Több mint 2500 kibertámadás hetente: az oktatás a második legintenzívebben támadott szektor a világon

A kiberbűnöző ott támad, ahol a leggyengébb a védelem, ugyanakkor értékes adatokat lehet megszerezni – ezért került legújabban az oktatás a támadások célkeresztjébe. A Microsoft legfrissebb Cyber Signals jelentése szerint világszerte átlagosan, hetente több mint 2500 alkalommal kísérlik meg csalók feltörni az egyetemek védelmi rendszereit, vírusokkal, adathalász támadásokkal, illetve a hálózatokhoz kapcsolódó mobil eszközök sérülékenységeit kihasználva. 2024 második negyedévében az oktatás lett a második leggyakrabban támadott szektor a világon. A támadók egyre gyakrabban élnek a mesterséges intelligencia kínálta lehetőségekkel, amire az oktatási intézmények nincsenek kellően felkészülve – a hazai egyetemek sem.

Az oktatás a „szektorok szektora”, ahol gyakorlatilag az összes iparág jelen van valamilyen formában: üzleti, egészségügyi, pénzügyi és más szenzitív információk cserélnek gazdát az egyetemeken, iskolákban; fizetési rendszereket, kiterjedt hálózatokat és egyéb digitális infrastruktúrákat üzemeltetnek, anélkül, hogy az intézmények a más iparágakra jellemző erős kibervédelmi eszköztárral, ezek beszerzéséhez és működtetéséhez szükséges anyagi forrásokkal rendelkeznének. A Microsoft legfrissebb Cyber Signals jelentése azt állapítja meg, hogy a kiberbűnözők felfigyeltek az oktatási intézmények sérülékenységére és arra, hogy az ott tárolt, továbbított, kezelt adatok milyen értéket képviselnek. A jelentés szerint világszerte hetente, átlagosan 2507 alkalommal támadták kiberbűnözők az egyetemeket és a velük kapcsolatban álló egyéneket 2024 második negyedévében. Az incidensek során alkalmaztak vírusokat, adathalász módszereket, és igyekeztek kihasználni az egyetemi hálózatokhoz kapcsolódó eszközök sebezhetőségeit is. Érdekesség, hogy a Microsoft Defender for Office 365 az említett időszakban naponta több mint 15 000 olyan emailt fülelt le, amelyek vírussal megfertőzött QR kódot alkalmaztak a támadások végrehajtásához. A jelentés szerint, mindezek eredményeként, az oktatás vált a második leggyakrabban támadott szektorrá a világon. Az oktatási szektor Magyarországon is egyre intenzívebb kibertámadásoknak van kitéve, amelyek kifinomultságával a védekezés csak nehezen tudja tartani a lépést.

A Microsoft világszerte emberek milliárdjait szolgálja ki termékeivel, így hatalmas mennyiségű adat birtokában kivételesen pontos rálátással rendelkezik a kiberbiztonsági folyamatokról a legkülönbözőbb szektorokban. Az elmúlt évben 65 ezerről 78 ezer milliárdra emelkedett azoknak az jelzéseknek a száma, amelyeket a Microsoft rendszerei az informatikai felhőben, a hálózathoz kapcsolódó eszközökön, különféle szoftvermegoldásokban és partner ökoszisztémákon belül naponta megvizsgálnak. Ezek segítenek jobban megérteni a támadások és fenyegetések természetét és felkészíteni a rendszereket azok kivédésére.

Merényi Ádám, a Microsoft Magyarország oktatási üzletágának vezetője arra hívta fel a figyelmet, hogy szervezeti autonómiából adódó széttagoltság sérülékenyebbé teszi az egyetemi informatikai rendszereket, ezért az egységesítés a IT terén fontos feltétele a biztonság fokozásának. A szakember hangsúlyozta: a modern támadások elhárításához manapság elengedhetetlen egy viselkedésalapú védelmi rendszer, amely egyaránt védi az identitásokat, számítógépeket és szervereket, a teljes levelezőrendszert, valamint az egyetemi rendszerekben tárolt adatokat. Ezt egészíti ki a magas fokú automatizáció, amely a támadások felderítését és elhárítását segíti. Az intézményeknek Zero Trust, azaz a „Zéró bizalom elvét” érdemes követniük, amely folyamatos ellenőrzést, hitelesítést, illetve engedélyezést követel meg minden egyes hozzáférési kísérlet előtt.

Kisiskolások, hallgatók és iskolai alkalmazottak: egy heterogén, gyanútlan és felkészületlen felhasználói kör

A Cyber Signals szerint az amerikai egyetemek az átlagosnál is jobban ki voltak téve a támadásoknak, amelyben szerepet játszhatott az is, hogy az amerikai diákok gyakrabban használják iskolai célokra a saját mobileszközeiket, mint európai társaik. Ennek azért van jelentősége, mert a saját eszközök nem részei az intézmény által felügyelt rendszernek és nem futnak rajtuk azok a szoftverek, amelyek a megfelelő szintű védelemről gondoskodnának.

Függetlenül azonban a használt eszközök tulajdonosaitól és felügyeletüktől, általában is jellemző az oktatásban a kibervédelem elégtelensége, a felhasználók nagyfokú nyitottsága és bizalma egymás és a külvilág iránt, az éberség hiánya és az időhiányból fakadó elhamarkodottság.

Egy általános iskolában ráadásul kisiskolások, az egyetemeken pedig többek között sportolók, ügyintézők, egészségügyi dolgozók, gondnokok, egyéb szakemberek, és persze a világ minden tájáról érkező hallgatók alkotnak egy rendkívül heterogén felhasználói kört, eltérő szokásokkal, beidegződésekkel. A kisiskolásoktól például viszonylag egyszerűen lehet kicsalni társadalombiztosítási számokat, amelyekkel annál is könnyebb visszaélni, hogy a valódi tulajdonosaik ritkán használják őket. Az intézmények szerteágazó tevékenységeket végeznek: bejelentéseket, hirdetéseket tesznek közzé, e-maileznek, különböző személyes adatokat kezelnek, ugyanakkor ritkán van elég forrásuk ahhoz, hogy jólképzett, a kiberbiztonságban jártas szakembereket alkalmazzanak, vagy jól védett infrastruktúrát építsenek ki.

A hibrid- vagy távtanulás révén az oktatás ráadásul az otthonokba és az irodákba is eljut, ezzel is növelve az IT által nem kontrolált, de esetlegesen a központi rendszerekhez kapcsolódó eszközök számát – úgy, hogy a tanulók ritkán vannak tudatában a kiberbiztonsági kockázatoknak.

Veszélyes QR kódok

Az Egyesült Államok Szövetségi Kereskedelmi Bizottsága (the US Federal Trade Commission), a közelmúltban tett közzé felhívást arról, hogy bűnözők fertőzött QR kódokat használnak felhasználói adatok megszerzésére, vagy vírusok rejtett telepítésére. Ezeket nyilvánosan elérhető és hivatalos szoftverek segítségével állítják elő, majd vagy elektronikus úton továbbítják potenciális áldozataiknak, vagy egyszerűen hirdető felületekre, plakátokra helyezik el őket. A hagyományos kódszkennerek nem detektálják a kódba elbújtatott vírust, ezért is volna fontos, hogy a diákok – és a munkavállalók is – olyan eszközt, illetve olyan böngészőt használjanak, amely el van látva a védekezéshez szükséges legkorszerűbb vírusírtó programokkal.

Ezeket érdemes első lépésben megtenni a hatékonyabb védekezés érdekében

Az intézmények sajátos helyzete, forráshiánya, a kihívások komplexitása miatt a kiberbiztonság kérdését nem lehet kizárólag technikai oldalról megközelíteni az oktatásban. A hatékonyabb védekezés felé vezető első lépés az alapvető kiberhigiénia megerősítése – például a többfaktoros azonosítás és a Zéró bizalom bevezetése. Ezzel párhuzamosan fontos az érintettekben tudatosítani a biztonsági kockázatokat és megismertetni velük a védekezés bevált módszereit. A következő lépésben a rendszer központi irányításáról érdemes gondoskodni, amely segíthet a rendszeren belül előforduló incidensek naplózásában, és nyomon követesében – áll a jelentésben.

> „Az oktatási rendszerünkben – kevés kivételtől eltekintve – a szakemberek és az IT infrastruktúra még nincs felkészülve a mesterséges intelligenciát is alkalmazó támadások elhárítására. Kétségtelen azonban, hogy a fejlettebb eszközpark sem elégséges önmagában az incidensek megakadályozására: szemléletváltásra és edukációra is szükség van. Az egyetemi hallgatóknak és az intézmények alkalmazottainak tisztában kell lenniük azokkal a módszerekkel, amelyekkel a bűnözők az éberségüket igyekeznek kijátszani. Ennek érdekében a Microsoft rendszeresen tart workshopokat és konzultációkat a hazai egyetemek vezetőinek.” – mondta el Merényi Ádám.

Hozzátette, hogy a Microsoft Learn platformon ingyenesen elérhetők kiberbiztonsági tréningek kezdőtől a haladó szintig, de a biztonsági megoldások megtervezéséhez is hasznos útmutatókat lehet találni ezen a felületen.

Sajtókapcsolat:

- Karolina Krizenecka, PR vezető
- kkrizenecka@microsoft.com

Eredeti tartalom: Microsoft

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/16548/tobb-mint-2500-kibertamadas-hetente-az-oktatas-a-masodik-legintenzivebben-tamadott-szektor-a-vilagon/