KÖFOP-2.1.2-VEKOP-15- 2016-00001
A jó kormányzást megalapozó közszolgálat-fejlesztés

Az okos város (Smart City)

2.6. rész

Nemzeti Közszolgálati Egyetem

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Az okos város (Smart City)

Okos biztonság
(Okos város kiberbiztonsága)

Dr. Krasznay Csaba

adjunktus

Nemzeti Közszolgálati Egyetem

Elektronikus Közszolgálati Intézet

Budapest, 2018

Tartalomjegyzék

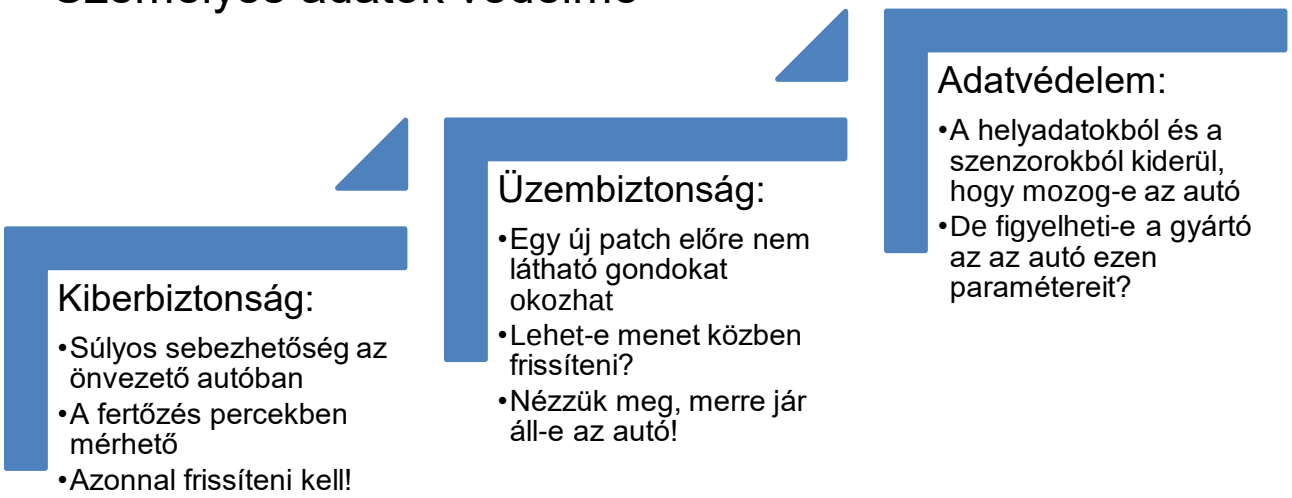
- Kiberbiztonsági kihívások napjainkban
- Kiberbiztonság az okos városokban
- Lehetséges fenyegetések
  - a közlekedési rendszerben
  - az energiaellátásban
  - a vízellátásban
- Esettanulmány
- Megelőzés: tudatosság, szabályozás, műszaki védelem

Kiberbiztonsági kihívások napjainkban

- A Cybersecurity Ventures becslései alapján:
  - A kiberbűnözés **6 billió dollárnyi** kárt fog okozni 2021-ben, ez 2015-ben **3 billió dollár**.
  - 2017-2021 között **1 billió** dollárt fogunk költeni kiberbiztonsági termékekre és szolgáltatásokra
  - Mindeközben **1 millió** nyitott állás van kiberbiztonsági területen, mely **1,5 millióra** fog nőni 2019-ig. A munkanélküliségi mutató **0%.**
- Eközben:
  - A NATO szerint 2016-tól a kibertér hivatalosan is hadviselési színtér
  - Egyes becslések szerint 2016-ban az internetezők **2-3%-a** találkozott zsarolóvírussal
  - A Wannacry zsarolóvírus miatt Nagy-Britanniában össze kellett hívni a nemzeti kríziskezelésért felelős miniszteri tanácsot
- Már ma olyan szinten ki vagyunk téve a kibertér fenyegetéseinek, amit nehezen tudunk felmérni. Az okos városok elterjedése ezt a kitettséget határozottan növelni fogja!

