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

Az adatbiztonság alapelvei

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

Az adatbiztonság alapelvei

Az informatikai rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az informatikai rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az informatikai rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

Adatbiztonságon nem csak a szűken értelmezett elektronikus adatok biztonságát értjük, hanem az ezen adatok elérését biztosító informatikai alkalmazások, az alkalmazás működését biztosító hardverelemek, hálózati eszközök, a hardverelemek tárolására szolgáló helyiségek, illetve ezen rendszerelemeket működtető személyzet biztonságát is. Teljes körű védelem alatt tehát az informatikai, a fizikai és a személyi biztonsági komponensek összességét értjük.

Gondoskodni kell továbbá az informatikai rendszer és elemeinek zárt, teljes körű, folytonos és kockázatokkal arányos védelméről.

bizalmasság: annak biztosítása, hogy az információfeldolgozás folyamatában az információ csak az arra jogosultak számára érhető el

sértetlenség: az információ pontosságának és megbízhatóságának biztosítása, azaz az adatot csak az arra jogosultak tudják módosítani

rendelkezésre állás: az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható

zárt védelem: olyan védelem, amely az összes releváns fenyegetést figyelembe veszi

teljes körű védelem: a védelmi intézkedések a rendszer összes elemére kiterjednek

folytonos védelem: a védelem az időben változó körülmények és viszonyok ellenére is folyamatosan megvalósul

kockázatokkal arányos védelem: a védelem költségei arányosak a potenciális kárértékkel

négy szem elve: minden végrehajtási és pénzügyi tranzakció engedélyezését megelőzően az adott feladatot ellátó személy munkáját egy másik személy teljes körűen felülvizsgálja, beleértve az ellenőrzési listák és a kitöltési útmutatók alkalmazását is

legkevesebb jogosultság elve: a felhasználónak mindig a lehető legkevesebb jogosultság mellett kell feladatát végeznie

legszűkebb funkcionalitás elve: a szervezet meghatározza az informatikai rendszerek tiltott, korlátozott, nem szükséges funkcióit, szolgáltatásait, és az informatikai rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa