AMIKOR A VÁLLALAT MAGA OKOZZA A KIBERBIZTONSÁGI INCIDENST

Hat IT-biztonsági hiba, amelyeket fel kell ismerni önmagunkban

FORRÁS: 123RF.COM

Az üzleti vezetők közül sokan a kiberbiztonságot olyan problémának tartják, amely elegendő pénz befektetésével és a megfelelő szakértelemmel rendelkező emberek alkalmazásával könnyedén kordában tartható. Az igazság azonban az, hogy többnyire nem a technikai hozzáértés vagy a pénz hiánya okozza a súlyos incidenseket, hanem az IT- és nem-IT vezetők közötti rendszerszintű és kulturális ellentétek.

Nem könnyű az IT-biztonságot megteremteni és hatékonyan dolgozni egyszerre, minden téren kompromisszumokat kell kötni. A home office-t egy nagyvállalatnak számító pénzügyi szolgáltatónak dolgozó férjemmel osztom meg. Az elmúlt közel két évben rengeteg feszültségnek voltam akaratlan fültanúja, amelyeket az IT-sek a biztonság érdekében támasztott, néha irreális elvárásai okoztak. De mivel a belsős irodai munka már nem alternatíva, mindkét fél kompromisszumra kényszerült.

Sok esetben a vállalat és az alkalmazottak magatartásukkal és az IT-biztonsági kultúra hanyagolásával saját maguk okozzák a legtöbb kiberbiztonsági incidenst. A felmerülő kérdések lehetőséget biztosítanak a CIO-k és a CISO-k számára egyaránt, hogy átgondolják, hogyan teszik prioritássá az IT-biztonságot a többi üzleti vezető számára. Ha őszintén és nyíltan kezeljük az alább felsorolt problémákat, akkor a kiberbiztonsági incidensek kockázatát jelentősen csökkenthetjük.

1. A láthatatlan, rendszerszintű kockázatok

Az üzleti vezetők gyakran hoznak olyan döntéseket, melyek a vállalat biztonsági felkészültségét negatívan befolyásolják: például nem hajlandóak leállítani egy szervert ahhoz, hogy megfelelően frissítsék vagy régi hardverekkel és szoftverekkel dolgoznak, hogy így spóroljanak némi pénzt. Néha ezek a döntések rejtve maradnak az IT-vezető előtt, ami hamis biztonságérzetet kelt a vállalatban, miközben megnöveli a kiberbiztonsági incidens bekövetkezésének valószínűségét.

Ezek a rendszerszintű kockázatok a vállalat működésének részei, ezért nem lehet a szőnyeg alá söpörni ezeket. A megfelelő szintű IT-biztonság megteremtésének érdekében a problémákat jelenteni kell és foglalkoznunk kell velük, bármennyire is kényelmetlen.

2. Kulturális disszonancia a vezetők között

A nem-IT vezetők természetesnek veszik az IT-biztonságot, az valahogy mindig ott van, mint a levegő vagy a víz. Ez azt is jelenti, hogy a kiberbiztonság nem része az üzleti követelményeknek. Az az üzleti vezető, aki egy új alkalmazás fejlesztését kéri, nagy valószínűséggel nem sorolja fel a követelmények között biztonsági megfelelőséget.

Ez az attitűd olyan termékeket és megoldásokat szül, amelyek komoly kiberbiztonsági kockázatot hordoznak önmagukban, és nemcsak saját magunk részére. Például az IoT Security Foundation 2021. novemberi vizsgálata szerint a divatcégek vagy a konyhai eszközöket gyártó vállalatok IoT-eszközei többnyire nem biztonságosak, míg az IT-fejlesztés területén tapasztalattal rendelkező cégek biztonságosabb (és drágább) eszközöket gyártanak.

Az a megoldás, ha az IT-vezető a kiberbiztonságot üzleti kontextusban találja, hogy az üzleti vezetők is szembesüljenek döntéseik hatásával.

> Legyen végre közhely: nincs teljes biztonság, csak ismert, tervezett, és ezért elfogadhatóan alacsony kockázat

3. A pénz nem boldogít

A világ összes pénzével is csak csökkenteni tudjuk a kiberbiztonsági kockázatokat, de százszázalékos biztonságot vásárolni nem tudunk. A top IT-biztonsági szakértők alkalmazása sem jelent teljes garanciát az incidensmentes működésre. Elég csak egy elégedetlen alkalmazott, és máris a sok pénzből megépített vár kapuja belülről nyílik. Erre a legutóbbi példa, az Ubiquiti esete, amikor kiderült, hogy egy elégedetlen fejlesztő, aki alapból hozzáfért a vállalat adataihoz, támadta (zsarolta) meg a céget 2020-ban, nem pedig kívülről értek hozzá a cég rendszereihez egy sérülékenységen keresztül. Megoldás lehet a „belsős” kockázatot is csökkentő, ma divatos „zero trust” koncepció.

Amikor a hatóság frissíti a rendszereket

Még akkor is késlekednek a vállalatok a frissítésekkel, amikor a támadóknak csak fel kell térképezniük, milyen rendszereket használnak. Például a 2021 márciusában bejelentett MS Exchange hibák után egy héttel több tízezer olyan rendszer volt elérhető az interneten, amelyeket nem frissítettek. A probléma súlyosságát felismerve példátlan módon az amerikai szövetségi nyomozóiroda, vagyis az FBI a szükséges bírósági engedélyek megszerzése után maga hatolt be ezekbe a rendszerekbe, és távolította el a sérülékenységeket, amiről persze emailben értesítették az érintetteket.

4. Nem merünk felelősséget vállalni

Amikor elfogadjuk, hogy az üzleti működésnek kockázatai vannak, akkor ennek felelősségét valakinek vállalnia kell. De érthetően senki nem vállalja a felelősséget, ha ez azt jelenti, hogy az illetőt azonnal kirúgják, ha valami baj történik.

Az is problémát jelent, ha a vállalat által „kényelmesnek” tartott kockázati szinteket nem határozzuk meg pontosan. Előre meghatározott paraméterek mellett el lehet dönteni, hogy vállalható a kockázat vagy sem, mire van szükség a kockázat megfelelő szintre hozásához.

A megoldás része, ha díjazzuk azokat a vezetőket, akik mernek egyensúlyozni az IT-biztonság és az üzleti elvárások között.

5. Irreális társadalmi elvárások

Isten őrizz, hogy olyan súlyú kiberbiztonsági incidenst szenvedjünk el, hogy tele legyen vele a média. De ha megtörténik, a társadalom és az ügyfelek a felelős menesztését kérik. Amikor a biztonságot fekete dobozként kezeljük, akkor mindenképp ez történik. Senki sem érti, hogy pontosan hogyan is működik, ezért a kívülállók úgy vélekednek, valaki biztosan hibázott. A társadalom és az ügyfelek elvárásai akkor változnak, ha a szervezet és az IT-csapat elkezd másképp beszélni az IT-biztonságról. A bűnbak keresése helyett őszintén kell beszélni a biztonságos működés és az üzleti elvárások közötti törékeny egyensúly megteremtésének nehézségeiről.

6. A transzparencia hiánya

Vannak felső vezetők, akik egyszerűen nem hajlandók elfogadni, hogy nincs teljes IT-biztonság. A céges IT-biztonsági beszámolók csupa jó hírekkel van tele, hogy milyen téren mennyit fejlődött a biztonság, de a fejlesztési lehetőségeket vagy a hiányosságokat ritkán mutatják be. A megoldás a fejekben, a gondolkodás megváltoztatásában rejlik: az IT- és a nem-IT vezetőknek egyaránt el kell fogadniuk az IT-biztonság realitásait.

Vass Enikő