MITŐL ÁLMATLANOK AZ ÉJSZAKÁI EGY IT-BIZTONSÁGI VEZETŐNEK?

Rémálmok és lidércek

SCHNECK ZSOLT, SHIELD-INFORMATICS

FORRÁS: ITB

Érdekes kérdést kaptam a minap Sziebig Andreától (az ITBUSINESS főszerkesztőjétől) egy telefonbeszélgetés közben: „Szerinted, Zsolt, mitől tartanak a legjobban a jelenlegi helyzetben a CISO-k?” Azt gondolom, hogy már elég régen vagyok a szakmában, így persze könnyen megválaszolhattam volna a kérdést a szokásos formulával, hogy „Ha jól és körültekintően végzik a munkájukat, akkor mindentől – is”. De ezúttal úgy gondoltam, hogy kihagyom az udvariassági köröket, és azt válaszoltam, hogy nem tudom. Derítsük ki! (A szerző Schneck Zsolt, a Shield-Informatics ügyvezetője)

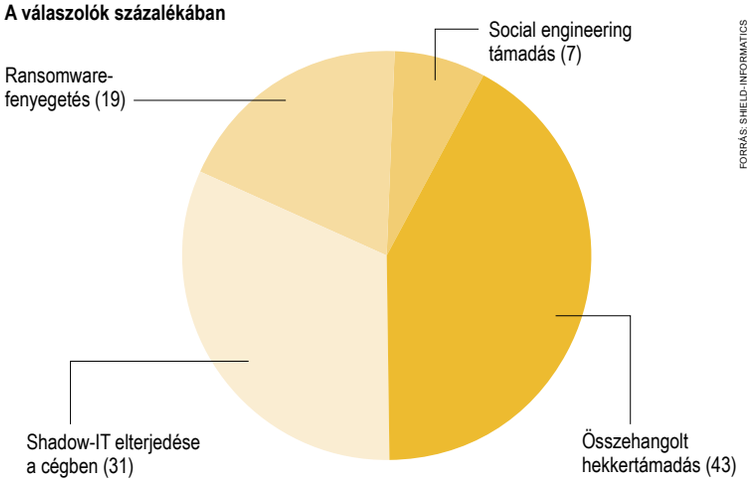
Egy szó, mint száz, készítettünk egy rövid közvélemény-kutatást egy szakmai portálon – nehogy szó érje a ház elejét, hogy csak az ismerőseimet kérdezem meg a dologról –, és bevallom, az eredmény, bár nem lepett meg túlságosan, de elgondolkodtatott, hogy piaci szegmensenként mennyire eltér az, hogy mitől is tart egy vállalkozás biztonsági menedzsmentje. A felmérésnél természetesen csak olyan cégeket vettünk figyelembe, ahol van IT-biztonságért felelős szakember, ami feltételez egy bizonyos vállalkozásméretet. *(A kérdést lásd a „Kutatásunk kérdése" keretben!)*

