A VISSZATÉRÉS BIZTONSÁGI AGGÁLYAI A SZAKEMBER SZEMÜVEGÉN ÁT

Változásfolyam kihíváslavinával: IT-biztonság a back-to-office folyamán

FORRÁS: THINKSTOCKPHOTOS

A koronavírus-járvány első hulláma csendesedni látszik, a lapuló görbével párhuzamosan pedig a szigorú korlátozások is enyhülni kezdtek. Az elmúlt két hónap után szépen lassan kezd visszatérni a nyüzsgés a belváros utcáira, és az irodaházak sem merednek a sugárutak fölé búskomor magányukban. De nemcsak a belváros, hanem az üzleti élet minden szereplője a back-to-office jelenséggel van elfoglalva, ami IT szempontból tartogat meglepetéseket. Hogy nagyobb kihívás-e, mint a tömeges home office-ba küldés, illetve tartogat-e olyan változásokat, amelyeket csak a komplett végpontvédelem átalakításával lehet megoldani, arról két IT-biztonsági vezetővel beszélgettünk.

Nem kérdés, hogy az informatikai biztonságra befolyással van az irodába való visszatérés, ám arról már megoszlanak a vélemények, hogy ezutóbbi vagy a tömeges home office-ba küldés jelentette-e a legnagyobb próbatételt. Beszélgetőpartnereim is a skála két végén helyezkednek el a kérdés tekintetében.

„Azoknak a cégeknek, amelyek úgy tértek át a home office-ra, hogy az nem volt megfelelő előkészítve, elképzelhető, hogy magasabb biztonsági kockázatokkal kell számolniuk. A jellegzetes mulasztások: nem volt VPN-csatlakozás kialakítva, az eszközök biztonsági szempontból nem voltak megfelelően felkészítve, menedzselve, vagy esetleg nyitott portokon keresztül, távoli asztalon érték el a munkahelyi számítógépeiket, esetleg otthoni eszközöket használtak és azon keresztül csatlakoztak az irodai hálózathoz. Egyébként, ha a munkakultúra részét képezte már a home office, és a technikai háttér mellett a kollégák is rendelkeztek a megfelelő biztonságtudatossággal, akkor nem jelenthet különösebb kihívást az irodába való visszatérés IT-biztonsági szempontból”, mondta *Hagen István,* a Bonafarm információbiztonsági vezetője.

A fenti probléma, azaz, hogy laptopot, tabletet egyéb eszközt biztonsági felkészítés nélkül adták ki a nem megfelelő vagy alacsony biztonságtudatossággal rendelkező munkavállalóknak, főként a nem nagyvállalati környezetre jellemző. Ettől függetlenül, bárhol érheti meglepetés a biztonsági szakembereket.

„Technológiai és emberi szempontból is kihívás a visszatérés. Azt tapasztalom, hogy változik mind a munkaadók, mind pedig a munkavállalók hozzáállása a home- és open office-hoz. A munkahely fogalmát a járvány hetek alatt újraértelmezte, és ez a változás jelentősebb lesz, mint azt sokan gondolják. Egyre több digitálisan érett szervezet fogja engedélyezni a szabad munkahelyválasztást, így lesznek, akik ritkán fognak bemenni az egy légterű irodákba. Technológiai oldalról pedig azt látom, hogy annak a rengeteg eszköznek a begyűjtése, rendbetétele, akár szoftveresen, akár hardveresen, amennyit a munkavállalóknak kijuttattak, komoly terhelést fog jelenteni a biztonsági szakembereknek, és jelentős erőforrást fog elvonni”, fejtette ki véleményét *Tóth Zsolt,* a delaware International CISO-ja.

Anomáliák a felhasználói magatartások összességéből

Akár nagyobb kihívásként, akár kisebb feladatként élik meg az IT-biztonsági szakemberek a visszatéréssel járó feladatokat, az tény, hogy általánosságban mindegyikőjük ugyanazzal szembesül. A dolgozók ugyanis hajlamosak a kiadott eszközt a sajátjuknak tekinteni, ami a használaton is meglátszik. A látogatott oldalak közt ugyanis gyakran előfordulnak az olyanok, amelyek komoly biztonsági kérdéseket vetnek fel. A kiberbűnözők előszeretettel használják ki a céges policy-re fittyet hányó felhasználók nyílt wifis szörfölését, és dobják be a megtévesztés összes trükkjét, ami a tarsolyukban van.

HAGEN ISTVÁN, BONAFARM

FORRÁS: ITB

TÓTH ZSOLT, DELAWARE

FORRÁS: DELAWARE

Az irodai hálózaton kívül sokkal védtelenebb a felhasználó. Ideális esetben az informatikai csapatnak el kellene érnie távolról az adott gépet, hogy frissítéseket és egyéb beállításokat tudjanak végrehajtani rajta. A felhasználónak pedig tudomásul venniük a biztonsági követelmények rájuk vonatkozó részét. „Ha nyílt wifire csatlakozik a dolgozó, tudomásul kell vennie, hogy lehallgathatják, és pillanatok alatt megszerezhetik a legszenzitívebb céges adatokat, jelszavakat. De a konferenciahívások is aggályosak lehetnek adatbiztonsági szempontból, hiszen a hirtelen népszerűvé vált megoldások használata során előfordulhat, hogy illetéktelen is hozzájutnak bizalmas információhoz”, fűzte hozzá Hagen István. „A nagyvállalati megoldások használata, a naprakészség, a tudatosság és a professzionális menedzselés a kulcsszó ezekben a helyzetekben”, szögezte le,

Ugyanakkor a felhasználó is szükséges ahhoz, hogy a gép hálózatba visszaintegrálása ne jelentsen a kelleténél nagyobb kihívást. Ezért érdemes bejelenteni minden olyan eseményt, melyet az internetes aktivitás során tapasztaltunk, és ami IT-biztonsági szempontból aggályos lehet. Mert hiába minden előkészület és védelmi intézkedés, ha trójai falóként visszük be a céges hálózatba a kockázatot jelentő sérülékenységeket.

> Nincs ideális visszatérés. Az erőforrások megfelelő allokálása, a dolgozók internetes magatartásának önbevalláson alapuló felmérése egyértelműen zökkenőmentesebbé teszi IT-oldalról a back-to-office jelenséget

A leáldozó irodák és az új generációs védelmi rendszerek kora?

„Azt gondolom, hogy a tűzfalnak, mint klasszikus hálózati védelmi eszköznek megváltozik a szerepe, erre pedig a koronavírus még jobban rávilágított. A klasszikus hálózat alapú biztonsági rendszereket fel fogják váltani (ki fogják egészíteni) a végpontokra, mobileszközökre és a felhőre optimalizált védelmi rendszerek. Észre kell vennünk, hogy a munkavállalók mobillá váltak, nem akarnak egy helyről dolgozni csak azért, hogy védve legyenek. A technológia és a cégek berendezkedése is a mobilitást ösztönzi, és léteznek már ennek megfelelő gyakorlatok. Persze, ez innovatívabb szemléletmódot igényel. Mindenesetre a bizalom még nem tért vissza a nyílt légterű irodák felé, így kérdés, hogy merre mozdulnak el a cégek, ha teljes biztonságban akarják tudni az adataikat”, zárta gondolatait Tóth Zsolt.

Kiss Franciska