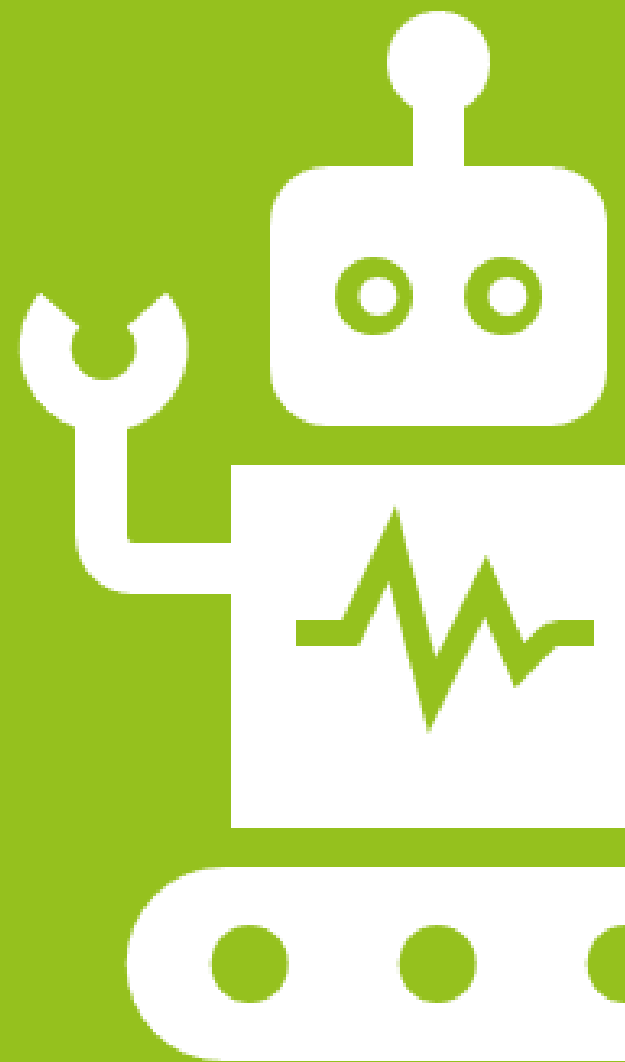
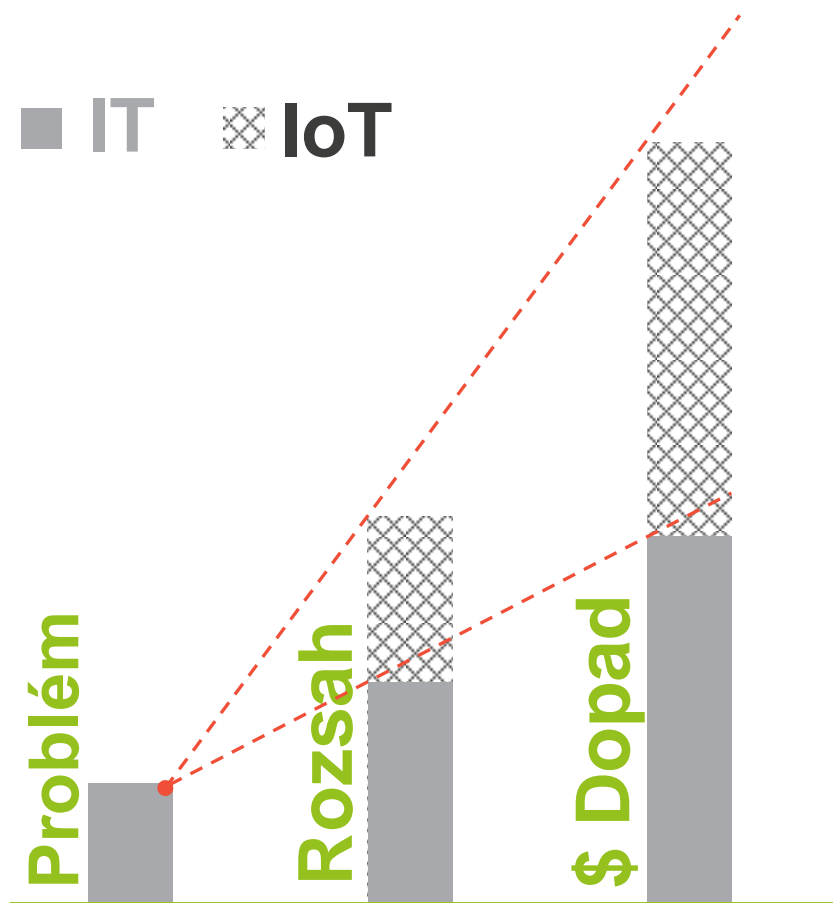


PROČ VÁS NEBEZPEČNÉ IOT ZRUINUJE?

ANTONÍN ŠEFČÍK
DANIEL PŘÍVRATSKÝ



Proč je riziko tak velké?



Faktory způsobující multiplikaci dopadu u IoT

- Velký počet zařízení
- Široká geografická distribuce
- Jednoúčelové přístroje fungující ve vzájemné symbióze

Co nám hrozí?

PŘÍMÉ POŠKOZENÍ UŽIVATELE

Jude Medical musela kvůli hackerům změnit svůj SW u 750 000 kardiostimulátorů

ZNEUŽITÍ / ZTRÁTA DAT

Rozsáhlý DDoS útok postupně znepřístupnil značnou část webů (Netflix, Amazon, Twitter,..).

Útok proběhl skrz IoT přístroje (CCTV, routery)

ZTRÁTA KONTROLY NAD ZAŘÍZENÍM

Výzkumné ovládnutí vozu Jeep Cherokee – plná kontrola nad celým vozidlem včetně volantu a brzd

ZNEUŽITÍ VÝPOČETNÍ HO ZDROJE

Například k těžbě kryptoměn

Jaká odvětví jsou ohrožena?

Město



Průmysl



Domácnost



Zdravotnictví



Automobily



Kdo musí myslet na bezpečnost?

VŠICHNI ZÚČASTNĚNÍ!



Nositel
know-how



Vendor



Integrátor



Provozovatel



Koncový
uživatel

Ale kdo nese největší zátěž? INTEGRÁTOR!



Nositel
know-how



Vendor



Integrátor



Provozovatel



Koncový
uživatel

Nevyčíslitelná finanční a reputační ŠKODA!

AKTUÁLNÍ stav

1 **Konsorcia**
několika společností

2 Bezpečnost
vnímána pouze
v **technické** rovině

3 **Metodiky** zpracovány
zejména
k technickému řešení

4 **Normy a zákony** k
bezpečnosti IoT jsou
na samém počátku

IDEÁLNÍ stav

1. Využití odolných technologií včetně šifrování
2. Výběr „bezpečných“ partnerů a dodavatelů
3. Posouzení zabezpečení prostředí ke kterému je IoT zařízení připojováno
4. Zajištění fyzické bezpečnosti koncových bodů IoT
5. Pravidelná aktualizace a monitoring IoT zařízení

Komplexní řešení bezpečnosti od analýzy po pravidelné přezkoumání a zlepšování

Core Areas of Cybersecurity Standardization	Standard Organization
Cryptographic Techniques	ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C
Cyber Incident Management	ČR, ETSI ; ISO/IEC JTC 1; ITU-T; PCI
Hardware Assurance	ISO/IEC JTC 1; SAE International
Identity and Access Management	ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C
Information Security Management Systems	ČR, ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group; UL
Network Security	3GPP; 3GPP2; IEC; IETF; IEEE; ISO/IEC JTC 1; ITU-T; The Open Group; WiMAX Forum
Physical Security	ASIS International; IEC; IEEE; ISO/IEC JTC 1; NEMA; SIA
Security Automation and Continuous Monitoring	ASIS International; IEC; IEEE; ISO/IEC JTC 1; NEMA; SIA
Software Assurance	ASIS International; IEC; IEEE; ISO/IEC JTC 1; NEMA; SIA
Supply Chain Risk Management	ASIS International; IEC; IEEE; ISO/IEC JTC 1; NEMA; SIA
System Security Engineering	ASIS International; IEC; IEEE; ISO/IEC JTC 1; NEMA; SIA

Konkrétní kroky řešení pro každou oblast: **DATA, SÍTĚ, ZAŘÍZENÍ**

Analýza řešení

Rozsah bezpečnosti
Srovnávací analýza
Analýza rizik
Návrh bezpečnostních požadavků

Návrh řešení

Návrh cílů bezpečnosti, bezpečnostní strategie a politiky
Návrh bezpečnostních opatření, plán zvládnání rizik

Implementace

Dozor nad implementací opatření
Správa a kontrola vývoje rizik
Postupy pro zavedení systému řízení bezpečnosti
Závěrečná zpráva a upravený plán zvládnání rizik

Přezkoumání

Pravidelné přezkoumání stavu bezpečnosti

Legislativní řešení aneb v dále svítá



- V Kalifornii byl přijat zákon [SB-327](#) **Information privacy: connected devices** který nařizuje výrobcům zavést „rozumnou“ úroveň bezpečnosti a vyžaduje, aby připojená zařízení IoT měla jedinečná hesla, která mohou uživatelé měnit
- Velká Británie ohlásila **návrh zákona k zajištění bezpečnosti IoT**, který bude vyžadovat, že:
 - hesla zařízení IoT budou jedinečná a nebude je možné vrátit na výchozí tovární nastavení
 - výrobci IoT produktů poskytnou veřejné kontaktní místo
 - výrobci budou výslovně uvádět minimální dobu, po kterou bude zařízení přijímat bezpečnostní aktualizace
 - bude vytvořen systém označování zařízení IoT pro spotřebitele, k rozpoznání zařízení, která jsou „Secure by Design“

Děkujeme za pozornost.

Prostor pro vaše otázky.

**Jsme vám také k dispozici na našem stánku
nebo nás kontaktujte na www.ngss.cz**