

IDC pohled na nové hrozby – bezpečnost (nejen) kritické infrastruktury

Jan Alexa, Senior Research Analyst, Government Insights

Kde jsme?

V rámci EU se připravuje harmonizace kyberbezpečnosti napříč klíčovými sektory

- EU NIS Directive schváleno EP IMCO Committee in January 2016
- Energetika, doprava, bankovní sektor, finanční trhy, zdravotnictví a zásobování vodou
- Členské státy budou identifikovat „operátory klíčových služeb“ v na základě stanovených kritérií
- Klíčoví ISP (internet service providers) budou muset zabezpečit svoji infrastrukturu a reportovat incidenty



Zákon o kybernetické bezpečnosti

- Klíčová role NBÚ
- Kritické informační systémy
- Významné informační systémy
- Mezinárodní kooperace s EU, NATO, CECSP, a národními autoritami.

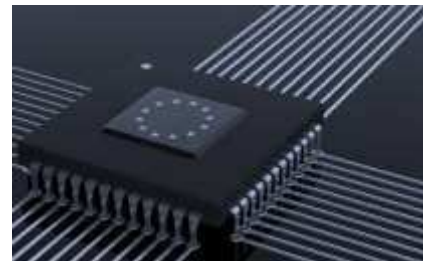
Kam v oblasti kyberbezpečnosti směřujeme?

Závisí na dvou klíčových faktorech:



1. Legislativa

- Naplnění současných zákonných požadavků
- Další vývoj zejména v souvislosti s pravděpodobných schválením Nařízení EU



2. Vývoj v oblasti bezpečnostních hrozeb

- Struktura bezpečnostních hrozeb se mění
- Geopolitická situace
- ..ale hlavně – technologické změny



3. Platforma (3rd Platform technologies)



3. platforma

Triliony

“věcí”

Miliardy

uživatelů

Stovky milionů

uživatelů

Miliony
uživatelů

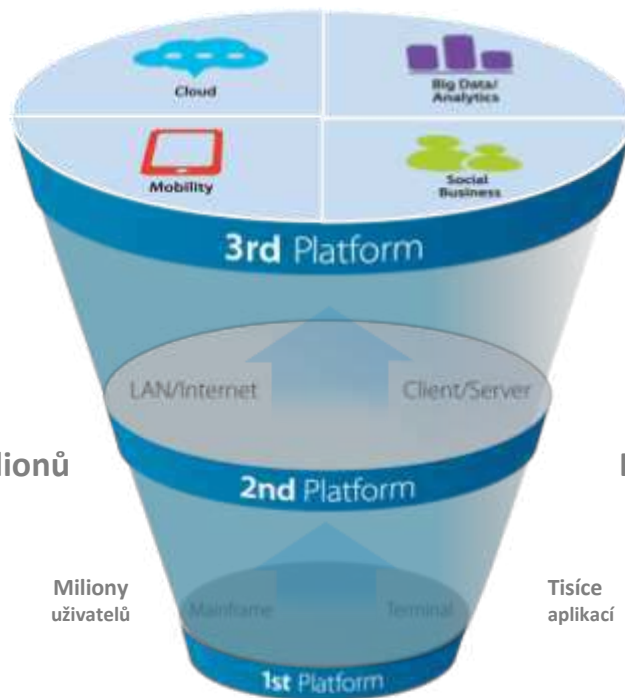
Miliony

aplikací

Desítky tisíc

aplikací

Tisíce
aplikací



Růst objemu dat - Digital Universe



2013 – 4.4 ZB

2020 – 44 ZB



1ZB \approx 1000³ GB



Veřejný sektor v ČR

- Registry
- eHealth
- IZS
- Obce – služby seniorům, wearables

Jistě ne ZB, nicméně objem dat může růst zhruba stejným tempem – tj. zdesetinásobit se do roku 2020.

IDC Predikce #1: Kyberútoky začnou ovlivňovat „fyzický“ svět



Kyberútoky začnou ovlivňovat „fyzický“ svět



- Doposud prakticky všechny kyberútoky měly za cíl krádež dat (případně následně peněz) nebo zneprístupnění či poškození webu či služby. V roce 2016 5% kyberútoků bude mít za následek poškození fyzické infrastruktury či jiný přímý dopad na „fyzický“ svět
- První „vlaštovky“ jsou již několik let staré – Stuxnet, nejnovější závažný případ – Ukrajina 2015 a výpadek proudu pro 225 tisíc obyvatel.

Internet věcí ve zdravotnictví je mimořádně citlivá oblast

- Inzulínové pumpy
- Kardiostimulátory
- Chytré náramky



NEWS ANALYSIS

Researchers hack a pacemaker, kill a man(nequin)

Researchers decided you don't need to be a pen tester to wirelessly hack a pacemaker, to successfully launch brute force and denial of service attacks that can kill iStan simulated humans.

