Mit hoz 2019? Trendek a vállalati biztonságban

computerworld.hu/biztonsag/mit-hoz-2019-trendek-a-vallalati-biztonsagban-258282.html

Csizmazia-Darab István

| 2019 január 16. 12:15

Hetente érkeznek hírek újabb és újabb gigantikus méretű adatlopásokról, kiszivárgásokról. Az okokat kutatva azt láthatjuk, hogy az incidensek jelentős része emberi hiba, szándékos károkozás vagy felelőtlen mulasztás miatt történik.

Sajnos tavaly is okoztak komoly adatvesztéseket súlyosan felelőtlen és figyelmetlen munkavállalók, például úgy, hogy céges jelszavakat sima szövegként tároltak, fontos hibajavításokat hagytak figyelmen kívül, vagy hogy bizalmas vállalati anyagok titkosítását mulasztották el.

Az elmúlt 30 év során hatalmasra nőtt a szakemberek és az átlagfelhasználók tudásszintje közötti különbség, így a dolgozók rendszeres oktatására sokkal nagyobb hangsúlyt kellene fektetni. Egy 2016-os kutatás rámutatott, hogy a megkérdezett cégek közel felénél egyáltalán nem tartottak biztonságtudatossági képzést, és bár a háttérben ott dolgoztak a rendszergazdák, semmilyen kommunikáció nem folyt azokkal a kollégákkal, akik napi szinten használják a céges felületeket. Ahol pedig tartottak efféle képzést, ott mindössze évi egyszeri alkalommal 30 percet fordítottak biztonságtudatosításra. A válaszadók több mint negyede pedig soha egyetlen munkahelyén sem részesült biztonságtudatosságról szóló képzésben.

Pro és kontra

A zsarolóvírusok támadása és az erre reagáló média figyelme pozitív folyamatot is elindított: vállalati környezetben, ahol eddig nem mindenütt alkalmaztak rendszeres és kipróbált biztonsági mentéseket, végre kellő figyelmet kapott ezek fontossága. A felelősök belátták, hogy tudatos tervezés, adatvagyon-felmérés és folyamatos kibervédelem nélkül nincs biztonságos és folyamatos üzletmenet - ezt a szemléletváltást nagyban segítette az időközben hatályba lépett GDPR is.

A megfelelően beállított vírusvédelem és a rendszerek hibajavításainak naprakészen tartása mellett egy kis- vagy középvállalkozás életében számos adatvédelmi problémára jelenthet megoldást a megfelelő titkosítás alkalmazása - például az ESET Endpoint Encryption. A felhasználóbarát, skálázható és egyszerűen menedzselhető titkosítás biztosítja a végponti titkosítókulcsok, valamint merevlemezekre, hordozható eszközökre és e-mailekre érvényesíthető házirendek központi kezelését. Amellett, hogy ezzel megelőzhető a jogosulatlan hozzáférés az érzékeny információkhoz, a felhasználói adatok lehetséges kiszivárgásából fakadó kockázatok is minimálisra csökkenthetők. Ha ezeket a megoldásokat kiegészítjük például a banki felületre történő belépésnél már régóta használt kétfaktoros azonosítással (például ESET Secure Authentication), akkor még magasabb

szintű védelem érhető el vállalati környezetben is.

Már 2015-ben is azt láthattuk, hogy napi 12 támadás ért egy átlagos vállalatot; ez a szám azóta valószínűleg sokkal magasabb lett. A "nem történt támadás" vagy a "nem vettem észre" között óriási a különbség, ráadásul a komoly cégek - amelyeknél látszólag minden erőforrás adott ahhoz, hogy a védelmükre költsenek - is szenvednek el érzékeny veszteségeket, adatlopásokat, kibertámadásokat. Sok esetben tapasztalhatjuk, hogy először szándékosan a kisebb, gyengébben védett alvállalkozói, beszállítói kört támadják, ahol a szűkösebb büdzsé csak korlátozott kibervédelmet tesz lehetővé, majd ezeken a gyengébben védett partnereken keresztül támadják a kiemelt jelentőségű célpontokat. A képet pedig tovább árnyalja az úgynevezett Shadow IT (árnyékinformatika), az olyan rejtett eszközök, erőforrások (például privát Dropbox-fiók stb.) használata a céges munkában, amiről sem a cégvezetés, sem az informatikai részleg nem tud.

A java hátravan

És hogy mire számíthatunk 2019-ben? Az ESET éves előrejelzése szerint idén a kiberbűnözők egyre inkább kihasználjak majd az automatizálásban és a gépi tanulásban rejlő lehetőségeket, hogy még több adatot gyűjtsenek a személyre szabottabb és

kifinomultabb támadások megtervezéséhez. Olyan webes eszközöket alkalmazhatnak, amelyek követik az áldozatokat a webhelyek közötti böngészés alatt, vagy adatokat vásárolhatnak az adatbrókerektől a profilok megalkotásához.

A kriptovaluták terjedése, valamint a hálózatba kötött eszközök számának növekedése azt jelentheti, hogy az intelligens otthoni eszközök és asszisztensek ugyancsak a támadók célpontjaivá válhatnak egy esetleges bányászfarm kiépítése során. Korábban már láthattuk, hogy a kiberbűnözők hogyan képesek kihasználni az IoT-eszközöket a komolyabb DDoS-támadásokhoz. Mivel egyre több ilyen eszköz csatlakozik a hálózatra, és válik az emberek mindennapi életének részévé, a támadók várhatóan 2019-ben is kiemelten keresik majd a sebezhetőségeket, hogy kihasználják azokat újfajta csalásokhoz, adatlopáshoz, zsarolóvírus-támadásokhoz vagy kriptovaluta-bányászathoz.