NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

Információbiztonság vs. kiberbiztonság – az okos város szempontjából

Dr. Krasznay Csaba
NKE Kiberbiztonsági Akadémia

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Definíciók

Információbiztonság: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Mi a kiberbiztonság ma?

5% technika

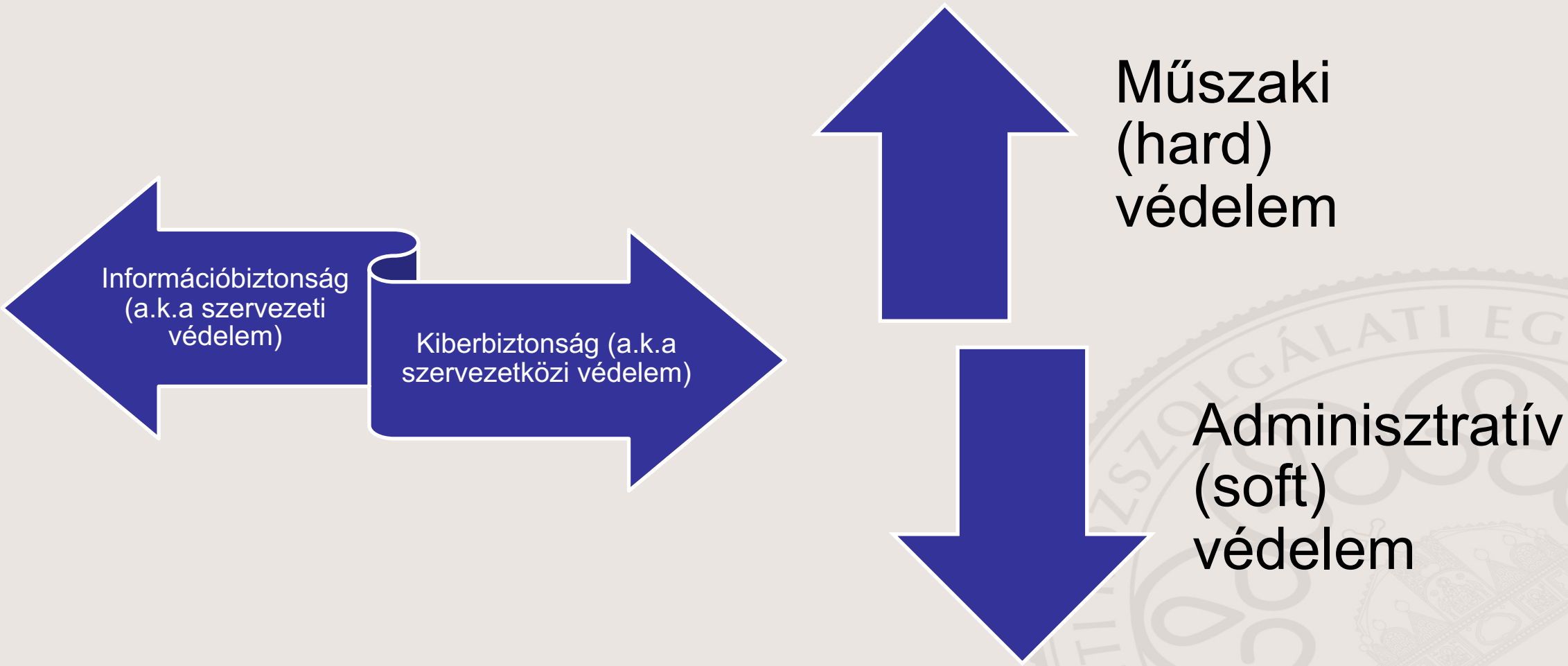
Michael Schwarz, Daniel Gruss, Moritz Lipp, Stefan Mangard – TU Graz, az idei Pwnie Awards díjazottjai

95% stratégia*

Toomas Hendrik Ilves és Marina Kaljurand, Észtország korábbi elnöke és külügyminisztere

* Legalábbis az EDA képviselője szerint

A dilemma

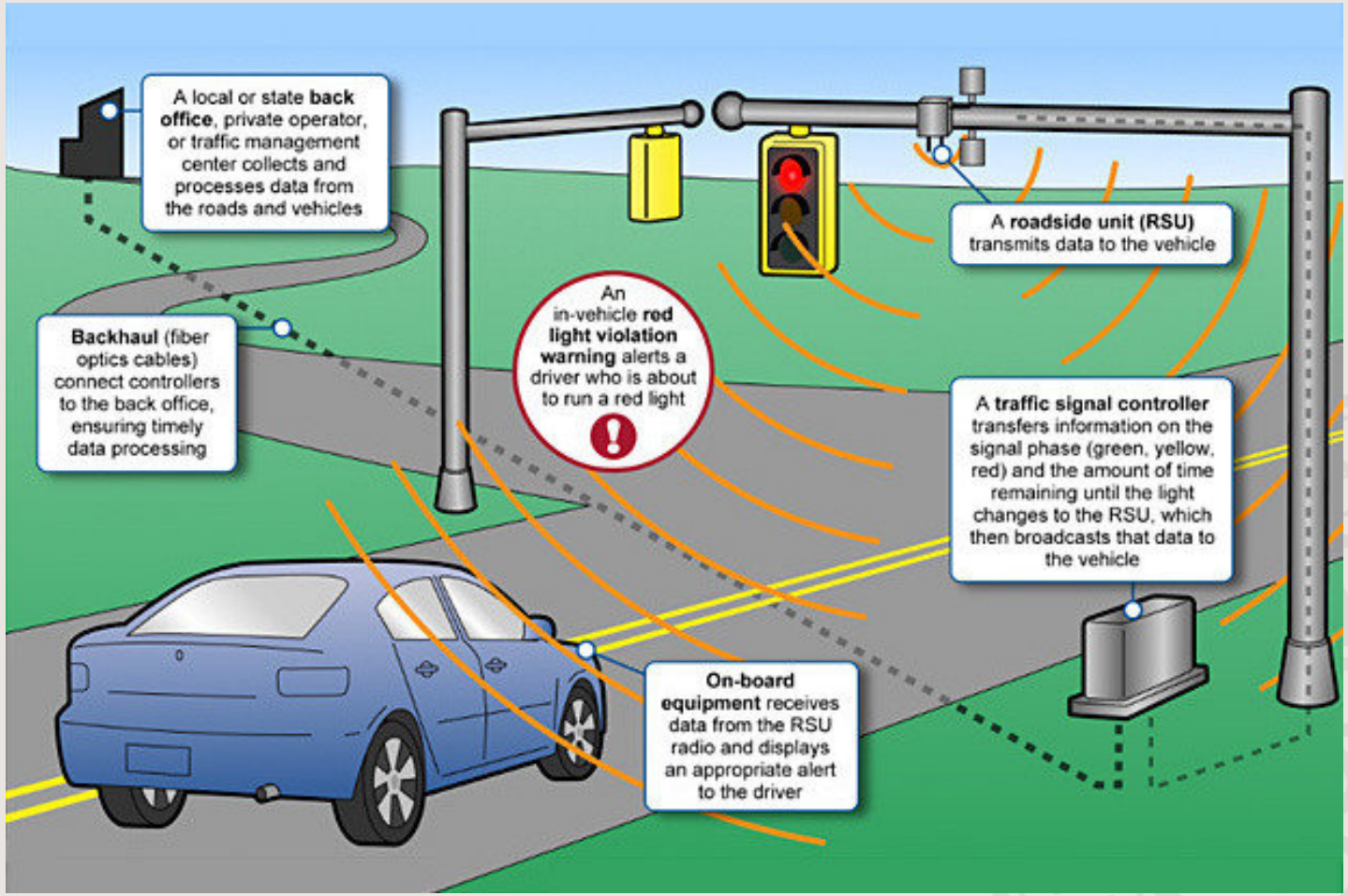

Információbiztonság (a.k.a szervezeti védelem)
Kiberbiztonság (a.k.a szervezetközi védelem)
Műszaki (hard) védelem
Adminisztratív (soft) védelem

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Mindez a gyakorlatban: ki véd meg a pirézektől?

	Műszaki	**Adminisztratív**
Szervezeti	• Cél: Célzott és tömeges (malware) támadások kivédése a szervezet IT biztonsági infrastruktúrájának segítségével • Feladat: Biztonságos és az elvárásoknak megfelelő alkalmazás és infrastruktúra fejlesztés és üzemeltetés	• Cél: A szervezet információs vagyonának és hírnevének megóvása az üzleti folyamatok támogatásával. • Feladat: A compliance és a tulajdonosi elvárásoknak megfelelő biztonsági kultúra kialakítása és fejlesztése
Szervezetközi	• Cél: A releváns információk alapján létrejövő helyzeti tudatosság (situational awareness) defenzív vagy offenzív reagálás. • Feladat: Műszaki információk gyűjtése, megosztása, threat hunting, digital forensics, exploit fejlesztés	• Cél: A nemzeti ellenállóképesség (resiliency) fejlesztése. • Feladat: A nemzeti szabályozási környezet kialakítása, működtetése, kezdeményezés és reagálás a nemzetközi együttműködés rendszerében

Smart city példa

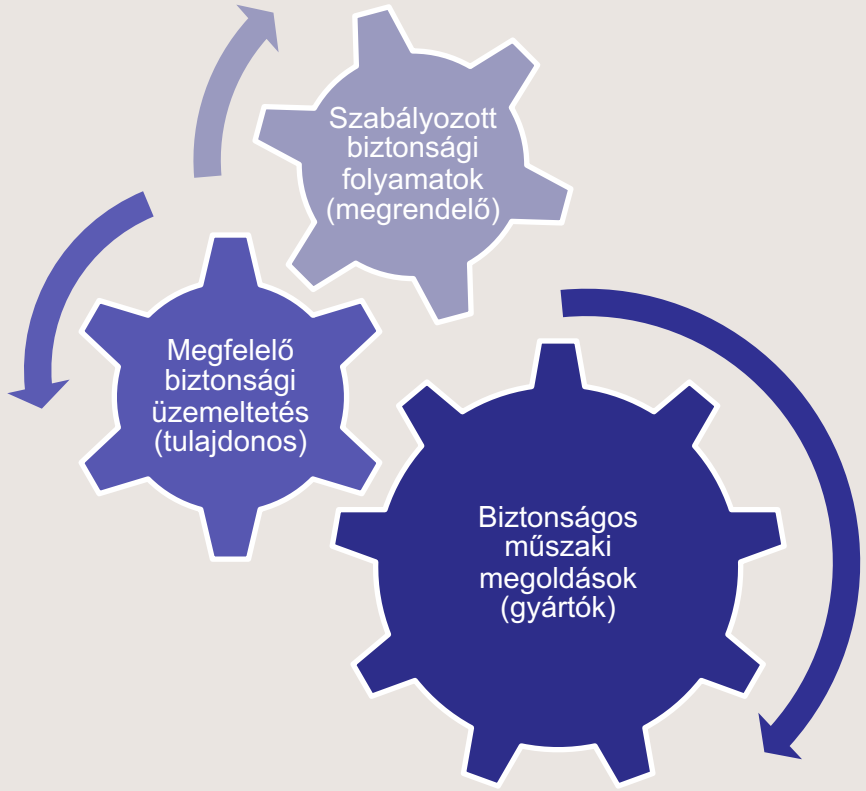


Forrás: https://www.networkworld.com/article/2993888/security/six-key-challenges-loom-over-car-communication-technology.html

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Kinek mi a feladata?

(Ön)kormányzati információbiztonság



Kormányzati kiberbiztonság

Európai szabályozások

Nemzeti stratégiai védelem

Kormányzati műszaki intézkedések

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

NIS Direktíva

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE

(2016. július 6.)

a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

14. cikk

(1) A tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők megfelelő és arányos műszaki és szervezési intézkedéseket tesznek a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. A hálózati és információs rendszerek tekintetében az említett intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell biztosítaniuk.

(2) A tagállamok gondoskodnak arról, hogy az alapvető szolgáltatásokat nyújtó szereplők megfelelő intézkedéseket tesznek az ilyen alapvető szolgáltatások nyújtása során alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére annak céljából, hogy biztosítsák az említett szolgáltatások folytonosságát.

(3) A tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők indokolatlan késedelem nélkül bejelentik az illetékes hatóságnak vagy a CSIRT-nek az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket. A bejelentéseknek tartalmazniuk kell az ahhoz szükséges információkat, hogy az illetékes hatóság vagy a CSIRT meg tudja határozni az adott biztonsági esemény esetleges határon átnyúló hatásait. A bejelentés nem róhat többletfelelősséget a bejelentő félre.

„alapvető szolgáltatásokat nyújtó szereplő”: a II. mellékletben említett típusú olyan közjogi vagy magánjogi szervezet, amely megfelel a 5. cikk (2) bekezdésében meghatározott kritériumoknak; pl. 2. Közlekedés, d) Közúti közlekedés: A 2010/40/EU európai parlamenti és tanácsi irányelv 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetői

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Cybersecurity Act

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)

- „A bizalom és biztonság megteremtése és megőrzése érdekében az IKT-termékekbe és -szolgáltatásokba már a műszaki tervezés és fejlesztés korai szakaszaiban közvetlenül be kell építeni a biztonsági elemeket (beépített biztonság). Továbbá a vásárlóknak és felhasználóknak meg kell tudniuk állapítani az általuk beszerzett vagy megvásárolt termékek és szolgáltatások biztonsági szintjét.”
- „A jelenlegi javaslat meghatározza az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó szabályok átfogó keretrendszerét.”

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Feladatok Magyarországon

- Hazai és nemzetközi együttműködések
- Kiberbiztonsági tudatosság
- Oktatás és képzés
- K+F+I
- NIS implementáció
- (Ön)kormányzati smart city infrastruktúrák megerősítése
- IT biztonság a fejlesztésekben
- Kritikus információs infrastruktúra védelem
- Nem állami, nem KII üzemeltetők motiválása
- Kiberbűnözés elleni fellépés
- A kibervédelem szervezeti rendszerének fejlesztése

E-mail: krasznay.csaba@uni-nke.hu

KÖSZÖNÖM A FIGYELMET!