ERŐSÖDIK A HACKERAKTIVITÁS A KIBERTÉRBEN

Baljós árnyak

„Különleges katonai művelet”, hogy maradjunk a hivatalos megközelítésnél. Sokan, sok mindent és sok helyen elmondtak már erről a századunkat mindenképpen meghatározó eseményről. Ne szépítsük, ahol repkednek a golyók, bizony háború van. Azonban a nem elhanyagolandó fizikai veszély mellett mindenkinek számolnia kell a virtuális térben, az interneten egyre szaporodó támadásokkal. A kirakatban természetesen a nemzetállamok állnak. *(Schneck Zsolt, a Shield Informatics ügyvezetője írása.)*

A fizikai konfliktust megelőzően hackertámadás érte az ukrán parlament, és a külügyminisztérium oldalát, valamint kabinet és egy sor kulcsfontosságú infrastruktúrát üzemeltető magáncég rendszerét, amelyeknek az ország működtetésében kiemelt a szerepe. Persze a válaszcsapás sem késett, a Kreml és az orosz kormányzati portálok sem úszták meg az Anonymous támadásait. Ez a háború felértékeli a kiberbiztonságot, és természetesen a kiberbiztonsággal foglalkozó cégeket, megoldás-

FORRÁS: ITBUSINESS

SCHNECK ZSOLT, SHIELD INFORMATICS

szállítókat is. Egy hatékony kibertámadás gazdasági hatása felérhet a fegyverekkel okozott károkkal.
Ez a konfliktus nem beszivárgott, hanem egyenesen belecsapódott a mindennapjainkba, téma a villamoson, a kávézókban és persze a céges megbeszéléseken. Mindenhol.
A multi és nagyvállalatok humán és anyagi erőforrások bevonásával és egyre komolyabb biztonsági protokollok bevezetésével sokat tesznek azért, hogy a saját rendszereik biztonságát megerősítsék. A kkv azonban más kávéház.

A veszélyes tolvaj nem csap zajt

A nagyon látványos dolgok többnyire – kivéve, ha mondjuk egy hírportált vagy webshopot érintenek – kevesebb veszélyt rejtenek magukban, mint gondolnánk. Ha leáll a weboldal, elég gyorsan kiderül, a felkészült IT-csapat hamar orvosolja, az élet megy tovább. Azok az incidensek jelentenek igazán nagy gondot, amelyek láthatatlanul történnek, a támadók hosszú időt töltenek a rendszerben, gyakran csak megfigyelve annak jellegzetességeit, keresve a hibákat, feltérképezik a felhasználókat és azok szokásait.
Ezért a fenyegetés az esetek jelentős részében nem közvetlenül a nagy céghez érkezik. Sokkal egyszerűbb a támadók dolga, ha egy kisebb beszállító vagy más üzleti partner informatikai eszközeit törik fel, esetleg felhasználóit hackelik meg. Ahol nem áll rendelkezésre a megfelelő határ- és végpontvédelem, nincs elég erőforrás a hálózatok monitorozására, ott egyszerűbb kártékony kódokat elhelyezni. Egy jókor és jó helyen elindított adathalász-kampány többet ér, mint a vállalat webszerverének leállítása, a lényeg az adat és az információ.

Mi legyen a kkv dolga?

A multicégeknek érdekük, hogy a beszállítóik rendszereiről képet kapjanak, azaz minősítsék őket az informatikai rendszerük alapján is. A CIO-k előbb vagy utóbb ki fogják dolgozni azokat a megfelelőségi protokollokat, amelyeket a beszállítóknak teljesíteni kell, az együttműködéshez. A kisvállalati üzemeltetőknek és cégtulajdonosoknak pedig már most, jó előre érdemes gondolkodni a megoldásokon, megcsináltatni a belső és külső auditokat, azaz meg kell győződni a rendszereik valós állapotáról. Ezután tudnak döntéseket hozni, hogy melyek az elengedhetetlen beruházások, milyen intézkedési terveket kell elkészíteni, és hogyan kell adott esetben újragondolni a rendszereiket.
Itt az idő, hogy minden felelős vezető elgondolkodjon a vírus- és határvédelmi rendszerek korszerűsítésén, a levelezőrendszerek megfelelő védelmén, és úgy általában azon, hogy az IT-üzemeltetés és az IT-biztonság nem a szükséges rossz. Emberek, ezzel dolgoztok, ezzel kerestek pénzt! És sajnos a kritikus rendszerek támadása már mindennapos. A kiberháború már itt van, és hasonlít a fegyverekkel vívottra. Sokkal jobban az életünk része, mint az gondolnánk. *(X)*

SHIELD
Informatics
We never close