Egészséges kétkedés és profi szolgáltatás az IT biztonság kulcsa

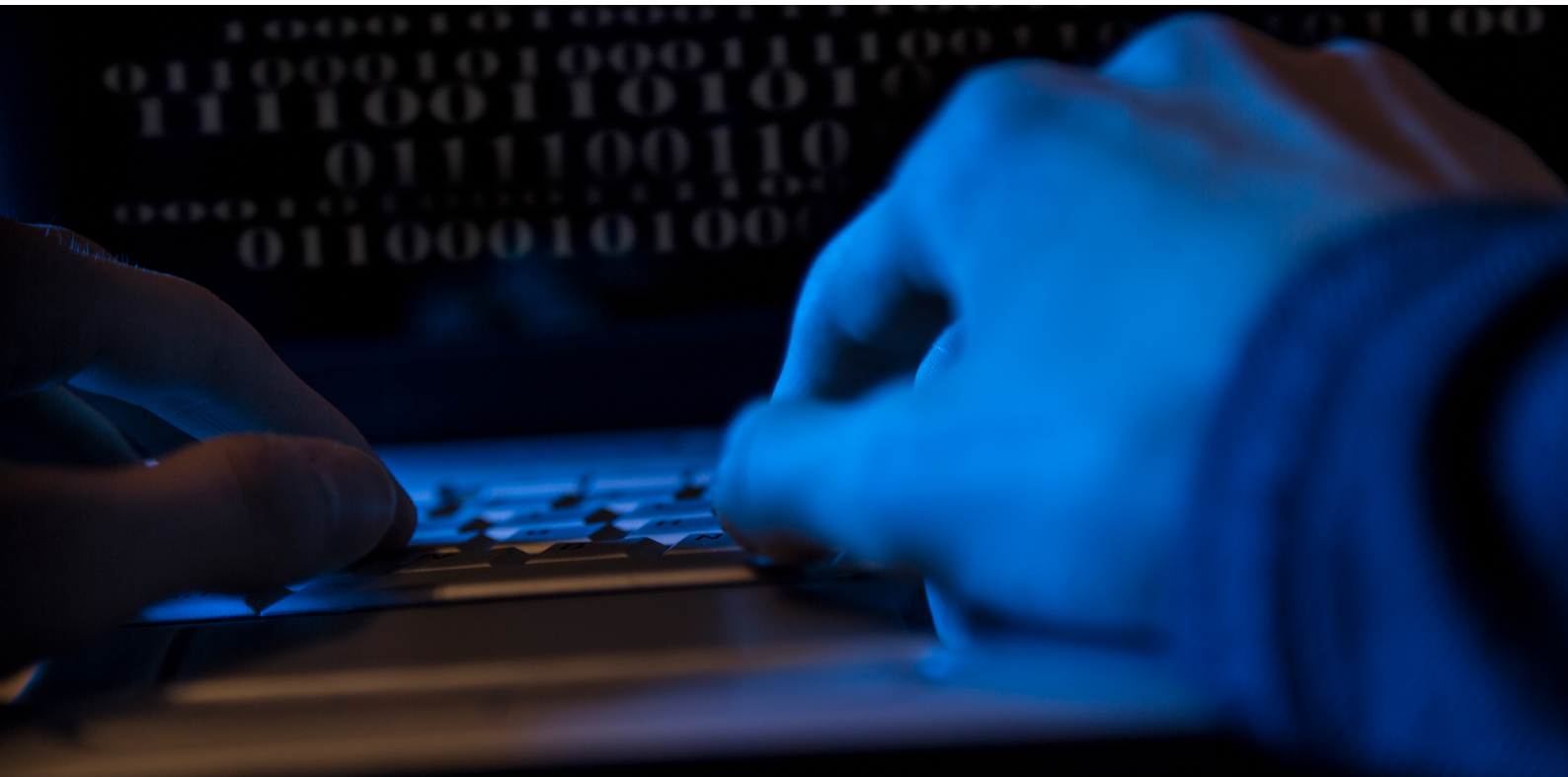
Teljesen természetesnek vesszük, hogy irodáinkat, épületeinket és az ott található értékeket védjük a fizikai behatolóktól. Miért nem fordítunk akkor legalább ugyanekkora figyelmet számítógépes rendszereink és adataink védelmére, és akadályozzuk meg, hogy megbénítsák szervezetünk, vállalatunk működését?
Az ehhez szükséges eszközök ugyanolyan könnyen elérhetőek, mint a fizikai védelem.

Microsoft

Egészséges kétkedés és profi szolgáltatás az IT biztonság kulcsa

A legtöbb vállalat vagy intézmény vezetője még mindig nem veszi elég komolyan a kibertámadások jelentette fenyegetéseket. Pedig a rosszindulatú kódok és támadások száma és költsége folyamatosan nő szerte a világban. A Cybersecurity Ventures tanulmánya szerint 2021-ben a kiberbűnözés 6 ezer milliárd dolláros kárt okoz a világgazdaságnak. Ez már önmagában is óriási összeg – a kiberbűnözés ezzel az USA és Kína mögött a harmadik legnagyobb gazdaságnak mondható a világon --, de évente 15 százalékkal még emelkedik is, így 2025-re meghaladja majd a 10 ezer milliárd dollárt. Ehhez képest 2017 és 2021 között összesen 1 ezer milliárd dollárt költöttek globálisan védekezésre a cégek és más szervezetek.

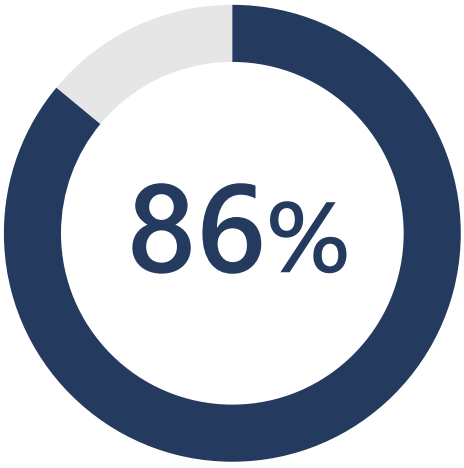
Ráadásul egyetlen szervezetet sem véd meg az, hogy kicsi és magyar – az automatikus terjedő támadásokat nem érdekli, hogy ki hol van a világban, csak az, hogy kit lehet megfertőzni. 2016-ban például több magyar kórházat is ért zsarolóvírusos támadás. Akkor az intézmények gyorsan tudtak reagálni, és biztonsági mentéseik is voltak az adataikról, így kisebb döccenőkkel megúszták az incidenseket. De nem mindig és nem mindenki jár ilyen szerencsével: az időben fel nem fedezett zsarolóvírus a szervezet összes adatát (még a biztonsági mentéseket is!) elérhetetlenné teheti, megbénítva ezzel a működést. Ennek kapcsán nem árt emlékezni arra, hogy az állami szektorban a vezetők személyesen felelősek azért, hogy az alájuk tartozó szervezet információbiztonsági szempontból rendben legyen.



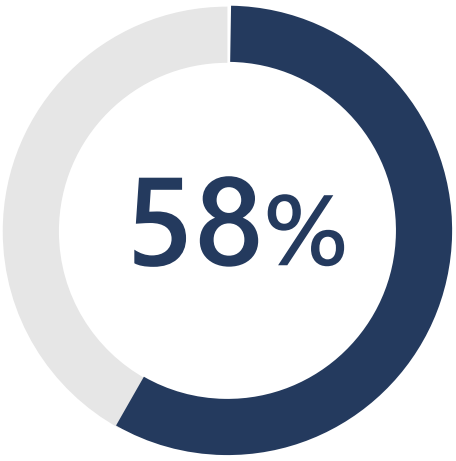
A kiberveszélyeket két nagy csoportba lehet osztani, és egyáltalán nem biztos, hogy az a veszélyesebb, amelyik látványosabb. Az egyik nagy csoportba azok a támadások tartoznak, amikor a hackerek gyorsan akarnak pénzt szerezni. Betörnek a rendszerekbe, látványosan felhívják magukra a figyelmet, és jelentkeznek a pénzért. Tipikusan így működnek a már említett zsarolóvírusok.

A másik nagy csoportot a rejtőzködő támadások alkotják. A támadók elsődleges célja itt az, hogy hozzáférést szerezzenek a rendszerekhez, majd észrevétlenül meglapuljanak, és minél több információt megpróbáljanak kiszivattyúzni a megtámadott szervezetből. Mivel a rendszerek működését nem gátolják, sokszor csak évek múltán leplezik le őket, addig pedig folyamatosan szabadon gyűjtik az adatokat. Az áldozat lehet gazdasági társaság vagy állami szervezet, intézmény – előbbitől üzleti információkat és titkokat, utóbbiaktól államtitkokat lehet megszerezni. A támadók között megtalálhatjuk a bűnözői köröket és az állami szereplőket – de hogy a kép bonyolultabb legyen, a nemzetállamok megfelelő szervei is gyakran a velük együttműködő bűnözői csoportokkal végeztetik el a piszkos munkát.

Pontosan a rejtőzködő támadások miatt sok vezető ringatja magát hamis biztonságérzetbe – „nem észleltünk támadást, hát minden rendben van, és különben is, tavaly vettünk biztonsági szoftvereket”, mondják gyakran. Ez a hozzáállás gyakoribb, mint gondolnánk. Egy nemrégiben elvégzett közös Microsoft-IDC felmérésben az első számú vezetők 86 százaléka nyilatkozott úgy, hogy elégedett vállalata biztonsági felkészültségével.

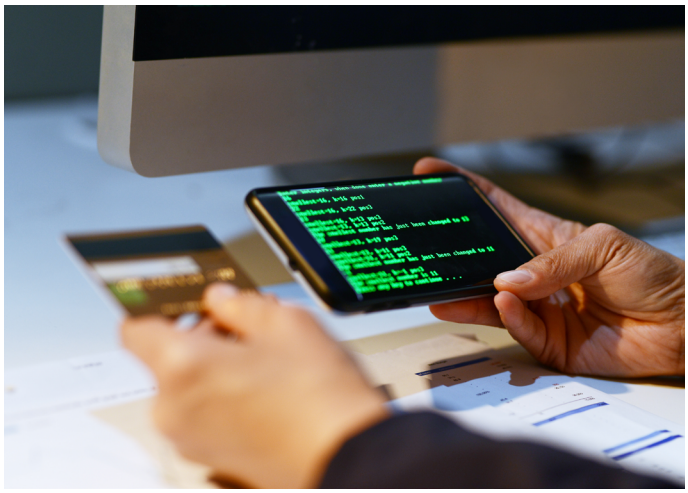


Ennek ellenére a többségük (86%) általában véve elégedett saját IT-rendszereinek biztonságával.



A cégek 58%-ának nincs átfogó biztonsági stratégiája.

Pedig az efféle elégedettség végzetes lehet. Az információvédelmi szakértők szerint kétféle szervezet van: amelyiket már megtámadták, és amelyik még nem tud róla. A kiberveszélyek világa folyton változik, ezért a védekezésben is újra és újra alkalmazkodni kell a friss kockázatokhoz. Nem elég egyszer kiépíteni egy védelmi rendszert, azt folyamatosan frissíteni, fejleszteni is szükséges, hogy képes legyen ellenállni a legújabb fenyegetéseknek. A hatékony védekezéshez az is elengedhetetlen lenne, hogy a szervezet valós időben figyelje a rendszereit, hálózati forgalmát – ehhez képest a szervezetek több mint fele még csak ezután tervezi egy erre képes rendszer beszerzését. Mindezeken túl arról sem szabad megfeledkezni, hogy a biztonsági láncolatban a leggyengébb szem többnyire az ember: a nem elég óvatos, a felelőtlen vagy éppen lusta felhasználó. A COVID-járvány alatt teret nyert távmunka pedig számos esetben csak újabb réseket nyitott az IT-biztonság eddig sem hermetikusan záródó falán.



