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

Információ-biztonsági kontrollok

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

Információ-biztonsági kontrollok

Alapvetően három dolog kell egy támadás által kiváltott biztonsági eseményhez:

- Fenyegetés,
- sebezhetőség, melyen keresztül a fenyegetés kifejti a hatását,
- cél, amiben vagy amivel kárt lehet okozni.

Biztonsági kontrollok

A fenyegetések elleni védelmi intézkedések:

- adminisztratív védelmi intézkedések,
- logikai védelmi intézkedések,
- fizikai védelmi intézkedések.

adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem.

Nekünk, mint felhasználóknak meg kell értenünk, hogy a biztonsági szabályok célja nem életünk megnehezítése, hanem a biztonságos munkakörnyezet megteremtése. A biztonsági szabályok megkerülése akár rövid távon is olyan káresemény bekövetkezéséhez vezethet, mely a munkavégzésünket teljes mértékben ellehetetleníti, adataink, dokumentumaink elveszhetnek, módosulhatnak.

A BIZTONSÁGI ELŐÍRÁSOK BETARTÁSA MINDANNYIUNK FELADATA ÉS FELELŐSSÉGE.

Leggyakrabban elkövetett felhasználói hibák

A felhasználók által vétett leggyakoribb hibák, melyekből fakadó károkért a felhasználó felel:

- idegenek objektumokba és rendszerekbe történő beengedése,
- a látogatók folyamatos kíséretére vonatkozó szabály figyelmen kívül hagyása,
- a „tiszta asztal politika” figyelmen kívül hagyása,
- a „tiszta képernyő politika” figyelmen kívül hagyása,
- nyomtatókban hagyott bizalmas dokumentumok,
- nem megfelelő jelszavak alkalmazása,
- jelszavak megosztása másokkal,
- iratmegsemmisítő használatának elmulasztása,
- ismeretlen forrásból származó hivatkozások megnyitása, dokumentumok, alkalmazások letöltése,
- biztonsági események jelentésének elmulasztása.