NÖVEKVŐ KITETTSÉG, KISZÉLESEDETT TÁMADÁSI FELÜLETEK

Támadások kereszttüzében: a működést beárnyékolják a kiberbiztonsági aggályok

RÓZSA ROLAND, 4iG

FORRÁS: 4iG

SZABADOS GÁBOR, NNG

FORRÁS: ITB

2021-ben a régről ismert kibertámadások reneszánszukat élik, de új belépők is felbukkantak a CISO-k legnagyobb „örömére". Milyen kiberbiztonsági incidenstől tartanak leginkább a cégek első számú biztonsági felelősei, hogyan készülnek fel ezek elhárítására, és milyen jövőképet vizionálnak az elkövetkező hónapokra? Két tapasztalt Chief Information Security Officerrel beszélgettünk.

Megdöbbentő összegről számolnak be a 2020-as évet összegző és a 2025-ig előre tekintő nemzetközi kutatások. A kiberbűnözés ezermilliárd dolláros üzletté nőtt a McAfee legfrissebb jelentése szerint, a „The Hidden Costs of Cybercrime" címet viselő összegzésükben pedig arra is rámutattak, hogy a 2018-as évhez képest megduplázódott a támadók kiberbűnözésből származó bevétele, és a támadások következtében létrejött anyagi kár is százmilliárd dolláros nagyságrendben mérhető.
A Cybersecurity Ventures a jövőbe tekintett, és azt összegezte, hogy a támadások mekkora anyagi veszteséget jelentenek 2025-ig. Számításaik szerint ezutóbbi, globálisan hatbillió amerikai dollárt jelent évente, ötszáz milliárdot havonta, száztizenöt milliárdot hetente, tizenhat milliárdot naponta, hatszáznyolcvannégy milliót óránként, tizenegymilliót percenként és százkilencvenezer dollárt másodpercenként. Drámai számsoruk jól érzékelteti, hogy a kiberbűnözés elképesztő méretet öltött, a koronavírus-járvány pedig még jövedelmezőbbé tette az üzletet, érthető okokból.

A kibertámadások száma még mindig növekszik, semmivel sem lesz könnyebb ez az év, mint az előző

Az idei év toplistás támadásai

„Mostanában a leggyakoribb támadás, amellyel a vállalatok találkozhatnak az a BEC (business email compromise). A támadás során a bűnözők a levelezőpartnerek email-fiókjaihoz, és ennek felhasználásával hajtják végre a támadást, megszemélyesítve a kommunikációban résztvevő felek egyikét. Ezek a támadások arra mennek ki, hogy a tolvajok beleavatkozzanak egy számlázási fázisban lévő projektbe, és meghamisítva a számlán szereplő információkat, eltérítsék a tranzakció összegét, nyilván a saját bankszámlájukra utalva azt", mondta *Szabados Gábor,* az NNG CIO-ja és CISO-ja.
A „hagyományos" támadások közül a ransomware éli másodvirágzását, ugyanakkor elsősorban az adathalász és az üzleti adatok megszerzését célzó támadások jelentik a leggyakoribb fenyegetést.

Hat adat a kiberbiztonságról

- A Gartner előrejelzése szerint az információbiztonsági piac mérete globális szinten 2022-ben eléri a 170,4 milliárd dollárt.
- A Cybint Solutions kutatása alapján az USA-ban a vállalkozások 62 százaléka élt át adathalász és social engineering támadásokat 2018-ban.
- A Marylandi Egyetem vizsgálódása azt mutatta, hogy minden 39. másodpercben hekkertámadás ér valakit az Egyesült Államokban.
- A Cybersecurity Media számításai szerint 2020-ra az emberek és gépek által világszerte használt jelszavak becsült száma 300 milliárd lesz.
- A Cisco becslése szerint 2023-ra a DDoS támadások száma világszerte elérheti a 15,4 milliót.
- A Symantec kutatása arról számolt be, hogy 36-ból egy mobiltelefonon található magas kockázatú applikáció.

„2020-ban ugyancsak megnőtt a vállalatok IT-biztonsági kitettsége, a támadási felület a home office nagyobb arányú használata miatt: új erőre kaptak a zsarolóvírusok, taroltak az emailben terjesztett rosszindulatú kódok. Ez a tendencia minden bizonnyal folytatódni fog idén is", mondta *Rózsa Roland,* a 4iG stratégiai cybersecurity tanácsadója.

Tavaly a felhő eddig nem látott szerephez jutott a vállalatoknál, és ez újfajta kitettséggel is jár

Egy lépéssel a támadók előtt

Ami a megváltozott helyzetet illeti, kifejezetten nehéz helyzetbe kerültek a cégek, hiszen eddig az adatok és a felhasználók a szervezet falain belül, a szervezet saját hálózatán voltak jelen, így a támadóknak először a jól felépített biztonsági pajzson kellett átjutni. „Most senki nincs a vállalatok hálózatán belül, hiszen szinte mindenki otthonról dolgozik, olykor privát eszközről, publikus internetet vagy otthoni wifi-hálózatokat használva, ki tudja milyen beállításokkal, amire az cégeknek nincs is ráhatása. Ezt a támadók ki is használják", tette hozzá Szabados Gábor.
Védekezni nem egyszerű, de vannak alternatívák. „Eddig elsősorban a céges hálózatra és a céges szerverekre fókuszáltunk, így a technikai védekezést is át kell helyezni a végpontokra, ennek köszönhetően a mobileszköz-felügyeleti megoldások most hangsúlyosabbak, mint valaha", mondta Szabados Gábor.
Ugyanakkor a legjobban beállított védelmi rendszer is meg tud bukni, ha a felhasználók biztonságtudatossága nem megfelelő, így az első és legfontosabb, a dolgozók képzése, tájékoztatása, hogy vegyék észre, ha baj van.
„A támadások során nemegyszer ugyanazokat a technikákat alkalmazzák új területeken. Emiatt a védekezésnél továbbra is elengedhetetlenek a már évek óta emlegetett lépések, például egy fejlett email-védelmi rendszer kiépítése. Nem szabad elhanyagolni a frissítések, javítócsomagok időben történő telepítését sem. Vállalati környezetben ennek végrehajtása gyakran a tesztelés és a jóváhagyás miatt csúszik. Nincs már 2-3 hónap letesztelni egy patch-csomagot: automatizálással, dedikált erőforrások biztosításával kell elérni, hogy minél hamarabb védettséget szerezzünk", fogalmazta meg Rózsa Roland.
„Szintén nagy figyelmet kell szentelni a felhőszolgáltatások védelmére is, különösen, az olyan esetekben, amikor sebtében vezették be. Tavaly a felhő soha nem látott szerephez jutott a vállalatoknál és ez egy újfajta kitettséggel is jár. A szolgáltatások federációja, a felhasználók biztonságos autentikációja és a tevékenység monitorozása mind lényeges feladattá lépett elő 2021-ben", zárta mondandóját Rózsa Roland.

Kiss Franciska