No de milyen konkrét támadási formák ellen kell védekeznie a szervezeteknek? Az egyik leglátványosabb veszély a zsarolóvírus. A már említett felmérés szerint a vezetők ettől félnek a legjobban – nem feltétlenül azért, mert ez a legveszélyesebb, hanem mert az utóbbi évek publicitása miatt ezt ismerik a legjobban.

A veszély ettől még valós. Ha egy ilyen kártevő bejut a rendszerbe, villámgyorsan képes titkosítani az összes adatot, gyakorlatilag egy szempillantás alatt működésképtelenné téve a szervezetet. A támadók pénzt – időnként nagyon komoly összegeket – kérnek azért, hogy megadják a titkosítást feloldó kódot, az áldozat pedig kénytelen fizetni, különben búcsút inthet adatainak. Újabban már egy újfajta változata is megjelent a támadásnak: a bűnözők már azért is pénzt kérnek, hogy a megszerzett bizalmas adatokat ne tegyék közzé az interneten.

Korántsem ennyire látványos és azonnali következményekkel járó, ám potenciálisan annál pusztítóbb fenyegetés az adathalászat, ami gyakran csak az első lépés a további támadások felé. Ez az áldozat gyanútlanságára, jóhiszeműségére alapoz. A támadók egy hivatalosnak látszó és első pillantásra megbízhatónak tűnő címről érkező levelet juttatnak el az áldozat postaládájába, és arra kérik, hogy a mellékelt linkre kattintva adjon meg bizonyos adatokat, cserélje le a jelszavát és így tovább. Mondanunk sem kell, hogy a betöltődő oldalt a kiberbűnözők üzemeltetik, és az ott megadott adatok már őket gazdagítják. Ha sikerül céges felhasználói azonosítókat és jelszavakat is kicsalniuk, máris szabadon besétálhatnak a vállalati rendszerekbe. Amióta pedig számítógépek vezérelnek gyakorlatilag mindent, a kiberbűnözés már nem csak az informatikai rendszereket, hanem fizikai világunkat is veszélyezteti. Ha a támadók átveszik a hatalmat az irányító számítógépek felett, szó szoros értelemben katasztrófákat tudnak előidézni. Nem kell különösebb képzelőerő ahhoz, hogy milyen következményekkel járhat, ha külső kontroll alá kerül egy repülésirányítási rendszer, egy vízközmű, egy erőmű vagy akár csak egy gyár termelésirányítási rendszere.

Nem túlzás tehát azt állítani, hogy a kibervilágban háború dúl. Az egyik oldalon ott sorakoznak a támadók – sokan vannak, jól képzettek, komoly anyagi és emberi erőforrások felett rendelkeznek, és szeretnék megszerezni, ami a miénk, legyen az pénz, üzleti titok vagy másféle adat. A másik oldalon vagyunk mi, akiknek folyamatosan védekeznünk kell.

A kiberháború megvívásában meglepően sokat tanulhatunk az igazi háborúktól. Képzeljük el, hogy egy erőd urai vagyunk, az erődben pedig ott él, dolgozik számos ember, és ott halmoztuk fel mindazokat az értékeket is, amelyek a túlélésünket biztosítják. Tudjuk, hogy az ellenség folyamatosan a közelünkben ólálkodik és a mi javainkra fáj a foga. Mit teszünk ilyenkor? Először, is nem engedünk be akárkit a várfalakon belülre. Az a minimum, hogy a kapuknál őrség áll, és minden belépni szándékozótól megkérdi a nevét és a jelszót, sőt, azt is megnézi, hogy tényleg az akar-e belépni, akinek a jelszó ki lett adva. A különösen védett helyekre (kincstárba, fegyverterembe) csak válogatott emberek és ők is csak külön jelszó birtokában léphetnek be. A megfelelő helyekre videokamerákat szerelünk fel (modern erőd vagyunk…), a felvételeket pedig megőrizzük, hogy tudjuk, mi zajlott az erődön belül. No de még jobb lenne, ha rögtön észrevennénk a nemkívánatos eseményeket. A videokamerák képét ezért nem csak rögzítjük, hanem az őrök folyamatosan nézik is a monitorokat, és ha szükséges, beavatkoznak. Mindeközben védjük a terveinket, titkainkat is. A fontos dokumentumokat jól védett páncélteremben őrizzük, de a többit sem hagyjuk szerteszéjjel, nem bízzuk akárkire, az üzeneteket pedig titkosírással küldjük, hogy az ellenség akkor se értse, ha elfogja a levelünket.

A fenti elemek mindegyike megfeleltethető az informatikai védelmi megoldásoknak és alapelveknek is. Az erődbe való bejutást és a helyiségek közötti közlekedést felhasználóazonosítással, jelszó- és jogosultságkezeléssel lehet megoldani. A történéseket figyelő videokamerákat a naplóállományok gyűjtése helyettesíti: ezekben benne van, hogy ki, mikor, milyen rendszerben mit csinált. Az élő videoképeket figyelő őrök informatikai megfelelői az incidenskezelő rendszerek, amelyek központi helyre gyűjtik és valós időben elemzik a naplóállományokat, hogy villámgyorsan észleljék a gyanús tevékenységeket. A tárolt adatokat titkosítjuk, és titkosított csatornát használunk külső kommunikációra is.

Az információbiztonság terén mostanában az egyik legfontosabb trend az úgynevezett teljes felügyelet (zero trust) megközelítés. Alapelve az egészséges paranoia. Abból indul ki, hogy minden rendszer fel lett törve, az ellenség már a kapukon belül van, folyamatosan támadás alatt állunk – vagyis a legélesebben szemben áll azzal a hamis elégedettséggel, amely a legtöbb első számú vezető sajátja. Ennek megfelelően a védelmi rendszert arra utasítjuk, hogy senkiről és semmiről ne higgye el, hogy az, aminek látszik. Ne a korzón sétálgató emberhez hasonlítson, hanem tegyen úgy, mintha aknamezőn lépdelne, és közben azt lesi, hogy honnan jöhet a következő támadás.

A teljes felügyelet megközelítésben a legfontosabb védendő értékek között szerepelnek a felhasználói identitások, az adatok és az eszközök. Az identitások védelmére szolgálnak az említett felhasználó-azonosító és jogosultságkezelő rendszerek, mint a Microsoft Active Directory. Egy ilyen rendszer garantálja, hogy valóban csak az jusson be a rendszerekbe, akinek erre felhatalmazást adtunk, és ott csak azokhoz a rendszerekhez, alkalmazásokhoz és adatokhoz férjen hozzá, amelyek a munkájához feltétlenül szükségesek. Központilag szabályozható, hogy milyen erősségű jelszót kell használni, azt milyen gyakran kell cserélni, szükség van-e egyéb azonosításra (például sms-ben kapott kódra). Ugyanakkor a felhasználók életét is megkönnyíthetjük, mert egyszeri bejelentkezéssel hozzáférhetnek minden alkalmazáshoz, amelyhez jogosultságot kaptak. Szintén a központi menedzsment akadályozza meg, hogy emberhez már nem rendelt, de a támadók által kihasználható „alvó” identitások legyenek a rendszerben.

