Egy átlagos felhasználó nagy feladatot kap, ha fel kell ismernie, mi valós és mi nem

⋮ 2024. 12. 03.

Fotó: Sebestyén László

Interjú

Interjú Csizmazia-Darab Istvánnal, a Sicontact Kft. IT-biztonsági szakértőjével, a lassan nagykorúvá érő Antivírus blog szerkesztőjével, aki szerint az MI-nek nem csak a sötét oldalát érdemes nézni.

A szokásos zsarolóvírus-támadások már nem menők, helyettük az ellopott adatok nyilvánosságra hozatalával lehet fenyegetőzni. A covid időszakot kiheverte a kiberbiztonsági szakma, a cégek tanultak a hibákból, de azért még most is vannak, akik a családi gépen tárolnak céges adatokat. Emberi hiba mindig lesz, a kritikus infrastruktúrák pedig már rég megacégek kezében vannak – itt már csak a szabályozás segíthet.

Forbes.hu: Utoljára négy éve beszélgettünk**, de ez idő alatt nagyon sok dolog történt. A covid magunk mögött van, megjelentek a nagy nyelvi modellek, a vírusokról pedig kevesebbet hallunk, a scamek és a kiberbiztonság inkább tematizálják a médiát. Mi az, ami téged a legjobban meglepett a trendeket illetően?**

Csizmazia-Darab István: Inkább azzal kezdem, amit gondoltam: abban hittem, hogy a ransomware, a zsarolóvírus, mint műfaj, kitart, és ez így is lett. Főleg, hogy a home office időszaknak hosszú kifutása volt. Ami viszont meglepett, hogy még tavaly és idén is olyan elképesztő felhasználói hibákból és emberi mulasztásokból eredő incidensek keletkeztek, amikre az ember azt gondolta, hogy na, ezeket már biztos senki sem követi el, már rég megtanulták a leckét.

Mondasz példát?

Mindjárt kettőt is. A legközelebb időben a júliusi Crowdstrike leállás esik, ami miatt nyolc és félmillió windowos gép kékhalállal világszerte megadta magát. Repterek, bankok, tévéadók, egészségügyi szektor, minden érintett volt.

Kiderült, hogy az egész világ Windowson fut. Most már tudjuk, hogy melyik cégek építkeznek a Microsoft infrastruktúrájára.

Igen, és az egész fennforgást egy hibás frissítés okozta. Az előzetes tesztelés egyértelműen a gyártó sara, és hogy ez elmaradjon, illetve a felhasználóknál ilyen mértékű leállás történjen, ez elképesztő volt.

Csizmazia-Darab István, vagy ahogy sokan ismerik: Rambo, a Sicontact Kft. IT-biztonsági szakértője. Fotó

És a másik példa?

Az is emberi mulasztás miatt történt: a 2022-ben az Egyesült Államok legnagyobb finomított olajhálózatát üzemeltető Colonial Pipeline számítógépes rendszerét támadta meg a Darkside nevű ransomware banda, aminek eredménye egy hetekig tartó leállás lett. Ki is fizettek egy irgalmatlan méretű váltságdíjat: 4,4 millió dollárt. Az csak apró érdekesség, hogy bár a bűnözőktől végül kaptak olyan visszafejtő eszközt, amivel a titkosított adataikhoz hozzáférhettek volna, ez olyan lassú volt, hogy mégis inkább a saját mentéseik alapján állították helyre a rendszert.

Ami miatt viszont említem ezt az egészet, hogy ugye covid időszak volt, a mérnökök távmunkában dolgoztak és irányították a rendszer vezérlését, innét szivárogtak ki a jelszavaik. Kiderült, hogy nem használtak se VPN-t, se kétfaktoros azonosítást.

Elég különböző esetek ezek. Az elsőnél egy szolgáltatás mondott csődöt, a második viszont kimondottan személyi mulasztás eredménye.

Igen, de közben szabályozási hiányosság eredménye is.

Ha már szabályozás: a Crowdstrike-balhé után újra nagy figyelem hárult a big tech cégekre, pontosabban arra a felelősségre, amit magukra vállalnak azáltal, hogy kritikus infrastruktúrákat üzemeltetnek. Egy reptéren nem igazán lehet hibázni, mert az életveszélyes. Jó ez nekünk? Nem kéne ezt jobban szabályozni?

Azért azt jegyezzük meg, hogy ezek nagyon ritka incidensek. Előfordul hébe-hóba egy-egy hibát tartalmazó frissítés, de hogy ekkora gond legyen belőle, az elenyésző, így itt még nem

mennék ilyen messzire.

A ransomeware-támadásoknál viszont azt látjuk, hogy egyre gyakoribbak, és a műveleteik is változnak. 2019-ben a Maze ransomware-banda megtámadta a pensacólai közigazgatást, és az addig szokásos ügymenettel ellentétben úgy követeltek váltságdíjat, hogy nem csak a letitkosított adatokért kértek pénzt, de ha esetleg ezekről van mentése az államnak, akkor azért fizessenek, hogy az adatokat ne hozzák nyilvánosságra a bűnözők.

> Azóta ez a fajta doxing ransomware támadás bevett gyakorlat lett, és iszonyú összegeket lehet vele kikényszeríteni a cégektől.

Vagy azért, mert nincs mentésük, vagy mert a személyes adatok nem biztonságos kezeléséért már szabad szemmel látható nemzetközi büntetések is kiszabhatók. A bűnözők megnézik, hogy a megtámadott cégnek mekkora a bevétele, majd az esetleges bírság összege alá lövik be a váltságdíjat – így talán a vállalkozásoknak is megéri fizetni.

Fotó: Sebestyén László

És ez most az új divat?

Igen, és már olyanok is csinálhatják, akiknek semmi közük az informatikához. Ransomware-as-a-service modellben szolgáltatják a bűnözők. Ha kell, 24/7-es supportot adnak, vagy részt vesznek a váltságdíj alkutárgyalásokban is. Ha az ügyfél nem akar fizetni, terheléses támadásokat küldenek rájuk, hogy serkentsék a fizetési kedvet.

És min segíthet a szabályozás?

Európában a NIS2 mindenkit arra sarkall, hogy igenis foglalkozzon a saját biztonságával. Vagy áttekinthető védelmet építek, vagy ennek az árát kifizetem bírságként – szóval érdemes ezt jól csinálni és biztonságra, megelőzésre, védelemre fordítani a pénzt.

Mit tanulhatunk a fenti két esetből? Azon túl, hogy teszteljük a frissítéseket. Mert emberi hiba mindig lesz.

Hadd hozzak fel még két esetet! Igaz, az egyik régebbi, még 2017-ben volt az egyik legnagyobb amerikai hitelminősítő Equifaxnál egy támadás, aminek eredményeként 143 millió személyes adat szivárgott ki. Az utólagos vizsgálatok megállapították, hogy ugyan az incidenst júliusban fedezték fel, de a támadók május óta már a rendszerükben voltak. Egy olyan sebezhetőséget használtak ki, amire március óta már volt elérhető hibajavítás. A

nyomozás megállapította, hogy szabályozási hiányosságok álltak a háttérben. A cégnél nem volt kinevezett felelős, sem frissítési policy – mindez egy pénzügyi óriásnál.

Aztán volt a 2020-as SolarWinds incidens. Egy hálózatfelügyeleti rendszereket üzemeltető céghez törtek be támadók, hogy a SolarWinds ügyfeleinek rendszereibe továbbjutva is telepíthessenek hátsó ajtókat. A nyomozás szerint kiszivárgott a cég egyik fontos jelszava, ami pedig a solarwinds123 volt.

Legalább egy felkiáltójelet tehettek volna a végére.

Na de ha tanulságot akar az ember, akkor íme. Az államigazgatás, az egészségügyi szektor, ezek sokszor nehéz helyzetben vannak, mert nem piaci alapon működnek, így a technikai személyzet és az infrastruktúra pénz hiányában hagyhat maga után kívánnivalót. De ezeknél a cégeknél, ahol látszólag ott a pénz-paripa-fegyver, nos, ez azt mutatja, hogy a biztonságtudatos hozzáállás, az ilyen tréningek nincsenek rendben. Eleve nem úgy kéne kinézzenek, hogy egyazon oktatásra ül be mindenki, a portástól a HR-esig, és hallgatja az előadást évente, vagy akár életében egyszer, hanem rendszeresen tesztelni kéne őket, és munkakörre szabni a képzéseket.

Az utóbbi hetekre is jutott egy érdekes sztori: a VBÜ sztorinak mi a tanulsága?

Keveset tudni erről, mi is csak a sajtóból értesültünk róla. Magyarországi cégek is áldozatul eshetnek, és a védekezés-megelőzés mindenkinek feladja a leckét. Ahogy olvastam, ott is feltettek az ellopott adatok közül képernyőképeket és az adatok publikussá tételével fenyegetőztek, hogy nyomást gyakoroljanak.

Említetted a beszélgetés elején a home office-t, amivel annak idején elég szkeptikus voltál. Most elkezdték visszahívni az embereket a cégek az irodákba. Tényleg több lett az otthoni munkavégzés miatt a támadás, vagy csak többet beszélünk ezekről?

Fotó: Sebestyén László

Az biztos, hogy többet beszélünk róluk. A helyzet akkor nagyon más volt, mint most, mert a covid váratlanul jött, olyasmi volt, amire nem tudtunk felkészülni. Hardverhiány volt, sok cégnél nem is tudtak dedikált gépeket adni a dolgozóknak, és volt, akinek otthon egy számítógépe volt, apa-anya ezen dolgozott, a gyerekek ezen írták a házifeladatot. A mostani hibrid munkavégzésre viszont fel lehetett készülni. Azt látjuk, hogy ebben a cégek is kiegyeztek.

És tanultunk a covidból? Megértették a cégek, hogy kell a dedikált eszköz, a felhasználók meg hogy a munkagép nem szórakozásra való?

Látunk ebben fejlődést. Sosem lesz olyan, hogy nulla incidens lesz, de a cégek egyre tudatosabbak.

Jó, hogy ezt mondod, mert egyébként kicsit de ja vu érzésem van. Négy éve is egy kávézóban ültünk, és akkor is úgy nézett ki a beszélgetés, hogy te elmondtad, hogy micsoda nehézségek és támadások vannak az online világban, én hümmögtem, és azzal zártuk, hogy hát, ez van. De miért nem történik változás? Amit fent mondtál a képzésekről, az sem lenne ördöngösség.

Azért látszik javulás. Vannak pozitív fejlemények, tanulunk mások hibájából, de a biztonság nem egy statikus állapot, hanem egy folyamat, amibe állandóan és sok erőfeszítést kell tenni.

> Még ahhoz is erőfeszítés kell, hogy az ember szinten tartsa magát, nem hogy fejlődjön.

Közben pedig a támadói eszköztár is bővül, érdemes szóba hozni a gépi tanulást és a mesterséges intelligenciát is. A bűnözői csoportok is profik, szinte cégként működnek, vannak fejlesztőik, rendszergazdáik, bedolgozóik, mindenki kiszolgálja a saját területét.

Ha már gépi tanulás és MI, már évek óta velünk van a ChatGPT, amit egy csomó dologra lehet használni, jóra és rosszra egyaránt. Négy éve, mikor az első interjúnk készült, ahhoz voltam szokva, hogy ha át is jön egy spam a szűrőn, azért látom, hogy a nigériai herceg, aki írt nekem, mert hogy nyertem a lottón, és egyébként is az unokaöccse vagyok, na szóval, hogy ez a levél nem lesz túl jól megírva, és az e-mailcím is bizarr lesz. De mostanság sok olyan spam kering, amiben az e-mailcímet maszkolják, a levél hihető. Ezekkel mi a helyzet?

Már nem is annyira a nigériai hercegek mennek, bár a randizós csalásoknál még elő-előkerül a jól kereső özvegy olajmunkás.

Vagy a gyémántmilliárdos fia, az ment nagyot legutóbb.

Igen. Ezeken sokat lendített az MI, főleg, hogy hangot is lehet klónozni vele. Volt egy eset, mikor felhívtak egy olajcéget, és a vezető hangján utaltattak el egy nagyobb összeget, mire kiderült, hogy bár még a tájszólás is stimmelt, nem a főnök telefonált.

A ChatGPT esetében a fordítások is sokat fejlődtek, már a spamek között is egyre több a hihető. És hogy mennyire jó szövegeket tudnak generálni ezek a modellek, arra jó példa a következő sztori. 2023-ban egy egyetemi kutatócsoport végzett egy kísérletet. Legeneráltak ChatGPT-vel ötven különböző publikációt öt elismert orvosi folyóirat stílusában, majd felbéreltek négy akadémikust, és pénzfeldobással kiosztották közöttük a hamis tanulmányokat, hogy bírálják el őket. Ezek egy harmadát valódinak minősítették, a valódi anyagok kontrollcsoportjából pedig 14 százalékot hittek hamisnak. És ehhez vegyük hozzá, hogy ők a terület szakértői voltak! Egy átlagos felhasználó nagy feladatot kap, ha fel kell ismernie, mi valós és mi nem az.

Az a sokkoló ebben, hogy ehhez nem volt elég a stílus, hanem a tartalomnak is meg kellett felelnie az elvárásoknak.

Igen, de azért örülünk a ChatGPT-nek, mert számos pozitív vonatkozása is van. És most eljutottunk oda, hogy sok konkrét előnyt és hátrányt egyszerre látunk. Itt vannak például azok a lehetőségek, amikor programot lehet írni mesterséges intelligencia segítségével.

Régen az volt a gyakorlat, hogy az ember kódolt 100 órát, majd debuggolt 20-at. Most lehet, hogy az AI kódol neked 2 percet, de debuggolhatsz, tesztelhetsz utána 100-at.

> Hibák, biztonsági rések, optimalizálási hibák azért vannak a pakliban, de lehetnek feladatok, amikor ezek ellenére is érdemes támaszkodni az MI-re.

Ezekkel az új eszközökkel kapcsolatban a legfontosabb, hogy alaposan megismerjük és tudjuk kezelni őket. Elutasítani és nem kiismerni viszont szerintem a legnagyobb hiba.

A home office-re visszatérve pedig előfordulnak szélsőségek. Az Amazonnál most nagy port kavart, hogy heti öt nap be kell járni. De vannak cégek, ahol látják, hogy a home office-nak van sok előnye, a munkavállalóknak pedig ez egy olyan szolgáltatás, amit nagyra tudnak értékelni, és az otthoni időtöltés nem megy az elvégzett munka minősége és mennyisége rovására.