TEKINTSÜNK BE AZ IT-BIZTONSÁG KULISSZÁI MÖGÉ!

Ne féljen külső segítséget kérni, ha túl nagy falatnak látja a megfelelő kiberbiztonsági védekezést!

BÁNSZKI ZSOLT, 4iG

FORRÁS: 4iG

Az IT-biztonság világa még mindig rejtelmesnek tűnhet egyes vállalatvezetőknek, ez azonban ne legyen akadálya, hogy elkezdjenek foglalkozni a kérdéssel. A lényeg, hogy ne ad hoc fejlesztésekkel vágjanak bele, ne akarjanak egyszerre túl sokat – és bátran kérjenek segítséget. Ezt a misztikumot igyekeztek feloldani a 4iG szakértői háromrészes webinárium-sorozatukkal, és rávilágítani az alapvető védekezési problémákra.

„Minden vállalat más, de az információbiztonság kialakításakor érdemes követni a rendelkezésre álló közös mintákat és a bevált gyakorlatot. Nem a technológiai megoldásokkal ajánlott kezdeni, hanem a meglévő kockázatok felmérésével és értékelésével”, figyelmeztet *Bánszki Zsolt,* a 4iG Nyrt. IT-biztonsági üzletágának vezetője. „Ha a kiindulási állapotot már ismeri a vállalat, meghatározható az is, hogy adott idő alatt hova szeretne eljutni, s annak elérésére milyen erőforrásokat tud fordítani. Ha a veszélyek és az általuk okozott potenciális kár mértékével már tisztában van, akkor szisztematikusan lehet haladni a védelem kiépítésével.”

A kevesebb néha több

„Erre a területre is érvényes azonban az »aki sokat markol, keveset fog« örökérvényű igazsága. Nem elég megvenni a legmodernebb védelmi eszközöket, mert úgy járunk, mint aki megvesz egy szupersportautót, miközben nincs jogosítványa: nézegetheti, beleülhet, de tudás hiányában nem lesz képes kihasználni és élvezni az autó funkcióit”, vont párhuzamot Bánszki Zsolt.

Hasonlóan nagy gondot okozhat, ha túl gyorsan akar mindent megoldani a vállalat. Akkor is igaz ez, ha nem saját eszközöket, hanem előfizetéses szolgáltatásokat vezetnek be. Bánszki Zsolt már találkozott olyan esettel, amikor a megvásárolt biztonsági csomag minden elemét bekapcsolták, bármiféle előzetes vizsgálat, elemzés nélkül. A következő nap a vezető nem kapott meg egy rendkívül fontos e-mailt, mert a túl szigorúra állított szabályok letiltották. Az eredmény borítékolható volt: lekapcsolták az összes biztonsági funkciót, amelyek azóta is kihasználatlanul állnak.

A hasonló esetek elkerülése érdekében rendkívül fontos, hogy a biztonsági szabályrendszert, valamint az azt kiszolgáló technikai környezetet egyszerre indítsa el, és párhuzamosan fejlessze a vállalat. Vizsgálja meg pontról-pontra a megfelelőséget, ahol pedig hiányosságot talál, oda keresse meg a megfelelő, a kockázattal arányos műszaki megoldást, a maradványkockázatokra pedig más módon figyeljen.

A spamszűrésen túl

Az IT-biztonság kiépítésének jó kiindulási pontja, könnyen megvalósítható része az email-védelem megerősítése, ami ma már jóval többet jelent egyszerű spamszűrésnél. Első ránézésre ezek a szoftverek haté-

REGYEP GYÖRGY, 4iG

FORRÁS: 4iG

konynak bizonyulnak, hiszen óriási mennyiségű kéretlen levelet távolítanak el – a teljes levélforgalom 80-90 százaléka is lehet spam. A problémát nem azok jelentik, amelyeket kiszűrnek, hanem azok, amit nem – az átengedett és teljesen legitimnek látszó levelek között ott lapulnak az adathalászatra utazó, a hamis URL-eket tartalmazó vagy éppen kártevőket – sok esetben zsarolóvírusokat – rejtő küldemények.

„A gyanútlan felhasználó csupán egyetlen kattintására van szükség, hogy megtörténjen a baj. Kifinomult social engineering támadásokra is előszeretettel használják az e-maileket a támadók: például, ha egy pénzügyi igazgató címéről érkezik egy formailag helyes levél a céges postaládába, utalási felszólítással, nincs az az ügyintéző, aki gyanakodni kezd" – mutatja be egy valós példán keresztül a veszély forrását *Regyep György,* a 4iG Nyrt. IT-biztonsági szakértője.