Az adatok védelme minden szervezet számára az egyik legfontosabb információbiztonsági feladat, mind a saját működőképességének biztosítása, mind a jogszabályi megfelelések (például a GDPR) szempontjából. Védeni kell az adatokat tárolás, feldolgozás és küldés közben is. Ennek első lépése, hogy fel kell mérnünk, milyen adatokkal is rendelkezünk, majd ezeket osztályokba kell sorolni érzékenységük szerint – ez alapján dönthetjük el, hogy milyen adattípushoz milyen védelmet alkalmazzunk. Titkosíthatjuk az adatokat a szervereken, a felhasználói számítógépeken és titkosíthatjuk őket akkor is, amikor elhagyják a szervezetet. Ennek köszönhetően akkor sem ér kár bennünket, ha ellopják az adatainkat vagy elvész egy laptop, mert a támadó semmit nem tud kezdeni a birtokába jutott adatokkal. Megfelelően beállított szabályokkal megakadályozhatjuk azt is, hogy az értékes dokumentumok, állományok kijussanak a szervezeten kívülre, mert mondjuk nem engedélyezzük, hogy külső e-mail címre továbbítsák őket, átmásolják a vágólapra vagy akár kinyomtassák. A Microsoft adatvédelmi megoldásai révén automatizálható az adatok biztonsági besorolása, és házirendek alakíthatók ki a hozzáférés korlátozására. A zero trust értelmében a felhasználói tevékenységet is ellenőrizzük, és ha felelőtlen vagy kártékony tevékenységre utaló nyomot találunk, egyből beavatkozunk.

Az eszközök védelme is fontosabb, mint valaha. A vállalati rendszereket már nem csak az irodában működő, könnyebben védhető számítógépekről érik el a felhasználók. A végpontok között van céges és saját laptop, tablet, mobiltelefon, a legkülönfélébb operációs rendszereket futtatva és sok esetben megkérdőjelezhető biztonsági állapotban. Ilyen körülmények között létkérdés, hogy tisztában legyünk azzal, milyen eszközökről próbálnak hozzáférni hálózatunkhoz, alkalmazásainkhoz, adatainkhoz. Itt nyer igazán értelmet a teljes felügyelet „semmiben se bízz, mindig ellenőrizz" alapelve. Ennek értelmében minden, a vállalati rendszerekhez hozzáférő végpontot, a céges Windowsos laptoptól a dolgozó tulajdonában lévő Apple okos óráig ugyanazoknak a biztonsági procedúráknak vetünk alá, akár a vállalati hálózatról, akár az otthoni wifiről, akár egy kávézóból jelentkezik be. Ezek a központilag meghozott és betartatott szabályok döntik el, hogy az eszközre kell-e biztonsági frissítést telepíteni, mielőtt engedjük a hozzáférést; fertőzött-e az eszköz, jelent-e veszélyt a rendszereinkre; és végül, hogy mihez kaphat hozzáférést az eszköz.

Fontos elemét alkotják a teljes védelmi környezetnek azok a rendszerek, amelyek a védelmi infrastruktúra összes eszközéről egy helyre gyűjtik a jelzéseket, adatokat, majd ezek között összefüggéseket keresnek. Az ilyen rendszerek, mint a Microsoft Sentinel is, folyamatosan monitorozzák az informatikai rendszereket és összefüggéseket keresnek az egyes események között. Önmagában ugyanis egy-egy esemény nem feltétlenül jelez veszélyt, de bizonyos körülmények együttállása már támadásra vagy belső visszaélésre utalhat.

Egy fájl letöltése nem gyanús; de ha egy felhasználó öt másodperc alatt tízezer fájlt tölt különböző helyekről, biztosan egy kártékony program élt vissza az azonosítójával. Egy felhasználó létrehozása mindennapi eset. De ha a rendszergazda létrehoz egy magas jogosultságokkal rendelkező felhasználót, majd húsz perc múlva törli, feltételezhető, hogy rosszban sántikál. Ha a rendszer ehhez hasonló gyanús jeleket észlel, egyből riaszt és szükség esetén be is avatkozik. Egy ilyen biztonsági megoldás az utólagos nyomozásban is sokat segíthet: egy támadás után vissza lehet fejteni, hogy hol jött be a támadó, milyen sérülékenységet használt ki, milyen rendszerekhez fért hozzá.

Mindez talán bonyolultnak hangzik, és valóban nem egyszerű. Megpróbálhatunk saját belső erőforrások felhasználásával védekezni a kiberháborúban, ahogy képzeletbeli erődünket is védhetjük egy maroknyi saját katonával, de a siker mindkét esetben legalábbis kétséges. Ahogy említettük, a támadók sokan vannak és jól felszereltek; ha ők drónokkal és rakétákkal jönnek, nem sokat érnek ellenük a kézifegyverek. A szakképzett, tapasztalt információbiztonsági szakember ráadásul ritka, mint a fehér holló, sokba kerül és többnyire és specializált IT-biztonsági cégeknél dolgozik. A szervezetek többsége nem engedheti meg magának, hogy a veszélyekkel egyenrangú védelmi csapatot és eszköztárat hozzon létre magának.

Jobban járunk, ha profi katonákra bízzuk az őrzést, akik számtalan más erődöt is védenek, tudják, hogy mire kell figyelni, hogyan kell kiépíteni és hatékonyan működtetni a védelmi rendszert. Nekik vannak olyan fegyvereik is, amelyeket mi nem engedhetünk meg magunknak és használni sem tudunk. És ami talán még fontosabb: saját belső kommunikációs rendszerükön keresztül értesülnek arról, ha szomszédos, vagy akár a távolabbi erődöket támadás éri, és még azelőtt felkészülnek, hogy a betolakodók megjelennének a kapunk előtt.

Ilyen profi csapattal rendelkezik a Microsoft is, amely a globális fenyegetésekre globális válaszokat tud adni a felhőből kínált biztonsági szolgáltatásaival. A vállalat szerte a világon több milliárd ügyfelet szolgál ki, így a vállalatok és szervezetek igen széles spektrumából tud biztonsági információkat gyűjteni az egész Földet behálózó szenzorhálózata révén. A bejövő adatokat 77 országban több ezer biztonsági szakember elemzi, és az így megszerzett tudás alapján teszi meg a szükséges lépéseket. A felhő alapú rendszereket pillanatok alatt frissíteni lehet. Ha a Microsoft szakemberei észlelik, hogy hackerek új támadási módszereket alkalmaznak, a mintázatok azonnal bekerülnek a biztonsági megoldásokba is, és mire a támadás eléri Magyarországot, már hatástalannak bizonyul. Ezt a fajta reagálóképességet és gyorsaságot helyben telepített védelmi rendszerekkel nem lehet biztosítani, de a globális szolgáltatók közül is kevesen képesek rá.

Mivel a támadók a legmodernebb, automatizált felhős megoldásokat használják, ugyanilyen eszközökkel kell védekezni is. A Microsoft biztonsági felhőszolgáltatásaival a legújabb technológiákat alkalmazó és a legfrissebb tudást magába foglaló megoldást kapunk, amihez jól képzett, harcedzett szakembergárda is a rendelkezésünkre áll. Nekik köszönhetően nem kell azonnal óriási költségekbe vernünk magunkat, mégis nagyobb biztonságban tudhatjuk szervezetünket, mintha kizárólag saját erőforrásokkal próbálnánk védeni rendszereinket. Néhány felhőszolgáltatás igénybevételével biztosíthatjuk, hogy a kibertérből érkező támadások 99 százaléka hatástalanul pattanjon le szervezetünkről.

Előzetesen szakemberek segítségével érdemes felmérnünk, milyen a biztonsági rendszerünk állapota, hol vannak hiányosságaink, hol kell erősíteni a védelmet. Ebből az is kiderül, hogy milyen kockázatokkal kell szembenéznünk, és milyen üzleti előnyökkel jár ezen kockázatok csökkentése. Az így előálló biztonsági stratégiában már konkrét számokkal lehet alátámasztani, hogy milyen megoldásra miért van szükségünk és miért éri majd meg a szervezetnek azok igénybevétele.

A közhiedelemmel ellentétben a felhőszolgáltatások az állami szféra vállalatai elől sincsenek elzárva – az információbiztonsági (2013:L) törvény szigorúbb passzusai nem vonatkoznak rájuk. A felhő és a helyi infrastruktúra nem zárja ki egymást, sőt hatékonyan ötvözhetők és kimondottan előnyökkel jár az integrációjuk. A vírushelyzet világosan megmutatta, hogy könnyen előállhatnak olyan helyzetek, amikor hirtelen kellenek újabb rendszerek, alkalmazások, kapacitások – a saját infrastruktúra bővítése viszont sokáig tart, miközben a felhőben gyakorlatilag néhány kattintással lehet újabb és újabb kapacitásokat, szolgáltatásokat vásárolni.

A felhő persze nem csak biztonsági szolgáltatásokra vehető igénybe, hanem az irodai rendszerektől kezdve a levelezésen át a biztonsági mentésekre számtalan feladatra. Bármelyiket is vegyük igénybe, számolhatunk az alábbi előnyökkel:

- egyszerűsödik a belső üzemeltetés (frissítések, patchek telepítése automatikusan történik)
- jól integrálható a belső rendszerekkel – nem kell kitenni a felhőbe, amit nem akarunk, a szervezetben meglévő szaktudás nem vész el
- nem kell beruházni az induláskor, a szükséges költségek jól kalkulálhatóak
- folyamatosan rendelkezésre áll a szakértelem, nem jelent veszélyt, ha kilép egy-egy kulcsember – a felhős megoldások beépítve tartalmazzák a legjobb gyakorlatokat
- igény szerint, villámgyorsan bővíthető szolgáltatások és kapacitások, amelyek lekapcsolhatóak, ha már nincs rájuk szükség
- a távoli munkavégzés egyszerű és biztonságos megvalósításának lehetősége

Microsoft

Amikor sokba került a zsarolóvírus

1.

ISS World

A dán céget 2020 februárjában érte támadás, aminek következtében alkalmazottak ezrei voltak képtelen elérni az alkalmazásokat, e-maileket. A rendszerek feletti ellenőrzések visszaszerzése és az üzleti alkalmazások újraindítása becslések szerint 74 millió dollárjába került a vállalatnak.

2.

University of California San Francisco

A UCSF orvosi karát érte támadás júniusban, de azt sikerült megakadályozni, hogy a fertőzés továbbterjedjen. A végén az egyetem több mint 1 millió dollár váltságdíjat kifizetett az eredetileg kért 3 millióból, csak hogy ne vesszenek el pótolhatatlan kutatási anyagok.

3.

Egyetemi kórház, Düsseldorf

Szeptemberben a düsseldorfi egyetemi kórház több mint 30 belső szerverét fertőzték meg, így kénytelen volt felfüggeszteni a sürgősségi ellátást. Ennek következtében meghalt egy nő, akit egy 30 kilométerrel távolabbi kórházba kellett átirányítani. A támadók végül ingyen megadták a titkosítást feloldó kódot, miután a német rendőrség emberölésként vizsgálta az esetet.

4.

Argentin határőrség

Egy szeptemberi támadás miatt négy órán keresztül szünetelt a határátkelés Argentína minden határátkelőjénél. A támadók 4 millió dollárt követeltek az ellopott adatok megsemmisítéséért és a titkosítást feloldó kulcsért. Az eset jól példázza, hogy egyetlen támadásnak egy egész országot érintő következménye lehet.

Microsoft

A Microsoft biztonsági hálózata számokban

A Microsoft globális információvédelmi rendszere az alábbi adatforrásokból dolgozik minden hónapban:

1,2 milliárd
PC, szerver és egyéb, hálózatra kötött eszköz

18 millió
ellenőrzött URL

470 milliárd
ellenőrzött e-mail

600 milliárd
ellenőrzött dokumentum

4,1 milliárd
percnyi videokonferencia

630 milliárd
felhasználóhitelesítés

1,8 millió
gigabájtnyi felhős és hálózati naplóállomány

1 milliárd
felhasználó

5 milliárd
blokkolt támadás