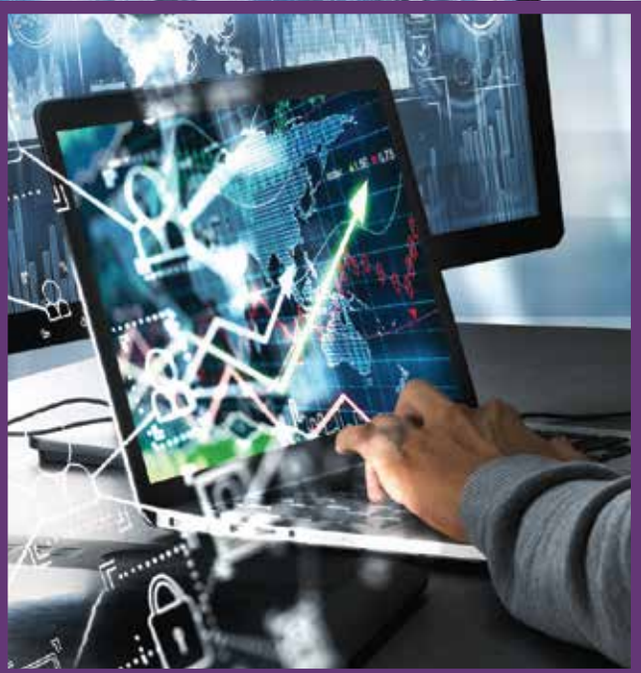


SZIGORÚAN BIZALMAS

Még keményebb csaták jönnek a kibertérben

FORRÁS: 123RF.COM

Több és profibb támadás érte a múlt évben a vállalkozásokat, intézményeket és magánszemélyeket, mint eddig bármikor, a kiberbűnözők egyre szervezettebbek, és a módszereik is sokat fejlődtek. A mesterséges intelligenciát a támadók és a védekezők is egyre aktívabban használják.

Azt már hosszú évek óta megszokhattuk, hogy a kibertérből érkező támadások elsődleges motivációja az anyagi haszonszerzés, és hekkert játszó fiatalok helyett jól szervezett bűnözői csoportok utaznak a felhasználók, vállalkozások pénzére, titkaira. A múlt évben azonban olyan érzésünk lehetett, mintha szintet léptek volna a kiberbűnözők. Az ITBUSINESS által megkérdezett szakértők szerint valóban komoly változások történtek, és a szervezettség, a támadások kifinomultsága minden korábban tapasztaltat felülmúlt.

Azonnal lecsapnak

Három dolgot érdemes kiemelni a múlt év informatikai biztonsági trendjei kapcsán – jelezte érdeklődésünkre *Szappanos Gábor,* a Sophos kiberbiztonsági szakértője. Az egyik ezek közül az, hogy a kiberbűnözők a teljes védelmi láncot támadják, vagyis nem feltétlenül közvetlenül vesznek célba egy céget, hanem a kiszolgáló rendszereken keresztül támadnak. Erre több példa is volt 2021-ben, volt olyan eset, amikor nagyvállalatoknál használt adminisztrációs szoftvert fejlesztő társasághoz hatoltak be, és rajtuk keresztül jutottak el a nagyobb célpontokhoz.
De jó példa az ilyen jellegű fenyegetésre a múlt év végén kiderült Java segédprogram-sérülékenység, a biztonsági hibán keresztül webes szolgáltatásokba, szerverekbe tudnak betörni a támadók. Jól megfigyelhető egyébként az is, hogy a kiberbűnözők részéről nagy figyelmet kapnak a gyenge pontok, sérülékenységek, és egyre rövidebb idő telik el azok felfedezésétől addig, hogy megjelennek az első, ezeket kihasználó támadások.

Kiszervezett feladatok

„A másik fontos trend már évekre visszamenőleg velünk van, ez pedig a zsarolóprogramok térhódítása. A mi ügyfélkörünkben ez tekinthető a legkomolyabb problémának. Jól látszik, hogy kezd nagyon jól szervezett iparággá válni a bűnözők részéről ez a tevékenység, több csoport is foglalkozik vele és beindult már a specializálódás is. Ez a gyakorlatban azt jelenti, hogy ma már nem arról van szó, hogy egy zsarolóvírust használó csoport betör egy céghez, lefuttatja a programot és begyűjti a pénzt, hanem vannak megbízók, akik kiszervezik a feladatokat. A feketepiacon hozzáférést vásárolnak a feltört rendszerhez, viszont a »kétkezi munkát« már kiszervezik másoknak, így különböző csoportok foglalkoznak a vírus bejuttatásával, a zsarolás menedzselésével és a pénz begyűjtésével. Ráadásul nagyon nehéz védekezni az ilyen akciók ellen, mivel jellemzően olyan országokban tevékenykednek ezek a bűnözői csoportok, ahol nem lépnek fel velük szemben elég határozottan”, vázolta a helyzetet Szappanos Gábor.
Majd folytatta, „a harmadik trend a Covid-járvány és az ezzel kapcsolatos problémák. A pandémia kitörését követően a legtöbb cégnél átálltak távmunkára, viszont idő és erőforrás hiányában ezt nem tudták megfelelően előkészíteni. Mivel nagyon rövid idő alatt kellett megoldani a helyzetet, a gyorsaság volt a fő szempont és nem az, hogy a lehető legbiztonságosabb architektúrát alakítsák ki az otthonról dolgozó munkatársak számára. Ez azt eredményezte, hogy sokkal könnyebben támadhatók lettek a vállalati rendszerek, és ezt természetesen felismerték a kiberbűnözők is, sokszorosára nőtt például a távoli elérést biztosító megoldások elleni akciók száma. Több és gyengébben védett kaput nyitottak meg a cégek

