

Kiberbiztonság és a bizalom építőkövei

Magyarország, 2018. június 7.

Mika Lauhde
Kiberbiztonságért és globális személyi
adatbiztonságért felelős alelnök

A digitális technológiák és a társadalmunk

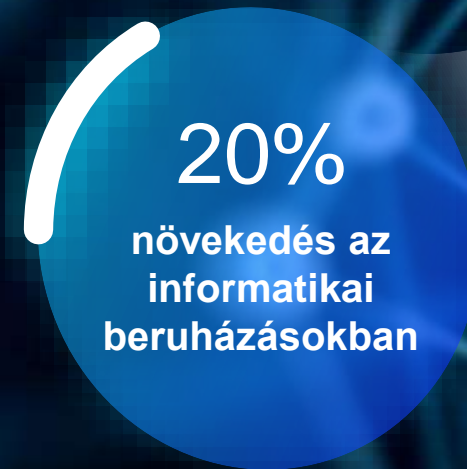
- A digitális technológiák egyre fontosabb szerepet töltenek be a társadalmunkban
- A technológiai fejlődés megállíthatatlan, gyorsul és egyre szerteágazóbban terjeszkedik
- Számos új technológia, szereplő és ökoszisztéma jelenik meg e fejlődést elősegítve, a jelen pillanatban is folyamatosan

Új technológiák

mozgatják

a digitális társadalmat

és gazdaságot



Egy

hipermértékben

hálózatorientált

világ felé tartunk

Intenzívebb adatkapcsolatok

1 millió

kapcsolat minden km²-en

5G

Gyorsabb reakciók

50x rövidebb

reakcióidő

Szupergyors

8GB méretű film:

6 másodperc

„Nincs rózsza tövis nélkül

Új lehetőségek

Minden eszköz hálózatba
kapcsolt

Erőforrás-megosztás és nyílt
környezetek

Mélyebb betekintés
adatokba



Új kihívások

Nagyobb támadási felület,
fokozott sebezhetőség

A hagyományos védelmi
határok összemosódnak

Fokozódik az adatszivárgás
kockázata, nagyobb károk

Ne hagyjuk figyelmen kívül a klasszikus kiberbiztonsági problémákat!

T1 -
SS7 / IPX /
Diameter
támadások

T2 -
IoT-hez kötődő
biztonsági
veszélyek

T3 -
Hamis GSM-
bázisállomások



T4 -
Rádiós protokoll
alapú felhasználó
követés

T7 -
Hálózati funkciók
virtualizálásához
kapcsolódó veszélyek

T6 -
3G/4G üzemmód
2G-re kényszerített
visszakapcsolása

T5 -
Szolgáltatás-
blokkoló
támadások
rádiós felületen

A hírközlés nem ismer határokat

A világ hírközlő rendszerei határok nélküli, többszereplős értékesítési környezetben alapulnak

Ezért a kiberbiztonságnak is határokon átívelőnek kell lennie

A kormányok számára már egyértelmű a létfontosságú infrastruktúra fogalma, és annak védelmére szolgáló eszközöket, módszereket keresnek

Az országukban alkalmazott lehetőségek keretein belül

A hírközlés és a kiberbiztonság

Időigényes, pragmatikus, holisztikus munka

A szabványosítástól a termékek kifejlesztéséig évek telnek el

A ma meghozott döntések a következő évekre, esetleg évtizedekre is hatással lesznek

Technológia

Önmagában nem
alakít ki bizalmat



Intelligens ener-
getikai hálózatok



Intelligens
robotok



Neurális
kötelek

Diagnosztikai
segédeszközök

Mesterséges
intelligencia

Blokklánc
technológia

**A bizalomhoz több kell, mint kiváló
műszaki termékek**

**Nemcsak az számít, hogy milyen jó
termékeket hozunk létre**

**Az is fontos, hogy milyen módon hozzuk
azokat létre**

A vállalatokba vetett belső kiberbiztonsági bizalom megteremtése

Jövőkép, Stratégia, Vállalatpolitika, Folyamatok

Emberi erőforrás

Kutatás-fejlesztés

Visszaigazolások és auditok

Külső beszállítók kezelése

Gyártás

Termékek, megoldások és szolgáltatások biztosítása

Problémák, hibák és gyenge pontok kiküszöbölése

Fenntarthatóság

A vállalatokba vetett külső kiberbiztonsági bizalom megteremtése

Fejlesztés és külső kutatási programok

Szabványosítási javaslatok

Hozzájárulás nyílt forráskódú rendszerekhez

Szabadalmi védelem és keresztlicenc-szerződések

Együttműködési képességek tesztelése

Tanúsítás

Átláthatóság megteremtése

Együttműködés kormányokkal, hatóságokkal és vámhivatalokkal

Szál- és biztonsági információk megosztása

Média- és PR-tevékenység



**A biztonság
együttműködésre épülő
fokozása
erősíti a bizalmat**

Komoly erőfeszítések az EU-n belüli átláthatóság megteremtése érdekében

Az EU legutóbbi rendelkezéseinek megértése

Értékek

A lehető legjobb helyi erőforrások kiaknázása

Bizalom felépítése műszaki megoldások és együttműködés révén

Személyes adatok és az európai GDPR

„Az Általános Adatvédelmi Rendelet (GDPR) egy újonnan bevezetett szabályrendszer, mely révén az Európai Bizottság az egyéni adatok Európai Unió (EU) belüli védelmét kívánja egységesíteni és megerősíteni.”

- Személyes adatok védelme már a tervezéstől kezdve, magától értetődően -



A NIS-irányelv és az Európai Létfontosságú Infrastruktúra

„A NIS-irányelv jogi eszközöket nyújt a kiberbiztonság EU-n belüli általános szintjének fokozásához, az alábbiak révén:

- A tagállamok felkészültségének fokozásán keresztül, megfelelő felszereltséget elvárva tőlük, például számítógép-biztonsági incidenskezelő csoport (CSIRT) és illetékes nemzeti NIS-hatóság felállításával.”

- Személyes adatok védelme már a tervezéstől kezdve -



A Huawei és az Európai Átláthatósági Központ

- Brüsszelben található
- 2018. őszén nyílik meg
- Kormányzati ügyfelek számára
- A kormányok és az ügyfelek számára lehetővé teszi a termékeik és rendszereik helyszíni tesztelését, valamint a kiállítási és bemutató környezetben többek között távközlési, banki, oktatási, egészségügyi, vasúti és okos városhoz kapcsolódó funkciókat nyújtó rendszerek biztonsági szintjének felmérését.

The industry mainstream security tools, and Huawei self-development security tools opened to customer testing

	Commercial	Open source or free	In-house
Source Code Audit	coverity, Snyk, klocwork	FindBugs™	Source Code Rule Customization
Antivirus Scan & Digital Signature	Symantec, McAfee, Trend Micro, Avast, AVG		Virus Scan Cloud, Digital Signature service platform
DoS / DDoS Attack	Spirent, Mu-8000	hping, TFN	Attacker
Scanning Tools	AppScan, Acunetix, AppCheck, NGSSQuintel, Nessus	OpenVAS, Nmap	Security testing Cloud
Fuzzing Tools	Insomniac, Spirent, beSTORM	Protos, Hackingtastic, Sully	Fuzz Platform, Fuzz lib
System Security Audit	Nessus, Nexpose, Retina	Baseline Security Advisor	SecureCAT
Simulation Penetration Testing	IDA, Burp Suite, JEB by IRIS, IRIS	Olydbg, tcpdump, Metasploit	Fiddler, Websecart

BUILDING A BETTER CONNECTED WORLD Huawei Confidential 11 HUAWEI

A szabályozó hatóságok szerepe

**Megbízható, átlátható,
konstruktív és nyitott
kibervilág létrehozása**



Thank You.

Copyright © 2016 Huawei Technologies Co., Ltd. All Rights Reserved.
The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Huawei Technologies Co., Ltd.

Questions & Answers?

mika.lauhde@huawei.com