NEMZETI KIBERVÉDELMI INTÉZET

GOVCERT

Az adatvédelem minden felhasználó alapvető érdeke, ezért a Nemzeti Kibervédelmi Intézet (NKI) az állami kibervédelem támogatásán, fenntartásán és fokozottabb működtetésén túl az egyéni felhasználók tudatosítására is egyre nagyobb hangsúlyt helyez.

Az NKI célja, hogy az IT biztonságot érintő tematikus tájékoztatói segítségével a lehető legtöbb hasznos információt jutassa el a felhasználók részére.

Nemzeti Kibervédelmi Intézet
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu

Céges és magánadatok biztonsága

Készült a Nemzeti Kibervédelmi Intézet megbízásából, az Ön informatikai egészségének megőrzése érdekében.

Céges és magánadatok biztonsága

A támadók is tudják, hogy minden rendszer annyira gyenge, mint amennyire a leggyengébb láncszeme, és a leggyengébb láncszem mindig az ember. A támadók ezért előszeretettel alkalmazzák az emberi ráhatással történő támadások módszereit, ehhez viszont szükségük van egy olyan támadható személyre, akiről elegendő céges és magánadat áll rendelkezésre, valamint akin keresztül egyszerűen és rövid időn belül hozzáférést nyerhetnek az informatikai rendszerhez.

Pszichológiai manipulációt alkalmazó támadások gyakori módszerei:

- zsarolás (pl.: családdal)
- megvesztegetés
- ellenszenv kihasználása (blogok, fórumok)

Minden emberi ráhatással történő támadás más és más, a legtöbb támadási formához hasonlóan azonban ennek is van egy forgatókönyve, melynek az első fázisa minden esetben az információszerzés.

Néhány órás keresés eredményeként – kizárólag a nyilvánosan elérhető adatforrásokra támaszkodva – megtudhatják egy kevésbé biztonságtudatos személy:

- e-mail címét; telefonszámát; családi állapotát; ismerőseit; rokonait; iskolai kapcsolatait; hobbiját; rendszeres szokásait; aktuális tartózkodási helyét; tervezett programját; munkahelyére, munkavégzésére vonatkozó információkat.

Gyakori esetek:

- Az érdeklődő ügyfél kártevőt tartalmazó Word dokumentumot küld.
- A vicces kedvű „kolléga" egy olyan videó hivatkozását adja meg, amellyel kártevőt töltünk le az internetről.
- A kutyás ismeretlen olyan képet küld, amellyel a képmegjelenítő programon keresztül lehet hozzáférést szerezni a gépre.
- A gyerek által talált, „véletlenül" a kapu előtt hagyott pendrive a géphez történő csatlakoztatás után kártevőt telepít.
- A magát kellően lusta rendszergazdának kiadó támadó az áldozattal telepítteti fel a károkozót, aki mellesleg önként kiadja a szervezetnél használt jelszavát is.

A pszichológiai manipulációval történő támadás ellen a láthatatlanság, az elérhetetlenség a legjobb védekezési mód. Ennek érdekében:

- Ne használjuk munkahelyi e-mail-címünket, telefonszámunkat magáncélokra (pl.: apróhirdetésekben).
- Figyeljünk arra, hol, kivel és milyen információt osztunk meg munkahelyünkkel, munkánkkal, magánéletünkkel kapcsolatban.
- Gondoljuk végig, hogy az adatlapunkon lévő információkat valóban szükséges-e bárki számára láthatóvá tenni (pl.: munkahely, elérhetőség, képek, tervezett programok stb.).
- Győzzük le kíváncsiságunkat, legyünk gyanakvók! Ne kattintsunk rá a gyanús levélben lévő hivatkozásra, ne nyissunk meg bizonytalan forrásból származó dokumentumot, illetve ne csatlakoztassunk számítógépünköz bizonytalan forrásból származó adathordozót.

Ne keverjük a privát szférát a munkahelyi közeggel!