SAJTÓKÖZLEMÉNY

Budapest, 2017. október 10.

Európai kiberbiztonsági hónap
Tippek a vállalatok és munkavállalóik tudatosabb felkészítéséhez

Idén is megrendezésre kerül az Európai Kiberbiztonsági Hónap. Az Európai Hálózatbiztonsági Ügynökség (ENISA) által immár 5. alkalommal szervezett októberi kampány célja a kiberfenyegetések részletes bemutatása és a biztonságtudatosság növelése. A kezdeményezéshez kapcsolódóan az ESET szakemberei összegyűjtöttek néhány biztonsági tanácsot, valamint több szakmai rendezvényen tartanak előadásokat nemzetközi és hazai viszonylatban is.

A téma fontosságát mutatja, hogy az idei évben igazán nagyszabású kibertámadásoknak lehettünk tanúi (Ukrán energiaipari támadások, Equifax, brit egészségügyi szolgáltató stb.), amelyek esetében az anyagi károk mellett, az érintett szervezetek jóhíre is jelentősen sérült. Aggasztó, hogy a vállalatok jelentős része felkészületlennek érzi magát a támadásokkal szemben. Az Európai Kiberbiztonsági Hónap célja felhívni a szervezetek figyelmét a tudatosabb biztonsági intézkedések meghozatalára, hogy minél felkészültebben nézzenek szembe a fenyegetésekkel.

A kiberbiztonság közös felelősség, így a szervezeteknek fontos, hogy a munkatársaik felkészítésére is figyelni kell. Az ESET szakemberei ehhez gyűjtöttek össze néhány tanácsot, amelyek segíthetnek megbirkózni az egyre gyakoribb kibertámadásokkal:

Legyünk tájékozottak

Ahhoz, hogy a munkatársaink hatékonyabban tudják megvédeni számítógépüket és adataikat a fenyegetések széles skálájával szemben, ismerniük kell a fenyegetések módszereit, a kártékony kódok működését, és különféle támadók céljait, gondolkodásmódját. A leggyakoribb fenyegetésekről (rosszindulatú programok, adathalászat, zsarolóvírusok) működésének ismerete segíthet abban, hogy a dolgozók alaposabban megértsék a veszélyeket és kevésbé legyenek kiszolgáltatottak a támadásoknak.

Ügyeljünk a jelszavak biztonságára

Jelszavakat kitalálni és emlékezni rájuk – sokaknak frusztráló feladat, ezért az emberek nagy része mindenhol ugyan azt a kódot használja. Ráadásul ezek a jelszavak bár nekik könnyen megjegyezhetők, azonban éppen emiatt gyakran nem biztonságosak, könnyen kitalálhatóak (feltörhetőek), például 123456, qwerty, abc123, stb. Segíteni kell tehát a munkavállalóknak megérteni, hogy mitől lesz biztonságos egy jelszó (például 10 karakternél hosszabb, egyedi, kis- és nagybetűt, számot valamint különleges karaktert is tartalmaz, stb.), és az általuk használt hálózatok biztonsága érdekében a jelszavakhoz kötődő szabályok betartatását is biztosítani kell. Még jobb ha jelmondatokat használunk.

Óvatosság, gyanakvás és biztonságtudatosság

Az egyik leginkább alábecsült fenyegetés, a pszichológiai manipuláció (social engineering), amelynek során a bűnözők trükkös módszerekkel személyes adatokat csalnak ki a felhasználótól. Az egyik leggyakoribb forgatókönyv, hogy kapunk egy emailt, amely úgy néz ki, mintha a bankunk, vagy más pénzügyi szolgáltató (pl. PayPal) küldte volna. A levélben arra kérik a felhasználót, hogy nézze meg számlája vagy fiókja adatait, és a mellékelt linken adja meg személyes adatait. Természetesen a levelet nem a bank vagy a szolgáltató küldte, hanem adathalászattal foglalkozó kiberbűnözők. Az Egyesült Királyságban évente 96 000 hasonló támadás történik. Minden esetben gondolkodjunk, mielőtt szokatlan, gyanús üzenet linkjére, vagy mellékletére kattintanánk. Ha nem vagyunk biztosak a dolgunkban, előtte inkább ellenőrizzük le az üzenet hitelességét úgy, hogy a feladót telefonon felhívjuk.

A biztonság közös ügyünk

A biztonságtudatos viselkedés szabályainak minden alkalmazottra vonatkozniuk kell, függetlenül attól, hogy ki, melyik osztályon és milyen szinten dolgozik az adott szervezeten belül. Különösen fontos ez a vezetői szintű munkatársak esetében, akik sokszor kiemelt célpontjai a támadásoknak. A munkatársaknak fel kell ismerniük, hogy meggondolatlan cselekedeteik a szervezet egészére nézve igen hátrányosak lehetnek, emiatt a rendszeres képzéseken történő tudatosságnövelés elengedhetetlen. Ennek keretében azt is célszerű konkrét eseteken keresztül bemutatni, hogy miként védhetjük meg cégünk adatait a különféle rosszindulatú próbálkozások ellen.

Összességében elmondhatjuk, hogy az európai kiberbiztonsági hónap kiváló alkalom arra, hogy felhívja a figyelmet a kiberbűnözők jelentette fenyegetésekre, és az ez elleni védekezésben megoldási javaslatokkal, információkkal segítse minden szervezet munkáját. Fel kell ismerniük a vállalatoknak, hogy a biztonság egyetemlegesen mindenkinek a felelőssége.

Előadások szakembereknek

Az ESET biztonsági tanácsadói és mérnökei a kampány során több előadást is tartanak Európa szerte és Magyarországon is. Hazánkban a kampányhoz kapcsolódó Ethical Hacking Day! konferencián tart az ESET szakembere, *Csizmadia-Darab István* előadást a zsarolóvírusok problémájának témakörében. A már most teltházas szakmai rendezvény előadásait a rendezvény napján a következő linken lehet megtekinteni: https://www.twitch.tv/ingame_budapest

**

Az ESET-ről:

A több mint 30 éves, díjnyertes NOD32 technológiát kifejlesztő ESET a proaktív védelem úttörője, az üzleti és otthoni biztonságtechnikai szoftvermegoldások nemzetközi szállítója. A vállalat piacvezető a fenyegetések észlelésében és megelőzésében. Az 1987-ben megjelent ESET NOD32 Antivirus világelső az elnyert Virus Bulletin "VB100" díjak számát tekintve, illetve a vizsgálatok 1998-as fennállása óta eddig minden szabadon terjedő vírust vagy férget észlelt és kivédett. Az ESET NOD32 Antivirus, ESET Smart Security és az ESET Cyber Security (biztonsági megoldás Mac-re), valamint a mobiltelefonok és táblagépek védelmét biztosító ESET Mobile Security a legajánlottabb biztonsági megoldások közé tartoznak, a termékekben milliók bíznak

meg világszerte. A vállalat központja Szlovákiában, Pozsonyban található, regionális terjesztési központokkal rendelkezik San Diegóban (USA), Buenos Airesben (Argentína) és Szingapúrban, valamint irodái vannak São Paulóban (Brazília) és Prágában (Csehország). Az ESET több mint 180 országban, köztük Magyarországon, rendelkezik kiterjedt partneri hálózattal. További információ: www.eset.hu

A Sicontactról:

A Sicontact Kft. az egyik legjelentősebb, IT biztonsággal foglalkozó hazai szoftverdisztribútor. Mottója és küldetése, ami köré termékportfolióját kialakította: „biztonság a digitális világban". A Sicontact Kft. Magyarországon az ESET NOD32 technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik.

A Sicontact Kft. több ízben elnyerte a kitüntető Business Superbrands díjat. Az ESET Smart Security programcsomagot többször is az év antivírus megoldásának választották. A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban kínálja. Az ESET biztonsági szoftverek licencelése során a gyorsan változó körülményeket is figyelembe veszi, így például az ESET szoftverek a licencidőszak alatt bármikor újratelepíthetők az adott számítógépre, továbbá az unilicenc konstrukció keretében a munkaállomásokon a megvásárolt ESET licenccel egyaránt használhatók a Windows, Linux és Mac operációs rendszerre fejlesztett ESET termékek, így az operációs rendszer cseréje esetén nem szükséges új licencet vásárolni. A Sicontact Kft. az ESET szoftverekhez díjmentes terméktámogatást és távsegítséget biztosít, mind az otthoni, mind a vállalati felhasználók számára, így az ügyfelek jelentős időt és pénzt takarítanak meg.