A belsősök gondatlanságából ered a biztonsági zűrök többsége

Egy friss felmérés szerint ma már a biztonsági incidensek több mint fele vezethető vissza a céges alkalmazottak és partnerek gondatlanságára, ami összegszerűen is nagyobb károkat okoz a direkt rosszindulatú tevékenységnél.

Közhely, hogy az üzleti szereplők egyre szaporodó kiberbiztonsági kihívásokkal kénytelenek szembenézni, legyen szó a végponti biztonságról, a cloud rendszerekről, a javítatlan vagy nulladik napi szoftveres sebezhetőségekről, a dolgok internetéről (IoT) vagy a távoli munkavégzés erőltetett ütemű bevezetéséről. Ahogy azonban a Proofpoint felméréséből is kiderül, a kockázati tényezők között előkelő helyen szerepel az alkalmazottak képzettségének és biztonsági tudatosságának hiánya, illetve a szándékos károkozás is, amit ugyanilyen fontos figyelembe venni a fenyegetésészlelés és válaszadási képességek szempontjából.

A kiberbiztonsági vállalat 2022-es Cost of Insider Threats Global Report kutatása szerint ezek a bennfentes fenyegetések átlagosan évi 15,4 millió dollárjába kerülnek a nagy szervezeteknek, ami 34 százalékos növekedést jelent a 2020-as becslésekhez viszonyítva. A Ponemon Institute közreműködésével készített riport ezernél is több olyan informatikai szakember válaszait dolgozta fel világszerte, akik a közelmúltban ehhez kapcsolódó kiberbiztonsági incidenseket tapasztalt.

A rendellenességek észlelését követően átlagosan 85 napba telt az adott problémák megoldása, ami ugyancsak érdemi növekedést jelent a Proofpoint korábbi jelentésében szereplő 77 naphoz képest. A bejelentett incidenseknek (beleértve bennfentesek által okozott károkat, adatlopásokat vagy rosszindulatú programok szándékos telepítését is) mindössze 12 százalékát sikerült 30 napon belül elsimítani, esetenként több mint 184 ezer dolláros átlag költség mellett.

Mindenkiből csábító támadási felület lesz

Ez az összeg persze az érintett cégek méretétől függően jóval magasabb is lehetett. A Proofpoint megállapítja, hogy az amerikai vállalatok tavaly 17,5 millió dollárt költöttek a szóban forgó eseményekre, európai társaik pedig nem egész 15 milliót. Az irodából hazatelepülő és a vállalati adatokat is magukkal hurcoló munkavállalók folyamatosan növelik a kockázatokat, összességében pedig nem csak ők, hanem a bedolgozókés a külső beszállítók is olyan széleskörű hozzáférésekkel rendelkeznek, amelyek nyomán egyszeriben vonzó támadási vektorokká változnak.

Nem csoda, hogy az elmúlt két évben a bennfentes fenyegetések drámai módon elszaporodtak, és a jelentés alapján az incidensek nagyobbik része, 56 százaléka egy-egy alkalmazott hanyagságára volt visszavezethető. Az incidensek 26 százaléka kapcsolódott valamilyen belső felhasználó rosszindulatú akcióihoz, míg 18 százalék a dolgozók azonosságainak ellopásával kezdődött, ami a személyes eszközök biztonsága és a jelszavak gyengeségével függött össze.

A ZDNet tanulmányt összefoglaló beszámolójából kiderül, hogy az alkalmazottak vagy a bedolgozók hanyagsága átlagosan 6,6 millió dollárjába került a kutatásba bevont szervezeteknek, miközben a belső bűncselekményekkel "csak" 4,1 millió dollárt, a hitelesítő adatok ellopásával pedig 4,6 millió dollárnyi kárt hoztak összefüggésbe. Ezek a számok természetesen csak tájékoztató jellegűek, de a nagyságrend és az arányok mindenképpen figyelmet érdemelnek.

Válogatta: Fonyó Istvánné
Forrás: www.bitport.hu