Computerworld | Sep 8, 2015 8:08 AM PT

Forbes / Entrepreneurs
Hacking Insulin Pumps And Other Medical Devices From Black Hat

Researcher shows a ridiculously easy way to hack into smart bracelets like Fitbits
CALE GUTHRIE WEISSMAN (@HTTP://WWW.BUSINESSINSIDER.COM/AUTHOR/CALE.GUTHRIE.WEISSMAN)
MAR 27 2015 1:30 PM

Kyberútoky začnou ovlivňovat „fyzický“ svět – trend je patrný již několik let

Top Threats 2014	Top Threats 2015	Change in ranking
1. Malicious code: Worms/Trojans	1. Malware	→
2. Web-based attacks	2. Web based attacks	→
3. Web application /Injection attacks	3. Web application attacks	→
4. Botnets	4. Botnets	→
5. Denial of service	5. Denial of service	→
6. Spam	6. Physical damage/theft/loss	↑
7. Phishing	7. Insider threat (malicious, accidental)	↑
8. Exploit kits	8. Phishing	↓
9. Data breaches	9. Spam	↓
10. Physical damage/theft/loss	10. Exploit kits	↓
11. Insider threat	11. Data breaches	↓
12. Information leakage	12. Identity theft	↑
13. Identity theft/fraud	13. Information leakage	↓
14. Cyber espionage	14. Ransomware	↑
15. Ransomware/Rogueware/Scareware	15. Cyber espionage	↓

- Pořadí hrozeb je meziročně stabilní, výjimkou je právě ohrožení fyzické infrastruktury.
- Druhým závažným trendem je zvětšující se závažnost hrozeb „zevnitř“

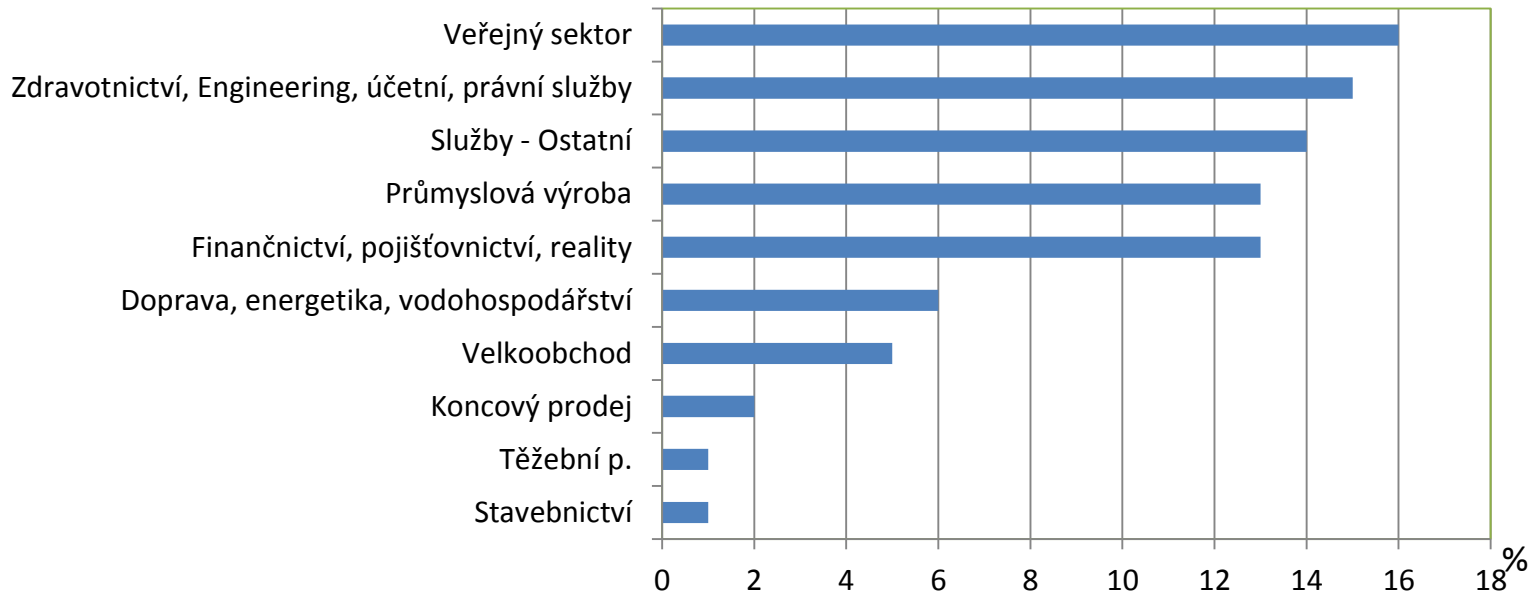
IDC Predikce #2:

Výdaje vládního sektoru na kybernetickou bezpečnost
vzrostou



Sektory v ohrožení

Top 10 sektorů cílem tzv. Spear-Phishing útoků 2013



Source: Symantec Internet Security Threat Report 2014

Vládní sektor – bezpečnostní prostředí se mění

V zahraničí dochází k rozsáhlým případům špionážní a záškodnické činnosti, od prvního významnějšího medializovaného incidentu uplynulo již skoro 10 let (útok hackerů na Estonsko v roce 2007)

Česká republika není imunní, jakkoliv se na veřejnost dostávají zatím jen ojedinělé incidenty a to jak ve vládním tak soukromém sektoru

US government hack stole fingerprints of 5.6 million federal employees

Office of Personnel Management hack, which US believes China is responsible for, originally thought to have compromised prints of only 1.1 million workers

Hackers did indeed cause Ukrainian power outage, US report concludes

US officials say well-coordinated hack cut power to 225,000 people.



23. 10. 2012 | poslední aktualizace: 24. 10. 2012, 09:33

V Česku se objevil případ špionážního viru. Denně odesílal gigabyty dat do Číny

Společnost AdvaICT odhalila v jedné z českých organizací špionážní vir, který odesílal gigabyty interních dat na čínské servery. Po případech nalezení škodlivého malwaru v oblastech Středního východu nebo Peru se tak špionážní malware objevuje také v Česku.

Novinky.cz

Neonacisté zveřejnili e-maily z údajné soukromé schránky premiéra Sobotky

Bezpečnost 3. platformy

	Cloud	Mobile	Social Networks	Big Data (Threat Intelligence)
Predictive	<ul style="list-style-type: none"> Privileged Access Management Federated Identity Multi-factor Authentication Data Protection Vulnerability Assessment 	<ul style="list-style-type: none"> Strong Authentication Data Protection Web/Messaging SaaS SSO 	<ul style="list-style-type: none"> DLP with data protection Global regulatory policy monitoring Real-time policy enforcement & education 	<ul style="list-style-type: none"> Raw & analyzed threat feeds from multiple sources integrated with management consoles
Proactive	<ul style="list-style-type: none"> VPN Single Sign-On Encryption Strong Passwords 	<ul style="list-style-type: none"> Mobile Device Management 	<ul style="list-style-type: none"> Keyword-based monitoring & logging 	<ul style="list-style-type: none"> Network monitoring SIEM
Reactive	<ul style="list-style-type: none"> Access control 	<ul style="list-style-type: none"> Device Password 	<ul style="list-style-type: none"> Acceptable Use Policy 	<ul style="list-style-type: none"> Signature-based detection

“Výdaje na kybernetickou bezpečnost vzrostou do roku 2018 celosvětově z 2% na 5%.”

IDC předpokládá celosvětový růst výdajů na kybernetickou bezpečnost ve veřejném sektoru (Zdroj: IDC FutureScape: Worldwide Governments 2016 Predictions)

- V Česká republika pravděpodobně nedosáhne stejných čísel, nicméně trend bude stejný
- Důvody lze nalézt jak v technologickém vývoji, tak i obecně ve vývoji bezpečnostního prostředí
- Výzva Kybernetická bezpečnost z IROP (1 411 764 706 Kč)

Shrnutí

- **Legislativa na národní i evropské úrovni začíná reflektovat komplexitu a závažnost kybernetických hrozeb.**
- **3. platforma - podstatně zvětšuje bezpečnostní perimetr (mobilní zařízení, BYOD a zejména IoT) a i v ČR bude pravděpodobně časem otevřena otázka nových dimenzí regulace**
- **Nové hrozby budou nutit státní sektor k větším investicím a větší míře spolupráce napříč organizacemi. Zvláště u zdravotnických prostředků si nové technologie vyžádají multidisciplinární přístup**
- **Mezinárodní spolupráce rovněž nabyde na důležitosti. Státy, které se cítí být nejvíce ohroženy již začali na tomto poli aktivně konat a spojovat své síly (Pobaltí)**
- **Odpovědí není uzavřít se novým technologiím, ale být si při jejich zavádění vědom rizik a tyto rizika minimalizovat vhodně nastavenými procesy a ochranou.**

Jan Alexa

Senior Research Analyst

janalexa@idc.com

Mark Child

Research Manager

mchild@idc.com

DĚKUJI VÁM ZA
POZORNOST