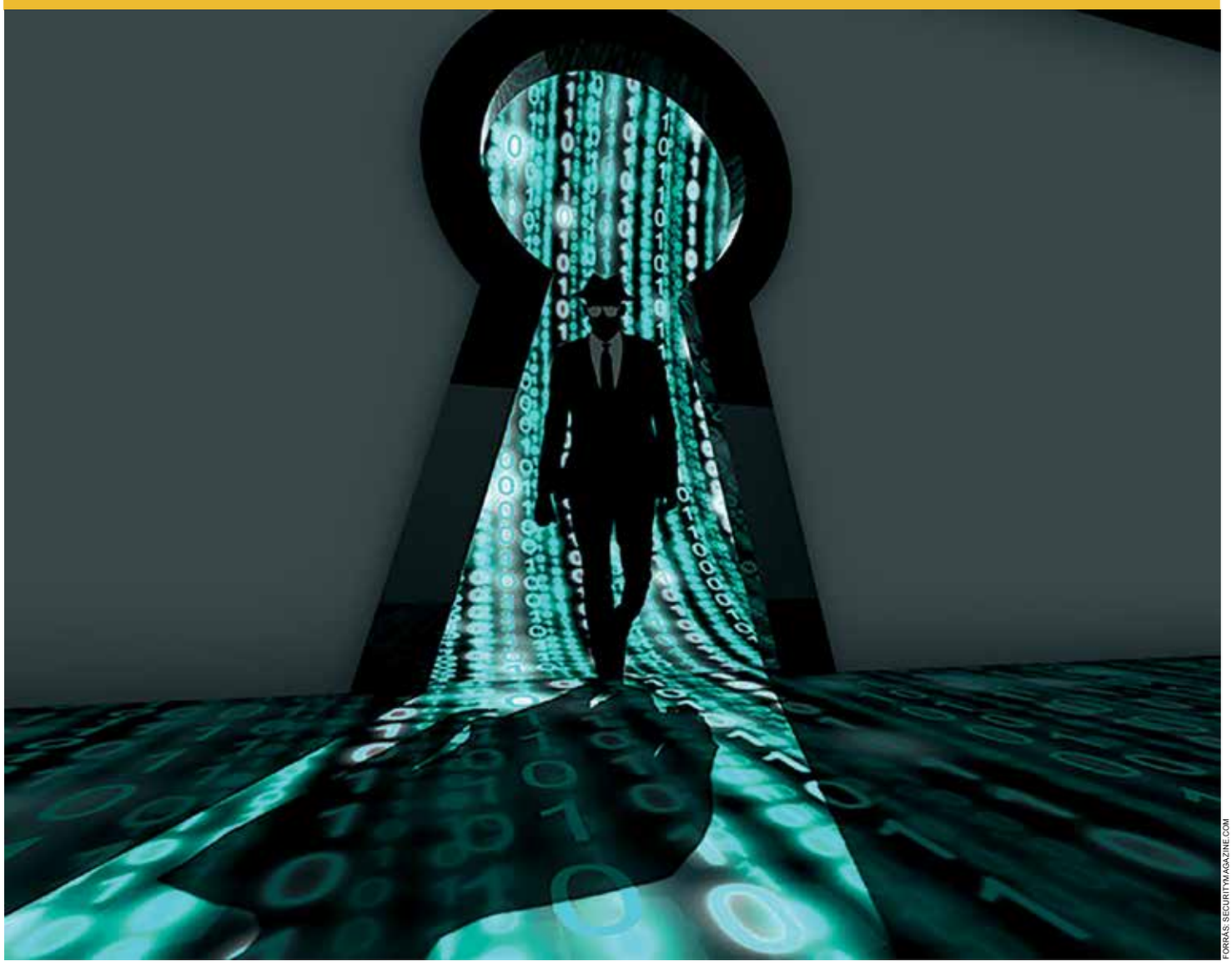
NEM TARTJÁK BE A „NE FIZESS A ZSAROLÓNAK!" SZABÁLYT

A sikeres kibertámadás ára



FORRÁS: SECURITYMAGAZINE.COM

Az azonnali pénzügyi veszteségek mellett hosszú távú következményei is vannak egy sikeres kibertámadásnak. A vállalatoknak számolniuk kell a reputációs veszteséggel, a kulcsfontosságú vezetők, a stratégiai partnerek és ügyfelek elvesztésével egyaránt, de saját fennmaradásukat is kockáztatják. Ha innen nézzük, a kiberbiztonságra nem lehet eleget áldozni.

