Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Mi az a vezetői átverés?**
- **Így védekezzünk!**

Vezetői átverés

Mi az a vezetői átverés?

A kiberbűnözők nagyon trükkösek – folyamatosan újabb és újabb utakat keresnek annak érdekében, hogy megszerezzék azt, amire szemet vetettek. A leghatékonyabb módszerük az, hogy olyan embereket vesznek célba, mint amilyenek mi magunk is vagyunk. Az már régóta közhely, hogy a leggyengébb láncszem mindig az óvatlan alkalmazott, viszont az OUCH! hírlevél olvasói mindig jól informáltak, ezért sokkal nehezebb becsapni őket.

A szerzőről

Angela Pappas a Thomson Reuters információ biztonsági képzéssel és tudatosítással foglalkozó vezetője, aki ebben a minőségében irányítja a nagykövet programot, az eLearning-et és az alkalmazottak adathalászattal szembeni védekezés oktatását.

A kiberbűnözők egyik legújabb módszere az ún. vezetői átverés, más néven „hivatalos levél csalás” (angolul: Business Email Compromise -BEC). Az ilyen támadásokban a kiberbűnözők a cég vagy szervezet vezérigazgatójának vagy más magas beosztású döntéshozójának adják ki magukat. A támadás úgy zajlik, hogy egy email-t küldenek az alkalmazottnak, amivel megpróbálják rávenni, hogy olyat tegyen meg, amit magától nem csinálna. Az ilyen támadások azért tudnak nagyon hatékonyan működni, mert a kiberbűnözők előzetesen információt gyűjtenek a célpontokról. Felhasználják a cég weblapján található információkat, például ki a vezérigazgató, hol található a cég, vagy, hogy milyen más vállalkozásokkal működik együtt. A következő lépésben a cég munkatársairól gyűjtenek be információkat például a LinkedIn, a Facebook vagy a Twitter segítségével. Miután sikeresen feltérképezték a vállalat szervezeti felépítését, a potenciális célpontok után kezdenek kutatni, akit mindig az elérendő cél alapján választanak ki. Ha a pénzre utaznak, akkor a célpont a pénzügyi osztályon dolgozók közül fog kikerülni. Ha az adózással kapcsolatos információkra kíváncsiak, akkor a személyzeti osztály munkatársait próbálják meg becsapni. Ha pedig az adatbázisokhoz akarnak hozzáférni, akkor az IT osztályon dolgozók kerülhetnek célkeresztbe.

Miután a támadók eldöntötték, hogy mit akarnak megszerezni, és hogy ehhez kin keresztül jutnak el, megkezdik a tényleges támadást. A leggyakoribb módszer az adathalászat. A klasszikus adathalász támadásban a támadók milliószámra küldik ki a kéretlen leveleket, amelyekkel azt próbálják elérni, hogy a címzettek megnyissanak egy a levélhez csatolt fertőzött állományt, vagy pedig rákattintsanak egy káros szoftvert tartalmazó weboldal linkjére. A célzott adathalászat ehhez hasonló, annyi különbséggel, hogy ezeket az adathalász email-eket nem tömegesen küldik, hanem célzottan és névre szólóan, előre kiválasztott személyek részére. A célzott adathalász támadásokban felhasznált hamis email-ek nagyon meggyőzően néznek

Vezetői átverés

ki és nehéz felismerni azokat. Gyakran úgy néznek ki, mintha olyan személy vagy cég küldte volna, akivel a célpont együtt dolgozik, például egy munkatárs vagy akár egy felettes. Az email-ek azért tűnhetnek valódinak, mert a támadók például ugyanazokat a kifejezéseket használják, mint a munkatársaink, használják a vállalati logókat, vagy éppen a felettesünk aláírását. Az ilyen email-ek gyakran sürgetik a címzettet, azonnali intézkedést és diszkréciót várnak el. A kiberbűnözőknek pedig pont az a céljuk, hogy a siettetéssel olyan hibát kövessünk el, amit ők a maguk javára tudnak fordítani. Az alábbi esetekben kell kétszer is meggondolni minden lépésünket:

A vezetői átverés a leghatékonyabb támadási forma, amellyel megkerülhetők a biztonsági eljárások, viszont a józan eszünkre hallgatva mi tudunk a leghatékonyabban védekezni ellene.

