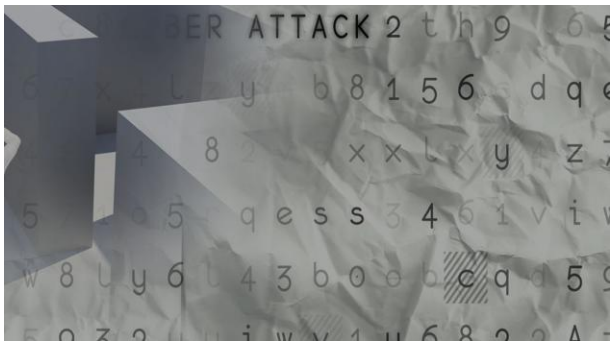
Ezek lesznek biztonságunk sarkalatos kérdései

Új stratégia kell a megváltozott környezettel járó kockázatok kezeléséhez, csak egyelőre nem látszik, honnan lesz szakember a megvalósításához



Gyökerestül forgatta föl a vállalatok életét (is) tavaly a koronavírus-járvány. Az IT-biztonsági csapatoknak extrém terhelés alatt kellett dolgozni: a sok helyen bevezetett táv- és hibrid munkavégzés miatt egyik napról a másikra megsokszorozódtak a kezelendő kockázatok, és megugrott a támadások száma is. Emiatt a CISO-knak gyorsan át kellett írniuk a múlt évre vonatkozó terveiket. A kérdés, hogy idén csökken-e a nyomás, vagy maradnak a tavalyi viszonyok.

A vállalati kiberbiztonsággal kapcsolatos kutatások többé-kevésbé egy irányba mutatnak. 2021 sem lesz könnyebb a múlt évnél, de a kibervédelmi cégek sokat tanultak, és a tapasztalataik jelentős része már ott figyel a védelmi eszközeikben. Nőtt azoknak a szállítóknak a termékeire a kereslet, melyek képesek komplex, minden szegmensre kiterjedő megoldást biztosítani a végponttól a felhős rendszereken át a gyártóipari OT-ig (Operation Technology – a gyártóipari cégek hálózatba kapcsolt termelőeszközei), netán mindezt szolgáltatásként is kínálják. (Tavaly a befektetői érdeklődés is nőtt az IT-biztonsági piac iránt.)

A Trend Micro egy friss kutatása pedig azt mutatja, hogy a vállalatok a tavalyi változások hatását hosszabb távúnak gondolják, és hamarosan további tényezők is színesítik. Az 5G például átalakítja a hálózati és biztonsági infrastruktúrát. A biztonság a mesterséges intelligenciával (MI) önmenedzselővé válik, ám ezzel együtt a kiberbűnözők is MI-alapú támadásokat indítanak majd.

Az alapoktól mindent újragondolni...

Talán az elmúlt év legfontosabb élménye IT-biztonsági szempontból annak a fizikai megtapasztalása volt, hogy a vállalatok egyre kevésbé írhatók le a fizikai határaikkal. Ma már egy gyár sem ér véget az üzemterület kerítésénél, hiszen a vállalati végpontok, melyek közvetve-közvetlenül kapcsolatban állnak a gyártásirányítással, szinte bárhol lehetnek a világban. Így valójában megvalósult a régen sokat emlegetett buzzword, a BYOD (Bring Your Own Device), ha nem is úgy, ahogy azt néhány éve elképzelték: olyan eszközök kerültek a vállalati hálózat közelébe (pl. otthoni routerek), melyekre az üzemeltetésnek, illetve a kiberbiztonsági csapatnak szinte semmi ráhatása sincs.

Az a felismerés, hogy ez az állapot hosszabb távon is fennmaradhat, a digitális transzformáció gyorsítására ösztönözte a vállalatokat. Azokban a szektorokban is elmozdultak a felhő felé, amelyekben erre korábban kicsi volt a hajlandóság. Mivel azonban hibrid rendszerek jöttek létre (compliance okokból sok vállalat nem teheti minden adatát publikus felhőbe), az IT-biztonsági infrastruktúrának is olyannak kell lennie, ami átfogó védelmet biztosít az on-premise és a felhős rendszerelemekre egyaránt. Egy ilyen rendszer kialakításához, hatékony üzemeltetéséhez újra kell gondolni a vállalati IT-biztonsági stratégiát, beleértve a felhasználóktól megkövetelt biztonsági szabályokat is.

Az új feladatokhoz új emberek is kellenek – esetleg új kompetenciákkal. Ám jó szakembert találni a munkaerőpiacon idén sem lesz egyszerű, jósolja az amerikai *CSO Online*. Az IT-biztonsági szakemberekből eleve hiány volt, és a tavalyi leépíté-

sek nem érintették őket jelentősen – miközben a fenti okokból a kereslet nőtt. (A növekedést jól mutatja az az amerikai adat, mely szerint a járvány előtti állapothoz képest harmadával nőtt a meghirdetett kiberbiztonsági állások száma, csakhogy az álláskeresők száma ennek még a 40 százalékát sem éri el.)

A CISO-nak a kiberbiztonsági stratégia megújításánál ezt mindenképpen figyelembe kell vennie. A szakemberhiány megoldására több út is van: a belső képzés költséges ugyan (kieső munkaidő + tanfolyami költség), de olyan szakemberhez juttatja a szervezet, akinek jó a domaintudása. Együtt lehet működni egyetemekkel (pl. gyakornoki programok), továbbképző intézményekkel is, de ilyenkor rendszerint nem „kész" szakember érkezik a szervezethez. Valamint ott van lehetőségként a szolgáltatás kiszervezése, amikor csak a doimainismeretet igénylő biztonsági területeket viszi saját hatáskörben a szervezet, minden általános biztonsági területet kiszervez szolgáltatóhoz, például egy független Security Operations Centerbe (SOC).

Bharat Mistry, Trend Micro: Az MI egyelőre csak emberrel együtt hatásos IT-biztonsági területen

És ahogy a Trend Micro kutatásában megnyilatkozó IT-vezetők mondják, valóban egyre reálisabb a munkaerő kiváltása mesterséges intelligenciával, illetve az automatizálással is. Érdemes azonban megfontolni a Trend Micro műszaki igazgatójának, *Bharat Mistrynek* az ezzel kapcsolatos figyelmeztetését. Mint a ZDNetnek mondta, az MI hasznos, a fenyegetések elleni védekezésben, de csak emberi szakértelemmel együtt használható.

A műszaki igazgató szerint a vállalatoknak a jelenleginél sokkal nagyobb hangsúlyt kellene fektetniük a biztonságtudatosság oktatására és arra, hogy a biztonsági best practice-eket a távmunkások otthoni működésére is kiterjesszék (személyes eszközök használata, szigorú hozzáférés-ellenőrzés, Zero Trust modell alkalmazása stb.).

Ismét zsarolóvírusok a toplisták élén

2019-ben a szakértők még arra fogadtak, hogy a zsarolóvírusok visszaszorulnak, vagy legalábbis átalakulnak, és már nem a rendszerek titkosítással történő zárolása az elsődleges cél. Ehhez képest tavaly berobbantak a ransomware-ek, amelyek okosabbak és gonoszabbak lettek. Az USA-ban és Kanadában kiberbiztosításokat kínáló Coalition például azt állította, hogy 2020 első félévében az ügyfeleik kárigényének 41 százaléka ransomware-támadás miatt keletkezett.

Mivel sok szervezet (vállalat, egészségügyi és oktatási intézmény, önkormányzat stb.) a pandémia miatt kényszerhelyzet volt, egy globális felmérés szerint legalább negyedük fizetett is a zsarolóknak, csak ne keletkezzen még nagyobb zavar a működésükben – ráadásul nem is keveset: átlagosan 1,1 millió dollárt. Pedig biztonsági szakértők a zsarolók megjelenése óta hangsúlyozzák: a fizetéssel csak újabb támadásokat generálunk.

Ma már egyébként vannak olyan weboldalak, ahol a bűnözők azoknak az adatait teszik nyilvánossá, akik nem hajlandók váltságdíjat fizetni. Ennek ellenére biztonsági szakértők továbbra is fenntartják: nem szabad fizetni, mert semmi sem garantálja, hogy a bűnözők tartják magukat az ígéretükhöz.

Felerősödött tavaly óta a különböző országok kormányai által támogatott hekkertevékenység is. Egy globális felmérésben a válaszadó IT-biztonsági vezetők 87 százaléka nyilatkozott úgy, hogy ezt munkája során is tapasztalja. 73 százalékuk szerint pedig jelenleg ez a támadástípus jelenti a legnagyobb fenyegetést.

Új védelmi fegyverekkel a parancsnoki állásban

Az, hogy a biztonsági kockázatok jelentősen megnőttek az elmúlt egy évben, a vállalatok felső vezetésének (cégvezető, pénzügyi igazgató, igazgatótanács stb.) hozzáállását is megváltoztatta a biztonsági területhez. A járvány kikényszerítette, hogy lépjenek a digitalizációban egy nagyot előre, de továbbra is biztonságban akarják tudni a vállalatukat – például akkor is, ha a dolgozók számottevő része otthonról dolgozik. Mivel a megoldást a CISO-tól várják, ki is terjesztik a jogkörét. Egyes szervezetek egyenesen beemelik a felső vezetésbe. (Jó példa a McDonald's: a vállalat globális CISO-ja, *Tim Youngblood* alelnöki rangban bekerült a cég boardjába.)

Mindazonáltal egy dolgot továbbra sem szabad elfelejteni: a vállalat célja a profittermelés, és a profitot az üzleti oldal hozza. Tehát a jó CISO soha nem az üzlettel szemben, hanem azzal együttműködve, az üzleti célok mentén határozza meg a biztonsági prioritásokat. Ehhez persze az is kell, hogy a CISO képes legyen elmagyarázni az üzleti vezetőknek: a biztonság voltaképpen nagyon is üzleti kérdés.

Forrás: https://bitport.hu/ezek-lesznek-it-biztonsagunk-sarkalatos-kerdesei-iden

Válogatta: Fonyó Istvánné