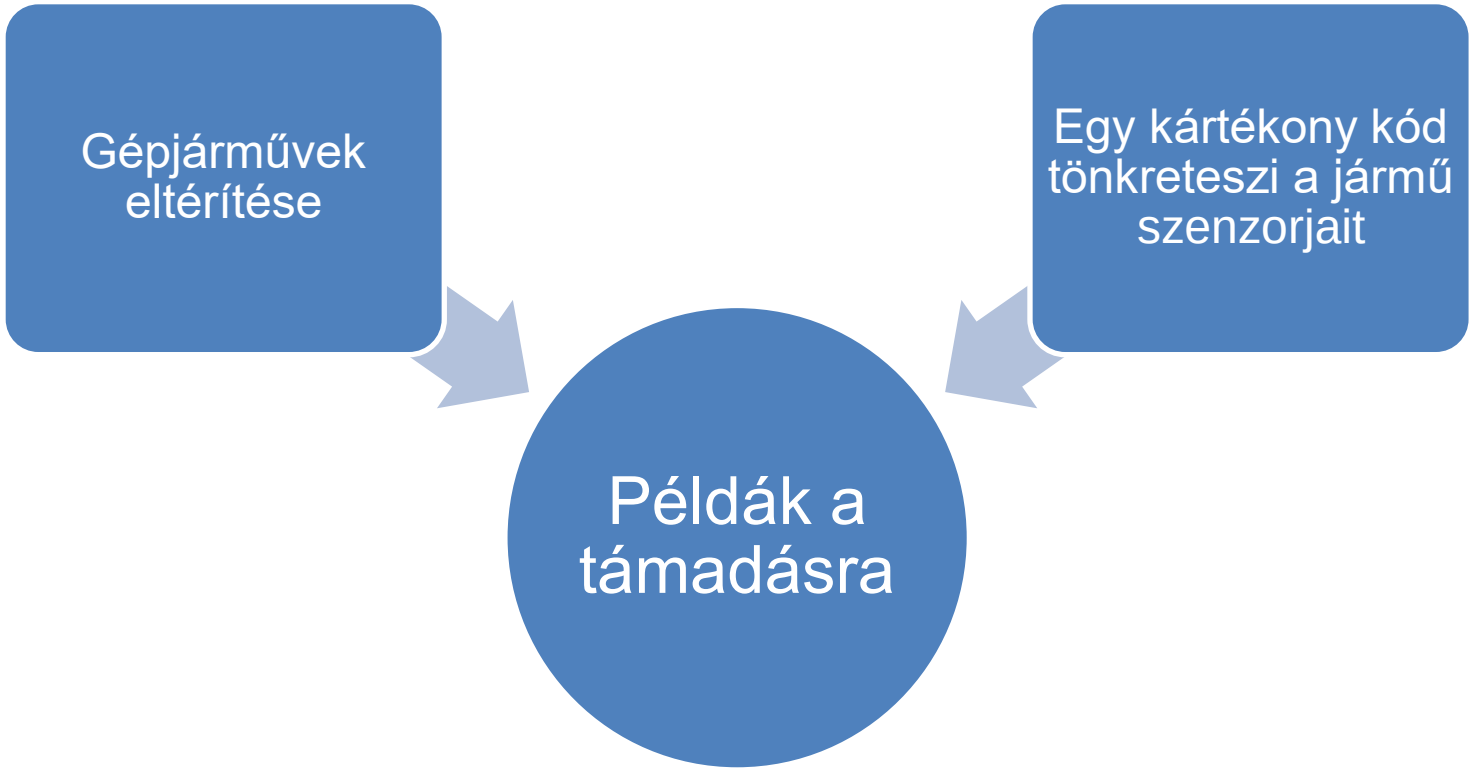
Az okos város biztonsági kihívásai

- Az okos városok biztonsági szempontból a specialitása, hogy egyszerre kell figyelembe vennie a következőket:
  - Üzembiztonság
  - Kiberbiztonság
  - Személyes adatok védelme

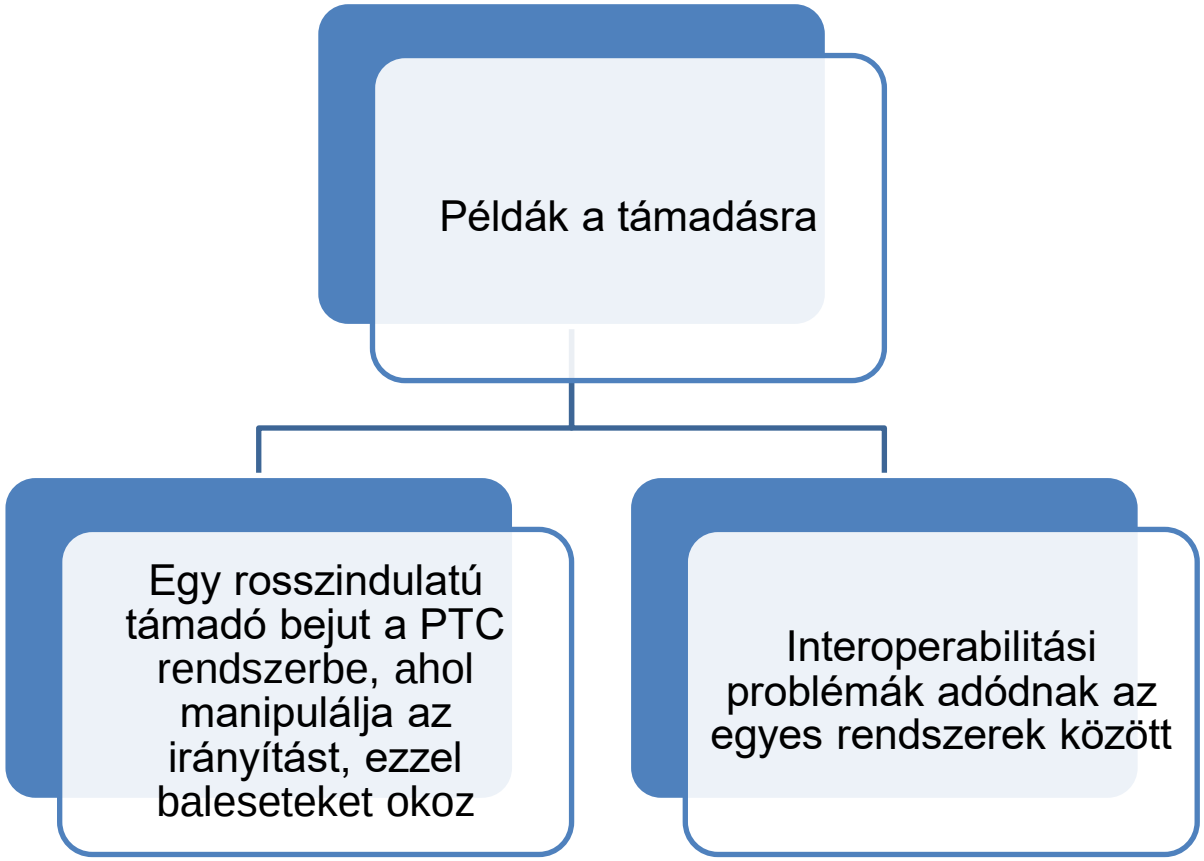


A következő példák a U.S. Department of Homeland Security *The Future of Smart Cities: Cyber-physical Infrastructure Risk* tanulmánya nyomán a közlekedés, az energiaellátás és a vízközművek területén mutatják be, hogy az okos város koncepció milyen új biztonsági kockázatokat jelenthet!

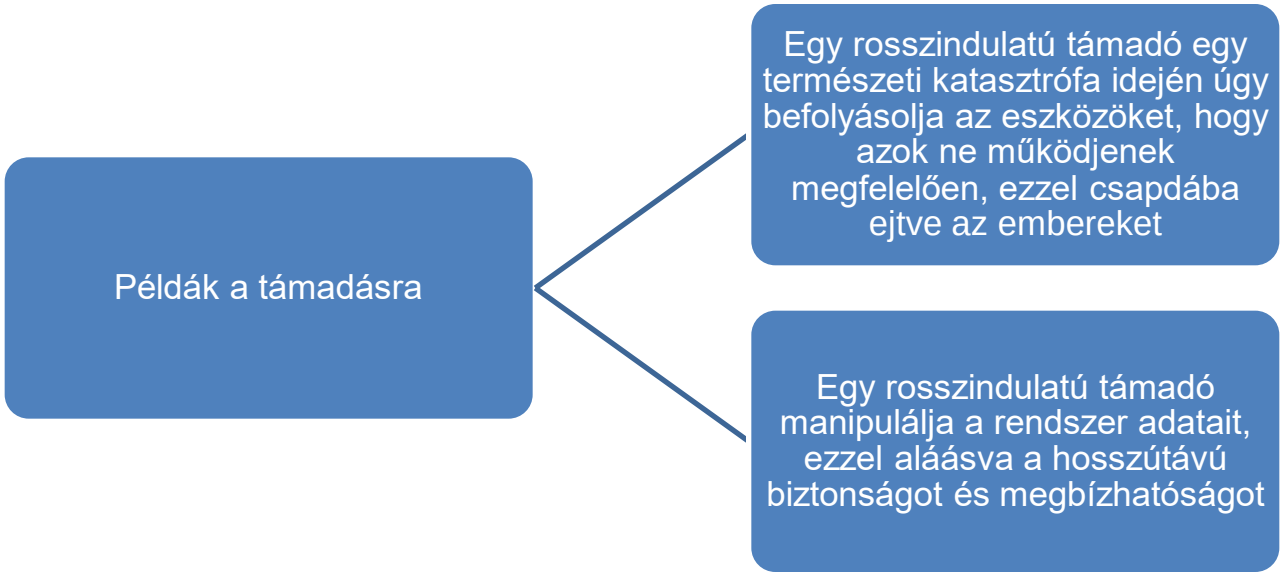
Autonóm közlekedés



Pozitív vonatbefolyásolás



Intelligens közlekedésirányítási rendszerek



V2V és V2I kommunikáció

Példák a támadásra

- Egy rosszindulatú támadó manipulálja a V2V és V2I jeleket
- Egy rosszindulatú támadó megzsarolja a gépjármű-tulajdonosokat vagy gyártókat (pl. ransomware)

Intelligens erőművek

Példák a támadásra

Egy rosszindulatú támadó hozzáférést szerez a SCADA rendszerhez

Egy rosszindulatú támadó jogosulatlan hozzáférést szerez az erőmű hagyományos IT rendszereihez

