TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás

A potenciális kritikus fenyegetettségek elleni kiberbiztonsági intézkedésekről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki ügyfélköre részére **a potenciális fenyegetettségek elleni kiberbiztonsági intézkedésekről.**

Az utóbbi időszakban megemelkedett a kibertámadások kockázata. Az elosztott szolgáltatás-megtagadással járó (DDoS) támadások, illetve a magánszektor jelentései a kártékony programokról (HermeticWiper), indokolttá teszik az azonnali kiberbiztonsági intézkedések bevezetését.

A destruktív, rosszindulatú szoftverek azonosítása különösen aggasztó, tekintettel arra, hogy a rosszindulatú szereplők hasonló szoftvereket már korábban is bevetettek ─ pl. a NotPetya és a WannaCry zsarolóprogramokat ─, amelyek jelentős károkat okoztak a kritikus infrastruktúrákban.

Figyelemmel a fenti eseményekre az NBSZ NKI az alábbi védelmi intézkedések végrehajtását javasolja:

- Ellenőrizze a szervezet hálózatához távoli hozzáféréssel rendelkezők jogosultságait, és állítson be kétfaktoros azonosítást a magasabb jogosultsági szinttel rendelkező fiókokon!
- Használjon naprakész szoftvereket, valamint részesítse előnyben azokat a frissítéseket, amelyek az ismert sebezhetőségeket foltozzák!
- Tiltsa a szervezet működéséhez nem szükséges portokat!
- Dolgozzon ki egy, a szervezet egészére kiterjedő válságkezelési tervet!
- Az informatikai szakértők összpontosítsanak minden váratlan esemény vagy szokatlan hálózati viselkedés azonosítására és gyors felmérésére!
- Használjon naplózó rendszert a gyanús események gyors és hatékony detektálása érdekében!
- Használjon naprakész védelmi szoftvereket pl.: vírusirtó, és rendszeresen frissítse annak vírusdefiníciós adatbázisát!
- Amennyiben külföldi szervezetekkel közös hálózaton vagy rendszeren dolgozik, fokozottan ügyeljen a hálózati forgalom figyelésére és elkülönítésére, valamint korlátozza a hálózati forgalom hozzáférését!
- Jelöljön ki válságkezelési csoportot, és legyen biztosítva a kulcsfontosságú személyzet folyamatos rendelkezésre állása!
- Biztosítsa gyakorlatokkal, hogy mindenki megértse szerepét, feladatát és hatáskörét egy esetlegesen bekövetkező biztonsági esemény kezelése során!

- Ellenőrizze a biztonsági mentési eljárásokat annak érdekében, hogy zsarolóvírus támadás esetén gyorsan visszaállíthatók legyenek az adatok!
- Győződjön meg arról, hogy a biztonsági mentések izolálva legyenek a hálózatról!
- Amennyiben ipari vezérlőrendszereket vagy üzemeltetési technológiát használ, végezze el a kézi vezérlések tesztelését annak biztosítása érdekében, hogy a kritikus funkciók működőképesek maradjanak, ha a szervezet hálózata nem elérhető vagy nem megbízható!
- Kísérje figyelemmel a folyamatosan frissülő bejegyzéseinket honlapunkon az aktuális sérülékenységekről, valamint használja RSS-feed csatornáinkat!

Hívja fel munkatársai figyelmét, hogy ne csatlakozzon kiberhadsereghez a saját vagy munkahelyi hálózat igénybevételével, mert nem tudhatja, hogy milyen fájlt tölt le és ezáltal kinek a kezébe ad valójában fegyvert illetve, hogy ki ellen használják azt fel!

Hivatkozások:

https://nki.gov.hu/figyelmeztetesek/serulekenysegek/

https://nki.gov.hu/intezet/tartalom/rss-csatornak/

Kibertámadás esetén az NBSZ NKI segítséget tud nyújtani ügyfélkörének, illetve az incidensbejelentésekből származó információk hasznosnak bizonyulhatnak az esetleges jövőbeni eseményeknél.

A 2013. évi L. törvény, valamint a 2001. évi CVIII. törvény alapján ügyfeleink kötelesek bejelenti Intézetünk felé minden informatikai biztonsági incidenst és gyanús tevékenységet a CSIRT@nki.gov.hu címre.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu