A legmagasabb szintű kiberbiztonság ma már a kisvállalkozások számára is megfizethető

A BlueVoyant kelet-közép-európai, valamint a közel-keleti térségekért felelős értékesítési igazgatója osztotta meg a gondolatait a kiberbiztonság hazai helyzetéről

Azok a kis-, és középvállalkozások, amelyek felhőtechnológiát használnak, jellemzően fejlettebb kibervédelemmel rendelkeznek – véli Csendes Balázs, a kibertér felől érkező kockázatok feltárására és leküzdésére szakosodott BlueVoyant értékesítési igazgatója. A magyarázat szerinte részben az, hogy a Microsoft Azure kibervédelmet támogató technológiával rendelkezik és részben az is, hogy az Azure-t használó szervezetek rendszerint tudatosabban készülnek a kibertérből rájuk leselkedő veszélyek kivédésére. A kiberbiztonsági szolgáltatások megrendelői Magyarországon egyelőre elsősorban a középvállalatok. A piac további bővülését bizonyos tévhitek is akadályozzák – főként ezekről kérdeztük a szakembert.

Az amerikai székhelyű BlueVoyantot 2017-ben New York-ban alapították. A mára iparágvezető kibervédelmi vállalat mintegy 30 országban több mint 900 ügyfél számára nyújt kiberbiztonsági megoldásokat, hazánkban két éve van jelen. A magyar műveleti központ (SOC) munkatársai a hét minden napján, a nap 24 órájában kiszolgálják a cég ügyfeleit nem csupán Magyarországon, hanem világszerte. A BlueVoyant havonta mintegy félmillió kiberbiztonsági incidenst kezel, rendkívül rövid, néhány perces reakcióidővel. A vállalat ezért széleskörű tapasztalatokkal rendelkezik a támadások természetéről, és arról is, hogy milyen tényezők befolyásolják a globális kiberbiztonsági piacot.

Csendes Balázs szerint Magyarország jelenleg belesimul a saját régiójába az információbiztonsági szolgáltatások penetrációja tekintetében, ami elmarad a nyugat-európai, de a balti országok szintjétől is. „Úgy látjuk, hogy a kiberbiztonsági szolgáltatások iránti keresletet a felhőtechnológia elterjedtsége is befolyásolhatja” – magyarázza a szakember. Erre példaként említi a Covid19-járvány alatt a felhőmegoldások hirtelen terjedését.

Magyarországon a BlueVoyant ügyfélkörébe tipikusan az 500-3000 főt foglalkoztató közép- és nagyvállalatok tartoznak. Az értékesítési igazgató szerint idehaza jellemzően ez az a cégméret, ahol a kibervédelem igénye tudatossá válik. A kiberbiztonsági piac Magyarországon érezhetően bővül, ugyanakkor bizonyos, széles körben elterjedt tévhitek továbbra is gátjai a gyorsabb növekedésnek. Ezeket a hiedelmeket foglalta össze számunkra Csendes Balázs.

Tévhit 1 – Rendelkezünk biztonsági eszközökkel, tehát védve vagyunk

A biztonság feltételei a kibertérben folyamatosan változnak. Abban az esetben sem feledkezhetünk meg erről, ha egyébként a szokásos tűzfalat és hálózatvédelmi eszközöket működésbe állítottuk. A szervezeteknek a nap 24 órájában, folyamatosan ellenőrizniük kell a hálózataik integritását, amihez a fegyvertárukat is karban kell tartani – vagy rá kell bízniuk ezt a feladatot egy profira. Csak ebben az esetben válnak ugyanis láthatóvá az infrastruktúrán belüli változások, és válik lehetővé az azonnali válasz az esetleges incidensekre. A szervezeteknek nyomon kell követniük az új biztonsági fenyegetések megjelenését is, és ennek megfelelően kell frissíteniük a védekezésben használt eszközeiket.

A felhőtechnológia igénybevételével a biztonság iránti felelősség megoszlik a felhőszolgáltató és a felhasználó között. Ám nem célszerű a védelmet teljes egészében a felhőszolgáltatóra bízni. A szervezeteknek azért is folyamatosan ellenőrzés alatt kell tartaniuk a saját infrastruktúrájukat, mert mindig számolniuk kell azzal, hogy még a legjobban védett rendszereket is meg lehet hekkelni.

A megfelelő kibervédelem fontosságát a jogszabályalkotók is felismerték, a biztonságos kibertér kiépítése érdekében egyre szigorúbb kibervédelmi elvárások és intézkedések születnek. Ilyen például a közelmúltban hatályba lépett módosított kibervédelmi direktíva (NIS2), amely az egész Európai Unión belül szabályozza a kiberbiztonság erősítését célzó törekvéseket. A módosítás jelentős változásokat tartalmaz: új kötelezettségeket ír elő, bővül az érintettek köre és a szervezetek akár több milliós bírságot is kaphatnak mulasztás esetén.

Érdemes tehát valóban komolyan venni a fenyegetéseket, mert a hagyományos védelmi eszközök mára nem jelentenek teljes körű védelmet.

Tévhit 2 – A felhő nem biztonságos

Sokan úgy vélik, biztonságosabb a szerverparkot a telephelyen üzemeltetni, mint felköltöztetni a felhőbe. Pedig ennek éppen az ellenkezője az igaz. Az on-premise rendszerek általában kevésbé védettek, sérülékenyebbek, mint a felhő, hiszen a vállalatoknál általában nincsenek meg sem az infrastrukturális feltételek, sem a szakértelem a megfelelő védelem kiépítéséhez. Támadás viszont ugyanúgy érheti őket, mint a felhős rendszereket. A kiberbűnözők ma már rendkívül szervezetten és cégszerűen működnek, ahol a feladatok gondosan fel vannak osztva. Folyamatosan keresik a sérülékenységeket. Sőt, értékesítik is az általuk kifejlesztett, egyre kifinomultabb módszereket alkalmazó vírusokat és egyéb rosszindulatú szoftvereket, különböző sikerrátákat ígérve. Ezek ellen hatékony védelmet csak a felhőszolgáltatásokba eredendően beépített technológiák (Defender Exploit Guard, Azure Sentinel, stb.), és az információvédelemre szakosodott szolgáltatók tudnak nyújtani. „Fontos megérteni, hogy a felhő nem „egy másik számítógép valahol máshol”, ahogy azt sokan feltételezik, hanem – és erre az Azure tökéletes példát nyújt – egy szolgáltatás. Ilyen standardizált szolgáltatás a biztonság is, amelyet használatarányosan vesz igénybe a felhasználó” – magyarázza a szakember.

Tévhit 3 – Különböző igények, különböző kiberbiztonsági szolgáltatások

Más védelmet kíván meg egy biztonságkritikus szektorban tevékenykedő nagyvállalat, mint egy KKV – gondolják sokan azok közül, akik nem ismerik a kibertámadások természetét. Csendes Balázs hangsúlyozza: a kiberbiztonság elvárt szintjét illetően nincs különbség a vállalatok között sem méret, sem iparág szerint, mert mindegyikük ugyanazoknak a támadásoknak van kitéve. Valójában minden vállalkozást az elérhető legkorszerűbb technológiával érdemes védeni a kibertámadásokkal szemben, és ez ma már egyáltalán nem megvalósíthatatlan. Néhány éve még valóban csak a „nagyok” engedhették meg maguknak a magasszintű kiberbiztonságot, ám mára ez bármely vállalkozás, akár a néhány főt foglalkoztató kisvállalkozások számára is megfizethetővé és beszerezhetővé vált. A korszerű technológia így egyenlíti ki a versenyfeltételeket és „demokratizálja” a piacot. „A BlueVoyant gyakorlatilag azért született meg, hogy ugyanazt a biztonságot, amely egy évtizede még a nagyok luxusa volt, elérhetővé tegye a KKV-k számára is. A célunk az, hogy egy kisvállalkozás is ugyanazt a magas szintű szolgáltatást kapja meg, mint az állami szervek vagy nagybankok.”

Tévhit 4 – Drága, úgysem tudom megfizetni

„A nagyvállalatok képesek megfizetni a biztonságot, a KKV-k nem engedhetik meg ezt maguknak” – szól az érvelés. „Sokszor azért sem jutunk el az ügyfélhez, mert már eleve esélytelennek érzi az együttműködést velünk a feltételezett magas ár miatt” – erősíti meg Csendes Balázs. A nagyok is komolyabb kiadásra számítanak, ezért néha úgy döntenek, inkább rábízzák a feladatot a saját munkatársaikra, és kiépítik a kibervédelemhez szükséges fizikai infrastruktúrát maguk – ennek a költsége a valóságban egészen biztosan sokkal magasabb, mint havidíjas szolgáltatásként megrendelni az információvédelmet egy olyan cégtől, amely erre szakosodott. Egy olyan vállalatnál, mint a BlueVoyant, már kiépültek a feltételek és rendelkezésre áll a szaktudás is a feladat elvégzéséhez. „A szolgáltatásaink standardizáltak, ezért tudunk egyszerre több száz ügyfelet kiszolgálni viszonylag alacsony erőforrásigénnyel és költséghatékony módon” – mondja Csendes Balázs.

Tévhit 5 – Kicsi vagyok, miért épp engem támadnának?

A kiberbűnözők éppenséggel a kicsikre utaznak. Egyfelől azért, mert a feltételezésük az – és néha joggal –, hogy kevésbé védettek, másfelől rajtuk keresztül tudnak betörni a jól kiépített védelemmel rendelkező nagyvállalatokhoz, amelyeknek a kisebbek a beszállítói. Ismert példa, amikor egy olyan tajvani, viszonylag kis vállalatot ért sikeres kibertámadás, amely után annak partnerét, az Apple-t zsarolták meg a bűnözők. A nagyvállalatokat könnyen érhetik támadások nemcsak a leggyakoribbnak tekinthető közvetlen phishing behatolási kísérletek révén, hanem közvetett módon, a saját beszállítóik oldaláról is. Erre hívja fel a figyelmet az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) 2022-es jelentése is, amely megállapítja az elmúlt év legfontosabb kiberbiztonsági trendjeit, köztük a beszállítói lánc fokozott sérülékenységét. A kiberbűnözők ugyanis érzékelhetően nagyobb érdeklődést mutatnak az ellátási lánc iránt: egy-egy sikeres támadással képesek megbénítani a teljes beszállítói láncot, ezzel ellehetetlenítve nem csupán a megtámadott vállalat, hanem az összes többi érintett cég működését is. Szintén az ENISA egy másik beszámolója 2030-ig a top 10 kiberfenyegetés közé sorolja az ellátási lánc kompromittálódását.

A kiberfenyegetés céges és vállalati mérettől független veszély – ráadásul a hiperméretű fenyegetések világában minden szervezetnek szofisztikált és az elérhető legmodernebb védelemre van szüksége. Csendes Balázs szerint a mai védelmi rendszerek egyik legpozitívabb tulajdonsága, hogy a védelem szintje és erőssége ma már minden vállalati méretben rendelkezésre áll és a különböző árazási modellek révén elérhetők is.

Sajtókapcsolat:

- Kovács Ágnes Veronika, PR és vállalati kommunikációs vezető
- +36 1 267 4636
- sajto@microsoft.com

© Microsoft
Csendes Balázs, BlueVoyant értékesítési igazgató

Eredeti tartalom: Microsoft

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el: https://hellosajto.hu/2083/a-legmagasabb-szintu-kiberbiztonsag-ma-mar-a-kisvallalkozasok-szamara-is-megfizetheto/