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

Otthoni munkavégzés és utazás

ADATBIZTONSÁG A MUNKAHELYEN KÍVÜL

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

Otthoni munkavégzés és utazás

ADATBIZTONSÁG A MUNKAHELYEN KÍVÜL

A távoli eléréssel dolgozó alkalmazottak sokkal nagyobb mértékben ki vannak téve az informatikai támadásoknak. A távoli kapcsolat - jellegéből adódóan - sokkal könnyebben megzavarható, illetve adott esetben le is hallgatható.

Emellett a támadók könnyebben meg is tudnak személyesíteni egy rendszeresen távoli eléréssel dolgozó alkalmazottat, illetve maga a dolgozó is könnyebben megtéveszthető, ha nem veszik körül a kollégái és nincs velük mindennapi kapcsolatban.

Amennyiben a szervezetnél nincs lehetőség távoli munkavégzésre, gyakori, hogy a támadásokat a szabadságolások, illetve a tervezett külső munkavégzések és utazások idejére időzítik. Ennek során a támadók könnyebben tulajdoníthatnak el eszközöket, illetve zavarhatják meg a kommunikációt.

Mit is jelent ez a hétköznapokban ?

Amennyiben távoli eléréssel, otthonról dolgozunk, figyelembe kell vennünk, hogy ilyenkor az egyetlen kapcsolatunk a szervezeti infrastruktúrával a számítógépünk vagy esetleg a telefonunk. A személyes kapcsolat hiánya nem csak az információáramlást nehezíti meg, hanem azt is, hogy meggyőződjünk a hozzánk érkező kérések eredetéről, illetve a velünk kapcsolatba lépők személy-azonosságáról. Ezáltal fokozottan ki vagyunk téve a különböző pszichológiai befolyásolási technikáknak.

Az otthoni munkavégzés és utazás során ugyanakkor nem, vagy csak korlátozott mértékben véd minket a szervezet biztonsági infrastruktúrája is. A ránk bízott eszközökért és kapcsolatuk biztonságáért ilyenkor teljes mértékben mi felelünk, és meg kell védenünk őket a megnövekedett fenyegetésekkel szemben.

Hogyan védekezzünk?

Otthoni munkavégzés során nagyon fontos, hogy figyeljünk a következőkre:

- csak a szervezet által biztosított eszközről (notebook, telefon) dolgozzunk;
- csak titkosított (VPN) kapcsolaton keresztül érjük el a szervezeti infrastruktúrát;
- ha műszaki problémánk adódik, a szervezet informatikai csapatával lépjünk kapcsolatba, ellenőrzött telefonszámon és ne fogadjunk el segítséget másoktól;
- ha e-mail-ben vagy telefonon keresnek meg minket, csak akkor adjunk át információt, ha a megkeresés a szervezet e-mail címén, vagy belső telefonszámról érkezett.

Utazás során kiemelten figyeljünk:

- a szervezeti számítógépünk és telefonunk biztonságára, ezek az eszközök rengeteg információt tartalmaznak, így egy támadó számára rendkívül értékesek lehetnek;
- ne használjunk publikus hálózatokat (pl.: éttermi wifi) munkavégzésre, mert ezek biztonsága nem ellenőrizhető.