Krasznay Csaba – Koczka Ferenc

A távolléti oktatás jelentette kiberbiztonsági és adatvédelmi kihívások

A Covid-19-et okozó vírus megjelenése számos területen azonnali intézkedés megtételét tette szükségessé. A rendkívüli helyzetben azonnal végrehajtott intézkedések elsődleges célja a lakosság egészségének védelme és a károk elkerülése volt, azok másodlagos hatásaival az adott helyzetben nem feltétlenül lehetett számolni. A távolléti oktatás feltételeinek megteremtéséhez, a gazdaság működőképességének fenntartásához szükséges távoli munkavégzés kialakításához az informatikai rendszerekben rövid idő alatt nagy módosításokat kellett végezni, emellett új szoftverek bevezetése vált szükségessé. Ennek során számos, a rendszereket és felhasználóit egyaránt érintő kiberbiztonsági kérdés merült fel. Tanulmányunkban ezeket rendszerezzük és mutatjuk be.

Bevezetés

2020 márciusában egy nap alatt állt át a magyar közoktatás a távolléti, digitális oktatásra. A felsőoktatásnak erre két hét állt rendelkezésre. A Központi Statisztikai Hivatal 2019-es adatai alapján ez Magyarországon 1,8 millió olyan felhasználót jelentett, akik közül a legtöbben soha korábban nem tapasztalták meg az interneten keresztül történő tanulást.[1] Természetesen az oktatás egyetlen szereplője sem volt felkészülve erre a gyors váltásra, mert bár számos jó gyakorlat terjedt el, illetve kiváló külföldi példák is rendelkezésre álltak, ezek széles körben történő alkalmazását sem a jogszabályok, sem a Nemzeti Alaptanterv (NAT) nem ösztönözték. Törvényszerűen az informatikai infrastruktúra sem volt készen ennek a közel 2 millió embernek a fogadására.

A pedagógiai kihívások mellett az egyik legtöbbet emlegetett probléma az információbiztonsághoz és az adatvédelemhez kapcsolódott. A felhasználók mellett az oktatási intézmények, sőt a digitális oktatási platformokat nyújtó szolgáltatók sem voltak felkészülve arra, hogy miként védjék meg magukat és egymást a kibertérből érkező fenyegetésekkel szemben. A valós kiberfenyegetések mellett ráadásul olyan információbiztonsági és adatvédelmi jogszabályi kötelezettségek is megjelentek az intézményeknél, amelyekről korábban a legtöbben nem is hallottak. Jelen tanulmány tételesen áttekinti, hogy milyen jellemző kérdések merültek fel a távoktatás időszakában az adat- és kibervédelem területén, és milyen jó gyakorlatokat alkalmaztak hazánkban ezek feloldására. A szerzők a Nemzeti Közszolgálati Egyetem (NKE) és az Eszterházy Károly Egyetem (EKE) példáin keresztül mutatják be a felsőoktatási gyakorlatokat.

[1] KSH: Oktatási adatok, 2019/2020 (előzetes adatok). *Statisztikai Tükör,* 2019. december 20.

https://doi.org/10.36250/00925_13

Jogszabályi kötelezettségek

A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény a következőképpen határozza meg a távoktatást: „sajátos információ-technológiai és kommunikációs taneszközök, valamint ismeretátadási-tanulási módszerek, digitális tananyagok használatával az oktató és hallgató interaktív kapcsolatára és az önálló hallgatói munkára épülő képzés, amelyben a tanórák száma nem éri el a teljes idejű képzés tanóráinak harminc százalékát." A nemzeti köznevelésről szóló 2011. évi CXC. törvény a távoktatás helyett a digitális munkarend fogalmát használja: „Az (1) bekezdésben meghatározott tantermen kívüli digitális munkarendben a nevelés-oktatás, a tanulási folyamat ellenőrzése és támogatása a pedagógusok és a tanulók online vagy más, személyes találkozást nem igénylő kapcsolatában – elsősorban digitális eszközök alkalmazásával – történik." E sajátos oktatási formák adatvédelmi és információbiztonsági követelményeivel azonban egyik mérvadó jogszabály sem foglalkozik. Egyedül a köznevelési törvény tesz említést arról, hogy az internet akár veszélyt is jelenthet a gyermekekre nézve: „A köznevelési intézmény köteles a gyermekek, tanulók számára hozzáférhető, internethozzáféréssel rendelkező számítógépeket a gyermekek, tanulók védelmét lehetővé tevő, könnyen telepíthető és használható, magyar nyelvű szoftverrel ellátni a gyermekek és tanulók harmonikus lelki, testi és értelmi fejlődése védelmének érdekében." Ez azonban csak az iskolai számítógépek védelmére vonatkozik; arra, hogy az otthoni gépeken bármit is tenni kellene, nem tér ki.

Jól mutatja a magyar oktatási rendszer felkészületlenségét a biztonságos és adatvédelmet figyelembe vevő távoktatásra a 1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról áttekintése. A kormányhatározat alapján kiadott részletes stratégia pontosan bemutatja, hogy milyen feladatokat tervezett megoldani a jogalkotó 2020-ra. Ebben számos fontos kérdés szerepel, amelyek járulékosan ugyan hozzá tudtak volna járulni néhány részprobléma leküzdéséhez, de konkrétan a távoktatás, távolléti oktatás vagy a digitális munkarend fogalmak nem szerepelnek a dokumentumban. Az eszközrendszerben nyoma sincsen az otthoni számítógép-használat biztonsága növelésének vagy akár a pedagógusok adatvédelmi és információbiztonsági tudásával kapcsolatos fejlesztésnek. Egyetlen intézkedés van a szövegben, amelynek megvalósulása talán hasznos lehetett volna a vészhelyzet kihirdetésének időpontjában: „Az Ekertv. gyermekek megóvását célzó szabályainak, valamint az online-kereskedelemmel kapcsolatos fogyasztóvédelmi jogérvényesítést bemutató ismeretterjesztő és tájékoztató anyagok elkészítése és az iskolákba való eljuttatása, továbbá az egyes köznevelési intézmények honlapján az online gyermekvédelem területén alkalmazható jogszabályokról, védelmi lehetőségekről és a médiaműveltség növelését célzó programokról szóló naprakész információk elérhetővé tétele."

A felsőoktatási intézmények esetében valamivel kedvezőbb helyzetben indult a távolléti oktatás. Az intézmények jelentős része rendelkezett információbiztonsági szabályzattal, az oktatók több intézményben részesültek kötelező információbiztonsági tudatossági oktatásban, minden egyetemen kötelező az adatvédelmi felelős alkalmazása, informatikai rendszereik pedig jobbára tartalmaznak információbiztonsági megoldásokat. A hallgatók, legalábbis a nappali tagozatokon, jellemzően tudatosan, „életvitelszerűen" használnak információs rendszereket, azok biztonsági és adatvédelmi kihívásairól legalább említésszinten többnyire hallottak már. Ez természetesen nem azt jelenti, hogy tökéletesen tisztában lennének a kibertér veszélyeivel, de a tizenéves vagy akár még fiatalabb „távtanulókhoz" képest lényegesen biztosabb tudással rendelkeznek. Külön meghatározott jogszabályok viszont nem rendelkeznek itt sem a távoktatás biztonsági követelményeiről. A veszélyhelyzet kihirdetése tehát arra kényszerítette az érintetteket, hogy a létező jogszabályokból vezessék le a követelményeket, és a jó gyakorlatok felhasználásával csökkentsék a kockázatokat.

Adatvédelmi elvárások

A digitális munkarend sajátja, hogy a diákok, hallgatók, tanárok, oktatók jellemzően a saját eszközükön keresztül kommunikálnak egymással egy külső szolgáltató által kezelt platformon; olyan adatokat, információkat osztanak meg, amelyek a személyes adatok körébe tartoznak. Belátható, hogy komoly aggályokat vet fel egy olyan szituáció, amikor egy kiskorú gyermek videókapcsolaton keresztül csatlakozik be egy online tanórára, miközben otthoni élettere is látszódik a háttérben; mindezt olyan platformon, amelyet a tanár ingyenesen regisztrált, így jóváhagyva azokat az általános szerződési feltételeket, amelyeket a szolgáltató nyilvánvalóan a platformon áthaladó adatok maximális kihasználása érdekében alakított ki. Adatvédelmi szempontból szintén kérdéses gyakorlat az, amikor a tanár – például a testnevelés óra elvégzésének bizonyítása érdekében – videófelvételt kér a gyermektől, aki ezt egy felhőszolgáltatón keresztül osztja meg a tanárával. A videó tárolásával ugyanis adatkezelés valósul meg olyan környezetben, ahol az adatvédelmi szabályozás nem egyértelmű. Mivel a távolléti oktatás első időszakában a legtöbb pedagógus a saját legjobb belátása szerint oldotta meg a tananyag átadását, olyan kimondottan rossz gyakorlatokról is lehetett hallani, mint hogy a tanár elvárása alapján kellett a 13. életévét be nem töltött gyermeknek regisztrálnia a Facebookra, amivel nemcsak a szülők addigi nevelési céljait, de a közösségi hálózat saját felhasználási szabályzatát is meg kellett sérteni.

Ezeket az anomáliákat az Általános Európai Adatvédelmi Rendelet (*General Data Protection Regulation* – GDPR) keretein belül kellett megnyugtatóan rendezni, a különleges jogrend ugyanis nem tehette semmissé ennek rendelkezéseit. A köznevelési intézmények – bár többnyire nem rendelkeznek adatvédelmi felelőssel – ezt aránylag könnyen meg tudták tenni, mivel a tanulók adatainak kezelését a köznevelésre vonatkozó jogszabályok alapján különösebb gond nélkül meg lehetett oldani. A közösségi hálózaton

létrehozott tanári fórumokban azonban egyértelműen érződött, hogy a pedagógusok felesleges nyűgként tekintenek az adatvédelmi előírásokra. A szülői fórumokban eközben teljesen jogosan azok a hangok váltak meghatározóvá, amelyek a gyermekek és ezen keresztül a családok privát szférájába való minél kevesebb beavatkozást várták el.[2]

A gordiuszi csomót végül a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) NAIH/2020/2888 számú ajánlása oldotta fel. Egy szülő azzal a kérdéssel fordult a Hatósághoz, hogy „mennyiben felel meg az adatvédelmi jogszabályok előírásainak, ha a koronavírusra tekintettel bevezetett digitális oktatás során a gyakorlati órákon (így például a testnevelés óra) kiadott feladatok teljesítésének ellenőrzése céljából a tanár a feladat teljesítését igazoló videófelvétel elkészítését és a részére – e-mail vagy Messenger útján – történő elküldését kéri a 14–16 év közötti diákoktól anélkül, hogy ehhez a Ptk. 2:48. §-a alapján előzetesen kérné a diákok vagy a szülői felügyeletet gyakorló személy hozzájárulását, illetve bármilyen tájékoztatást nyújtana az adatkezeléssel kapcsolatosan". További kérdésként merült fel, hogy milyen módon és ki adhat hozzájárulást az adatok megosztására, ha a gyermek még nem töltötte be, illetve ha már elmúlt 16 éves.[3]

Az állásfoglalás alapján egyrészt kiderült, hogy ilyen esetekben az adatkezelő egyértelműen a közoktatási intézmény, tekintettel arra, hogy a megosztott adatok a nemzeti köznevelésről szóló 2011. évi CXC. törvény alapján az iskolai nevelés és oktatás mint köznevelési alapfeladat ellátása körébe tartoznak. Vizsgálni kell azonban, hogy vannak-e olyan megoldások, amelyek kevésbé avatkoznak be a gyermekek magánszférájába, és lehetőség szerint ezeket kell előnyben részesíteni. A Hatóság összességében felhívta a figyelmet az adattakarékosság, a korlátozott tárolhatóság, a bizalmasság és integritás elveinek betartására, kiemelve továbbá az adatbiztonságot és az adatkezelés átláthatóságát, az adatok pontosságát is. Az adatkezelési tájékoztatás és az adatvédelmi elvek betartása tehát a köznevelési intézmények feladata, amelyet a digitális oktatás műszaki eszközrendszerének kialakításakor is figyelembe kell venniük.

Információbiztonsági követelmények

Az iskolai informatikai rendszerek működését szabályozó specifikus törvényi szabályzás nem létezik ma Magyarországon. Működésüket, adattartalmukat és azok védelmét az általános törvények határozzák meg, a legnagyobb mértékben talán a GDPR állít kereteket. A GDPR szempontjából az információbiztonság legfontosabb eleme a bizalmasság, amely a távolléti oktatás gyors bevezetése következtében a legkönnyebben sérülhetett.

[2] Elsősorban a témában létrejött legnagyobb, *Online otthonoktatás* nevű Facebook-csoportban olvasható vélemények alapján.

[3] NAIH: *NAIH/2020/2888/ állásfoglalás* (2020. április 2.).

Az oktatási rendszerek biztonságos üzemeltetése adminisztratív és technikai szempontból is komoly kihívást jelent az egyes intézmények üzemeltetői számára. Sok általános és középiskolában nem létezik informatikai biztonságot szabályzó dokumentum, ennek következtében nem definiáltak az informatikai rendszer működtetésének folyamatai sem. Az iskolai informatikai rendszerek üzemeltetését gyakran csak félállásban vagy órakedvezményért ellátó oktatók feladata kimerül az infrastruktúra működőképességének biztosításában és az ehhez kapcsolódó iskolai adminisztráció segítésében. Ebben a körben optimális megoldást az informatikai szakrendszerek működtetésének kiszervezése jelentené, így olyan központosított szolgáltatás igénybevétele, ahol az üzemeltetési feladatokat képzett szakemberek látják el. Azon rendszerek esetében, ahol a külső szolgáltatás nem vehető igénybe, saját rendszer felépítésével próbálnak megoldást adni, amelyek hosszú távon biztonságos üzemeltetése számukra kockázatos feladat lehet.

Az iskolai rendszerek védelmére a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) önálló osztályt hozott létre. A nemzetközi kapcsolatokkal működő eseménykezelő központ (*Computer Security Incident Response Team* – CSIRT)[4] a felsőoktatási és köznevelési intézmények számára nyújt biztonsággal, támadások megelőzésével és azok elhárításával kapcsolatos információkat, segítséget nyújt hálózati incidensek kivizsgálásában és elhárításában. Tapasztalatuk szerint azonban a biztonsági problémák nem iskolaspecifikusak, hanem az általános levelezési, kéretlenlevél-küldéssel kapcsolatos, weblap-sérülékenység kihasználását célzó ügyek voltak, aminek fő okaként a már említett rendszer-üzemeltetési tapasztalatlanság mellett a felhasználók adatbiztonsági ismereteinek hiányosságait említik.

