IT-biztonság: csak az ember és a technológia kooperációjaként működik

Dervenkár István

A technológia jó védelmet nyújt – ha a felhasználó is betartja a játékszabályokat.

Nincs és nem is lehetséges olyan rendszer, amit minden emberi hibával szemben fel lehet vértezni. A végfelhasználó szuverén joga, hogy tévedjen – a szoftvergyártóé pedig, hogy ezzel ne foglalkozzon. Ez igaz az üzleti és a IT-biztonsági rendszerekre egyaránt (a szoftverek EULA-jában nem véletlenül korlátozzák a gyártók felelősségét a használatából eredő esetleges károkért).

Az IT-biztonságra mindebből az következik, hogy biztonság optimális szintje nem érhető el csak technológia eszközökkel, ahhoz a végfelhasználó aktív együttműködésére is szükség van.

Nincs mindent (is) tudó technológia

Ha egy kellően magas szintű jogosultsággal rendelkező (vagy ahhoz valamilyen módon hozzájutó) alkalmazott szándékosan helyez el backdoort a rendszerben, tölt le illegálisan adatokat, szivárogtat ki fiókadatokat stb., technikai eszközökkel csak korlátozottan lehet megakadályozni. Az elkövető esetleg utólag azonosítható forensic módszerekkel.

Más a helyzet a véletlen felhasználói hibák esetében. A vállalati környezetben használt védelmi eszközöket ebből a szempontból két csoportra lehet osztani, de nincs közöttük éles határvonal:

– Vannak védelmek, melyek akkor is magas hatásfokkal védik az IT-infrastruktúrát a támadási kísérletektől a végfelhasználó magatartásától függetlenül. Ilyen eszközök például a spamszűrők, hiszen el sem engedik a végfelhasználó fiókjáig a gyanús/veszélyes leveleket.

– Csak a felhasználó együttműködésével nyújtanak optimális védelmet, hatásfokuk anélkül alacsony. Ilyenek például az adatszivárgás elleni védelmek. Ha ezeket teljes mértékben automatizálnák a gyártók, akkor a rengeteg fals pozitív riasztás valószínűsíthetően lelassítaná vagy akár meg is akaszthatná az üzleti folyamatokat.

Összességében az a tendencia, hogy miközben látványosan fejlődtek a védelmi technológiák, egyre fontosabbá vált a tudatos és szabálykövető rendszerhasználat.

Az emberi tényező, azaz a leggyengébb láncszem

Jól mutatja ezt a koronavírus-járvány és a home-office miatt elszaporodó zsarolóvírus-támadások változása. A támadások 30–40 százalékát adathalász linkeken megadott fiókadatok segítségével hajtják végre. Csak míg korábban tömeges levelekkel, spameléssel próbáltak fiókadatokhoz jutni, a támadók az utóbbi időszakban áttértek a célzott támadásokra.

Mint *Vaspöri Ferenc*, az Invitech információbiztonsági üzletágának technológiai szaktanácsadója, mondta, Magyarországon is egyértelműen megfigyelhető ez a trend. Az automatikusan küldött tömeges levélszemétre (spam) ma már úgy tekintenek az IT-biztonsági szakemberek, mint egyfajta internetes háttérzajra, amit ennek megfelelően is kezelnek a spamszűrők. A célzott támadások sokkal veszélyesebbek: a helyes magyarsággal megfogalmazott, sokszor a címzett személyes vagy munkahelyi körülményeinek ismeretére utaló tartalmakkal megtűzdelt megtévesztő leveleket a gyakorlottabb felhasználó is nehezen azonosítja. És itt kap szerepet a biztonsági tudatossága mértéke.

Bár olykor az is kevés. A social engineering ott van a legtöbb támadástípus mögött, és ahogy finomulnak a módszerei, a megtévesztés is tökéletesebb. Korábban egy-kéthavonta voltak ilyen támadások, ma az ügyfelek havi több kísérletről is beszámolnak, mondta saját tapasztalatát Vaspöri. A BEC (Business E-mail Compromise) típusú támadások pedig annyira elszaporodtak, hogy a legtöbbször már nem is jelentik a végfelhasználók. Pedig arra kiemelten kellene figyelni. Egy globális kutatás szerint a vállalatok 98 százalékát (!) érik ilyen támadások.

Az Invitech szakértője is találkozott olyan BEC incidenssel, amelyben egy egyébként körültekintő, és a biztonsági szabályokat teljes mértékben betartó pénzügyi vezetőtől csaltak ki jelentős összeget. Mivel a támadók célzottan és nagy összegre mentek, alapos social engineering tevékenységgel feltérképezték az illető kapcsolatrendszerét, még azt is tudták, hogy a partner vállalatoknál dolgozó kollégái közül ki hogyan szólítja levélben (pl. tegezés/magázás). Tudták, hogy mikor lesz szabadságon az az illető, aki validálhatta volna az adott pénzmozgást. Így a támadás sikeres is volt, és a pénzügyi vezető a támadók által megadott számlára utalt jelentős összeget.

Az emberi tényezőt felértékeli az is, hogy egyre több támadástípushoz társul zsarolás. A biztonságtudatosság éberen tartása, valamint a jól kialakított biztonsági folyamatok ugyanis jelentősen csökkentik a támadási felületeket.

Amikor csak a technológiában bízhatunk

Vannak támadástípusok, melyek esetében a felhasználói magatartás másodlagos (bár egy zombihálózat részeként lehet benne szerepe, mert például nem biztonságtudatos a géphasználata, nem frissítette az operációs rendszerét, nem használt tűzfalat, vírusvédelmet stb.). Ilyen például a DDoS (elosztott túlterheléses) támadás, amikor az a cél, hogy a támadók lebénítsák a támadott vállalat rendszerét, megakadályozzák az munkatársak és az ügyfelek hozzáférését.

Az újdonság az, hogy a DDoS egyre gyakrabban párosul zsarolással. Ez történt például tavaly szeptemberben Magyarországon is, amikor nagyvállalatokat, köztük pénzintézeteket ért támadás. A pénzintézeteket meg is zsarolták: ha nem fizetnek, egy még nagyobb támadás indul ellenük.

Mint lapunknak Vaspöri mondta, egy ilyen támadásnál csak egy hatásos védelmi technológia segít, hiszen egy vállalatnak az IP-forgalma egyik pillanatról a másikra akár ezerszeresére is nőhet. Egy nagyobb magyar vállalat esetében ez már olyan növekedés, ami az egész magyar internetforgalomban meglátszik.

A legkorszerűbb védelmi módszer az, amikor a vállalat rendszerire zúduló forgalmat elterelik egy erre a célra kialakított szolgáltatásba, ahol kiszűrik támadó forgalmat, és a hasznos forgalmat pedig visszajuttatják a rendszerbe. Ha a szolgáltató tisztítókapacitás megtelik, átmenetileg igénybe lehet venni publikus felhőszolgáltatást is erre. Ilyen szolgáltatást kínál az Invitech is, de mint Vaspöri mondta, a forgalomtisztítás sem triviális probléma: fogadni kell a teljes forgalmat, hogy aztán elkülöníthető legyen a támadó és a hasznos forgalom. Ha jól sikerül megoldani a szűrést, a felhasználó csupán elenyésző lassulást érzékel a rendszerben.

Utóbbi azért is fontos, mert a DDoS-támadásoknál beindul egyfajta öngerjesztő folyamat is. Ha egy nagy forgalmú szolgáltatás (pl. kártyás fizetési rendszer) akadozni kell, akkor a végpontok egymás után többször is megkísérlik a kapcsolódást, ami tovább növeli az amúgy is túlterhelt szolgáltatás terhelését.

Meg kell találni a helyi egyensúlyt

A fenti példákból is jól látható: nincs generális megoldás a technológia és a biztonságtudatos rendszerhasználat összhangjának a megteremtésére. Ezt minden területen egyénileg kell kialakítani, és rögzíteni – akár részlegekre bontva – egy IT-biztonsági szabályzatban. Ez az, ami a végfelhasználói magatartás keretét adja.

A szabályzat azonban önmagában kevés, ha a benne foglaltak nem válnak napi rutinná. Utóbbin segíthetnek a rendszeres mérések, de még inkább a hatékony biztonságtudatossági képzések.

Forrás: https://bitport.hu/it-biztonsag-csak-az-ember-es-a-technologia-kooperaciojaban-mukodik

Válogatta: Fonyó Istvánné