OUCH! 2020. november

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Pszichológiai manipuláción alapuló támadások

Áttekintés

A számítógépes támadókkal kapcsolatban általános tévhit, hogy kizárólag magasan fejlett eszközöket és technikákat alkalmaznak a számítógépek vagy fiókok feltörésére. A számítógépes támadók már rég megtanulták, hogy az információlopásának, fiókfeltörésnek vagy a rendszerek megfertőzésének legegyszerűbb módja az, ha pszichológiai manipuláció segítségével ráveszik az áldozatot, hogy azt elvégezze helyettük. Tanuljuk meg, hogyan működnek ezek a támadások, és mit tehetünk a saját védelmünk érdekében.

Mi is az a pszichológiai manipuláció?

A pszichológiai manipuláció során a támadó különféle manipulációs technikák segítségével vesz rá valamire, amit egyébként nem tennénk meg. Legyen szó csalókról vagy szemfényvesztőkről, az alapötlet ugyanaz. A mai technológia azonban sokkal könnyebbé teszi a támadóknak, hogy a világ bármely pontjáról, bárkinek kiadhassák magukat, és bárkit megcélozzanak, Önt is beleértve. Nézzünk két példát a való életből:

Telefonos hívást kap valakitől, aki azt állítja, hogy egy állami intézménytől keresi Önt azzal kapcsolatban, hogy adótartozása van, és amennyiben ezt nem egyenlíti ki, pénzbírságot kap vagy letartóztatják. Ezután nyomást gyakorolnak Önre, hogy telefonján fizessen hitelkártyával, ajándékkártyával vagy banki átutalással, folyamatosan emlékeztetve Önt arra, hogy ha nem fizet, börtönbe kerülhet. A hívó fél valójában nem egy kormányhivataltól keresi Önt, hanem egy támadó, aki megpróbálja becsapni, hogy pénzt adjon neki.

Egy másik példa az adathalászatnak nevezett, e-mail alapú támadás. Ebben az esetben a támadók létrehoznak egy e-mailt, amellyel megpróbálják becsapni Önt és rávenni arra, hogy hajtson végre egy műveletet, mint például egy fertőzött e-mail melléklet megnyitása, egy rosszindulatú linkre kattintás vagy bizalmas információk megadása. Az adathalász e-mailek néha általánosak és könnyen észrevehetők, például azok, amelyek bankokat személyesítenek meg. Máskor az adathalász e-mailek nagymértékben testre szabottak és célzottak. Ilyenkor a támadók először felkutatják a célpontjaikat, és az adathalász e-mailt úgy küldik, mintha az áldozat főnökétől vagy egy kollégájától érkezne.

Ne feledje, hogy a pszichológiai manipulációs támadások nem korlátozódnak a telefonhívásokra vagy az e-mailekre; bármilyen formában megtörténhetnek, például SMS és közösségi médián keresztül terjedő üzenetek formájában, vagy akár személyes kontaktus útján is. A legfontosabb az, hogy tudjuk, milyen nyomokra kell figyelnünk.

A pszichológiai manipulációs támadások általános jellemzői

A józan ész a legjobb védelem. Ha valami gyanúsnak tűnik, vagy nem érzi megfelelőnek, akkor az támadás lehet. A leggyakoribb nyomok a következők:

- Sürgetés vagy pánikkeltés. A támadók megpróbálják hibába hajszolni. Minél nagyobb a sürgetés, annál valószínűbb, hogy támadásról van szó.
- Nyomásgyakorlás a munkahelyi biztonsági irányelvek vagy eljárások megkerülésére vagy figyelmen kívül hagyására.
- Olyan bizalmas információk iránti érdeklődés, amelyekhez nem férhetnek hozzá, vagy amelyeket már tudniuk kell, például a számlaszámok.
- E-mail vagy üzenet egy ismerőstől vagy munkatárstól, akit Ön ismer, de az üzenet nem úgy hangzik, mint ha ők írták volna - például furcsa a megfogalmazás, vagy az aláírás nem megfelelő.
- Úgy tűnik, hogy egy munkatárstól vagy egy legitim cégtől érkezik az e-mail, de azt egy privát címről (például @ gmail.com) küldték.
- A kíváncsiság kihasználása vagy egy olyan ajánlat, ami túl szép ahhoz, hogy igaz legyen. Például értesítést kap arról, hogy a csomagja késik, miközben Ön semmit sem rendelt, vagy hogy díjat nyert egy olyan versenyen, amelybe sohasem nevezett be.

Ha felmerül Önben a gyanú, hogy valaki megpróbálja becsapni vagy átverni, ne kommunikáljon vele többet. Ne feledje: a józan ész a legjobb védelem.

A szerzőről

Christian Nicholson (@GuardianCosmos) a SANS SEC560 és a SANS SEC504 oktatója, valamint Partner/Cyber Lead az Indelible-nél (https://indelible.global). Christian szakterületei az alkalmazásbiztonság, a Purple Teaming és az automatizálás a biztonságos integráció, programozás és gépesítés terén.

Források

Telefonos támadások: https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams
Állítsuk meg az adathalászatot: https://www.sans.org/security-awareness-training/ouch-newsletter
CEO Fraud / BEC: https://www.sans.org/security-awareness-training/resources/ceo-fraudbec
Személyre szabott csalások: https://www.sans.org/security-awareness-training/resources/personalized-scams

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)