A felsőoktatásban az oktatói és kutatómunka támogatására a legtöbb esetben vállalati szintű informatikai háttér áll rendelkezésre, amelynek üzemeltetését vagy egy központi szervezeti egység, vagy pedig az egyes szervezeti egység önálló informatikusai végzik. A felsőoktatási intézmények túlnyomó többsége rendelkezik informatikai biztonsági szabályzattal, és bár nem vonatkozik rájuk egységes tartalmi szabályzás, a legtöbbjükből kiolvasható a 2013. évi L. törvény szellemisége. A rendszerek beszerzése során a szállító bizonyos körű oktatást is vállal, így az üzemeltetők valamennyire ismerik és képesek működtetni azokat. Számos intézmény rendelkezik olyan szerződéssel, amely az általános üzemeltetési feladatokon túl is biztosítja a szakszerű támogatást.

Az információbiztonsági tudatosság általános fejlesztése az oktatási intézményben kiemelt feladat kell, hogy legyen. A vírushelyzet megjelenésekor a távolléti oktatás műszaki hátterének gyors kialakítása nemcsak jogi, hanem üzemeltetési oldalon is háttérbe szorította a biztonsági szempontokat. A távoktatási platform kiválasztása csak az első lépés volt, azok telepítése és az oktatók oktatása a feladat azonnali megvalósítását célozta, de mivel a felsőoktatásban a távolléti oktatás

[4] A KIFÜ CSIRT részletes feladatszabása elérhető: https://kifu.gov.hu/szolgaltatasok/ikt/ugyfeltamogatas/it_incidens_kezeles

alapjai már rendelkezésre álltak, az oktatók a saját megoldásaikat preferálták. Ez az üzemeltetési feladatokat is megnehezítette, hiszen egy szolgáltatási kör helyett több, az üzemeltetés számára esetleg ismeretlen szoftvert kellett üzemeltetni, és ahhoz támogatást nyújtani. Ez a sokszínűség a hallgatók számára sem volt ideális, az Eszterházy Károly Egyetem (EKE) távolléti oktatás eredményességére vonatkozó felmérésében nagyszámú hallgató adott hangot az oktatási platform egységesítésére vonatkozó kérésének. A Nemzeti Közszolgálati Egyetemen (NKE) 1550 hallgató nyilvánított véleményt a távolléti oktatás tapasztalataival kapcsolatban. A megadott tantárgyi dokumentumokat és feladatokat a véleményezők nagy többsége teljesen megfelelőnek találta a tantárgy célja és tematikája szerinti önálló tanulás folytatására. A véleményezők több mint 90%-a szerint az oktatókkal folytatott e-mailes kommunikáció szintén megfelelő. A kérdőívet kitöltők kétharmada teljesen, egyharmada pedig megfelelőnek találta az NKE távoktatási portál szolgáltatásait. A tanév végi távolléti ismeretellenőrzés (vizsga) módszerével a véleményezők 93%-a egyetértett.[5]

A platformok kihívásai

A biztonságos és adatvédelmileg is elfogadható háttér-infrastruktúra 2020 márciusában nem állt rendelkezésre a teljes magyar oktatási rendszer számára. Voltak azonban olyan infrastruktúraelemek, amelyekre el lehetett kezdeni az építkezést, és amelyek a hónapok során folyamatosan fejlődtek. A köz- és felsőoktatási intézmények változó eredményességgel ugyan, de a tanév végére alkalmazkodtak az egyes platformok kereteihez, ez pedig jó alapot biztosít minden szereplőnek a későbbi digitális oktatás megvalósításához. Az egyes platformok azonban a legtöbbször nem fedik le az online oktatás teljes eszközkészletét, ezért az oktatási folyamat során több alkalmazást párhuzamosan kell igénybe venni. Az online oktatást támogató szoftverrendszer legfontosabb összetevői a képzésszervezési elemek, amelyekben a tanulók és órák egymáshoz rendelhetők, a tananyag leírására, annak nyomon követésére és számonkérésére szolgáló alrendszerek, valamint az élő kommunikáció és ahhoz kapcsolódó eszközök. A digitális oktatás tapasztalatai alapján egy kiválasztott platformnak a következő tulajdonságokkal kell rendelkeznie:

- teljesítenie kell az európai adatvédelmi elvárásokat;
- biztosítania kell a gyermekek adatainak különleges védelmét;
- legyen benne különleges adatvédelmi megoldás;
- lehetővé kell tennie az intézményi felhasználókezelést;
- biztosítania kell az intézményi adminisztrátorok számára az esetleges visszaélések felderítését;
- a fejlesztőnek minél előbb javítania kell a felderített sebezhetőségeket.

[5] NKE: *Elégedettek a hallgatók az NKE távolléti oktatásával* (2020. április 28.).

Microsoft Teams

Az oktatási intézmények legnépszerűbb választása a Microsoft Teams platform volt. Ez nem meglepő annak a tudatában, hogy a Microsoft termékpalettája Magyarországon évek óta ingyenesen rendelkezésre áll mindenkinek, aki részt vesz az oktatásban. Hátránya, hogy a fejlesztése csak 2017-ben kezdődött meg, a Skype for Business alkalmazás leváltására, így egyrészt viszonylag kevesen ismerték, kevés intézményben rendelkeztek megfelelő telepítéssel a lehetőségek maximális kihasználásához. Bár kiválóan támogatja az oktatást, számonkérést, adminisztrációja bonyolult, ha nincsen megfelelő informatikai támogatás, a laikus felhasználó nehezen boldogul vele. A biztonsági és adatvédelmi szempontrendszer alapján talán a legjobban teljesít.

A Microsoft a nagy informatikai vállalatok közül mindig is élen járt abban, hogy teljesítse a GDPR elvárásait. Számos adatközponttal rendelkezik Európában, így könnyen meg tudja valósítani a jogszabályoknak megfelelő adatkezelést. Fontos még, hogy bevételei nem elsősorban a felhasználói adatok hasznosításából származnak, így versenytársainál nagyobb bizalommal lehet feléjük lenni.

A Microsoft Teams ideális használatához intézményi felhasználói, úgynevezett O365-fiók szükséges, ám ez a távolléti oktatás kezdetekor a legtöbb helyen nem állt rendelkezésre. További megoldás volt egy Microsoft-fiók regisztrálása, illetve lehetőség volt az online órákon regisztráció nélkül is részt venni. A gyermekek adatvédelme mindhárom esetben megvalósítható, mivel az O365 fiókot az iskola kezeli a saját adatvédelmi elvei alapján. A Microsoft-fiók esetében lehetőség van olyan gyermekfiók létrehozására, amelyet a szülő felügyel, a regisztráció nélküli felhasználásban pedig értelemszerűen nem történik olyan személyes adat kezelése, amely kimondottan a gyermekhez kapcsolódna.

A Microsoft Teams tartalmazza a választható háttérfunkciót, így a tanuló, hallgató háttérkörnyezete elrejthető, ezzel erősítve a privát szféra védelmét. Az adatátvitellel és a telepített alkalmazással kapcsolatban nem merültek fel adatvédelmi aggályok.

Az intézményi felhasználókezelés megvalósítható, sőt az ideális felhasználáshoz meg is kell valósítani. Ehhez a Microsoft minden támogatást megad, részletes oktatási anyagok állnak rendelkezésre.

A biztonsági incidensek kivizsgálása lehetséges, de ehhez már mély informatikai tudás szükséges. Nem szabad elfelejteni, hogy a Microsoft Teams felhőalapú megoldás, így a biztonsági események részleteihez való hozzáférés nem lehet teljes, az adminisztrátor annyit lát, amennyit a cloudszolgáltató láttatni enged.

A távolléti oktatás időszakában komolyabb biztonsági sebezhetőség nem merült fel a platformmal szemben. Egyetlen olyan sérülékenységről számolt be a szaksajtó, amelynek segítségével egy támadó egy megkonstruált képfájl segítségével átvehette egy felhasználó fiókját, de ezt a hibát a Microsoft április végén befoltozta.[6]

[6] Omer Tsarfati: Beware of the GIF: Account takeover vulnerability in Microsoft Teams. *Cyberark,* 2020. április 27.

Google Classroom

A Google Classroom legnagyobb előnye az volt, hogy a Google-t kis túlzással mindenki ismeri, és mindenki használja is. Bár a Classroomot Magyarországon kevéssé ismerték, 2014-es indulása óta több százmillió felhasználója lett világszerte, az Egyesült Államok oktatási intézményeivel pedig szoros kapcsolatot építettek ki az évek folyamán, így a tanárok és a diákok számára is kézre álló, jól használható, faék egyszerűségű platformot kaphattak a magyar oktatás szereplői. Az ingyenes, saját felhasználói fiókkal indítható Tanterem és az intézményi, úgynevezett G Suite megoldás között ráadásul képességekben nincsen különbség. Természetesen, ha valami ingyen van, akkor mi magunk vagyunk az áru, tehát biztonsági és adatvédelmi szempontból mégis igen nagy az eltérés a két változat között. Az online órák megtartása a Google Meet szolgáltatásban lehetséges.

A Google esetében az adatvédelem mindig a legérzékenyebb kérdés. A Classroom esetében az, hogy milyen mértékben gyűjt adatot a felhasználókról, nagyban függ attól, hogy milyen beállítások mellett használják. Az ingyenes változat, amelyet ingyenes Google-fiókkal használnak, sokkal inkább kitett az adatgyűjtésnek, mint a szerződéses G Suite megoldás. Új-Mexikó állam 2020 februárjában nyújtott be keresetet a Google ellen azért, mert nem megfelelően kezelték a Classroom gyermek felhasználóinak adatait.[7] Mivel az amerikai adatvédelmi szabályozás sokkal megengedőbb, mint az európai, feltételezhető, hogy az ingyenes felhasználás számos kérdést vetne fel a GDPR-vizsgán. Nem meglepő, hogy a Google az iskolai felhasználásra a G Suite-et ajánlja, s ott is javasolja a GDPR-megfelelőséget lehetővé tevő szerződéses feltételek külön beállítását, amelyek egyébként alapértelmezésben nem élnének.

A Google lehetőséget biztosít gyermekfiókok létrehozására a Google Family Link szolgáltatáson keresztül, amelyek nagyobb fokú adatvédelmet biztosítanak, mint az általános felhasználói hozzáférések. Ezekkel használva a Classroomot a gyermekek adatvédelme lényegesen jobban biztosított, mint a normál fiókoknál.

A Google Meet szolgáltatásban a háttér elhomályosítása jó ideig nem szerepelt a lehetőségek között, a Microsoft Teams és a Zoom jelentette verseny azonban kikényszerítette ennek a privát szférát erősítő technológiának a használatát. Általánosságban azonban elmondható, hogy a Classroom és a Meet önmagában biztonságos, a Google pedig a világ egyik, ha nem a legjobb biztonsági csapatával rendelkezik, így kicsi a valószínűsége a komolyabb adatbiztonsági incidensnek. Külső támadótól tehát kevéssé kell féltenünk az adatainkat, azt viszont nem szabad elfelejteni, hogy a Google elsődleges bevételi forrása a felhasználók adatainak felhasználásában rejlik.

A G Suite megfelelő platformot biztosít a felhasználói fiókok intézményi kezelésére. Ez a megoldás az oktatáson kívül számos vállalatnál is használatban van, így az iskolák és egyetemek is sikerrel használhatják. Kezelése egyszerűbb a Microsoft megoldásánál.

[7] Nick Statt: Google sued by New Mexico attorney general for collecting student data through Chromebooks. *The Verge,* 2020. február 20.

A G Suite for Education licenc ingyenesen rendelkezésre áll az iskolák számára, ha azonban komolyabb információbiztonsági incidenst kellene visszakövetni, azt már csak a külön előfizetésben rendelkezésre álló G Suite Enterprise for Education licenc keretein belül lehet megtenni. Az intézményi adminisztrátorok lehetőségei tehát korlátozottak.

Mivel a Google platformja az egyik legbiztonságosabb a világon, ritkán fordul elő, hogy ezekben a felhőalapú szolgáltatásokban olyan hibát találnak, amely nyilvánosságra is kerül. Ennek megfelelően sem a Google Classroom, sem a Google Meet esetében nem írt a szaksajtó olyan sebezhetőségről, amellyel érdemben foglalkozni kellene.

Zoom

A járványhelyzet egyik legnagyobb nyertese vitathatatlanul a Zoom telekonferencia-megoldás. A felhőalapú szoftver az egyik leginnovatívabb versenyző volt a kommunikációs szolgáltatások piacán, de a világszerte hirtelen kitörő távoli munkavégzés és távoktatás meglepetésszerűen tornászta felfelé a 2011-ben alapított cég felhasználóinak számát. Ez érezhetően magát a Zoomot is meglepte, hiszen olyan adatvédelmi és információbiztonsági problémák derültek ki március–áprilisban, amelyek jelentősen megtépázták a cég renoméját. Bár technológiailag jól vizsgázott a szolgáltatás, egyszerűen nem voltak felkészülve arra, hogy kiskorúak milliói és nem mellesleg fontos kormányzati szervek fogják használni a Zoomot.

Az európai adatvédelmi elvek teljesítésével kapcsolatban nagyon hamar kételyek merültek fel, amikor kiderült, hogy a szolgáltatás aktívan használja a Facebook azon szoftvermegoldását (*Software Development Kit* – SDK), amely nagy mennyiségben továbbítja a felhasználói adatokat a közösségi hálózat felé. Azután az is napvilágot látott, hogy a beszélgetések, bár elvileg titkosított formában folytak, a cég szerverein a titkosítást feloldották, a Zoom hozzáfért ezek tartalmához, és a megszerzett adatokat felhasználta. Ezek a botrányok arra kényszerítették a Zoomot, hogy felülvizsgálja az adatvédelmi szabályzatát, és sokkal szigorúbban vegye az adatvédelmi elveket. Ezt 2020. április folyamán meg is tette.[8]

A Zoom nem oktatásra lett tervezve, éppen ezért az első időszakban nem is volt külön eljárásrend az iskolai órák támogatására. A tömeges igény azonban kikényszerítette egy kimondottan a gyermekek felhasználását meghatározó szabályozó létrehozását. Az egyszerűség kedvéért nincsenek külön gyermekfiókok, a 16 év alatti felhasználók nem hozhatnak létre felhasználói fiókot a Zoomban. Lehetőségük van viszont regisztráció nélküli használatra, illetve külön iskolai regisztrációra, amely esetében az intézmények felelősségi körébe tartozik a gyermekek adatvédelmének biztosítása.

[8] Paul Wagenseil: Zoom security issues: Here's everything that's gone wrong (so far). *Tom's Guide*, 2020.

Innovatív megoldásként a Zoom sokat tett azért (már a járványhelyzet előtt is), hogy felhasználói adatvédelmét biztosítani tudja, hiszen a kitakart háttér vagy a kommunikáló végpontok közötti (közel) teljes titkosítás már régóta a szoftver része. Sajnálatos módon kiderült azonban, hogy a teljes végponti titkosítás a Zoom szerverein megszakad, illetve az is, hogy számos szerver Kínában található, ami erősen visszavetette a platformmal szembeni bizalmat.

Az intézményi felhasználás teljeskörűen biztosított, ám jelentős költséggel jár a többi megoldáshoz képest. Ezért az a jellemző, hogy a tanárok ingyenes felhasználói fiókokat használnak az oktatás során.

Nem áll rendelkezésre részletes és kiterjedt incidensmenedzsment-lehetőség, így a szolgáltató támogatása nélkül nem lehetséges intézményi szinten megvalósítani az esetleges visszaélések felderítését.

2020. március 1-től kezdődően, jelen tanulmány írásáig, összesen kilenc sebezhetőséget hoztak nyilvánosságra a Zoommal kapcsolatban. Ezek közül egy kritikus, hét magas, egy pedig alacsony besorolást kapott.[9] A tömeges használattal párhuzamosan ugyanis több biztonsági elemző nézett utána alaposan annak, hogyan is működik a Zoom, ez pedig előhozta a kódbázisban lévő hibákat. Nem véletlen, hogy április elején a cég ügyvezetője egy 90 napos fejlesztési ciklust jelentett be, amikor kizárólag az adatvédelemmel és az információbiztonsággal kapcsolatos fejlesztéseket hajtottak végre.

KRÉTA/Neptun

Bár a közoktatásban használt KRÉTA és a felsőoktatás Neptun-rendszerének jogtulajdonosa két különböző cég, a technológiai alapjaik és a rendeltetésük is közös, ezért célszerű együtt elemezni ezeket a platformokat. A távolléti oktatás ideje alatt ezek voltak a hivatalos megoldások, ami nem csoda, tekintettel arra, hogy a vonatkozó jogszabályok szerint ezek töltik be a központi oktatási rendszer funkcióját. A Neptun-rendszert először 1997-ben vezették be a Budapesti Műszaki Egyetemen, később több egyetem, majd a teljes magyar felsőoktatás áttért a használatára. A KRÉTA-t a 2016/2017-es tanévtől először próbajelleggel mutatták be, utána fokozatosan tért át rá a közoktatás. A Neptun intézményi telepítésű, a KRÉTA központilag menedzselt, felhő jellegű megoldás.

Talán e megoldások helyzete a legtisztább adatvédelmi szempontból. Mivel használatukat jogszabály írja elő, az oktatás minden szereplőjének adatkezelése levezethető ezekből. Az intézményi és szolgáltatói adatkezelési szabályzatok is tiszta helyzetet teremtenek. Fel sem merül annak a kockázata, hogy az összegyűjtött adatokat üzleti célra használná fel a szolgáltató.

Szintén egyértelmű a gyermekek adatainak felhasználása. A jogszabályi felhatalmazás miatt az ebben pontosan megfogalmazott adatgyűjtés teljes

[9] Az adatok forrása: National Vulnerability Database.

mértékben törvényes. A gyermekek egyébként saját regisztrációval rendelkeznek a rendszerben, így hozzáférhetnek saját tanulmányi információikhoz. Fejlesztési lehetőség lehetne családi fiókok létrehozása, így a szülők és a gyermekek fiókjai elválnának egymástól.

Különleges adatvédelmi intézkedések, privát szférát erősítő technológiák használata nyilvános adatok alapján nem ismerhető meg ezekben a rendszerekben. Feltételezhető, hogy a fejlesztők jelentős energiát fordítanak a tárolt adatok védelmére, hiszen a kiterjedt felhasználói bázis ellenére nem érkezett hír adatszivárgásról az elmúlt években. A távolléti oktatás időszakában egyedül a Pázmány Péter Katolikus Egyetemről érkezett hír a Neptun-rendszert érintő, potenciális adatvédelmi incidensről, ahol egy zsarolóvírus tette elérhetetlenné a szolgáltatást.[10]

Az intézményi felhasználás alapvető tulajdonsága a rendszereknek, így a felhasználók kezelése az intézményi adminisztrátorokra van bízva.

Mivel a két rendszer az oktatás integráns része, az incidensmenedzsment nagy valószínűséggel nem állhat meg intézményi szinten, a biztonsági események kivizsgálásába az üzemeltetőt és a Nemzeti Kibervédelmi Intézetet (NKI) is be kell vonni.

A KRÉTA-rendszer honlapján nyomon lehet követni az egyes új frissítésekben megjelent változásokat. A 2020-as frissítések egyike sem utal arra, hogy biztonsági hibát kellett volna javítani. A nyilvánosság előtt sem ismert olyan sebezhetőség, amely a távolléti oktatás alatt akár a Neptunt, akár a KRÉTA-t érintette volna. Ha voltak is hibajavítások, akkor azokat a nyilvánossággal nem osztotta meg a fejlesztő.[11]

Moodle

A magyar felsőoktatás legelterjedtebb online oktatást segítő platformja a nyílt forrású, 2002 óta létező Moodle. A számos integrációt lehetővé tevő, intézményi telepítésekkel működő megoldás eredetileg ausztrál fejlesztés, ám nem áll mögötte semmilyen olyan üzleti érdek, amely a felhasználók személyes adatait fenyegetné. A nyílt forrás és a jelentős felhasználószám pedig lehetővé teszi a platform biztonságának a fenntartását is.

A Moodle adatvédelmi beállításai alapvetően attól az intézménytől függenek, amely telepíti és üzemelteti. Ennek megfelelően lehetőség van teljesen GDPR-konform működtetésre.

A rendszer alapvetően diákok adatainak kezelésére lett létrehozva, tehát külön gyermekfiók nem létezik. Létre lehet hozni viszont a szülői nézetet, amellyel a gyermekek fiókjai felügyelhetők. A rendszerből eredő adatvédelmi aggály nem merül fel, a gyermekek adatait az üzemeltető szervezet adatvédelmi szabályzatában foglaltak szerint kell kezelni.

[10] HVG: *Zsarolóvírus-támadás érte a Pázmányt, leállt a Neptun* (2020. április 24.).

[11] A frissítéseket az eKRÉTA honlapján lehet követni.

A Moodle moduláris felépítésének hála számos olyan kiegészítőt, úgynevezett plugint tartalmaz, amellyel az intézményi telepítés adatvédelmi beállításai fejleszthetők. Így például külön kiegészítő telepíthető a személyes adatok törlésével kapcsolatos kérésnek vagy éppen az oldal adatvédelmi szabályozásának átláthatóbbá tételéhez.

Az intézményi telepítésnek köszönhetően a felhasználókezelés teljes mértékben helyben történik, szinkronizáló pluginek is segítik, így a magyar felsőoktatásban jellemzően a Neptun-rendszer felhasználói adatbázisának alapján építik fel a Moodle felhasználói fiókjait.

A biztonsági események kezelése is teljes mértékben intézményi keretek között működik. A rendszer lehetővé teszi az egyes felhasználói események részletes naplózását, így jó lehetőség nyílik a visszaélések felderítésére.

Nyílt forráskódú szoftverként a Moodle-rendszer egyes biztonsági hiányosságai folyamatosan, a nyilvánosság előtt is követhető módon kerülnek jelentésre. 2004 óta összesen 401 biztonsági sérülékenység került nyilvánosságra, az utóbbi években jellemzően alacsony vagy közepes besorolással, bár 2019-ben egy kritikus besorolású hibát is találtak. 2020-ban két szoftveres sebezhetőség vált ismertté. A közösségi fejlesztők minden esetben javították a hibát, amely a vonatkozó fórumoldalon is jól követhető. A Moodle alkalmazásának azonban több biztonsági kockázata is felmerülhet. Egyetemi környezetben jellemzően ezres nagyságrendben hoznak létre tananyagokat, amelyek belső formátumai a Moodle különböző verzióiban eltérőek. A keretrendszer új változatának megjelenésekor a tananyagok konverziója komoly erőforrásigényt jelentene, és mivel erre gyakran nem jut erőforrás, a régi rendszerek felváltása helyett a meglévők életben tartásával egy újabb verzió üzembe állítását választják. A keretrendszer frissíthetőségét tovább rontja a korábbi verziók pluginjainak működésképtelensége az újabb változatokkal. Információbiztonság szempontjából ezek az egyedi fejlesztésű kódrészletek komoly veszélyforrást jelenthetnek, mivel azok nemcsak a tananyag leírásában, tesztekben kapnak szerepet, hanem képzésszervezési műveletekben is, így rajtuk keresztül a tanulmányi rendszer is támadható lehet.

Felhasználói attitűdök

A távolléti oktatás során számos olyan kiberbiztonsági problémával is szembesülhetett a közvélemény, amelyek egyértelműen a felhasználói viselkedésből és nem a technológiából adódtak. Sokszor elhangzik az a vélemény, miszerint a kibertér tulajdonképpen fizikai világunk leképezése, ahol az emberi viselkedés sokkal kevesebb társadalmi korlátba ütközik, így lényegesen könnyebben megjelennek a deviáns viselkedési formák. Az alábbi példák jól mutatják, hogy az iskolai terekben titkolt, vagy legalábbis visszaszorított viselkedési normák elementáris erővel jelentek meg a digitális oktatás során, hiszen az azt kezelni hivatott pedagógusok és oktatók kezében nem voltak évszázados megoldások.

Kortárs kiberzaklatás (cyberbullying)

A gyermekek online védelmével foglalkozó szakemberek között már a digitális oktatás kezdetén egyértelmű volt, hogy abból semmi jó nem fog származni, ha gyerekek milliói korlátlanul szabadulnak rá az internetre, ráadásul az oktatásban felhasználják azokat a közösségi hálózatokat is, amelyeken szülői és pedagógusi korlátozás nélkül lehet csetelni. Ez az aggodalom elsősorban az olyan szabad platformokra vonatkozott, mint például a Discord, amelyben a gyerekek válogatás nélkül írhatnak bármit.

A kortárs zaklatás mindig is az iskolai élet velejárója volt, gondoljunk csak az olyan klasszikus művekre, mint a *Pál utcai fiúk* vagy az *Iskola a határon*. Nincsen ez máshogy napjainkban sem, azzal a különbséggel, hogy a zaklatás nem ér véget iskolaidőben, az iskola falai között, hanem folytatódik a kibertérben, mindenki által látható módon. A cyberbullying napjaink egyik legkomolyabb problémája, kezelése ugyanis komplex iskolai programokat kíván meg. Az online oktatás során éppen ezért gyakran lehetett azt tapasztalni, hogy az interneten magukra hagyott gyerekek egymás ellen, illetve egy-két bizonyos személy ellen fordultak, és ha a pedagógusok ezt észlelték is, nem volt meg az eszköztárukban a probléma kezeléséhez szükséges megoldás.

Platformmal való visszaélés

Minden gyerek születésétől fogva hacker, aki törekszik a felállított szabályok áthágására. Idővel a legtöbben persze megtanulják és megszokják ezeket a társadalom és jog által felállított normákat, de a távolléti oktatás megmutatta, hogy ha egy platform nincsen kellő védelemmel ellátva, bizony a diákok bármit megtesznek, amit a jogosultságukkal megtehetnek. Gyakran lehetett például arról hallani, hogy a beadandó feladatokat egy adott mappába kellett feltölteni, azonban a leadási határidőben „varázsütésre" törlődött minden beadott dolgozat. A feladatdömpingben többeknek már nem volt meg az eredetileg leadott feladat, így ezt nem tudták pótolni. Az pedig sosem derült ki, hogy melyik diák törölte a többiek munkáját is azért, hogy ne látszódjon, hogy ő eleve le sem adta a feladatot. Az üzemeltetői jogok hiányában pedig ennek utána sem lehetett menni.

Ha pedig a diákok eminens módon viselkedtek, még mindig számítani lehetett a külső „támadókra", akik a platformok nem megfelelő beállításait kihasználva tudtak belépni egy-egy osztály életébe, jellemzően különösebb cél nélkül, pusztán a zavarkeltés céljából. A legismertebb ilyen „támadás" a *zoombombing* nevet kapta, ami a Zoom nem megfelelő beállítása mellett jelent meg. A „támadó" belépett egy olyan órára, amelynek hivatkozását valahogy megtudta (nyilvános megosztás vagy kitalálható URL segítségével), és ott oda nem illő, jellemzően pornográf videókat játszott le az erre közel sem felkészült gyermekeknek. A Zoom egyébként ennek a jelenségnek a kivédése érdekében alapértelmezetté tette az olyan beállításokat, mint például kötelező „előszoba" a felhasználóknak, amely lehetővé tette a külsősök kiszűrését.

Puskázás, csalás a vizsgán

A hagyományos vizsgák online térbe történő áthelyezésének első lépéseit a nyelviskolák tették meg. A külföldön már működő gyakorlat alapján négy nyelviskola dolgozta ki ennek hazai megoldását, és szigorúan ellenőrizték annak betartását. Az Origo írásbeli nyelvvizsgáját például egy erre a célra kifejlesztett speciális böngészőre, a Safe Exam Browserre (SEB) alapozták, miközben egy másodlagos számítógépen futó Zoom biztosította a vizsgázó megfigyelését. A SEB a személyazonosság hagyományos ellenőrzési eljárásai mellett a gépelési profil megváltozását is figyeli a csalások kiszűrésére. Bár e rendelkezésre álló rövid idő alatt szinte tökéletes megoldást adtak a szervezők, a vizsgák során kismértékben sérültek a GDPR-előírások, a vizsgázók személyes adatai más vizsgázók számára megismerhetővé váltak akkor, amikor a személyi igazolványukat a Zoom-videókonferencia során mindenki számára láthatóan fel kellett mutatniuk. A nyelvvizsgák korszerű, online lehetősége a távolléti oktatás után is megmaradt, most már határidő nélkül szervezhetők meg ebben a formában.[12]

A felsőoktatásban a szóbeli vizsgáztatás egyre kisebb arányban jellemző, az írásbeli vizsgák lebonyolítását a Neptun-rendszer modulja és a Moodle is támogatja. Az online vizsgák ellenőrzése komoly problémát jelentett az oktatók számára, számos hallgató nem rendelkezett webkamerával, vagy annak minősége nem tette lehetővé a vizsga tisztaságának ellenőrzését, amit egyetlen, a monitor felett elhelyezkedő kamerával ideális esetben is nehéz lenne megfelelően biztosítani. A felsőoktatási intézmények szabályzatokban írták elő a távolléti, elektronikus vizsgák szabályait, amelyeket teljes egészében nem sikerült érvényesíteni. A szóbeli vizsgáztatás legfontosabb megjelenése a záróvizsgákon történt. A magyar felsőoktatási intézmények változatos módszerekkel oldották ezt meg, de az nyilvánvalóvá vált, hogy célszerű lenne egységes, a legjobb gyakorlatok alapján kialakított módszert alkalmazni.

A vizsgán elkövetett csalások megakadályozására a legtöbb szoftver nem kínál támogatást, ideértve, hogy a vizsgázó ne futtathasson egyéb szoftvereket a folyamat során. Bár adatkezelési szempontból ingoványos terület a felhasználó gépének vizsgálata, ugyanakkor legalább az azon futó processzek felügyelete és a képernyőkép folyamatos ellenőrzése elvárható lenne a vizsga tisztaságának ellenőrzéséhez. Ennek hiányában a Discord háttérben történő futtatása jellemző megoldás volt az egyetemeken, amelylyel a vizsgázó megosztott képernyőjére segítői ráláttak, és interakcióba léphettek vele.

Ezek elkerülésére a felsőoktatásban megfigyelhető volt a videókamerás ellenőrzés elhagyása, és más módszerek keresése. A vizsgák tisztaságának eléréséhez jó lehetőség a szoros időkorlát állítása vagy a féléves munka során elkészítendő részkutatás, esszé kidolgozásának követelménye. A módszer további előnye a gyakorlati alkalmazás képességének hangsúlya, ugyanakkor az időkorlát a lassabb hallgatók számára komoly hátrányt jelentett. A hagyományos, a tananyag felidézésén, a törzsanyag memorizálásán alapuló számonkérések tisztasága online környezet esetében nehezen biztosítható.

[12] ITB: Továbbra is lehet online nyelvvizsgázni. *IT Business,* 2020. augusztus 22.

Kiberbűnözés

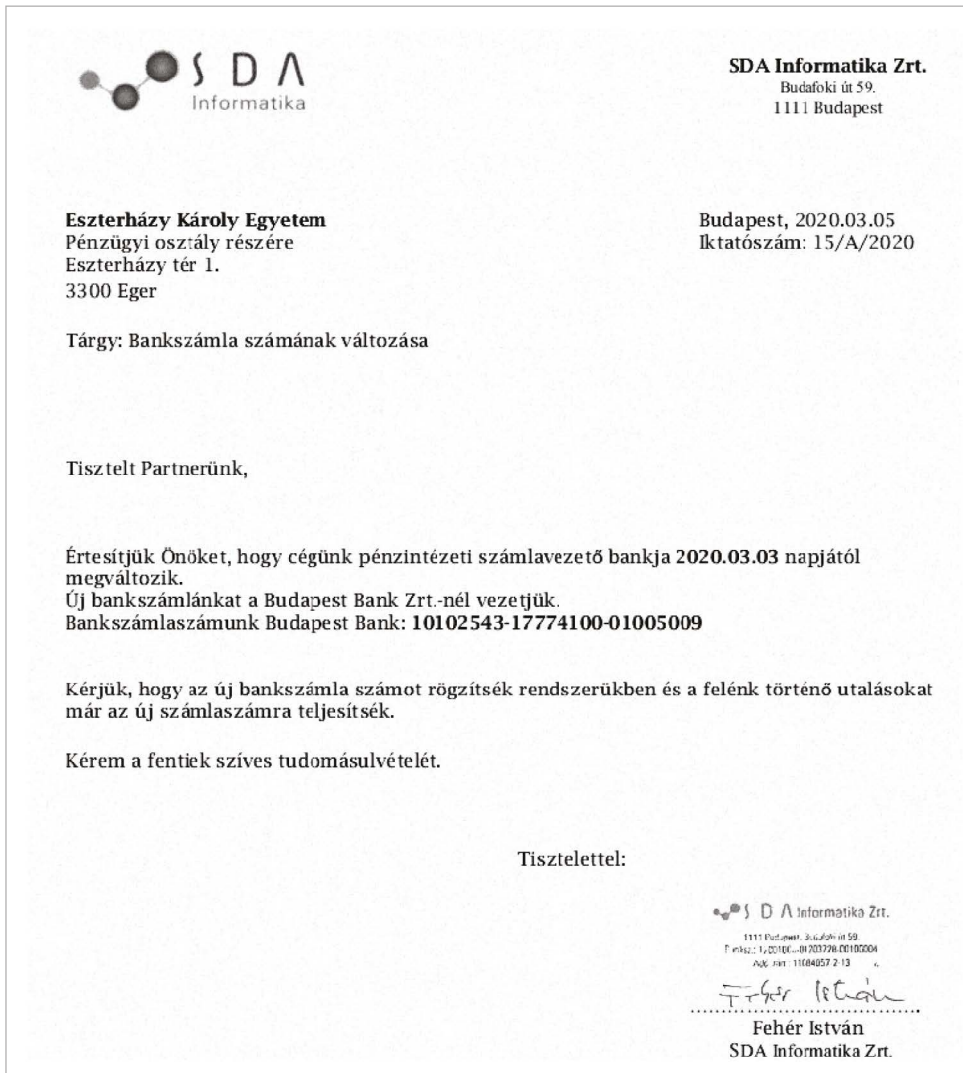
Az USA-ban 2004-ben lépett hatályba a Data Breach Notification törvény, amely előírja az informatikai incidensek jelentési kötelezettségét. Ettől kezdve állnak rendelkezésre amerikai adatok az oktatási rendszereket ért támadásokról is. Ilyen kötelezettség hazánkban a GDPR megjelenése óta van érvényben. Bár ezek az intézmények és rendszerek nem elsődleges célpontjai a kiberbűnözésnek, az ott tárolt személyes adatok a gyengébb védelmi infrastruktúra következtében esetenként könnyebb célpontot jelenthetnek. Nemzetközi szinten a kibertámadások hozzávetőleg 7%-a irányul az oktatási szektorra, és 6% körüli a kutatóintézetek elleni támadások aránya.[13] A támadók motivációi is változnak: a 2000-es évek elején a fő cél még a személyes adatok megszerzése volt, ezt a különféle csalási technikák során használható társadalombiztosítási szám (*Social Security Number* – SSN) megszerzése, majd a bankkártyaadatok eltulajdonítása követte. Megszaporodtak a tanulmányi rendszerben végzett jogtalan módosításokat célzó hallgatói cselekmények, amelyek az érdemjegyek mellett a szociális helyzetre vonatkozó adatok módosításán keresztül anyagi előnyhöz juttathatták a hallgatót. Egyre inkább előtérbe kerültek az elosztott túlterheléses támadások (*Distributed Denial of Service* – DDoS) támadások, illetve a felsőoktatási számítási és hálózati kapacitás felhasználása például kriptovaluták bányászására. Figyelemre méltó a támadási technikák eloszlása is: 2020 májusában az összes támadás 20%-a ismeretlen, feltehetően úgynevezett *zero day* technikával történt, amelyek felderítésére és kiszűrésére jelenleg csak a legdrágább védelmi termékek képesek, így az oktatási intézmények költségvetéséből nem fedezhetők.

A vírushelyzet okozta zűrzavart a támadók is igyekeztek kihasználni. A hagyományos, automatizált támadások jellege is ennek megfelelően alakult; a felhasználók megtévesztése és a gyors, hibás döntés kikényszerítése a bizonytalan felhasználók esetében nagyobb sikerrel kecsegtetett. Bár a támadások jellegének statisztikái a legnagyobb számban elsősorban gazdasági csalások elkövetését mutatják, megjelentek a helyzetet kihasználó megtévesztő levelek és csaló weboldalak is. Az otthoni számítógépek megnövekedett használati ideje további lehetőségeket kínált a kiberbűnözőknek, hiszen ezek a gépek azok, amelyek a legkevésbé karbantartottak, a frissítések elmaradása mellett az illegális forrásokból letöltött programok crackjei által feltelepített kártékony programok is nagy számban működnek rajtuk. A gyakoribbá vált támadások ellensúlyozására több szervezet is oktatási segédanyagokat készített, amelyek megismertetik a felhasználókkal az alapvető kiberbiztonsági szabályokat.

Magyarországon nem készült külön statisztika az oktatási rendszert érintő kiberbűnözésről, de az NKE Információs Társadalom Kutatóintézete által 2020 júniusában készített reprezentatív felmérés mutatja, hogy a teljes lakosság körében mindössze 28% képezi magát valamilyen módon annak érdekében, hogy védve legyen az online világ kihívásaival szemben. Közülük a legtöbben, 52,6% a barátoktól

[13] Paolo Passeri: June 2020 cyber attacks statistics. *Hackmageddon,* 2020. augusztus 13.

kapott információkkal képezik magukat, 47% szakcikkeket olvas, 20% pedig tanfolyamokon is részt vett. Feltételezhetjük tehát, hogy számos áldozata volt a kiberbűnözésnek a karanténidőszakban. Jól mutatja azonban a csalók tényked̈ését az alábbi ábrán látható levél, amely tipikus példája az úgynevezett vezérigazgatói csalásoknak, azaz *CEO fraud*nak.



SDA Informatika

SDA Informatika Zrt.
Budafoki út 59.
1111 Budapest

Eszterházy Károly Egyetem
Pénzügyi osztály részére
Eszterházy tér 1.
3300 Eger

Budapest, 2020.03.05
Iktatószám: 15/A/2020

Tárgy: Bankszámla számának változása

Tisztelt Partnerünk,

Értesítjük Önöket, hogy cégünk pénzintézeti számlavezető bankja **2020.03.03** napjától megváltozik.
Új bankszámlánkat a Budapest Bank Zrt.-nél vezetjük.
Bankszámlaszámunk Budapest Bank: **10102543-17774100-01005009**

Kérjük, hogy az új bankszámla számot rögzítsék rendszerükben és a felénk történő utalásokat már az új számlaszámra teljesítsék.

Kérem a fentiek szíves tudomásulvételét.

Tisztelettel:

S D A Informatika Zrt.

Fehér István
SDA Informatika Zrt.

1. ábra Csaló levél a Neptun tanulmányi rendszer fejlesztőjének nevében
Forrás: Koczka Ferenc felvétele

A levélben hitelesnek tűnő információt lehet találni arról, hogy a fejlesztő bankszámlaszáma megváltozott, és a licencdíjat ezentúl oda kell befizetni. Természetesen

ez nem igaz, az aláíró például már nem a cég vezérigazgatója, illetve a bélyegzőből kiolvasható a megfelelő bankszámlaszám is, mely nyilvánvalóan nem egyezik a levélben megadottal. Az ilyen és ehhez hasonló csalási kísérletek mutatják, hogy a kiberbűnözők a magyar intézményeket is támadják. Fontos tehát, hogy az oktatási rendszer minden tagja a lehető legfelkészültebb legyen. A biztonságtudatossági oktatások fontosságát tehát nem lehet eléggé hangsúlyozni.

Összefoglalás

A távolléti oktatás megvalósításánál az adatvédelem és az információbiztonság elveinek és követelményeinek betartása elkerülhetetlen. A kihívásokat elsősorban az oktatási rendszer szereplőinek tudatossághiánya és a digitális platformok érdekütközése jelenti. Jelen tanulmány felhívta a figyelmet néhány olyan jellemző problémára, amelyeket a 2020. március–július közötti időszakban lehetett tapasztalni. A szektor szereplőinek összefogásával, illetve az állami szereplők aktív szerepvállalásával a problémák jelentős része orvosolható.

Nincsen viszont gyors és egyszerű megoldás a gyermekek online biztonságának megteremtésére. A távolléti oktatás egyértelműen bizonyította, hogy mennyire fontos már a legfiatalabbakat is oktatni a megfelelő digitális eszközhasználatra, illetve odafigyelni az őket érő kibertéri veszélyekre. Itt is elsősorban a kortárs kiberzaklatást kell kiemelni, amely jelenleg az általános és középiskolák egyik legkomolyabb, de kevéssé kibeszélt veszélye.

Felhasznált irodalom

2011. évi CXC. törvény a nemzeti köznevelésről. Online: https://net.jogtar.hu/jogszabaly?docid=a1100190.tv

2011. évi CCIV. törvény a nemzeti felsőoktatásról. Online: https://net.jogtar.hu/jogszabaly?docid=a1100204.tv

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról. Online: https://net.jogtar.hu/jogszabaly?docid=A16H1488.KOR&txtreferer=00

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679

KSH: Oktatási adatok, 2019/2020 (előzetes adatok). *Statisztikai Tükör,* 2019. december 20. Online: https://www.ksh.hu/docs/hun/xftp/idoszaki/oktat/oktatas1920.pdf

HVG: *Zsarolóvírus-támadás érte a Pázmányt, leállt a Neptun* (2020. április 24.). Online: https://hvg.hu/tudomany/20200424_pazmany_peter_katolikus_egyetem_zsarolovirus_neptun_tanulmanyi_rendszer_szakdolgozat_leadasi_hatarido

ITB: Továbbra is lehet online nyelvvizsgázni. *IT Business,* 2020. augusztus 22. Online: https://www.itbusiness.hu/technology/kozigazgatas_n/tovabbra-is-lehet-online-nyelvvizsgazni

NAIH: *NAIH/2020/2888/ állásfoglalás* (2020. április 2.). Online: https://naih.hu/files/Adatved_allasfoglalas_NAIH-2020-2888.pdf

NKE: *Elégedettek a hallgatók az NKE távolléti oktatásával* (2020. április 28.). Online: https://www.uni-nke.hu/hirek/2020/04/28/elegedettek-a-hallgatok-az-nke-tavolleti-oktatasaval

Passeri, Paolo: June 2020 Cyber attacks statistics. *Hackmageddon,* 2020. augusztus 13. Online: https://www.hackmageddon.com/2020/08/13/june-2020-cyber-attacks-statistics

Statt, Nick: Google sued by New Mexico attorney general for collecting student data through Chromebooks. *The Verge,* 2020. február 20. Online: https://www.theverge.com/2020/2/20/21145698/google-student-privacy-lawsuit-education-schools-chromebooks-new-mexico-balderas

Tsarfati, Omer: Beware of the GIF: Account takeover vulnerability in Microsoft Teams. *Cyberark,* 2020. április 27. Online: https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams

Wagenseil, Paul: Zoom security issues: Here's everything that's gone wrong (so far). *Tom's Guide,* 2020. Online: https://www.tomsguide.com/news/zoom-security-privacy-woes