Nemzetbiztonsági Szakszolgálat

Az elmúlt időszak incidenskezelési tapasztalatai

2021.10.21.

Nemzetbiztonsági Szakszolgálat

Nemzeti Kibervédelmi Intézet

Előadás vázlata

- Bemutatkozás
- Problémafelvetés
- Amit kb. mindenki tud
- Tipikus incidensek és problémák
- Ahogy lehetne

Bemutatkozás

Nemzetbiztonsági Szakszolgálat

Nemzeti Kibervédelmi Intézet

Incidenskezelés

Nemzeti CSIRT
Biztonságirányítás

Eseményészlelés
Sérülékenységvizsgálat
Biztonsági elemzés

Hatóság

Ibtv.
Kritikus infra.
SPOC

Problémafelvetés

Mi a biztonsági esemény?

Kinek, mikor kell jelenteni?

Ki jelenti és ki vizsgálhatja ki a biztonsági eseményt?

A kívülálló esete

Incidensek havi eloszlása

Tapasztalatok

Biztonsági esemény

Biztonsági esemény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1. § (1) 9. pontja szerint :

„nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül”.

Kinek, mikor kell jelenteni?

A 271/2018. (XII. 20.) az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló korm. rendelet 8. § (1) szerint :

„ Az Ibtv. 19. § (1) bekezdés b)-c) pontja szerinti szervezetek – szerk.: **az állami és önkormányzati elektronikus információs rendszerek működését biztosító infokommunikációs infrastruktúrát, a nyílt elektronikus információs rendszereit, továbbá a létfontosságú rendszerelemek elektronikus információs rendszereit működtető szervezetek -** , valamint a közvetítő szolgáltató kötelesek a Központ részére az elektronikus információs rendszereikben bekövetkezett biztonsági eseményeket **haladéktalanul** bejelenteni.”

Hova kell jelenteni?

Nemzetbiztonsági Szakszolgálat

Nemzeti Kibervédelmi Intézet

csirt@nki.gov.hu

+36 (1) 336 4833

+36 (30) 344 0704

Ki jelenti és ki vizsgálhatja ki a biztonsági eseményt?

A 271/2018. (XII. 20.) az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló korm. rendelet 14. § szerint :

„Az állami és önkormányzati szervek elektronikus információs rendszereit érintő biztonsági események kivizsgálásában elsősorban a) az elektronikus információs rendszer biztonságáért felelős személy, valamint b) a hatáskörrel rendelkező eseménykezelő központ vehet részt.”

A kívülálló esete

Nem tartozom az állami és önkormányzati elektronikus információs rendszerek működését biztosító infokommunikációs infrastruktúrát, a nyílt elektronikus információs rendszereit, továbbá a létfontosságú rendszerelemek elektronikus információs rendszereit működtető szervezetek közé.

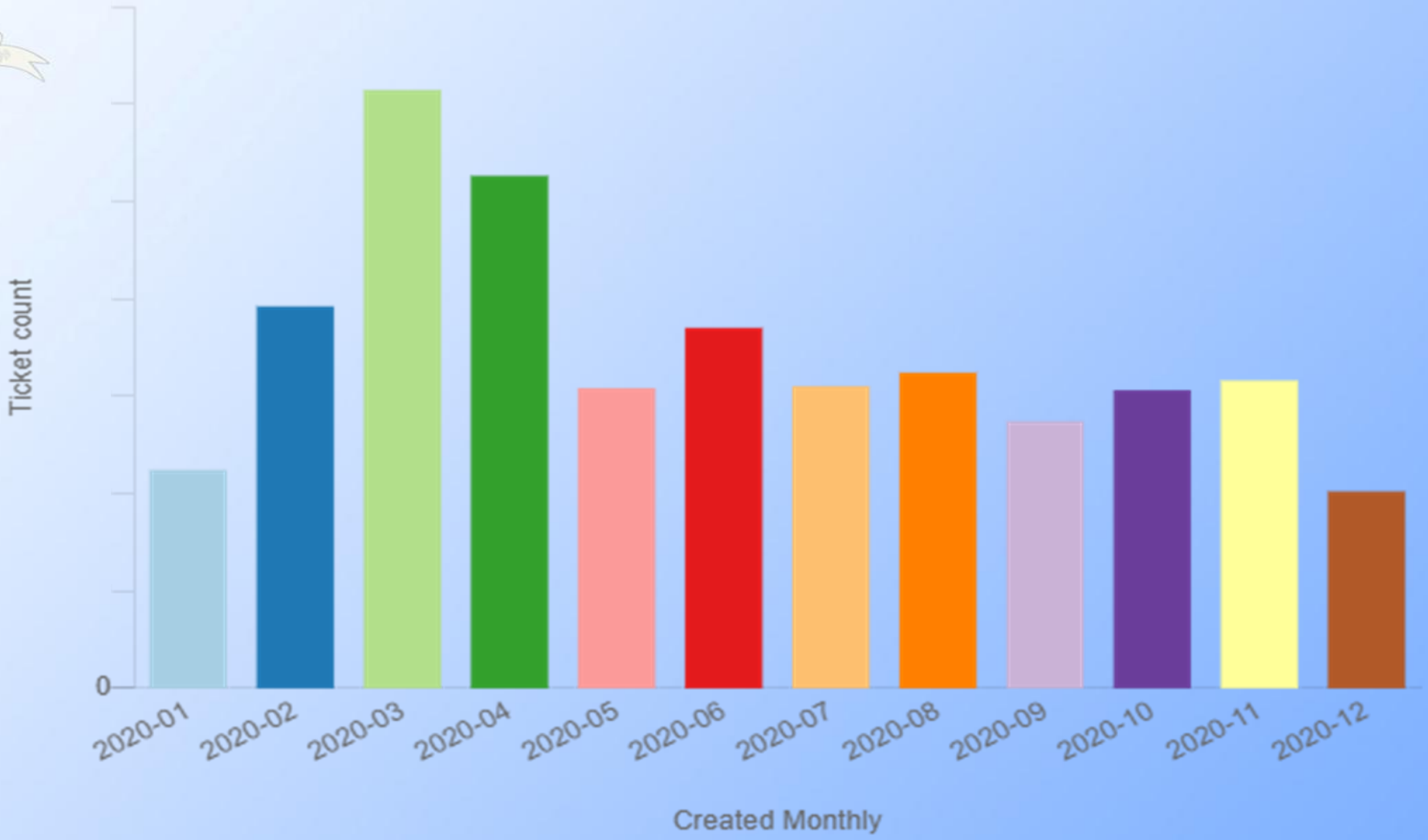
Jelenthetek biztonsági eseményt?

Kérhetek segítséget?

Kérhetek biztonsági esemény vizsgálatot?

Kérhetek sérülékenységvizsgálatot?

Incidensek havi eloszlása



Tapasztalatok

A 2019-s évhez képest fokozatosan emelkednek a bejelentések száma. Jelentős, a nyilvánosságot jobban elérő kampányok zajlottak (emotet, flubot), megjelentek a covid tematikus támadások, gyakoribbá váltak a zsarolóvírusok, DDoS tevékenység gyakorisága növekszik.

Javaslat: Tudatosság fejlesztése

Köszönöm a figyelmet!

Incidensbejelentés:

csirt@nki.gov.hu

Jelentkezés:

Török István

06 30 698 2875

hr@nbsz.gov.hu