Ahogy Bánszki Zsolt korábban említette, több fronton kell felépítenie védelmi vonalát a vállalatnak. Szükség van különféle technikai megoldásokra: hálózatmonitoringra a kémprogramok felderítésére; az egyszerű vírusirtón túlmutató végpontvédelemre a zsarolóvírusok és a támadások kiszűrésére; a mobil eszközök menedzsmentjére (MDM-re); és egy fejlett e-mail védelmi megoldásra is. A 4iG e-mail ATP megoldása sandboxban vizsgálja át a leveleket, majd számos szempontot figyelembe véve rendel hozzájuk kockázati értéket, ezt követően vagy továbbítja a címzettnek, vagy karanténba helyezi a gyanús levelet.

„Nem szabad elhanyagolni a szabályrendszert és az emberi tényezőt sem", folytatja Regyep György. „Az adatok hatékony megvédése nem megy előzetes adatvagyon-leltár készítése, valamint az adatok biztonsági, kockázati szempontú osztályozása nélkül. Időt és energiát kell fektetni a felhasználók tudatosságának növelésébe, amelyet elméleti és gyakorlati oktatásokkal, valamint a képzési eredmények rendszeres viszszamérésével érhetünk el. Rengeteg információval szolgálhat a technikai és emberi védekezési képesség szintjéről egy-egy szimulált támadás is."

A hálózat kulcsfontosságú

A hálózatok védelme nemcsak az e-mailek szűrése miatt fontos. Az adatok megfelelő áramlása nélkül ma már elképzelhetetlen a vállalati működés. Egyre több eszköz csatlakozik az internetre, amellyel a céges rendszerek eleve veszélynek vannak kitéve. Különösen fontos lehet ez ipari környezetben, ahol a termelési eszközök hagyományosan elszigetelten működtek, így a védelmükre sem fordítottak akkora figyelmet – az ipar 4.0 rendszerek megjelenése azonban változást hoztak. Ha zsarolóvírus, vagy akár más támadás áldozata lesz egy termelőüzem, akkor már egy pár órás leállás is több tízmillió forintos közvetlen kárt okozhat, nem beszélve a hosszabb távú közvetett veszteségekről, reputációs kockázatokról, amelyek a partnerek bizalomvesztéséből származhatnak.

„A fentiek miatt érdemes elkülöníteni egymástól a termelési (OT), valamint a hagyományos informatikai (IT) eszközöket és hálózatokat", mondja Regyep György. „Mindkettőt erősen kell védeni, de nem szabad szem elől téveszteni, hogy az OT-rendszereknek mások a sérülékenységei (érzékenyek például az adatok manipulálására), és üzleti szempontból is csak sokkal rövidebb kieséseket tolerálnak."

A jó hálózatmonitoring megoldással felmérhetők a hálózati forgalomra leselkedő veszélyek, így azokra már tud reagálni a vállalat, akár az üzletmenet-folytonossági terv átalakításával. Ha például nem megfelelő a VPN védelme, bevezethető kétfaktoros azonosítás; megbízható gateway-ek és IPS-rendszerek üzembe állításával megelőzhetők az adatszivárgások; a tanúsítvány alapú kommunikáció növeli a hálózatbiztonságot; az elosztott hálózatok kialakítása pedig redundanciát biztosít, hiszen, ha az egyik kiesik, a másik át tudja venni a feladatait. ■

Van segítség!

Egyre több vállalat érzi, hogy többet kellene tennie az IT-biztonságért. A szándék azonban sokszor félelemmel is társul, mert a vállalatvezetők hajlamosak túlgondolni a biztonság kérdését, és túl drágának, túl bonyolultnak találják, amihez ráadásul megfelelő szakemberük sincs. „Én mindenkinek azt tanácsolom, hogy ne féljen segítséget kérni. A 4iG olyan széles termék- és szolgáltatás-portfóliót nyújt, amellyel gyakorlatilag bármilyen igényt kielégíthetünk, a kisebb vagy nagyobb vállalatoktól érkező kéréseket ugyanazzal a hozzáértéssel kezeljük. Szakembereink kompetenciája világszínvonalú, legyen szó műszaki megoldásokról vagy tanácsadásról", mondja Bánszki Zsolt. Majd hozzáteszi: „tevékenységünk sohasem irányul arra, hogy bűnbakokat keressünk egy szervezeten belül, hanem kizárólag az ügyfelek digitális értékeinek biztonságba helyezésére fókuszálunk.