Előrejelzések 2022-re

A Sophos a múlt év végén hozta nyilvánosságra 2022-re vonatkozó fenyegetettségi jelentését (a Threat Reportot), amelyben vázolta az idei fő kiberbiztonsági trendeket. Az elemzés szerint a zsarolóvírus területe modulárisabb és egységesebb iparággá válik, a támadások „specialistái” szolgáltatásként fogják kínálni az akciók különböző elemeit, ezekhez forgatókönyveket, eszközöket és technikákat fognak biztosítani, amelyek lehetővé teszik a különböző bűnöző csoportok számára, hogy nagyon hasonló támadásokat hajtsanak végre.
A kiberbiztonsági cég szakértői szerint a meglévő kiberfenyegetések tovább adaptálódnak a zsarolóvírus terjesztéséhez. A kriptovaluták továbbra is elősegítik a kiberbűnök – zsarolóvírusos támadások és káros kriptobányászat – elkövetését. A Sophos arra számít, hogy ez a tendencia mindaddig folytatódik, amíg a globális kriptovalutákat nem szabályozzák jobban. 2021 során a cég kutatói olyan kriptobányászokat fedeztek fel, mint a Lemon Duck új variánsai vagy a kevésbé gyakori MrbMiner, amelyek az újonnan bejelentett sebezhetőségek által biztosított hozzáférést használták ki, illetve a zsarolóvírus-operátorok által már meghekkelt áldozatok számítógépeire és szervereire telepítettek kriptobányász-eszközöket.

KOVÁCS ZOLTÁN, T-SYSTEMS

FORRÁS: T-SYSTEMS

Egyre több, a kritikus infrastruktúrákat érintő incidensre kell felkészülni

SZAPPANOS GÁBOR, SOPHOS

FORRÁS: SOPHOS

a védelmükön, és ezért több támadás is történik. A másik nagy gond, hogy a munkavállalók se megfelelő szakmai támogatást, se megfelelő oktatást nem kaptak arra vonatkozóan, hogyan kellene biztonságosan és hatékonyan dolgozni a távmunka korában."

Jól szervezett csoportok

Kovács Zoltán, a T-Systems Magyarország CTRL-SWAT csoportjának operációs vezetője szerint is a múlt évben a legnagyobb hatású támadások a zsarolóvírusokhoz kötődtek. Szintén gyakori fenyegetés volt a túlterheléses, DDOS-támadás, amely egyébként időnként zsarolással is párosul, a kiberbűnözők ugyanis jelzik az áldozatoknak, hogy következő alkalommal még komolyabb károkat okoznak, ha nem fizetnek nekik. Felbecsülhetetlen károkat okoz, viszont az esetek többségében csak nagyon későn derül ki a csendes adatlopás, amelynek elsődleges célja az információszerzés. Főleg azok a vállalkozások kerülnek a célkeresztbe, amelyek intenzív kutatás-fejlesztési tevékenységet végeznek. Az autóipar, az élelmiszeripar és a hadiipar képviselői is a célpontok között vannak, ahogy a gyógyszergyártók is.

„Azt látjuk, hogy nagyon jól szervezettek, komoly anyagi és emberi erőforrással rendelkeznek a kiberbűnözői csoportok, ami például azzal jár, hogy jóval gyorsabban reagálnak a sérülékenységek napvilágra kerülésére, mint korábban. A támadói oldalon egyre gyakrabban figyelhető meg, hogy úgy működnek, mint egy nagyvállalat. Ha kifejlesztenek egy támadói módszert, gyakori, hogy felépítenek egy infrastruktúrát a terjesztéséhez, amely hasonló egy nagyvállalati rendszerhez: van backup, magas elérési szintet biztosító rendszerek, a szerverek állapotát folyamatosan monitorozó megoldások, fejlesztők, technikai támogatást nyújtó csapat, de még arra is van példa, hogy egy ransomware-csoport ügyfélszolgálatot tartson fenn. Az áldozatnak chaten keresztül segítenek bitcoin-tárcát létrehozni, bizonyítják, hogy valóban birtokukban vannak az információk, vagy képesek újra elérhetővé tenni a blokkolt tartalmakat, mindezt ráadásul nagyon udvariasan teszik meg", számolt be a tapasztalatokról Kovács Zoltán.

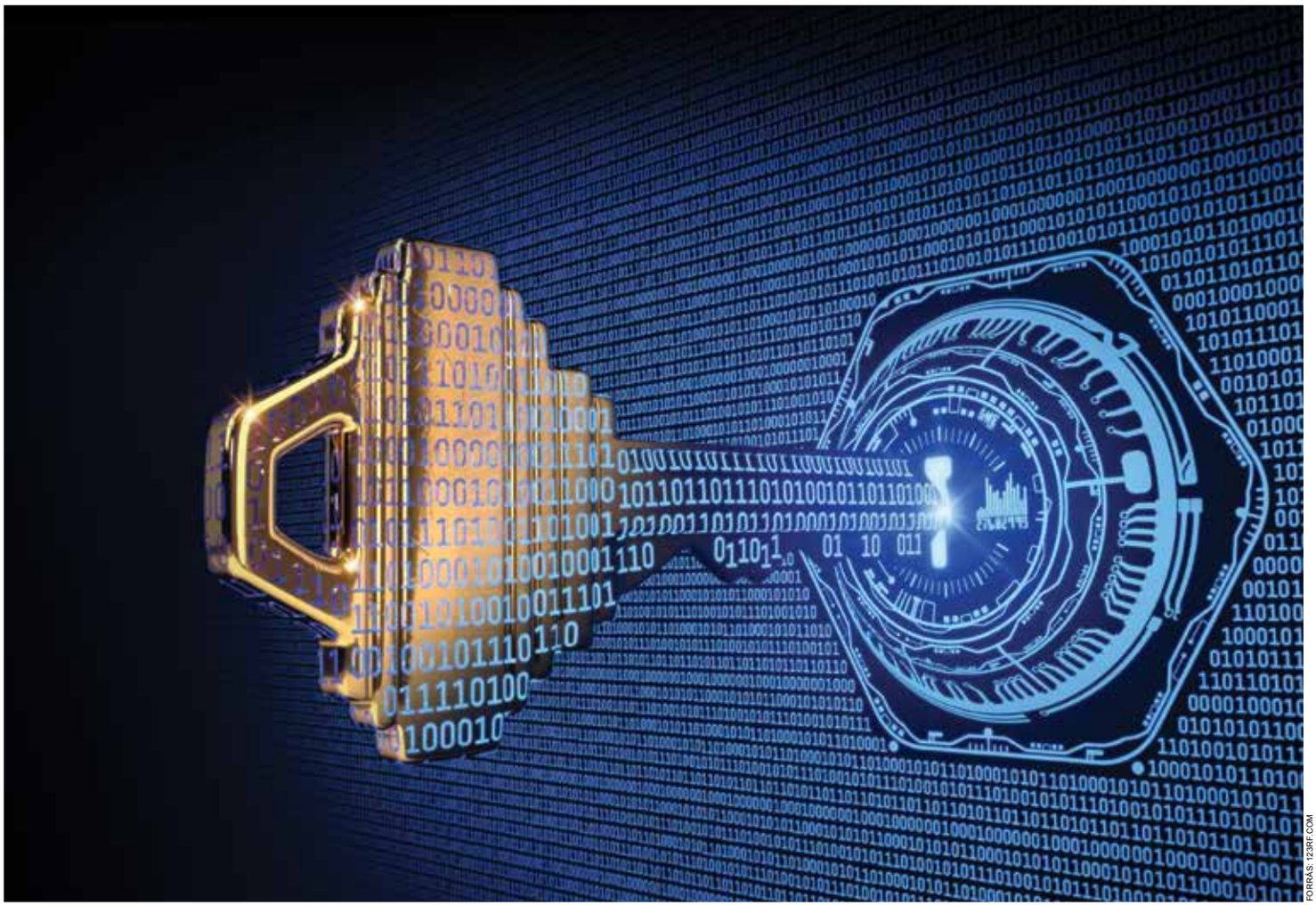
Szerinte az elmúlt időszak egyik fontos jellemzője, hogy nagy mértékben megnőtt az államilag támogatott csoportok aktivitása, ami azért különösen veszélyes, mert nincs az a védelmi vonal, amelyen ne tudnának áttörni. Aggodalomra adhat okot, hogy átfedésre is van példa a pénzszerzés által motivált bűnözők és az államilag támogatott támadók között.

Védett eszközök

Szappanos Gábor szerint a múlt év meghatározó kiberbiztonsági trendjei idén is velünk maradnak, sőt, várhatóan erősödni fog a támadók aktivitása, ami az incidensek számában, a sérülékenységek kihasználásának gyorsaságában és az akciók kifinomultságában is megfigyelhető lesz majd. A szakember szerint éppen ezért nagyon fontos lesz, hogy a megjelenő frissítéseket, hibajavításokat minél gyorsabban telepítsék a vállalkozások szakemberei. A védelem érdekében elengedhetetlen, hogy minden céges rendszeren és eszközök legyen vírusvédelem, ne hagyjanak „üres foltokat" a társaságok.

A szakember szerint a másik fontos tényező a védekezésben a határvédelem megoldása. „Várhatóan idén is a zsarolóprogram lesz a legnagyobb veszélyforrás, az ezt alkalmazó akciók pedig úgy indulnak, hogy támadók hozzáférnek a céges hálózathoz. Ez az esetek többségében egy webre kitett szolgáltatás biztonsági hibáján, gyenge jelszóvédelmén keresztül történik. Ezért célszerű minimálisra csökkenteni a külső elérési pontok számát, amelyeket pedig megtartunk, azokat védeni kell. Ha az alapértelmezett és/vagy gyenge jelszavakat megszüntetjük, lezárjuk a belépési pontokat, akkor a támadások nagy része lepattan.

Emellett fontos lenne, hogy foglalkozzanak a cégek a munkatársaik kiberbiztonsági képzésével is. „A bűnözők a leggyengébb láncszem felől támadják a rendszereket,



FORRÁS: 123RF.COM

és ha a munkavállalók felkészületlenek, nem ismerik fel a támadást, könnyen áldozattá válnak, és így az egész társaság az lehet. Úgy kell ezt felfogni, mint egy támadási felületet, amelyet a Covid miatt jelentősen megnöveltek, és ebben az esetben az oktatással lehet legjobban védekezni", fűzte hozzá Szappanos Gábor.

Az MI-t is bevetik

Kovács Zoltán szerint a nagyon felkészült és szinte végtelen erőforrásokkal rendelkező támadók miatt mindenkinek arra kell készülnie, hogy előbb-utóbb áldozattá válik. „Nem úgy kell kialakítanunk a védelmünket, hogy mi mindent kivédünk, hanem arra is fel kell készülni, hogy mi van, ha ez nem sikerül. A védelem másik fontos rétege a CTI, a cyber threat intelligence, azaz a bűnözői csoportok és technikáik figyelése. Vannak már speciális technikai információkat nyújtó cégek, szolgáltatásuk alapján bizonyos módszerekre fel lehet készülni.

Idén arra lehet számítani, hogy az államok közötti kiberhadviselésben tovább romlik a helyzet. Emellett egyre több, a kritikus infrastruktúrákat érintő incidensre kell felkészülni, az ezek működtetésére használt rendszerek ugyanis biztonsági szempontból egyelőre vakfoltot jelentenek. Az azokkal dolgozó szakemberek az ipari vezérlőrendszerekhez értenek ugyan, de nincs biztonsági képzettségük, nincs is ilyen elvárás feléjük. Amikor megtervezték ezeket a rendszereket, még egyáltalán nem volt téma, hogy kibertámadás célpontjaivá válhatnak.

Idén tovább erősödhet a felhasználók megtévesztése: deepfake, illetve deepvoice támadások jöhetnek, melyekhez egyre gyakrabban alkalmaznak a támadók gépi tanulást és mesterséges intelligenciát (MI-t). „Ezeket a technológiákat egyébként a védekezésben is bevetjük, a hálózati forgalmat például elég jól ki tudja már ismerni egy tanulásra képes algoritmus és ezt felhasználva riasztást tud küldeni a megszokottól eltérő, vagy gyanús forgalomról", közölte Kovács Zoltán.

Arra vonatkozóan csak becslések vannak, hogy mekkora károkat okoznak a kiberbűnözők, hiszen az incidensek jelentős része nem is kerül nyilvánosságra, nem beszélve arról, hogy a helyreállítás költségeit, vagy éppen egy adatszivárgás cégimázsra és ezen keresztül a bevételre gyakorolt negatív hatását nem is igazán lehet mérni. A Cybersecurity Ventures becslése szerint idén akár 6000 milliárd dolláros is lehet a kiberbűnözés által okozott károk összértéke, ami egészen elképesztő összeg, a világon csak két ország, az Egyesült Államok és Kína rendelkezik ennél nagyobb éves GDP-vel. A cég ráadásul nem biztat sok jóval a jövőre nézve, egy 2020 végi előrejelzésükben azzal számoltak, hogy 2025-re a károk mértéke eléri a 10,5 ezer milliárd dollárt.

Kalocsai Zoltán