NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

MCC MATHIAS CORVINUS COLLEGIUM
eivok

Mit lehet tudni a kibervédelmi gyakorlatokról?

Dr. Magyar Sándor
egyetemi docens

Változó környezet

- Növekvő számú elektronikus információs rendszerek.
- Kikerülhetetlen okos rendszerek.
- Mindezekkel együtt növekszik a felhasználók, hardverek, szoftverek száma, ezáltal a kockázatok is.
- Nyomás a fejlesztőkön:
  - Rövid határidőre.
  - Egyszerű használhatóság.
  - Könnyű telepíthetőség.
- Piaci előny annál, aki előbb kihozza a terméket.

Kihívások

- Kibertérből érkező fenyegetések azonosítása, kezelése.
- Kritikus infrastruktúrák ellen irányuló kibertér műveletek számának emelkedése.
- Kibertér szereplőinek azonosítása.
- Kibervédelem, mint támogató szerepkör.
- Feltörekvő és felforgató technológiák.

Kibervédelmi gyakorlatok fajtái

Table Top Exercise.

„Asztal mellett” lehetőséget a szakembereknek a forgatókönyv szerinti vészhelyzetek, támadások elleni intézkedések, cselekvési tervek kidolgozására.

Stratégiai döntéshozatali.

Pl. válságkezelési képességek fejlesztése

Technikai.

Eseménykezelési;

Nyomrögzítési;

Támadó-védekező (Red Team – Blue Team)

Stb.

Komplex.

A kibervédelmi gyakorlatok fázisai

A kibervédelmi gyakorlatok célja

- Felkészülés a kibertérből érkező fenyegetésekre.
- Képességek fejlesztése.
- Hiányosságok feltárása, azonosítása.
- Új eljárásrendek tesztelése.
- Együttműködés, információmegosztás elősegítése:
  - szakmai területek között;
  - szervezetek között;
  - nemzetek között.

Megelőzés

Célja a fenyegetések bekövetkezéseinek valószínűségét csökkenteni.

- Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok.
- Sérülékenységvizsgálatok.
- Behatolási tesztek.
- Szoftverek biztonsági bevizsgálása.
- Biztonsági tudatosítás.
- Hardening.

Észlelés

Célja a támadásra és eseményre a lehető legkorábban történő reagálás.

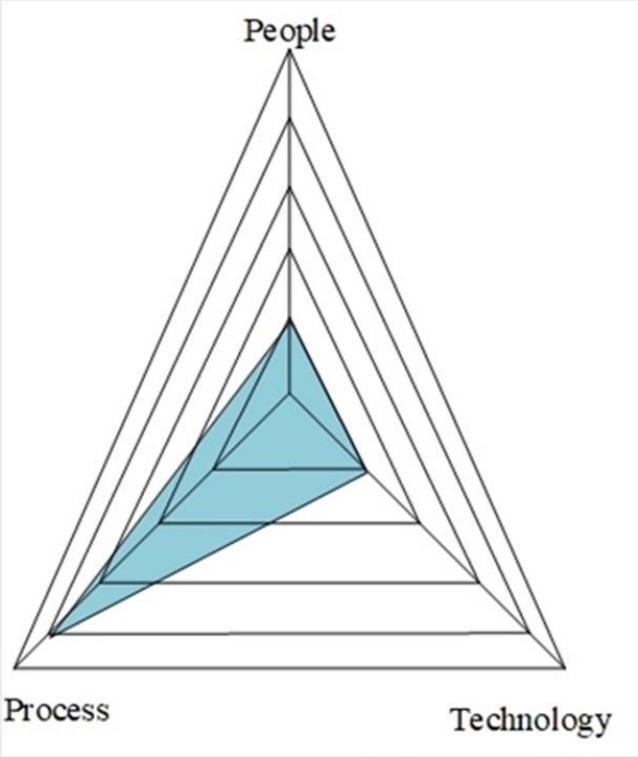
- Biztonsági Műveleti Központ (Security Operation Center).

Javítás, korrekció

Beavatkozás a későbbi károk valószínűségének csökkentése érdekében.

- A biztonsági események kezelése és műszaki vizsgálata.
- Új eljárásrendek kialakítása.
- Szükséges fejlesztési irányok meghatározása.

People, Process, Technology



Eljárásrendek kialakítása

- Kompromittálódásra mutató jelek (IoC) Jelentési folyamat

- IoC hiányában nincs mit megosztani.

Összegzés

- Ami az életben nem működik, akadozik, az a gyakorlat során is felmerül kihívásként.
- Nagy hangsúlyt kell fordítani a tapasztalatfeldolgozásra a gyakorlatok után.
- A megelőzés, észlelés, korrekció területei hatással vannak egymásra.
- Együttműködésnek kiemelt szerepe van.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

MCC MATHIAS CORVINUS COLLEGIUM eivok

Köszönöm a megtisztelő figyelmet!