Forrás: ITB

ITBusiness & Technology 2017

A teljes biztonság csak illúzió

Vass Enikő 2017. 03. 17.

Az IT-biztonság nem állapot, hanem folyamat, melyben a megelőzésnek, a felhasználók oktatásának rendkívül fontos szerep jut. A 2018 májusában életbe lépő Európai Uniós adatvédelmi szabályozás javíthatja a hazai vállalatok biztonságtudatosságát – derült ki az ITBUSINESS február 20-án tartott, SQUAD névre keresztelt konferenciájának IT-biztonsági előadásaiból.

Hozzászokhattunk már ahhoz, hogy a támadások, az adatlopások állandóak, az IT-biztonsági események egymást érik, szinte nincs olyan nap, amikor ne derülne ki újabb biztonsági incidens. Az IT-biztonság már a fejlesztés pillanatában elkezdődik – véli *Csizmazia-Darab István*, a Sicontact szakértője. Hibátlan szoftver ugyanis nem létezik, csak olyan, amelynek a futtatása hibátlanul megtörtént, vagyis a hibára még nem derült fény – idézte a programozóknak tanított örökérvényű aranyszabályt a biztonsági szakember.

Nem tartják be az alapvető szabályokat

A Szerinte a támadások egyre kifinomultabbak, egyre szerteágazóbbak lettek, a hackerek kreativitása kiapadhatatlan. Az IT-infrastruktúrát a biztonságot szem előtt tartva kell felépíteni, azonban a felhasználók biztonságtudatának erősítése nélkül ez minden esetben kidobott pénz.

Hiszen hiába van vírusirtó a felhasználó számítógépén, ha az első riasztáskor kikapcsolja azért, hogy a vágyott tartalmat telepíthesse. A felhasználókat oktatni kell, fel kell készíteni őket a biztonsági kihívásokra, az oly gyakori megtévesztésen alapuló támadásokra.

A kutatások azt mutatják, hogy vállalati szinten még az olyan alapvető szabályokat sem tartják be a felhasználók, mint a jelszavak rendszeres változtatása. Az is aggasztó, hogy a munkavállalók negyede hozzáfér korábbi munkahelyének belső rendszereihez, mert azok jelszavait nem változtatták meg a cégnél. Az elavult IT-infratruktúra is komoly kockázati tényező: a brit egészségügyben például a mai napig 15 ezer Windows XP-t futtató számítógép működik (a magyar egészségügy is hasonló mutatókkal rendelkezhet). A szakember szerint a 2018 májusában életbe lépő EU-s adatvédelmi szabályzat javíthat valamit a helyzeten (a szabályzatról részletesebben keretes írásunkban olvashat).

Csizmazia-Darab István szerint a biztonságon nem érdemes spórolni. Amikor a vállalkozás védelméről beszélünk, akkor az alvállalkozók, az alkalmi partnerek védelmére is gondolni kell. Figyeljünk a részletekre, fektessünk sok energiát a megelőzésre. A biztonság ugyanis nem állapot, hanem folyamat.

Védjük elektronikus vagyonunkat

Az elavult rendszerek jelentik a legnagyobb gondot, már ami a vállalatok biztonságát illeti – vélte *Bencsáth Boldizsár*, a BME kutatója mondja. Az új, frissen induló vállalatoknál egyszerű biztonságtudatosan felépíteni egy IT-rendszert, a régebbieknél viszont nehéz megtalálni a biztonsági kockázatot jelentő architektúrát. A szakember szerint vannak olyan vállalatok, ahol még mindig az 1980-as években népszerű Dbase adatbáziskezelő rendszert használják.

A biztonság területén a trendek lassan változnak, mindig van egy-egy kedvenc zsarolóvírus. Az emberek pénze viszont egyre nagyobb mértékben elektronikus formátumban létezik, emiatt a kiberbűnözők motiváltabbak támadni. Az viszont tény, hogy egyrészt magyar nyelvterületen élünk, ami megvéd minket, másrészt a hackerek is mennyiségi iparágban dolgoznak, kevesüknek éri meg a 10 milliós Magyarországgal foglalkozni.

Az EU-s adatvédelmi szabályozásról – dióhéjban

Tavaly áprilisában fogadta el az EU a General Data Protection Regulation, vagyis az Általános Adatvédelmi Rendeletet, amely két év türelmi idő után, 2018 elején válik kötelezővé minden EU tagország számára (a szabályozásról bővebben írtunk már az ITBUSINESS 2016. júniusi számában). Noha a hazai adatvédelmi előírások a meglévő európai szabályozásoknál szigorúbbak, a rendelet pár ponton különbözik a magyar szabályozástól. Például jelentősen növekedett az adatvédelmi hatóság által kiszabható bírság összege: súlyosabb jogsértés esetén a maximális összeg akár 20 millió euró is lehet, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 százalékát kitevő összeg. (A kettő közül a magasabbat kell kiszabni.) Adatvédelmi incidensek esetén – például, ha egy cég adattároló rendszerét hackertámadás éri és felhasználói adatokat lopnak el, vagy ha a cég egy munkatársa elveszít egy pendrive-ot, amin fontos ügyféladatok vannak – kötelező értesíteni az adatvédelmi hatóságot, és egyes esetekben a felhasználókat is, hogy minél előbb megtehessék a szükséges kockázatmérséklő intézkedéseket (például a jelszavak megváltoztatását).

Ha egy új technológia bevezetése valószínűsíthetően magas adatvédelmi kockázattal jár, akkor az adatkezelést megelőzően hatásvizsgálatot kell végezni. Ilyen eset például, ha egy szolgáltatás során felhasználói profilokat alkotnak marketing célból, vagy ha egy e-health megoldás nagyszámú egészségügyi adatot kezel. Ha az adatvédelmi hatásvizsgálat szerint az adatkezelési műveletek magas kockázattal járnak, amelyet a cég nem képes megfelelő intézkedésekkel mérsékelni, előzetesen konzultálnia kell az adatvédelmi hatósággal.

Szabályozás a biztonságért

Csinos Tamás, a Clico ügyvezető igazgatója szerint sincs tökéletes IT-biztonsággal rendelkező cég, csak olyan vállalat, amely ezt hiszi magáról – tévesen. A szakember véleménye szerint az egészséges biztonságtudat nélküli felhasználók jelentik a legnagyobb biztonsági kockázatot egy vállalatnál. Akkor tudunk ugyanis biztonságról beszélni, ha a biztonságtudatosság is megfelelő szintű. Nem elképzelhetetlen, hogy a következő világháborút kirobbantó támadás (persze ne legyen ilyen) színtere már a kibertérben lesz, ott folyik majd az adatokért a harc. A szakember szerint az EU-s adatvédelmi szabályozás – mely magas büntetési tételeket tartalmaz és komoly adatkezelési előírásai vannak – nagymértékben erősíti a biztonságtudatosságot.

A digitális transzformáció szempontjából az IoT-eszközök nélkülözhetetlenek, hiszen nem kérdés, hogy az elért hatékonyság növekedéssel, piaci értékkel bír. Az ezen a téren születő eszközöknek se szeri se száma, óriási biztonsági fejfájást okozva az iparágnak. Csinos Tamás szerint a biztonsággal foglalkozó szakemberek általában szabályozás ellenesek, mondván, a szabad piaci verseny rendet teremt, de IoT területén úgy tűnik, hatósági szabályozásra lenne szükség annak érdekében, hogy a biztonságot is beépítsék a termékekbe.

Spájzoljunk bitcoint

Csizmazia-Darab István mindig hatásosan fogalmaz: nem létezik száz százalékosan támadásbiztos rendszer. A zsarolóvírusos támadásokra figyelni kell, mert ha azokat nem szakszerűen hárítják el, akkor az első támadáskor nyitva hagyott hátsó ajtókon keresztül újból és újból fertőznek a támadók. Ezek a cégek vagy komolyan veszik a biztonságot és szakszerű segítséget kérnek a vírusok eltávolításához, vagy pedig bitcoin tartalékokat képeznek a sorozatos támadások gyors elhárításához. A szakemberek feladata a fejlesztőket rávenni arra, hogy biztonságszemléletű termékeket készítsenek. Az emberbe építhető orvosi eszközöket – mint például a szívritmus-szabályzót – is vezeték nélküli kapcsolat segítségével frissítik már, így a biztonságos, tudatos fejlesztés elkerülhetetlen.

Mit mond a piac

Mivel minden platformon elérhetők bérszámfejtő- és HR-megoldásaik (hiszen az ügyfelek részéről ez már elvárás), *Lovas Zoltán*, a NEXON cégvezetője szerint a mobil jelenti a legnagyobb kihívást számukra. Éppen ezért a mobiltelefonon, tableten futó alkalmazásaik segítségével adatokat nem lehet módosítani, így zárják ki annak lehetőséget, hogy például az otthon felejtett mobiltelefonon a gyermek véletlenül rossz adatot vigyen fel a rendszerbe.

Az állami, szabályozott környezet sok fogódzkodót jelent *Fritsch Róbert* IT-vezetőnek. A Fővárosi Vízműveknél az üzemirányítási rendszer biztonsága kritikus, ennek gondtalan működését öt diszpécser felügyeli. *Bodrogközi László*, a Neuron első embere pedig úgy fogalmazott, 17 éve fejlesztenek különböző értékesítési rendszereket és 17 éve félnek attól, mi lesz, ha egyszer valaki bejut rendszereikbe. Ezért a biztonság kiemelt náluk, és folyamatosan azon dolgoznak, hogy egy hasonló támadás kockázatát csökkentsék.

Barsi András, a biometrikus útlevelek biztonsági architektúráját fejlesztő Microsec képviselője szerint az IT-biztonság világában a tudatlanság erő, hiszen minél többet tud az ember a lehetséges fenyegetettségektől, annál jobban fél, mert nem tudja, honnan érkezik a következő pofon. A katonai eszközök gyártásával is foglalkozó GE Aviation képviseletében *Ortenszky Loránd* elmondta: náluk a biztonság alapkövetelmény. A rendszerek izolációja, szeparációja, az emberi tényező kiszűrése mind-mind fontos védekezési eszköz. A szakember azt is elmondta, hogy dolgoznak az IoT-rendszerek biztonságának szabványosításán, hiszen a GE rengeteg ipari eszközhöz gyárt és telepít különböző szenzorokat.