A „régi” és az „új” rendszerek találkozása előre nem látott problémákat okoz

Okos elosztás és átvitel

Példák a támadásra

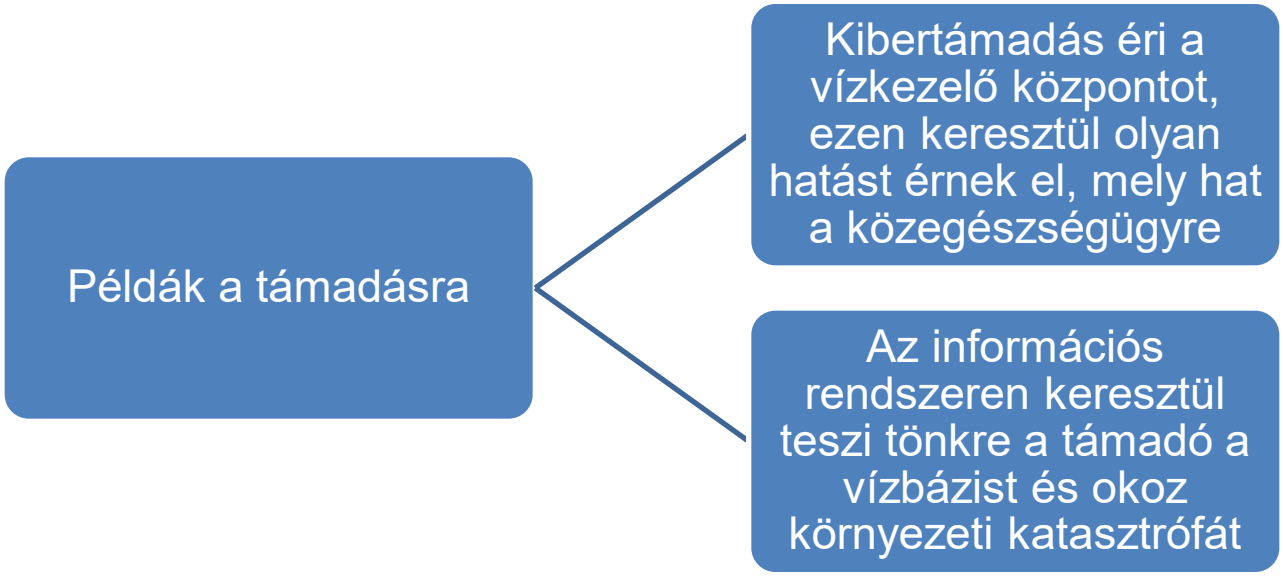
- Egy rosszindulatú támadó kompromittálja az átviteli rendszert, ezzel megfosztva a felhasználókat az áramellátástól
- Egy rosszindulatú támadó manipulálja az energiaárakat mutató adatokat, emiatt a rendszer inkonzisztens módon irányítja a megtermelt energiát

Okos mérőhelyek

Példák a támadásra

- A mérőhelyek elleni támadással a háztartások áram nélkül maradnak
- A mérőhelyek elleni támadással a támadó be tud jutni a háztartások belső informatikai hálózatába

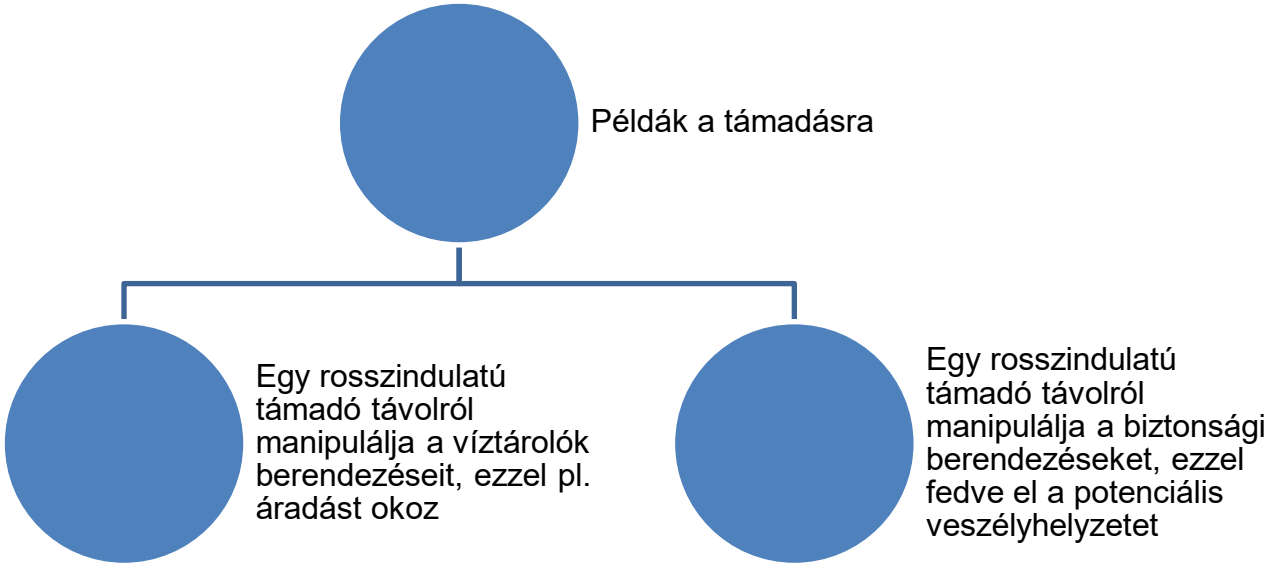
Okos vízkezelés



Okos vízelosztás

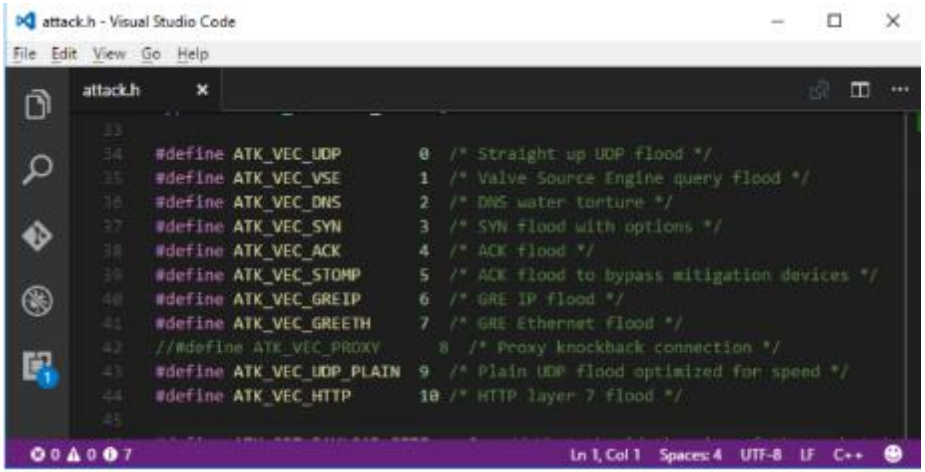
Példák a támadásra	Egy rosszindulatú támadó távolról behatol a rendszerbe és lekapcsolja az érzékelő szenzorokat, így szennyezett víz kerül a háztartásokba
	A támadó rendkívüli időjárási helyzetben teszi lehetetlenné, pl. a felgyűlt csapadékvíz elvezetését

Okos víztárolás



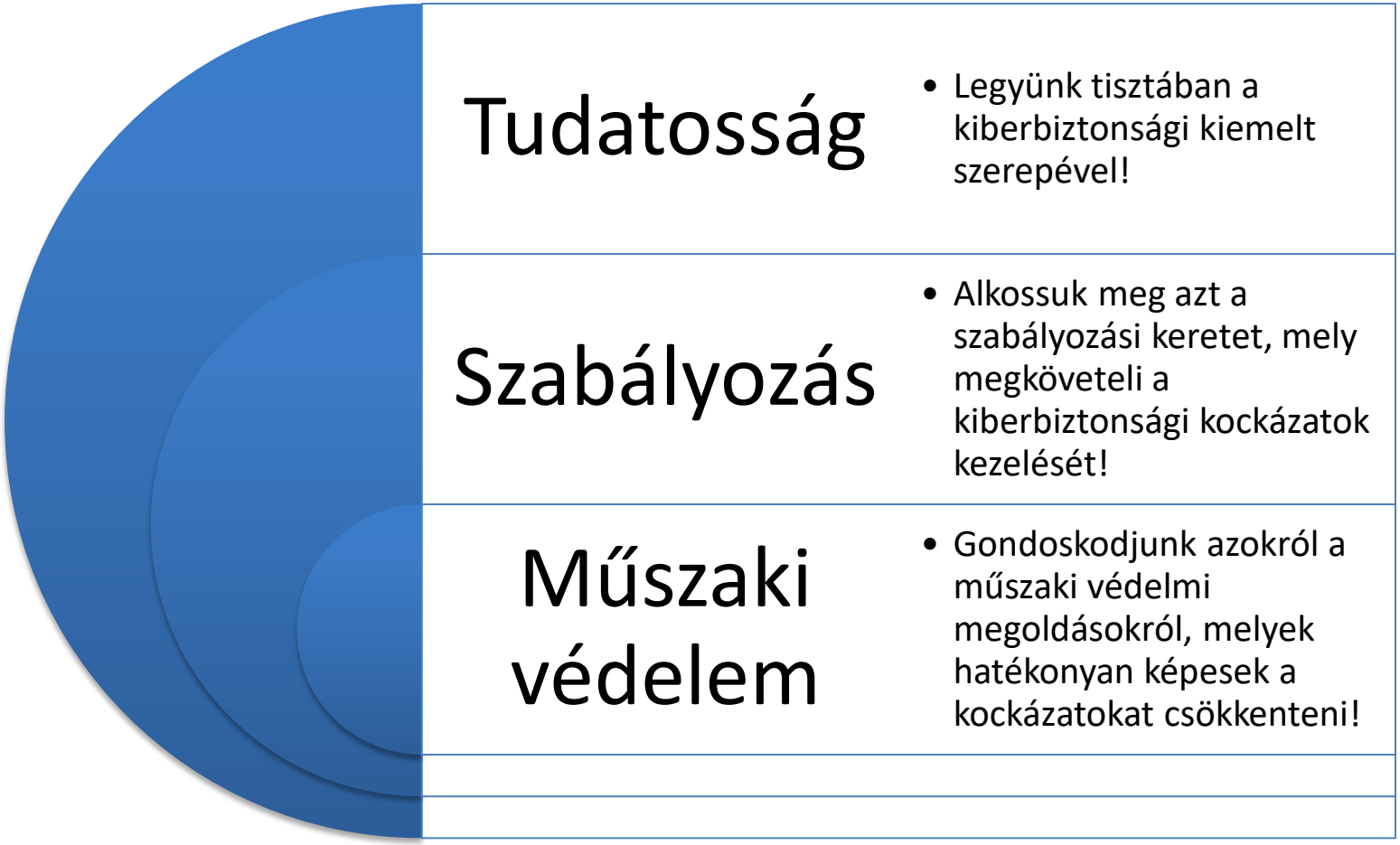
IoT esettanulmány: Mirai botnet

- Első megjelenés: 2016. augusztus
- Célpontok: régebbi Linux alapú IoT eszközök, elsősorban IP kamerák, routerek
- Fertőzési sorrend:
  - IP tartományok scannelése elérhető eszközök után
  - Sebezhető eszközök esetén hozzáférés beégetett jelszavakkal
  - A bot telepítése, a riválisok botok kiirtása
  - Csatlakozás a C&C szerverhez
  - Igény szerint támadás
- Célpont: DNS szolgáltatások, a legnagyobb a Dyn szolgáltató ellen -> Port 53 UDP flood, ~600GBps és ~1.2TBps között
- Számos szolgáltatás leállt, pl. Netflix
- **Tanulság: Frissítés, hálózati védelem, hozzáférés kontroll**.
  Enélkül jobb eredmény ne várjunk!



Forrás: Graham, R.: *Mirai and IoT Botnet Analysis*

Megelőzés, mint a legolcsóbb kockázatkezelési megoldás



Irodalomjegyzék
Okos biztonság

Elmaghraby, A. S., Losavio, M. M.: *Cyber security challenges in Smart Cities: Safety, security and privacy*. Journal of Advanced Research. Volume 5, Issue 4, July 2014, Pages 491–497. http://www.sciencedirect.com/science/article/pii/S2090123214000290

Graham, R.: *Mirai and IoT Botnet Analysis*, RSA Conference 2017, https://www.rsaconference.com/writable/presentations/file_upload/hta-w10-mirai-and-iot-botnet-analysis.pdf

Orbók, Á.: *Challenges and Risks in The Smart Cities,* In: Eva Kellnerová, Kateřina Pochobradská, Kristýna Binková (ed.): New Approaches to the National Security : 11th PhD Conference Proceedings. 443 p.

US. Department of Homeland Security: *The Future of Smart Cities: Cyber-physical Infrastructure Risk*. August, 2015.

Zhu, Y., Zuo, J.: *Research on Security Construction of Smart City*. International Journal of Smart Home, Vol. 9, No. 8 (2015), pp. 197-204 http://www.sersc.org/journals/IJSH/vol9_no8_2015/21.pdf

Az okos város (Smart City)

Okos biztonság

Köszönöm megtisztelő figyelmüket!

krasznay.csaba@uni-nke.hu

Nemzeti Közszolgálati Egyetem

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE