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

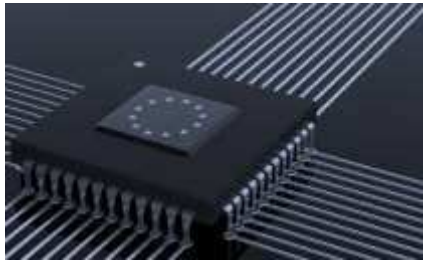
Zákon o kybernetické bezpečnosti

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

IDC
Analyze the Future

Kam v oblasti kyberbezpečnosti směřujeme?

Závisí na dvou klíčových faktorech:

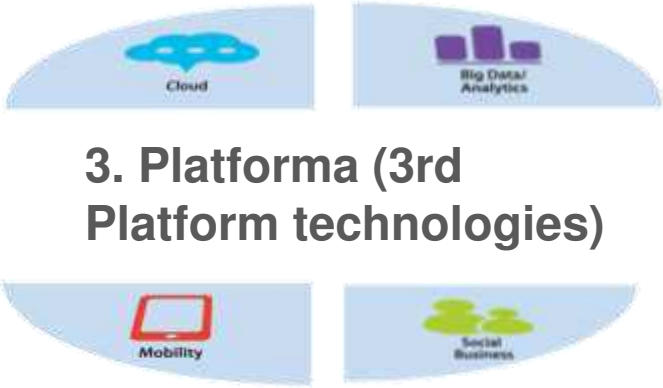


1. Legislativa

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

2. Vývoj v oblasti bezpečnostních hrozeb

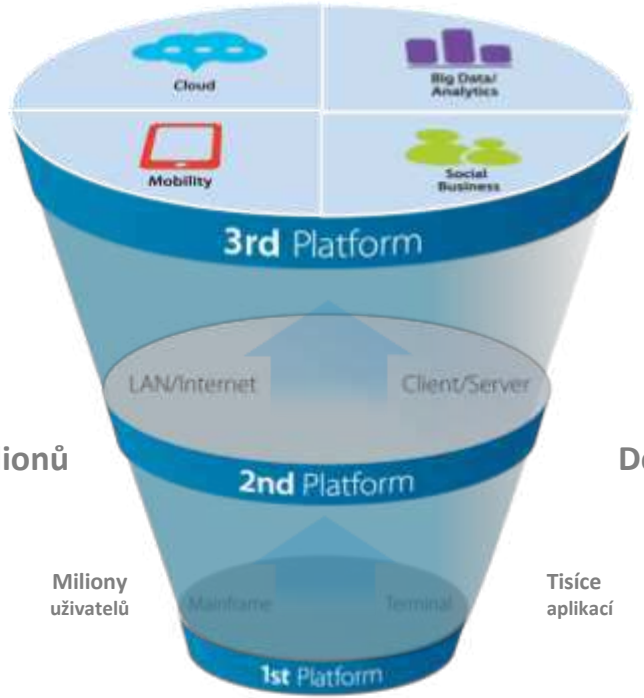
- Struktura bezpečnostních hrozeb se mění
- Geopolitická situace
- ..ale hlavně – technologické změny



3. platforma

Triliony
"věcí"

Miliardy
uživatelů



Miliony
aplikací

Stovky milionů
uživatelů

Desítky tisíc
aplikací

Miliony
uživatelů

Tisíce
aplikací

Růst objemu dat - Digital Universe

2013 – 4.4 ZB
2020 – 44 ZB

$1ZB \approx 1000^3$ 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 znepřístupnění 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

- Inzulinové pumpy
- Kardiostimulátory
- Chytré náramky

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	↓

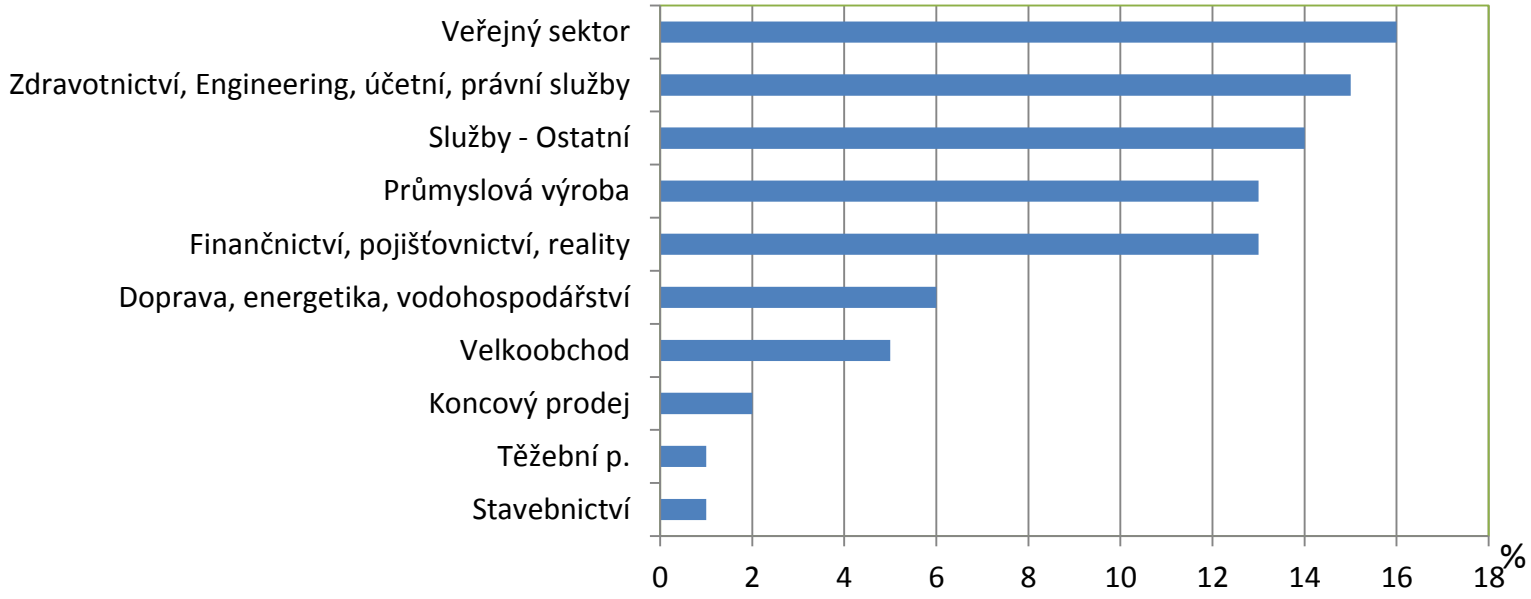
Zdroj: Enisa Threat Landscape 2015

- 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



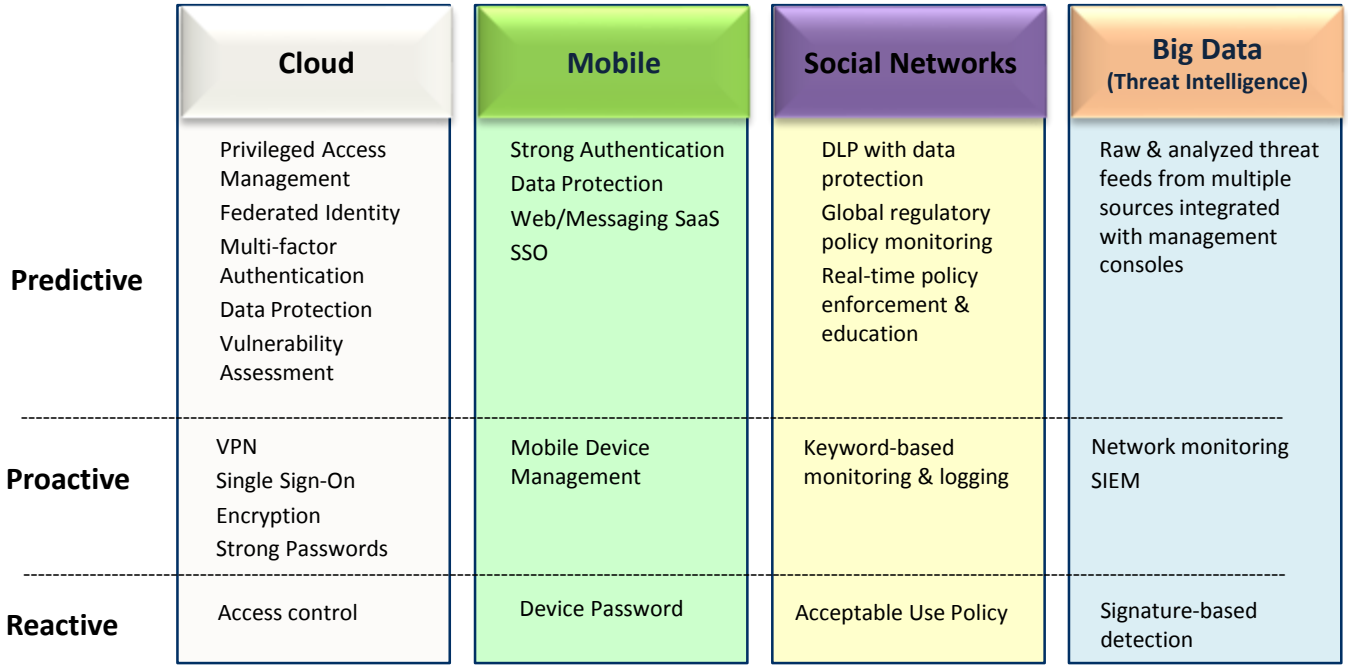
Source: Symantec Internet Security Threat Report 2014

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

Bezpečnost 3. platformy



“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)

IDC
Analyze the Future

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