Nemzetbiztonsági Szakszolgálat

Hogyan tudjuk megteremteni, hogy az otthoni munkavégzés biztonságos legyen?

Avagy nézzük meg a HomeOffice világát kiberbiztonsági nézőpontból

2021.01.21.

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

- **NCSIRT**
  - Incidens-kezelés
- **Incidens-kivizsgálás**
  - Forensics
  - Malware elemzés
- **Esemény-észlelés**
  - Korai előrejelző rendszer
- **Sérülékenység-vizsgálat**
  - Automata sérülékenység-vizsgálati rendszer
- **Biztonságirányítás**
  - SOC
  - EMIR, FAIR, IMIR
- **Hatóság**
  - Ibtv.
  - Kritikus infra.
  - SPOC

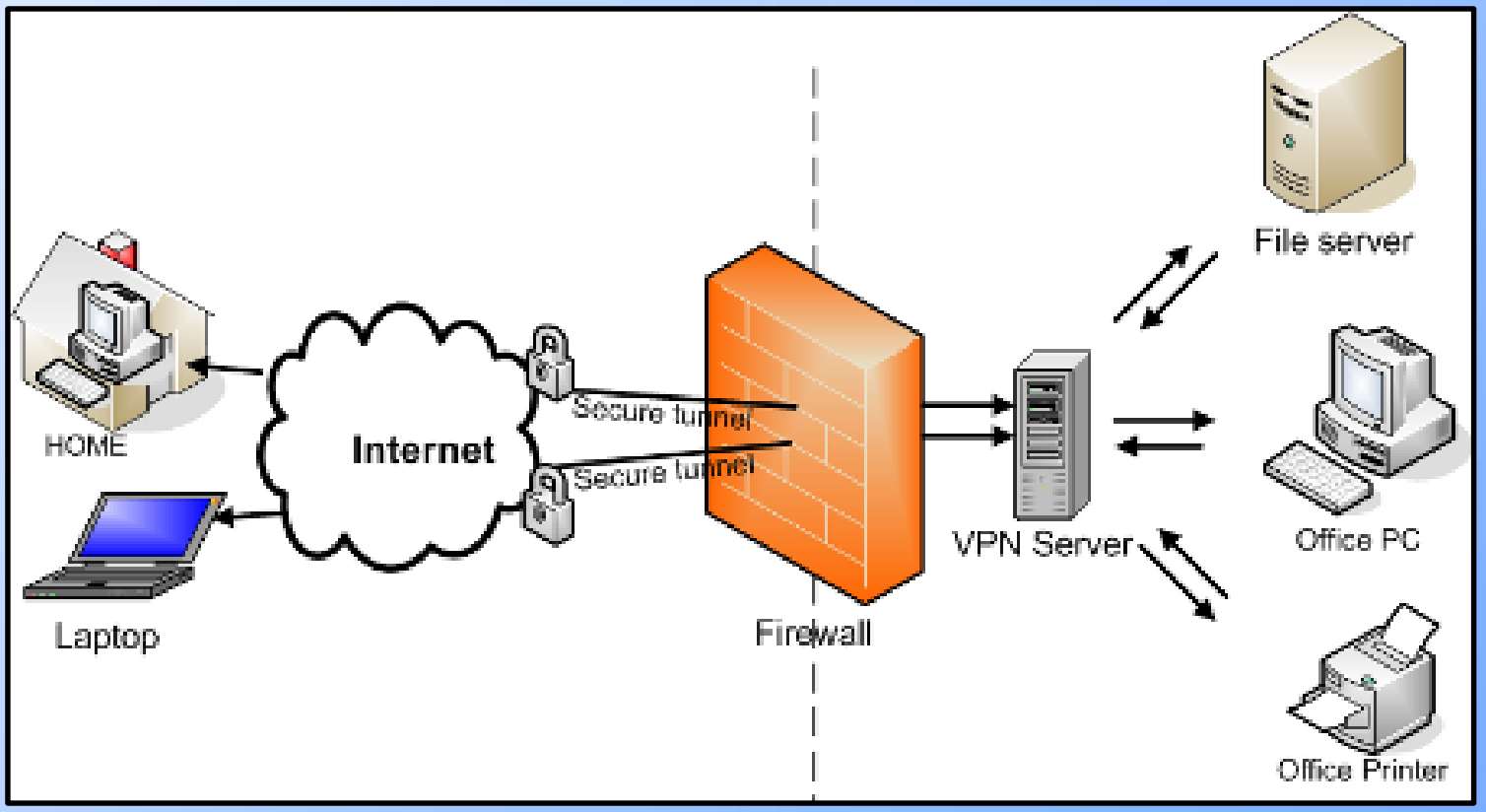
Problémafelvetés

2019-ben a COVID-19 kapcsán erős igény jelentkezett a világ minden táján az otthoni munkavégzés lehetőségének megteremtésére, olyan ágazatokban ahol ez értelmezhető.

Az igényt sokféle formában elégítették ki, de jellemzően a biztonsági megfontolások háttérbe szorultak a gyors eredmény reményében.

Amit kb. mindenki tud

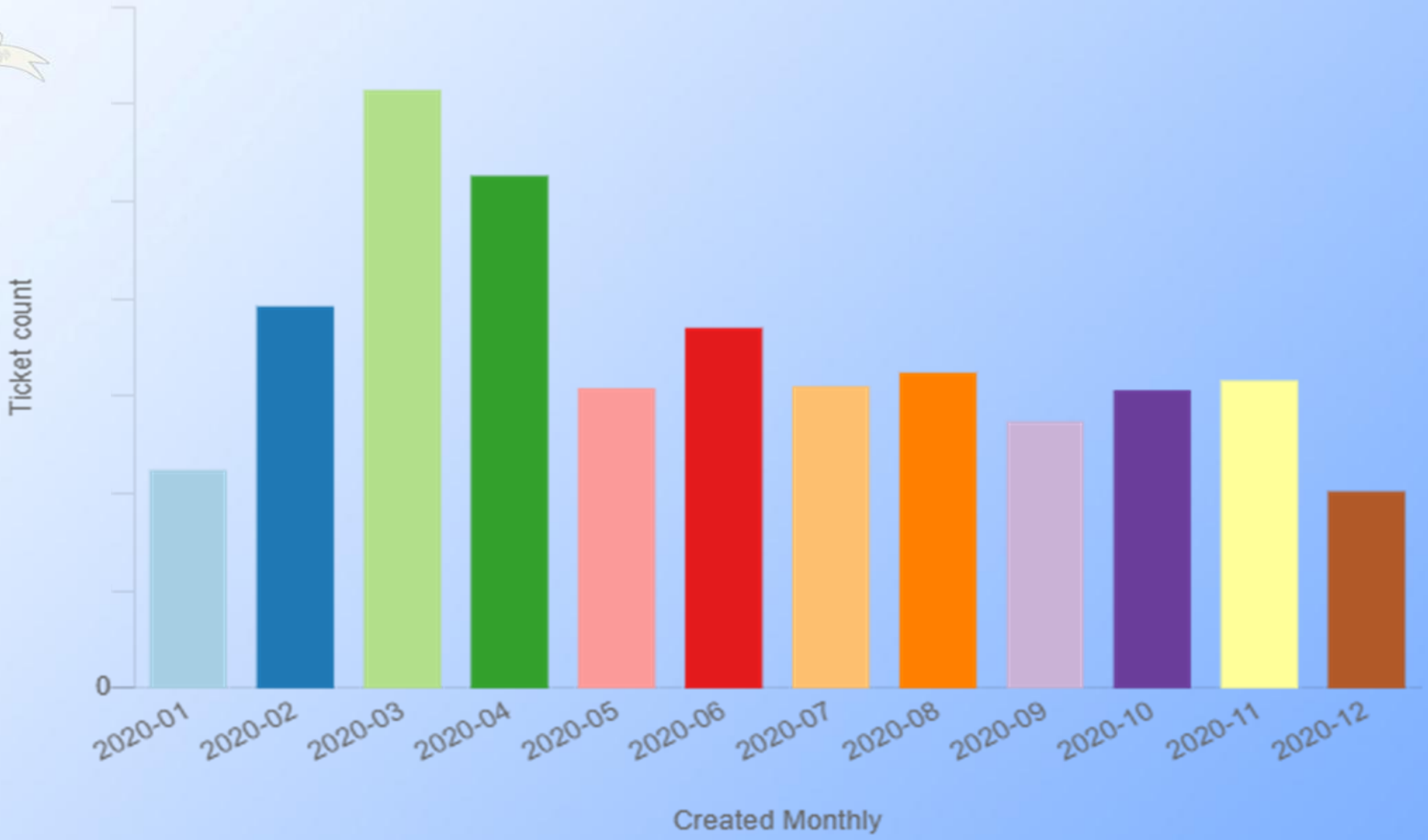
„A távoli munkaállomás, titkosított csatornán keresztül csatlakozik a szervezethez, és kell lennie vírusirtónak a távoli munkaállomáson, de jó az ingyenes is.”



Tipikus incidensek

- Adathalászat
- Malware, fertőzött privát munkavállalói gép a céges hálózaton
- Felhasználói hozzáférések kompromittálódása
- Adatszivárgás
- CEO Fraud

Incidensek havi eloszlása



Főbb problémák

Naplózási hiányosságok

Hálózatszegmentáció hiánya

Kockázat menedzsment hiánya

Szabályzati hiányosságok

Hitelesítési gondok

Biztonságtudatos magatartás hiánya

Nem biztonságos VTC megoldások

Ahogy lehetne

Szervezeti tulajdonú munkaeszköz rendelkezésre bocsájtása az alkalmazott számára, amely megfelelően be van állítva a munkavégzésre.

Az engedélyezett szoftverek telepítve.

Meghibásodás esetén a szervezetnél kell a javítást indítani.

Ahogy lehetne

Bekapcsoláskor az engedélyezett internet kapcsolaton keresztül kiépített vpn kapcsolat felépül, és a szervezeti címtárból hitelesíti magát a kolléga, multifaktoros authentikációt alkalmazva.

A kapcsolat működése során minden internet irányú forgalom a vpn csatornába terelődik, (split tunnel tiltása), és a szervezeti proxy-n és csomagszűrő (esetleg next-gen) tűzfalon keresztül folyik.

IDS, IPS alkalmazása, szabályok karbantartása.

Ahogy lehetne

A vpn kapcsolat során a vpn kliensek egy külön hálózati szegmensbe sorolódnak, és egymást nem érik el, egymás fájl megosztását nem használhatják.

A szervezet hálózata szegmentált, elkülönülnek szerep és funkció szerint a rendszerelemek. Pl. szerverek, DMZ, vagy üzleti folyamatok szegmens.

Ahogy lehetne

Érvényesül a legkisebb jogosultság elve, vagyis a felhasználó csak azt éri el, ami feltétlen muszáj. Ehhez lehet használni Access Control List-et (ACL) az alhálózatok közötti forgalom szabályozására, group policy-kat a szoftverek és jogosultságok kezeléséhez, Access Based Enumeration az SMB/CIFS megosztások korlátozására, stb.

Ahogy lehetne

Központilag menedzselhető végponti védelem alkalmazása.

Data Leak Prevention rendszer alkalmazása.

Kiemelt jogosultságú felhasználók és műveletek szigorú kontrollja, megerősített biztonságú kialakítása.

Magán email szervezeti felhasználásának szabályzati tiltása és betartatása.

Felhő alkalmazások kockázatelemzése, igény szerinti tiltása.

Ahogy lehetne

Központilag menedzselt mentés, mentési rend kialakítása, visszaállítási teszt végzése.

Több platformos kapcsolattartást/validáció/megerősítés – több szem elv.

Naplógyűjtés, naplóelemzés.

Képzés, tudatosítás.

Saját hostolású VTC rendszer.

Köszönöm a figyelmet!

Ajánló:

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kozigazgatasi-kibervedelmi-eszkoztar/

Incidensbejelentés:

csirt@nki.gov.hu