„ZERO TRUST" MENEDZSELT SZOLGÁLTATÁSOKKAL VÉDEKEZNEK A CÉGEK

Első számú üzleti kockázat: kiberbiztonság

A kiberbiztonság fontosságát jelzi, hogy rekordösszegű kockázati tőke áramlott tavaly a technológiákkal foglalkozó vállalatokba. Az üzleti vezetők is felismerték, hogy a kiberbiztonság a legfontosabb üzleti kockázat. A hibrid iroda jelentette új biztonsági kockázatokat a zero trust mentén szerveződő és a külső menedzselt biztonsági szolgáltatások is megerősítik.

FORRÁS: 123RF.COM

Az üzleti világot érintő rengeteg kihívás és kockázat mellett a kiberbiztonság a vezérigazgatók és az ügyvezető igazgatók legfontosabb üzleti kockázatává nőtte ki magát (az „Alianz Risk Barometer” 11. alkalommal elkészített, 2022-es kiadása szerint). Ez minden kétkedőt meggyőz arról, hogy a kiberháború tényleg minden vállalatot érint, és hogy az IT-biztonsági kockázatokat valahogyan mérsékelni kell.
Ahhoz, hogy a vállalatok hatékonyan meg tudják védeni szervezetüket, szükség van, hogy a döntéshozók tudják, milyen fenyegetettségek ellen kell védekezniük. A kisebb-nagyobb IT-biztonsági csapatok mellett mindezt külső vállalatok vagy menedzselt biztonsági szolgáltatások segítsége nélkül már nem is lehet kellőképpen ellátni.

Rekordösszeg kiberbiztonságra

Az sem meglepő, hogy a befektetési alapok a kiberbiztonságot vonzó befektetésnek tartják. Tavaly ugyanis rekordnak számító 21 milliárd dollárnyi kockázati tőkét fektettek be kiberbiztonsággal foglalkozó vállalkozásokba, egy évvel korábban, ez az összeg csupán 8,9 milliárd dollár volt. Érdekes párhuzam, és biztos, hogy véletlen egybeesés, hogy becslések szerint 2021-ben a bűnözők több mint 20 milliárd dollárnyi kárt okoztak a világnak tevékenységükkel.
Bármekkora összeget fordítanak a befektetők kiberbiztonságra, a támadások száma és gyakorisága nem csökken, ráadásul egyre makacsabbak, kitartóak, célzottabbak és szofisztikáltabbak. Nem meglepő tehát, hogy a vállalatok támadásokkal és fenyegetettségekkel kapcsolatos véleménye is változott. Az idén megjelent „2021 Malware Report” szerint a vállalatok 60 százaléka szerint a kártevők és a zsarolóvírusok extrém fenyegetettséget jelentenek számukra. Csupán 28 százalékuk számolt be moderált veszélyérzetről, míg 12 százalék szerint egyáltalán nem jelentenek fenyegetést vállalatukra, üzleti folyamataikra. A rossz hír, hogy ez a fenyegetettség a jövőben tovább nő. A válaszadók 82 százaléka tart még erőteljesebb zsarolóvírusos támadásoktól, és komolyabb incidenst vár a jövőben. Szerencsére a szervezetek tisztában vannak azzal,

Az IT-vezetők háromnegyede kiemelt fenyegetésnek tartja a home office-t

hogy a kiberbiztonsági események nem kerülhetők el, ez nem az a dolog, ami mindig a szomszéddal történik. A megkérdezettek 97 százaléka véli azt, hogy vállalata kibertámadás célpontja lesz az elkövetkező 12 hónapban, csupán 3 százalékuk tartja ezt a kockázatot nemlétezőnek.

Másképpen dolgozunk már

Az is kirajzolódik a kutatásból, hogy a megváltozott munkavégzés, a hibrid iroda komoly kihívást jelent az IT-biztonság szempontjából a vállalat számára. Hiszen a munkaállomások otthoni környezetbe kerülésével új kockázatok merültek föl. A felmérés szerint a válaszadók 74 százaléka a távoli munkavégzést moderáltól extrémig terjedő fenyegetésnek tartja. A fenyegetettségek ellen a válaszadók

FORRÁS: 123RF.COM

78 százaléka végpontvédelmi megoldásokkal védekezik, míg 70 százalékuk a felhasználók oktatásában és felkészítésében hisz.
A menedzselt IT-szolgáltatások és -megoldások iránt is megnövekedett az érdeklődés a kiberbiztonsági vezetők részéről. A cynet 2022-es CISO-kutatása szerint a kevesebb mint 5 fős kiberbiztonsági csapatokkal rendelkező vállalatok 90 százaléka használ menedzselt detektálási szolgáltatásokat MDR (managed detection and response) néven. Ez óriási változás a 2020-as adatokhoz képest, amikor csak a megkérdezettek 53 százaléka használt hasonló szolgáltatást. Az MDR-szolgáltatások mellett a megkérdezett CISO-k 21 százaléka menedzselt biztonsági szolgáltatásokat nyújtó céget is foglalkoztat, virtuális CISO-t pedig 15 százalékuk vesz igénybe.

Terjednek a „zero trust” megoldások

A menedzselt szolgáltatások terjedése mellett a „zero trust” biztonsági megközelítés is egyre nagyobb teret nyer a vállalati IT-biztonsági infrastruktúra felépítésében. A „zero trust” modell két alapfeltételezésből indul ki:
– a támadó már bejutott a vállalati hálózatba,
– a vállalat által birtokolt hálózat és munkakörnyezet nem különbözik a vállalaton kívüli hálózatoktól, tehát semmivel sem megbízhatóbb annál.
Ebben az új felállásban a bizalmat ki kell érdemelni, alapból senkiben sem bíznak meg. A vállalat folyamatosan elemzi és felméri az eszközök és üzleti folyamatok jelentette kockázatokat, és a kockázatok minimalizálására dolgozza ki védelmét. Az adatokhoz, számítás kapacitáshoz, alkalmazásokhoz és szolgáltatásokhoz csak azok férhetnek hozzá, akiknek valóban szükségük van. Ez az jelenti, hogy folyamatosan ellenőrizzük és engedélyezzük az összes hozzáférési kérés biztonsági besorolását. ■