Kis felmérés alapos értékelése

Bevallom, kíváncsian vártam az eredményt. Nos, nem meglepő módon a banki és nagyvállalati szektorban mindent vitt a hekkertámadás. Ami egyébként toronymagasan verte összetettben is a mezőnyt a maga 43 százalékos arányával. Azaz bizony a nagyvállalati CISO-k attól tartanak a legjobban, hogy profi hekkercsoportok kívülről hozzáférnek a rendszereikhez.
Ez valóban reális fenyegetés a szektorban, hiszen igazán komplex, összehangolt támadást csak nagy cégek ellen érdemes tervezni és indítani. Egész egyszerűen azért, mert a nyilvánvaló dicsőségen túl ez a tevékenység is leginkább a pénzről szól. Egy ilyen támadás pedig elég sok időt, pénzt és humánerőforrást emészthet fel, főképp akkor, ha a védekező oldalon is felkészült szakemberek állnak, és nekik is megvannak a szükséges eszközeik és erőforrásaik.
Előkelő helyen végzett a listánkon a shadow-IT: 31 százalékot kapott. Általános a probléma, a pandémia hatásai bizony jókorára fel is erősítették. A legtöbb IT-vezető számára valóban egy rémálommal ért fel a home office terjedésével elszabadult eszközpark. Már a kkv-szektort is fokozottan érintő problémáról van szó, hiszen a kisebb vállalkozások nem rendelkeznek megfelelő erőforrásokkal ahhoz, hogy a felhasználók minden eszközét kézben tartsák. Ilyenkor csak idő és támadói szándék kérdése, hogy mikor valósul meg a lista harmadik helyezettje: a zsarolóvírusos támadás. A megkérdezett szakemberek 19 százaléka gondolja úgy, hogy még mindig kiemelt és valós veszély a ransomware.
Azt hiszem, senkinek nem kell bemutatni a zsarolóvírusokat. Viszonylag gyors és könnyű pénzkereseti lehetőség a támadók számára. Szerencsére mostanra a biztonsági megoldásokat szállító cégek hatékony megoldásokat dolgoztak ki az ilyen típusú kártevők ellen, így az olyan vállalkozások, ahol a menedzsment nyitott és fogékony az új megoldások bevezetésére és a felhasználók oktatására, jó eséllyel védhetik ki az ilyen jellegű próbálkozásokat. Már, ha feltételezzük, hogy a felhasználóink is felkészülten várnak egy ilyen típusú támadást.

Mitől tartanak ma leginkább a CISO-k?

A válaszolók százalékában



FORRÁS: SHIELD-INFORMATICS

Kutatásunk kérdése

Nem kérdeztünk túl szakmait: „IT-vezető vagy biztonsági vezető vagy? Mi a legnagyobb rémálmod, amire izzadtan ébrednél?" Négy válaszlehetőséget adtunk:
– shadow-IT elterjedése a cégben;
– social engineering támadás;
– ransomware fenyegetés;
– összehangolt hekkertámadás.

Érdemtelenül dobogótlan az átverés

Leszorult a képzeletbeli dobogóról egy speciális, nem az eszközöket, hanem a felhasználókat kompromittáló megoldás: a social engineering. Ez érdekes módon mindössze 7 százalékot kapart össze, meglátásom szerint indokolatlanul keveset.
Nagyon nagy a potenciál támadói szempontból, szinte végtelen a módszerek tárháza, hiszen itt nem nullákkal és egyesekkel dolgozó berendezések, hanem hús-vér, érzésekkel és érzelmekkel rendelkező humanoidok az elsődleges célpontok. Nagy a merítési lehetőség, hiszen sokan vannak, és tegye fel a kezét, aki még sosem kapott phising-levelet.
Ez persze még csak a kezdet. Egy összehangolt hekkertámadás, amitől a CISO-k a legjobban tartanak, többnyire social engineeringgel, klasszikusan valamilyen phising-megoldással kezdődik, és ha már a felhasználó emocionális tűzfalán túljutott a támadó, hamar a belső informatikai rendszerben találhatja magát. Jó ideig talán észre sem vesszük, hiszen egy kollégánk érvényes adatait használja.

Három voltaképpen a negyedik

Gondolom, mostanra mindenki számára kiderült, hogy kicsit csaltam a kérdések összeállításánál. Bár minden felsorolt kérdés önmagában is elég veszélyt rejt magában, az első három bizony aktív része lehet egy összehangolt hekkertámadásnak. Hiszen egy otthoni számítógépet használó felhasználón történő sikeres social engineering után egyenes út vezethet egy jól megkomponált ransomware-támadáshoz, hogy csak egy egyszerű változatot említsek. Persze feltételezzük, hogy a biztonsági mentést minden vállalkozásnál megfelelően konfigurálták, de így is termelés- és időkiesést okozhat, az IT-szakemberek pedig a visszaállítás során rengeteg ősz hajszálra tehetnek szert.
Úgyhogy azt tanácsolom mindenkinek, hogy egyik fenyegetést se vegye félvállról, különben, ha a cég elég potenciált tartogat a hekkerek számára, hamar egy összehangolt támadás kellős közepén találhatja magát. *(X)*