Kiberbiztonsági fenyegetések és információs sebezhetőség

Az OSINT komplex vizsgálata

„Többet tudni rólad, mint te magadról – nyílt forrásból”

OSINT

Nyílt forrású adatgyűjtés

Szigedi-Tóth Noémi
Konzulens: Dr. Kelemen Roland

Előadás célja és felépítése

01 **Fogalmi alapok**

OSINT jelentése, jelentősége és jogi keretei.

02 **Hipotézisek**

Adatvédelmi paradoxon és az online adatmegosztás kockázatai.

03 **Kutatási eredmények**

Kérdőív, interjúk és OSINT-gyakorlat fő tanulságai.

Kutatói fókusz

Hogyan válik a nyílt forrású adatból kockázat, ha az információk összekapcsolhatók?

Bemutatkozás

- Kiber nyomozó szakirányú alapdiploma
- Személyes és szakmai kötődés a témához

Hipotézisek és módszertan

H1 — adatvédelmi paradoxon
A felhasználók nézetei és tényleges online viselkedése között jelentős eltérés lehet, ami túlzott adatmegosztáshoz vezet.

H2 — alábecsült digitális lábnyom
A felhasználók gyakran alulbecsülik, mennyi nyíltan elérhető adat kapcsolható össze róluk.

Kérdőív

Interjúk

OSINT-elemzés

Vegyes módszertan: kvalitatív és kvantitatív eljárások triangulációja

OSINT fogalma és jogi kerete

Mi az OSINT?
- Nyílt forrású információk gyűjtése és elemzése
- Bárki számára hozzáférhető forrásokra épül
- Nem hackelés, hanem elemző munka

Miért fontos?
- Mindenki hagy digitális lábnyomot
- Az adatok könnyen összekapcsolhatók
- A mozaikhatásból részletes profil épülhet

Adatvédelmi elvek
- adatminimalizálás
- célhoz kötöttség
- nyílt források jogszerű használata

Fő jogi keretek
- GDPR: személyes adatok
- Ptk.: személyiségi jogok
- Btk.: tiltott határok

Lényeg
Nem az OSINT legitimitása kérdéses, hanem annak jogszerű, arányos és etikus gyakorlása.

OSINT eredményeinek felhasználása

A nyílt forrásból összegyűjtött információk több bűncselekmény előkészítéséhez is alapot adhatnak.

$3,05 Mrd	89.129 db	$216 M
üzleti e-mailes csalás (BEC) okozott kára	Zsarolás bejelentési szám	adathalászat becsült kára

Tipikus kockázati utak

BEC • személyiséglopás • zaklatás • zsarolás • adathalászat • adatszivárgás

Kérdőíves kutatás

98 fő	62 / 37 / 1%	45%	torzítás
kitöltői minta	nő / férfi / egyéb	18–30 éves korcsoport	educated youth

A kérdések fókusza
- adatbiztonsági szokások
- internetes megosztási szokások
- digitális kompetenciák

A kérdőív célja
Tipikus „támadási felületek” kijelölése az esettanulmány-alapú OSINT-vizsgálathoz.

Kérdőív eredményei: három gyenge pont

Sütikezelés

29,6% csak szükséges sütiket engedélyez

28,6% minden sütit automatikusan elfogad

Tanulság: adatvédelmi tudatossági rés.

Technikai védelem

39,8% reklámblokk

16,3% kétfaktoros hitelesítés

3,1% VPN rendszeresen

Tanulság: nem egységes védekezési gyakorlat.

Jelszókezelés

66,3% csak szükség esetén változtat

15% rendszeresen változtat

Tanulság: kifejezetten gyenge gyakorlatok.

Összkép: a védekezési eszközök és a tudatos beállítások használata nem következetes.

Interjúk és OSINT-gyakorlat

Előzetes interjúk
A résztvevők önbevallása alapján alapvető tudatosság és adatminimalizálási törekvés látszott, de erős kontrollérzet is megjelent.

OSINT-lépések
- technikai előkészítés
- etikai és adatvédelmi mérlegelés
- adatok összekapcsolása → mozaikhatás

Megtalált adatok példái
konkrét lakcímek • kapcsolati háló • munkahely és beosztás • családtagok • hobbik és rutinok • arcképek és teljes alakos fotók

Fő felismerés: az online kontrollérzet gyakran erősebb, mint a tényleges kontroll.

Levont következtetések

Technológiai szint és humán tényező
A védelmi rendszerek fejlődnek, de önmagukban nem elegendők.

Tudatosság
A felhasználók túlértékelhetik saját adatvédelmüket.

Fő realizációk: kontroll illúziója, digitális lábnyom tartóssága, harmadik felek szerepe

Mozaikhatás
A nyílt forrású adatok összekapcsolása új jelentéseket és kockázatokat hoz létre.

Stratégiai következtetés
A védelem kulcsa az oktatás, a tudatosság és a kritikai gondolkodás fejlesztése.

Köszönöm szépen a megtisztelő figyelmüket!