„RENDSZERÜNK TÖKÉLETESEN BIZTONSÁGOS", MONDJA AZ IT. „DE OTT VANNAK A FELHASZNÁLÓK…"

Nemcsak külső kockázatok vannak

FORRÁS: CRYPTONEWSPOINT.COM

Az alkalmazottak komoly biztonsági kockázatot jelentenek a vállalat IT-biztonsága szempontjából. Mégis, a belső kockázattal kevés vállalat foglalkozik, gyakran nem is tudják, mit kezdjenek vele. Hiszen a kollégák a hálózaton belül vannak, gyakran emelt szintű hozzáféréssel rendelkeznek a vállalat kritikus adataihoz, rendszereihez és alkalmazásaihoz – valakinek dolgoznia is kell, nemde? A vállalat megbízható részét alkotják, emiatt a tőlük eredő rossz szándékú vagy véletlen támadást nehezebb észlelni, megfékezni.

Július közepén a Twittert furcsa üzenetek sorozata árasztotta el: olyan híres személyiségek, mint *Bill Gates* vagy *Elon Musk,* dupla pénzt ígértek minden bitcoinos befizetésre. A támadók akkora káoszt okoztak, hogy a mikroblog-szolgáltatást egy ideig fel kellett függeszteni. Később kiderült, a háttérben egy sikeres social engineering támadás állt: két tinédzser adathalász-emailek segítségével megszerezték az otthonról dolgozó, tehát kevésbé biztonságos környezetben lévő Twitter-alkalmazottak felhasználónevét, jelszavát.

Oktatással és biztonságtudatossággal lehet védekezni

Míg a rossz szándék érvényesülését megelőzni szinte lehetetlen, a véletlen károkozást a kiberbiztonsági tudatosság növelésével hatékonyan kezelhetjük. Jártam olyan vállalatnál, ahol végig kísérő volt mellettem, az ajtókat PIN-kód nyitotta, és arra is megkértek, hogy a telefonomat teljesen kapcsoljam ki. Máshol a belső rendszerekhez való jelszót simán leolvastam a képernyőre helyezett cetliről, miközben egyedül várakoztam...
A kibertudatossággal átitatott átlagos vállalatnak valahol a kettő között kell lennie. A biztonságot eleve építsük be minden üzleti folyamatba és részlegbe, vezetőinket kérjük

meg, mutassanak példát ezen a téren is. Ugyanakkor legyen a vállalati diskurzus része, így a kollégák a vállalati kultúra szerves részeként ismerkednek meg ezzel a kérdéskörrel.
Fontos meggyőződni, hogy az alkalmazottak nemcsak kipipálandó feladatként tekintenek a kiberbiztonság kérdésére. Nagyon gyakran a vállalatok próbálják ráerőltetni a biztonsági módszereket és szabályzatokat, miközben semmi magyarázatot nem adnak, hogy miért léteznek ezek a mindennapi munkát megnehezítő intézkedések. Fontos elmondani, miért kell rendszeres kiberbiztonsági tréningen részt venni, miért tiltjuk le esetleg a vállalatnál a külső adathordozók használatát és használunk helyette felhős tárhelyeket.

Nem kell gyakran változtatni a jelszót

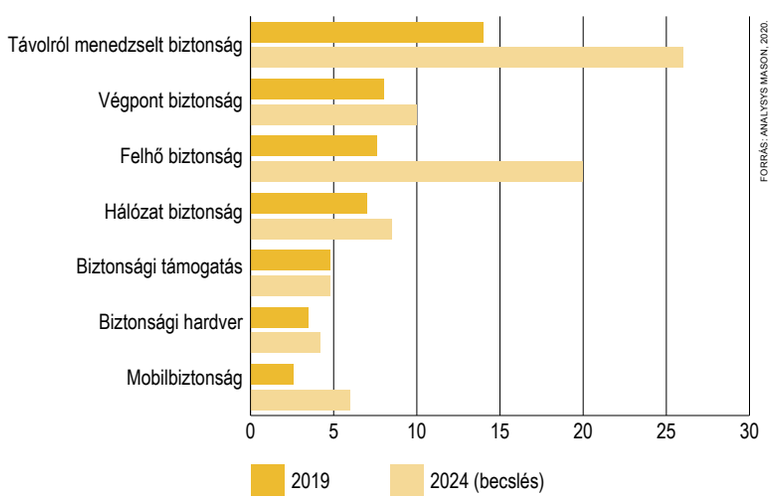
Merjünk újítani, és vállaljuk fel a kiberbiztonság új trendjeit. Például a vállalati körökben még mindig divatos gyakori jelszócserét a szakemberek már nem tartják biztonságosnak. A gyakori jelszócsere macska-egér játék kialakulásához vezetett a rendszergazdák és a dolgozók között: utóbbiak egy idő után nem vették komolyan a jelszóváltoztatást, és könnyen kitalálható azonosítót használtak. Válaszként a feladatukat komolyan vevő rendszergazdák feketelistára tették a gyakori jelszavakat, mire a dolgozók három hónapos váltásban használták ugyanazokat a jelszavakat – és így tovább.
A megoldás a hosszú (20+ karakteres), de értelmes jelszó: egy jelmondat (közmondás, versidézet). És csak akkor változtassuk meg, ha felmerül a gyanú, hogy illetéktelenek birtokába került.