Sokaknak az 1970-es évek olajválsága jutott eszébe, amikor 2021 májusában az Amerikai Egyesült Államok déli államaiban hosszú sorok kígyóztak a benzinkutak előtt, majd kifogyott az üzemanyag. A krízist most nem politikai vagy gazdasági machinációk okozták, hanem egy kiberbűnöző-csapat, akik zsarolóvírussal fertőzték meg a Colonial Pipeline nevű üzemanyag-társaságot.
Ez az ügy abban is érdekes, hogy a társaság rekordösszegű (4,4 millió dollár, vagyis nagyjából 2,1 milliárd forint) váltságdíjat fizetett. Szerencsére (?) az amerikai hatóságok segítségével és nyomozásának köszönhetően 2,3 millió dollárnyi Bitcoint sikerült visszaszerezni, így a veszteség feleződött.

Az tény, hogy a vállalatok egyre nagyobb váltságdíjat fizetnek adataikért. A támadók is változtattak taktikájukon: az adatokat nemcsak titkosítják, hanem ellopják, és azok nyilvánosságra hozatalával fenyegetőznek. A váltságdíjat egyre többen kifizetik. Holott semmi garancia arra, hogy adataikat tényleg visszakapják, és többet nem támadja őket újra senki. A Sophos adatai szerint 2020-ban az átlagos váltságdíj elérte a 170 ezer dollárt (kb. 50 millió forintot), és a legmagasabb kifizetett váltságdíj 3,2 millió dollár (950 millió forint) volt.

Nem elég a kiberbiztosítás, a rendszeres adatmentés, a fejlett visszaállítási technológia, a hírnév romlását is meg kell előzni

Rövid és hosszút távú veszteségek, romlik a márka

A Cybereason egy világszintű kutatásban (amelyben 1263 kiberbiztonsági szakértőt kérdeztek meg, különféle méretű vállalatoktól) felmérte, hogy milyen következménye és mekkora ára van egy zsarolóvírusos támadásnak.
Rövid távon gondot okoz a kritikus üzleti folyamatok leállása, hiszen a vállalat nem tud a működéshez szükséges adatokhoz hozzáférni. Pénzbe kerül az incidensre adott válasz is, a szakértői vagy a saját IT-csapat költségével is számolni kell. Csökken a munkatársak produktivitása, hiszen adatok híján nem tudnak dolgozni. A váltságdíj is komoly költségtételt jelent.
A hosszú távú következmények között gondolni kell az alacsonyabb éves bevételekre, a vállalat brandjét érő reputációs kárra, a kulcsfontosságú vezetők, stratégiai partnerek és ügyfelek elvesztésére, és az esetleges csődre is.
A kutatásban szereplő vállalatok 66 százaléka jelentős bevételkiesést szenvedett el a zsarolóvírusos támadás közvetlen következménye miatt. A vállalatok mérete nem befolyásolta az eredmények alakulását, a nagy cégek és kis vállalatok is hasonló eredményről számoltak be. A német vállalatok 75 százaléka, míg a spanyol cégek 80 százaléka számolt be veszteségről, a brit vállalatok esetében ez az arány 61 százalék volt. *(A támadók meglehetősen pontosan felmérik a megcélzott vállalkozás anyagi helyzetét, a váltságdíj pont akkora, hogy ha nehezen is, de ki tudják fizetni. – A szerk.)*
A SolarWinds támadás esete a legbeszédesebb, hiszen a vállalat neve az ellátási láncok elleni kínos támadással fonódott egybe. A brit állami egészségügyi szolgáltató, az NHS még 2017-ben szenvedett el egy masszív, WannaCry zsarolóvírusos támadást, melynek hatásait még ma is érzi. Számítások szerint több mint 100 millió dollár (29 milliárd forint) veszteséget szenvedett el a szolgáltató, 19 ezer időpontot töröltek.
A vállalatok hamis biztonságérzetbe ringatják magukat, amikor azt gondolják, hogy teljesen felkészültek egy zsarolóvírus-támadás hatásainak kezelésére, ha kiberbiztosítást kötöttek, előírás szerinti, rendszeres adatmentést készítenek, és felkészültek az adatok visszaállítására is. A Cybereason kutatásában szereplő vállalatok 53 százaléka szerint márkájuk komoly reputációs veszteséget is elszenvedett a támadás következtében a vállalat felkészültsége fokától függetlenül. Ráadásul ez a veszteség tartós is lehet.

A kiberbiztosítás megment?

A zsarolóvírusos támadást elszenvedő, kiberbiztosítással rendelkező vállalatok 42 százaléka arról számolt be, hogy a biztosító a veszteségeknek csak egy részét térítette meg. A váltságdíj kifizetése kérdéses: a biztosítók közül elsőként a francia AXA jelentette be nyár elején, hogy a jövőben megkötött biztosítások esetében már nem fedezi a váltságdíjat. (Ez egyenes következménye a váltságdíj-fizetési kedv javulásának. Amely abban is segít, hogy zsarolóvírus-ipar szárba szökkenjen, és a támadóeszközök folyamatos fejlesztésére is jusson pénz. – A szerk.) Az intézkedés egyelőre csak Franciaországot érinti, ahol az Amerikai Egyesül Államok után a második legtöbb zsarolóvírusos támadást szenvedik el a cégek, káraik éves szinten 5,5 milliárd dollárra (1612 milliárd forintra) rúgnak.

Emberáldozatok is vannak

A biztonsági események áldozata leggyakrabban a CISO, de a CEO sincs biztonságban: a Target áruházlánc, a Home Depot, a Sony is első embert cserélt. A kutatás szerint a vállalatok 32 százaléka veszített el felső vezetőt zsarolóvírus támadás után: vagy lemondott a vezető, vagy elküldték.
Az anyagi veszteségek miatt az alkalmazottak sincsenek biztonságban: a vállalatok 29 százaléka elbocsátásokra kényszerül a támadások következtében. Érdekes, hogy e kutatás szerint a kormányzati szektorban tevékenykedő szervezetek egyáltalán nem küldtek el embereket a támadás következtében, csak a versenyszféra.
Végső soron még az is előfordul, hogy a nem túl biztos alapokon álló vállalatnak a zsarolóvírusos támadás adja meg az utolsó lökést a teljes csődhöz. A kutatás szerint a vállalatok negyede a támadás után egy bizonyos ideig teljesen bezárt, felfüggesztve minden tevékenységet – szerencsére azután megtépázva, de sikerült talpra állniuk.
Egy látványos veszteséggel járó támadás indítja el igazán az IT-biztonsági megoldások vásárlását, vagyis az „eső után köpönyeg” hatás itt is érvényesül. *(Lásd a „Mit vesznek a cégek zsarolóvírusos támadás után?” című keretet!)* Szerencsére a magyar vállalatokat eddig elkerülték a nagyobb problémával járó támadások.

Vass Enikő

Mit vesznek a cégek zsarolóvírusos támadás után?

A védelmi megoldások slágerlistája (a válaszolók százalékában)

48% Security Operation Center (SOC)
48% Biztosságtudatossági programok, oktatás
44% Végpontvédelmi megoldások
43% Adatmentési és -visszaállítási megoldások
41% Emailszűrő megoldások

FORRÁS: CYBEREASON: „RANSOMWARE: THE TRUE COST TO BUSINESS, 2021”