Védekezés/Támadás a kibertérben

ELŐADÓ: VARGA ÁRPÁD (NMHH, ELTE ÁJK)

2023.05.22.

Vizsgált kibervédelmi szerepek

- Riasztásfeldolgozás
- Fenyegetésekkel kapcsolatos hírszerzési adatok felhasználása és előállítása (Threat Intelligence)
- **Incidenskezelés (Incident Response)**
- **Fenyegetettség feltárás (Threat Hunting)**

Feladata a megelőzés, a felderítés és a kiberbiztonsági fenyegetettségekre, eseményekre adható válaszok kidolgozása...

Mit jelent a hack-back tevékenység?

- A sértett, vagy a jogsértéssel érintett fél aktív magatartása
- Az elkövető információs rendszeréhez történő hozzáférés
- Bizonyítékok gyűjtése
- Átalomcsökkentés

Lépései:

- A behatolást végző infrastruktúra azonosítása
- Sérülékenység feltárása, technikai interakció a támadó és a védekező között
- Aktív visszatámadás (pl. zárolás, túlterhelés, malware stb.)
- Az eltulajdonított adatok törlése, információgyűjtés a behatolóról

A jogos védelem keretei és korlátai

Kérdés: A behatolás/behatoló adatainak aktív elérése, akár a visszatámadás tekinthető-e a védekezés részének?

<u>Jogos védelem</u>

Jogtalan támadás <-> jogszerű védekezés

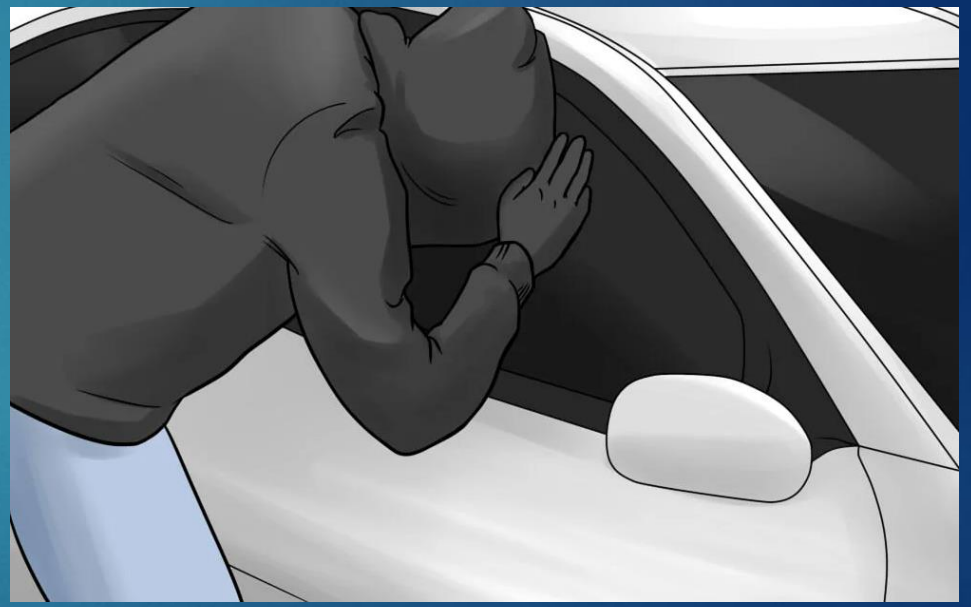
Közvetlen fenyegetés

Személy, javak vagy közérdek ellen

Nem feltétel, hogy ember fejtse ki

Az elvétel folyamatának védekező általi megszakítása

Kúria EBH 2018.B.11.



Legalizáció és dilemmák

Egyesült Államok

- Active Cyber Defense Certainty Bill (2017)
- Eltulajdonított adatok törlése
- Szerverek elérése
  - Támadó lokalizációja
  - Támadás megakasztása
  - A támadós megfigyelése a későbbi megelőzéshez

Korlátozások:

- Csak az USA területén
- Felelősség más sértetteknek okozott kárért
- FBI értesítése -> nemzetbiztonsági vizsgálat
- „önbíráskodás" a jogos védelmen túl
- 2017 óta álló jogalkotás

Ausztrália

- Information Warfare division
- Állami szervek „aktív" kibervédelme
- Bankszektor, nagyvállalati szféra

Legalizáció és dilemmák

Kibervédelmi szabályozás kiterjesztése, hírszerzés, adatok visszaszerzése, korlátozott behatolás (pl. NIS 2) – arányos és indokolt

Passzív védelmi eszközök, információgyűjtés, honeypot-ok, támadási technikák megfigyelése

Támadó információs rendszerében végzett aktivitás, kényszerítés (pl. malware, Dos/DDos)

Az állam „tétlensége” – Kibervédelmi ipar szerep vallásának bővülése

Konklúzió

Büntetőjogi értelemben van mozgástér az aktív védekezésre

De: korlátozott mértékben és felmerül a nemzetközi elhárítás problémája

Érvek mellette:

- A kibervédelmi tevékenység magánpiacának hatékonyabbá tétele
- Proaktív kiberbiztonság akár a műveleti központokban is (TH)
- Az állam védelmi feladatainak kiegészítése

Ellenérvek:

- Önbíráskodás és hatáskörtúllépés veszélye
- Nagy erőforrásigény
- Gyakorlati megvalósulás és valós idejű aktivitás nehézségei

Köszönöm a figyelmet!

E-mail: varga.arpad@nmhh.hu