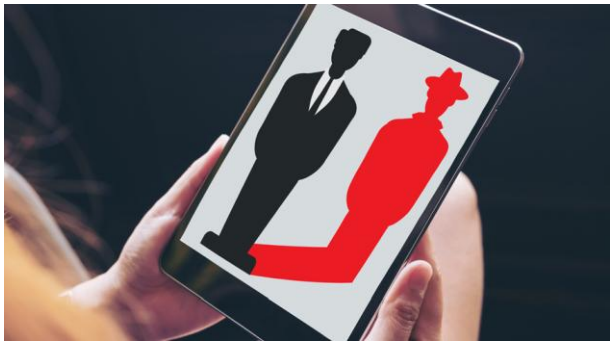
Koronavírus, recesszió, elbocsátások – és jönnek a belsős adattolvajok

Már vannak jelei annak, hogy a tömeges elbocsátások miatt fel fognak erősödni a bennfentes kibertámadások.



Másfél hete hozta nyilvánosságra a kanadai Shopify, hogy egy biztonsági incidens következtében 200 kereskedő partnerétől szivárogtak ki adatok. A vállalat belső vizsgálata szerint az incidens mögött a belső IT-támogató csapat két tagja állt. Ők nyúlták le a partnercégek nyilvántartásait, és szivárogtatták ki az abban talált érzékeny vevői adatokat (email, név, lakcím, a megrendelés részletei). Úgy tűnik, hogy egyéb személyes és pénzügyi információk nem kerültek ki, de a károk felmérése még folyik.

A Shopify esete jól példázza, mire kell felkészülniük a szervezeteknek a koronavírus-járvány következményeként. Mivel a járvány általános gazdasági visszaesést hoz, nagy valószínűséggel sokan veszítik el az állásukat. Ennek pedig egyenes következménye lesz, hogy megszaporodnak a belső munkatársak által elkövetett kibertámadások.

Amúgy is emelkedő tendenciát mutat

Mint a Centrify kiberbiztonsági evangelistája, *Torsten George* írta a Securityweeken, a bennfentesekhez köthető kiberbiztonsági incidensek száma az elmúlt két év alatt 47 százalékkal nőtt a Ponemon Institute 2020-as globális jelentése szerint. Ezzel párhuzamosan a támadások okozta átlagos költségek is emelkedtek 31 százalékkal, így a vállalatoknak már 11,45 millió dollár (anyagi és reputációs veszteség, helyreállítás költségei stb.) kárt okoz egy ilyen támadás. A szakértő szerint azonban az elbocsátások egyre többeket sarkallnak arra, hogy ne távozzanak üres kézzel, és könnyebben is megkörnyékezhetők lesznek, hogy vegyenek részt egy külsősök által szervezett támadásban.

Nem kell azonban minden esetben szándékosságot feltételezni a bennfentes incidensek mögött. Sokszor vezet adatszivárgáshoz tévedés, gondatlanság, vagy egy olyan személy felelőtlen magatartása, aki nem elégedett a szabályok adta kereteivel, vagy gyorsítani akar folyamatokon stb. Az incidensek közös nevezője, hogy az incidenst előidézők tevékenysége alapvetően legitim volt, ugyanis magasabb szintű hozzáférési jogosultságai voltak az érzékeny adatokhoz és alkalmazásokhoz.

A helyzet kezelése egyszerűnek tűnik: korlátozni kell a hozzáférést. Ez jól hangzik, ám sok esetben az ilyen korlátozások a folyamatok drámai lassulásához vezetnek. Egyre több biztonsági cég próbálja feloldani az ellentmondást olyan eszközökkel, melyek a felhasználói magatartást, annak változásait monitorozák. Így mindenki szabadon csinálhatja, amit kell, hiszen a rendszer minden esetben riaszt-letilt, ha valami szokatlant érzékel. Vannak azonban olyan folyamatbeli intézkedések, amelyekkel – a magas jogosultságú felhasználókra szabott speciális védelmi megoldásokon túl is – segítik a kockázatok csökkentését.

Oszd meg – és uralkodjon a biztonság

Nagyban növeli a biztonságot, ha a magas jogosultságokat igénylő feladatokat olyan részelemekre bontjuk, ami kikényszeríti több ember együttműködését, akik óhatatlanul felügyelik is egymás tevékenységét. Ki lehet alakítani úgynevezett „hozzáfé-

résí zónákat", amivel a felhasználói jogosultságokat meghatározott erőforrásokhoz lehet kötni.

Ezen túl érdemes olyan dinamikus jogosultságkezelési rendszert alkalmazni, amiben mindenkinek csak ahhoz és akkor kap hozzáférést, amihez és amikor az adott feladat elvégzéséhez szükség van. De amint a munka lezárul, a jogosultsága is azonnal megszűnik, hiszen alapesetben mindenkinek nulla jogosultsága van. A jogosultságkiosztás mögé érdemes olyan rendszert tenni, amely azt is pontosan rögzíti, hogy milyen körülmények között és ki engedélyezte az adott hozzáférést.

Mindezeket az intézkedéseket jól kiegészítheti a fentebb már említett, viselkedéselemzésen alapuló védelem, amelynek plusz hozadéka, hogy valós időben azonosítja a nagy kockázatú tevékenységek, így a beavatkozás is azonnali lehet.

Forrás: https://bitport.hu/koronavirus-recesszio-elbocsatasok-es-jonnek-a-belsos-adattolvajok

Válogatta: Fonyó Istvánné