- **Átutalás**: a kiberbűnözők célja a pénzszerzés. Ez azt jelenti, hogy utánajártak annak, hogy kinek van hozzáférése a bankszámlákhoz, vagy, hogy ki kezeli a vállalat pénzügyeit. Ha megvannak az információk, akkor a támadók a csoport vezetője nevében küldenek hamis email-t, amelyben például arra utasítanak, hogy utaljunk el valamekkora összeget egy bizonyos bankszámlára.

- **Adócsalás**: a kiberbünözők célja, hogy személyes információkat szerezzenek az alkalmazottakról, amikkel meg tudják őket személyesíteni, így pedig adócsalásokat elkövetni. Ebben az esetben a célpont a személyzeti ügyeket kezelő osztály alkalmazottja, és a hamis email-ben egy felettes vagy egy alkalmazott nevében próbálnak meg dokumentumokat szerezni.

- **Hatósági megkeresés**: egy vezetői átverés nem csak email segítségével történhet. Előfordulhat, hogy más kommunikációs eszközöket is felhasználnak a bűnözők (telefon). Például a támadó megszemélyesít egy vállalati vezetőt, aki email-ben felhívja a célpont figyelmét arra, hogy hamarosan megkeresést kap egy hatósági személytől fontos ügyben. Ezután a támadó telefonon is jelentkezik, és úgy tesz, mintha például egy ügyész lenne. A beszélgetés során azt próbálja érzékeltetni, hogy sürgősen szüksége van a kért információkra, amelyek minden esetben bizalmas adatok.

Védekezzünk!

A kérdés az, hogy mit tehetünk önmagunk és a munkáltatónk védelmében? A józan eszünk a leghatékonyabb védekezési eszközünk. Ha kapunk egy üzenet a főnökünktől vagy egy kollégánktól, de furcsának találjuk, akkor lehet, hogy átverés.

Vezetői átverés

Az üzenet sürgető hangneme, a nem megfelelő vagy megszokott aláírás, a szokatlan hangnem, vagy a szokásostól eltérő megszólítás mind olyan momentumok, amelyek gyanakvásra adhatnak okot. A fentieken kívül figyeljünk oda a korábban nem látott, de a munkatársaink és a főnökünk email címéhez hasonlatos helyről érkezett üzenetekre, illetve ugyanígy a telefonszámokra. Ha kétségeink vannak, akkor hívjuk fel az illetőt, vagy beszéljünk vele személyesen, de semmiképp ne válaszoljunk a gyanús levélre! Ne hagyjuk figyelmen kívül a biztonsági előírásokat és eljárásokat! A munkáltatónknak lehetnek olyan szabályai, amelyek pontosan meghatározzák, hogy milyen körülmények között lehet utalást indítani, vagy bizalmas információkat kiadni. Az olyan kérések, amelyek megpróbálják figyelmen kívül hagyni ezen szabályokat – függetlenül attól, hogy mennyire tűnik valódinak – óvatosan kezelendőek, és mindig meg kell győződnünk a valódiságáról! Ha ilyen üzenetet kapunk, és bizonytalanok vagyunk vele, akkor vegyük fel a kapcsolatot a közvetlen felettesünkkel, az ügyfélszolgálattal vagy az informatikai biztonsági csoporttal!

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Pszichológiai manipuláció:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_hu.pdf
Adathalászat:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_hu.pdf
Káros szoftverek:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf
Kétlépcsős hitelesítés:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_hu.pdf
A nap tippje (angolul):	https://www.sans.org/tip-of-the-day

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó

