagy akár a pénzügyi veszteség lehetséges hatásait is.

Esettanulmány

Ransomware támadás a Fairfax megyei állami iskolában (USA)

A Fairfax megyei állami iskola egy ransomware támadásos kibert biztonsági esemény áldozata lett. A támadók a dark weben tettek közzé az általuk lopott információkat.

A Ransomware egy olyan rosszindulatú program, amelynek célja, hogy megakadályozza a felhasználók fájlokhoz való hozzáférését, és bizonyos esetekben túszként tárolja az adatokat, amíg egy bizonyos váltságdíjat meg nem fizetnek érte. Egy nagyon kifinomult módszerekkel rendelkező számítógépes bűnözői csoport, az úgynevezett Maze vállalta a felelősséget a támadásért.

A digitális tanulás és a járvány által támasztott egyéb kihívások közepette a számítógépes bűnözők az ország több oktatási rendszerét is megcélozták a működés megzavarása érdekében. A Fairfax rendszere csupán egy, a több mint 1000 oktatási rendszer közül, amely ransomware támadást szenvedett az elmúlt évben. Csak az elmúlt héten több iskolai körzettől is érkezett jelzés, hogy ransomware támadások áldozatai lettek.

Sajnos jelen állás szerint egyes diákok és az alkalmazottak személyes adatai eltulajdonítással is érintettek a támadásban. Éjjelnappal folyik a munka, hogy az eltulajdonított információk azonosításra kerüljenek, és az érintett személyek értesüljenek róla.

Forrás:

<https://www.fcps.edu/blog/update-cybersecurity-incident>

1. Milyen adatok lehetnek érintettek a támadásban?

A cikkben említett személyes adatok olyan információkat tartalmaznak, amelyek segíthetnek egy személy vagy családjának beazonosításában. Az iskolai nyilvántartásokban ez lehet pl. a nevük, a címük, az elérhetőségük, a jelenléti és fegyelmi nyilvántartásuk, valamint a jegyeik és a félévi, évvégi eredményeik. További alkategória a személyes különleges adatok, amely magában foglalja pl. a diákok biometrikus adatait, fotóit, vallási meggyőződését, egészségügyi, vagy táplálkozásra vonatkozó információkat.

2. *Milyen szándékból követhették el a támadást, mi lehet a motiváció mögötte?*

A támadások mögött különböző indokok húzódnak. A cikk szerint az elmúlt időszakban több körzetből is jelentettek hasonló incidenseket, ezért kevésbé valószínű a személyes bosszú (pl. egy adott tanár ellen), vagy egy adott intézmény reputációjának a rontása. A zsarolóvírusok hátterében egyrészt általában pénzügyi motiváció áll, a váltságdíj megszerzése a legfőbb motiváció. A másik motiváció pedig lehet maga az adatlopás, mint szándékos károkozás, ahogy a cikkből kiderül, diákok és tanárok adatait lopták el és tették fel a „sötét webre” (darkweb) a zsarolóvírus segítségével.

3. *Milyen módszerrel lehet csökkenteni egy ilyen jellegű támadás bekövetkezési valószínűségét?*

Azon felhasználók körében, akik rendelkeznek oktatás, tudatosítás útján megszerzett információbiztonsági ismeretekkel, nagyobb valószínűséggel alkalmaznak védelmi intézkedéseket. Zsarolóvírusok esetében például a vírusvédelem, az e-mail biztonságos használata, illetve a rendszeres adatmentések. Ennek a kockázati tényezőnek az időben történő felismerése és prevenciója jelentősen javíthatja akár az egyén, akár egy oktatási intézmény adatvagyonának a védelmét.

Ellenőrző kérdések

1. *Milyen adatbiztonsági követelmények vannak elektronikus információkra vonatkozóan a kibertérben? Sorolja fel, röviden mutassa be és mondjon egy-egy példát mindegyik követelményre!*

Három adatbiztonsági követelmény, leírással és példákkal:

- Bizalmasság: valami, amit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerésre jogosultak köre, pl. a tanulók személyes adatainak kiadása illetéktelen kezekbe a bizalmasság megsértése
 - Sértetlenség vagy integritás: valami, ami az eredeti állapotának megfelelő és teljes, pl. a tanulók osztályzatainak szándékos, vagy véletlen módosítása, az integritás megsértése
 - Rendelkezésre állás: a szükséges infrastruktúrák, valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van, pl. az elektronikus oktatási környezet elérhető tanítási idő alatt
2. *Mi az általános mechanizmusa egy támadásnak a kibertérben? Mondja el mit tehet az áldozat egy támadás kivédésére, és illusztrálja példával!*

A támadások mechanizmusa az, hogy a támadó keres egy sebezhetőséget, amelynek segítségével megtámadja a kiszemelt rendszert. A rendszer tulajdonosa a kockázatot úgy csökkentheti, hogy megfelelő védelmi intézkedéseket tesz a sebezhetőségek kihasználhatósága ellen.

3. *Miért fontos az információbiztonsági tudatosság növelése, a biztonság fenntartása szempontjából?*

A naprakész információbiztonsági tudatosság elengedhetetlen, hiszen a fenyegetettségek felismerése, és ezzel a sérülékenységekkel szembeni védelem lehetősége arányosan csökken. Szerepe van még a tárgyi tudás növelésében, pl. a számítógép, az elektronikus levelezés, a böngészőprogramok és az elektronikus tanulási környezetek biztonságos használatának bemutatásában.

4. *Soroljon fel legalább 3 didaktikai tevékenységet, amelyhez a digitális tanóra során valamilyen eszközt, vagy program igénybe vétele szükséges! Mondjon mindegyikhez legalább egy-egy fenyegetettséget amelyre oda kell figyelni a biztonság növelése érdekében!*

Tanári-tanulói tevékenységek és lehetséges fenyegetettségek:

- Kapcsolódás az Internetre a számítógépen: Nyílt wifin kapcsolódás esetén engedély nélküli csatlakozás, lehallgatás
- Digitális oktatásra használt szoftver elindítása, bejelentkezés: Felhasználónév, vagy jelszó kompromittálódása, engedély nélküli, vagy más nevében történő bejelentkezés
- Az oktatási anyag feltöltése / letöltése, vagy elküldése: Az oktatási anyag kompromittálása, engedély nélküli letöltése, megismerése, módosítása
- Online kommunikáció a tanóra alatt tanár és diák között: Nem védett kommunikáció alatt engedély nélküli-, vagy más nevében történő bejelentkezés
- Számonkérés: a tanuló másnak adja ki magát, és más nevében teljesíti a számonkérést
- A számonkérés eredményeinek megjelenítése: Az értékelési osztályzatok engedély nélküli módosítása

5. *Soroljon fel legalább 3 védelmi intézkedést, amelyet alkalmazni tudna a digitális oktatáshoz kapcsolódóan, kifejezetten az információbiztonság megóvása érdekében!*

A digitális oktatáshoz kapcsolódóan számtalan védelmi mechanizmus is beépíthető, a lehetséges fenyegetettségek tükrében. Néhány példa:

- Tanórára bejelentkezett tanulók azonosítása.
 - A felhasznált kommunikációs csatorna biztonságának ellenőrzése.
 - Felhasználónevekhez tartozó jelszavak rendszeres cseréje.
 - Oktatási anyagok védelme, szükség esetén titkosítása.
 - Érzékeny adatok küldése/fogadása esetén titkosítás használata.
 - Számonkérések esetén a hitelesség ellenőrzése.
6. *Milyen szándékok húzódnak egy elektronikus információs rendszer elleni támadás mögött? Mondjon rá egy-egy példát!*

A támadások mögött jellemzően kétféle szándék áll:

- Pénzügyi haszonszerzés: pl. váltságdíj zsarolóvírussal, vagy áloldalakon keresztül pénzügyi tranzakciók, esetleg pszichológiai manipulációk révén átutalások kikényszerítése
 - Szándékos károkozás, rombolás: pl. rendszerek elérhetetlenné tétele, működésük megzavarása, adatmanipuláció, adatlopás bosszúvágyból
7. *Az 2020. október 25 - november 15 között elvégzett online felmérés eredményeképpen mely területeket emelné ki, mint sürgős beavatkozást igénylő feladatok, kifejezetten az információbiztonság javítására? Mondjon legalább 2 példát és javasoljon rá megoldást!*

A kutatás több hiányosságot is feltárt:

- Információbiztonsági tudatosság növelésére irányuló rendszeres oktatások, tréningek hiánya
- Információbiztonsági tárgyi ismeretek hiányossága (pl. böngészők, elektronikus tanulási környezet, internetre való kapcsolódás, elektronikus levelezés stb.)
- Az információbiztonsági ismeretek gyakorlati alkalmazásának hiánya, a tanárok többsége egyáltalán nem, vagy a rendszeresség teljes hiánya nélkül épít be védelmi mechanizmusokat a digitális tanórák menetébe
 - Megoldás 1: rendszeres oktatások szervezése, amely lefedi az egyes biztonsági témaköröket, a napi munka során előforduló kérdéseket, az aktuális támadási trendeket és a naprakész tárgyi ismereteket.
 - Megoldás 2: a tanultak beépítése a napi gyakorlatba, a digitális oktatás folyamatába való preventív kontrollók, védelmi mechanizmusok beépítése

8. *Mit tud kezdeni a támadó egy diák elektronikus levelezési címével?
Milyen károkat tud vele okozni, mondjon rá legalább két példát!*

Egy e-mail címmel többféle kárt is lehet okozni, például:

- Az áldozat nevében a támadó e-mailt küld, melyben úgy jelenti meg magát, mintha az áldozat lenne a valódi feladó. Ebben a levélben elhelyezhet egy vírust, álszöveget, csatolmányokat, linkeket stb.
- Névre utaló, vagy kikövetkeztethető e-mail címmel könnyedén megkereshet valakit a közösségi oldalakon, amellyel további információkhoz juthat pl. lakóhely, anyagi viszonyok, munkahely, melyet később további támadásokra lehet használni pszichológiai manipuláció (social engineering) segítségével.
- Fiókot is fel lehet törni vele, erre a célra készített jelszótörő programok segítségével, amelyen keresztül további érzékeny adatok ismerhetők meg, esetleg más fiókokba is könnyedén be lehet vele jutni (pl. elektronikus banki oldalak).

Felhasznált irodalom

- Erdősi Péter Máté – Solymosi Ákos (2018): *IT biztonság közérthetően*, Neumann János Számítógép-tudományi Társaság, Budapest
<https://archive.org/details/NJSZTITBiztonsagKozerthetoenV3>
- Risk Based Security Inc. (2019): *2019 Year End Report Data Breach*
<https://bit.ly/3qkvMIV>
- Harris Poll, Google Inc. (2019): *The United States of P@ssw0rd\$*
<https://bit.ly/3ajrJqQ>
- Berta István Zsolt (2011): *Nagy E-szigonó könyv*, Microsec Kft, Budapest
http://static.e-szigno.hu/anyagok/nagy_e-szigno_konyv.pdf
- Bottyán László (2020): *Információbiztonsági tudatosság az iskolákban*. Előadás: Digitális eredmények és lehetőségek a neveléstudományi kutatásokban és a pedagógusképzésbe Pécs, 2020. november 25-26.
- Benedek András – Horváth Cz. János – Molnár György – Nagy Gábor Zsolt – Nyíri Kristóf – Szabó Erzsébet Mária – Tóth Péter – Verebics János (2012): *Digitális pedagógia 2.0*, Typotex, Budapest
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
<https://net.jogtar.hu/jogszabaly?docid=a1300050.tv>
- 1102/2020. (III. 14.) Korm. határozat a koronavírus miatt a köznevelési és szakképzési intézményekben új munkarend bevezetéséről
<https://net.jogtar.hu/jogszabaly?docid=A20H1102.KOR>

Kulcsszavak: *információbiztonság | adatbiztonság | digitális oktatás
biztonsági kultúra | biztonság tudatosság*