A kisebbet is bántani szokták

AZ INFORMATIKAI TÁMADÁSOK MEGELŐZHETŐK

Egy cyber-támadás többet jelent, mint pár dokumentum elvesztése, egy komolyabb adatvesztés nagy rombolást okoz egy vállalkozásnak, legyen az nagy vagy kisebb cég. Fel lehet azonban készülni az ostromra, megfelelő védelem kiépítésével elkerülhető a baj és az abból adódó anyagi veszteség.

NEM VESZIK KOMOLYAN

A kisebb és közepes méretű vállalatok egy része még mindig nem fordít elég figyelmet a cyber- (ejtsd:szájber) biztonságra. Egy tanulmány szerint – amely 1000 kisvállalkozás körében készített felmérést az Egyesült Királyságban – a megkérdezettek fele állította: nem hinné, hogy cyber-támadás érheti őket. Mégis, a felmérésben részt vevő vállalatok java élt már át ilyet. Míg számos vállalat azt vallja, hogy azért nem védekeznek, mert túl kicsinek hiszik magukat a támadáshoz, a legtöbbjük egyszerűen nem akar pénzt és időt fecsérelni valamire, ami szerintük nem történhet meg velük. Mindazonáltal, első körben kivédeni egy támadást jóval kevesebbe kerül, mint helyreállítani a cégünket egy ilyen esemény után.

MIT JELENT A CYBER-TÁMADÁS?

A cyber-támadás egy hackerek általi kísérlet egy számítógépes hálózat

vagy rendszer megsértésére vagy tönkretételére. Rendszerint bizalmas adatok megtekintése, használata vagy ellopása történik illetéktelen személy által. Egy cyber-támadás történhet identitás lopás, vírusok, rosszindulatú programok, csalás és akár zsarolás formájában is.

A leggyakoribb cyber-támadások a ransomware (zsarolóprogram) támadások. Ezek adatokat titkosítanak, amik csak pénz befizetése ellenében válthatók ki. Egy másik verzió a sniffer (nyomkövető program), amit arra fejlesztettek ki, hogy begyűjtse a számítógépünkbe beáramló és onnan kimenő forgalmat. Habár ez lényegében ártalmatlannak tűnik, ez a típus képes a vállalatok kizsákmányolására.

HOGYAN TÖRTÉNIK EGY TÁMADÁS?

A cyber-támadások rendszerint adathalász e-maileken, mobiltámadásokon vagy az adatforgalom eltérítésén keresztül történnek. Van a támadásnak olyan módja is, amit ddos-nek, azaz szolgáltatásmegtagadással járó támadásnak hívnak, amely nagy mennyiségű adatforgalmat generál, a rendszer összeomlasztása céljából. A rendszer összeomlása által lehetetlenné teszi a weboldal vagy a szolgáltatás elérését. De a nagy felhasználói bázissal nem rendelkező kisebb vállalatok esetében rendszerint az adathalász e-maileké a főszerep. Mivel az adathalász e-maileket úgy tervezték, hogy biztonságos e-maileknek nézzenek ki, igen nehéz beazonosítani őket. A legjobb útja a cyber-támadások általi adattitkosítás és adatrongálás megelőzésének az alkalmazottak képzése és tréningje arra vonatkozólag, hogy miként néz ki egy adathalász e-mail.

MIKÉNT LEHET VÉDEKEZNI?

Az alkalmazottak naprakészen tartása és a képzésük az egyik legjobb megelőzés. Ám érdemes néhány plusz óvintézkedést is tenni. Elcsépelt figyelmeztetés, mégis fontos az antivírus telepítése. Bár a cyber-támadások rendszerint vállalatokra irányulnak, a vírusok véletlenszerűen bukkanhatnak fel és gyakoribbak. Egy vírus is képes ellopni az adatokat, megfertőzheti a gépünket, lelassítva a gyártást. A legjobb antivírus szoftverek is gyakran csak a vírusok 99%-ával képesek megbirkózni. Megvédhet minket a kémprogramok ellen is, amelyeket arra terveztek, hogy beleskelődjenek a vállalati tevékenységekbe és rögzítsék az adatainkat.

SZEREZZÜNK EGY TŰZFALAT

Egy tűzfal elsőrendű védelmet nyújt a vírusok ellen a számítógépnek. Míg egy antivirus szoftver rendszerint képes a vírusok detektálására és a tőlük való megszabadulásra, egy tűzfal azt akadályozza meg első körben, hogy a vírus megjelenjen a rendszerben. Egy tűzfal alapvetően egy rostát jelent a számtógép és az internet között. A neten böngészés közben szüntelenül információcsomagokat küldünk előre és vissza. Egy tűzfal megszűri ezeket a csomagokat és védelemként van jelen minden ártalmas csomaggal szemben. Mindazonáltal, ha egy vírus mégis átjutna, a tűzfal nem képes eltávolítani azt.

HASZNÁLJUNK EGY VPN-T

Ha kicsi vagy közepes méretű vállalat vagyunk, megvan az esélye, hogy az alkalmazottak távolról is dolgoznának. A mai technológia erre lehetőséget ad. De még a biztonságos hálózatok használata közben is ott a kockázat, hogy a vállalatot hackertámadás éri. Különösen, ha nyilvános WiFi-hálózatot használunk, a hackerek könnyedén lefigyelhetik, hogy az alkalmazottak milyen adatokat küldenek. Egy VPN, ami szinte bárhol és bármilyen készülékről használható, titkosítja az adatokat, jelentősen nehezebbé téve a hackerek számára a lefigyelést.

A VPN-ek, vagy Virtuális Magánhálózatok eredetileg nagyvállalatok és kormányzatok számára lettek kifejlesztve, hogy a távoli alkalmazottak biztonságosan kapcsolódhassanak a vállalati hálózatokhoz, anélkül, hogy veszélyeztetnék az adatokat. Egy VPN egy csatornát képez a dolgozó készüléke és a cég szervere között, megvédve a hackerektől és másoktól, akik adatlopásra vetemednének. Titkosítja is az adatokat, így még ha el is lopnák őket, majdhogynem lehetetlen a titkosítás megfejtése. ■

Forrás:
vpnmentor.com