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

Biztonsági események és kezelésük

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

Biztonsági események és kezelésük

Jelentési kötelezettség

Kötelességünk, hogy az informatikai rendszer kapcsán tapasztalt rendellenességet, a tapasztalt biztonsági eseményt haladéktalanul jelentsük a szabályzatokban meghatározott módon, az arra kijelölt személyeknek, illetve szervezeti egységeknek a károk minimalizálása érdekében.

Mit kell feltétlenül jelentenünk?

Nekünk mint felhasználóknak azonnal jelentenünk kell!

- Ha a kezelésünk alatt álló adat elveszett, módosult, illetéktelenek által ismertté vált vagy ezen események gyanúja merül fel;
- az informatikai eszközök jogosulatlan használatát vagy ennek gyanúját;
- ha az informatikai eszköz megbontásának gyanúja merül fel;
- ha nem tudjuk használatba venni az informatikai eszközt vagy alkalmazást;
- ha a felhasználói jelszó vagy egyéb általunk használt informatikai eszköz jogosultsági rendszeréhez tartozó adat vagy az azt tároló adathordozó elveszett, megsérült, illetéktelen kezekbe került vagy ezek gyanúja merül fel;
- ha az informatikai eszközzel kapcsolatban gyakran tapasztalunk a normális működéstől eltérő viselkedést, mint pl.: elvesznek állományok, gyakran „lefagy" a számítógép, jelentősen csökken a teljesítménye, nem a megszokott módon működik;
- ha támadást vagy támadási kísérletet tapasztalunk, vagy ennek gyanúja merül fel.

A biztonsági vagy gyanús események jelentését ne tekintsük az informatikai munkatárs zaklatásának!

Az események kivizsgálása során támogassuk az elemzést végrehajtó személyt, adjunk meg számára minden olyan információt, mely elősegíti az incidens hátterének megismerését, az esetlegesen kidolgozandó védelmi intézkedés megtervezését és bevezetését a későbbi biztonsági események elkerülése érdekében.

Tegyük meg a szükséges lépéseket, jelentsük az eseményt!

A nagyobb szervezeteknél a gördülékeny ügyintézés érdekében Call Center működik, ahol a hiba bejelentését követően az operátor eldönti, hogy a hiba távsegítséggel vagy személyes kontaktussal orvosolható.

Távsegítség esetén az IT szakember átmenetileg átveheti az irányítást számítógépünk felett, valamint hozzáférhet hálózati tartalmunkhoz.

Személyes kiszállás esetén az IT szakember fizikai hozzáférést nyer minden eszközhöz, ezért mindenképp ajánlott az azonosítása!