Segítsünk felismerni a fenyegetettségeket

A hatékony biztonságtudatosság-növelő programnak nem bonyolultak. Például, ha az onboarding része a kiberbiztonsági oktatás is, akkor már kezdettől közelebb vagyunk a biztonságtudatos felhasználókhoz. A kreatívan összeállított, rendszeres kiberbiztonsági tréningek nemcsak alapvető tudással látják el az embereket, hanem megértetik velük, miért van szükség a szabályok betartására, így motiváltabban tartják be azokat. Adjunk támpontokat a kollégáknak a kiberbiztonsági veszélyek felismerésére és elkerülésére. Például, biztos elég egyszer elmagyarázni, miről lehet egy adathalász-emailt első nézésre felismerni: furcsán néz ki, sok benne a helyesírási hiba, nem megszokott a megszólítás. Azt is mutassuk meg, hogyan tudja megnézni a kolléga, hogy az adott email valóban attól az embertől érkezett, akinek beállították. Ne legyen zavaró a visszakérdezés gyanús küldemény vagy csatolmány esetén.
Minden szokatlanság és kényszerítés keltsen gyanút. Például, ha emailben vagy telefonon érzékeny vagy szokatlan adatokat kérnek tőlünk. Az üzenet burkolt fenyegetést vagy sürgetést is tartalmazhat, vagy szeretne rávenni minket, hogy a levélben megadott linkre kattintsunk, netán nyissuk meg a csatolmányt. Mindenképp ellenőrizzük azokat a leveleket, melyben fizetésre szólítanak fel, vagy egy megváltozott bankszámlaszámot adnak meg.
A túlzott közösségi médiás aktivitás is problémát jelenthet, hiszen a támadásokat ezeken a felületeken készítik elő a bűnözők, itt gyűjtenek adatokat. Az alkalmazott taktikák folyamatosan változnak, legutóbb fejvadász cégnek kiadva magukat hálóztak be célpontokat kínai hekkerek.

Kkv-k kiberbiztonsági költései 2019-2024 között

Milliárd dollár



A vállalatok kétharmada érintett

A Bitglass 2020 júliusi adatai szerint a vállalatok kétharmada tapasztalt olyan IT biztonsági incidenst az elmúlt egy évben, melynek kiindulópontja egy belső munkatárs volt. A kutatás szerint a megkérdezettek cégek többsége nem biztos abban, hogy az alkalmazott személyes eszközeiről vagy a felhőből érkező fenyegetettségeket tudná egyáltalán detektálni. Öt vállalatból négy azzal is küzd, hogy egyáltalán felmérje, a biztonsági incidensek mekkora kárt okoztak. A vállalatoknak átlagosan egy hétbe tellett, míg felfedezték a problémát és még egy hét ment el azzal, hogy az incidens hatásait visszafordítsák.

Sajnos, néha költeni is kell

Az üzletmenet-folytonosság mantrája: „a biztonsági költés legyen arányos az adott esemény bekövetkezésétől elszenvedett kárral”. De ehhez azt a kárt egyszer ki is kell számolni! Mibe kerül, ha a konkurencia megszerzi az ügyféllistánkat?! A kétfaktoros azonosítás nem gyilkosan drága, de igen nagy mértékben csökkenti a sikeres támadások lehetőségét. Szánjunk időt a különböző jogosultsági szintek tényleges beállítására, és minden alkalmazott csak azokhoz a rendszerekhez, erőforrásokhoz férjen hozzá, amelyek nélkülözhetetlenek munkájukhoz. Az ezen túlmenő (szokatlan) jogosultság-igénylést pedig felül kell vizsgálni.

Vass Enikő