



Informace, lidské zdroje a technologie: Klíčové faktory pro zajištění kybernetické bezpečnosti

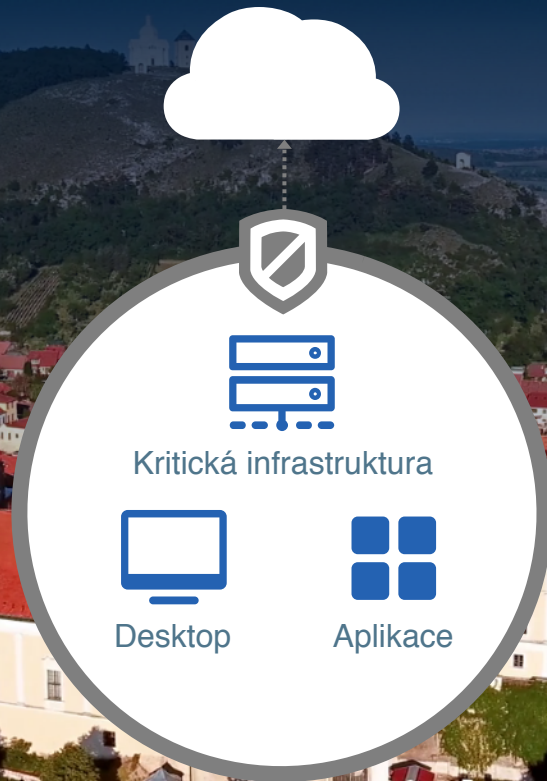
Petr Pavlů (ppavlu@cisco.com)
Systems Engineering Director, Eastern Europe

Mikulov, září 2018

Hlavní témata k diskusi

- Vývoj situace v kybernetické bezpečnosti
- Lidské zdroje
- Technologie a inteligence

Bylo nebylo...



Exponenciální konektivita

8,4 mld

Připojených věcí
v roce 2017

80 mld

Připojení v roce
2025

1 m

Nových IoT zařízení
připojeno každou
hodinu v roce 2020

Roustoucí digitální provoz rozšiřuje prostor pro bezpečnostní útoky

Globální IP provoz se do roku 2020 ztrojnásobí (!)



2.3x

Roční globální IP
provoz



66%

IP provozu bude z
bezdrátových
zařízení (WiFi,
mobilní sítě)



82%

uživatelského
provozu bude IP
video



2x

Průměrná
rychlost
připojení

Stále více komunikace
je mimo firemní síť

Pobočky



Azure, AWS, GCP



Critical Infrastructure



Desktops



Business
Apps

Vzdálení
uživatelé



Office 365, Salesforce,
atd.



88%

Respondentů, kteří byli
cílem kybernetického
útku v posledních 12
měsících

2016: 54%

Velké úniky dat v posledních letech

110 milionů ohrožených uživatelů
2013  **Target**

320 milionů uživatelů účtů
2013  **YAHOO!**

145 milionů ohrožených uživatelů
2014  **eBay**

DDoS útok – výpadek sítě a krádež dat prostřednictvím více než 1M IoT zařízení
2016   **Spotify**  **PayPal**
and others

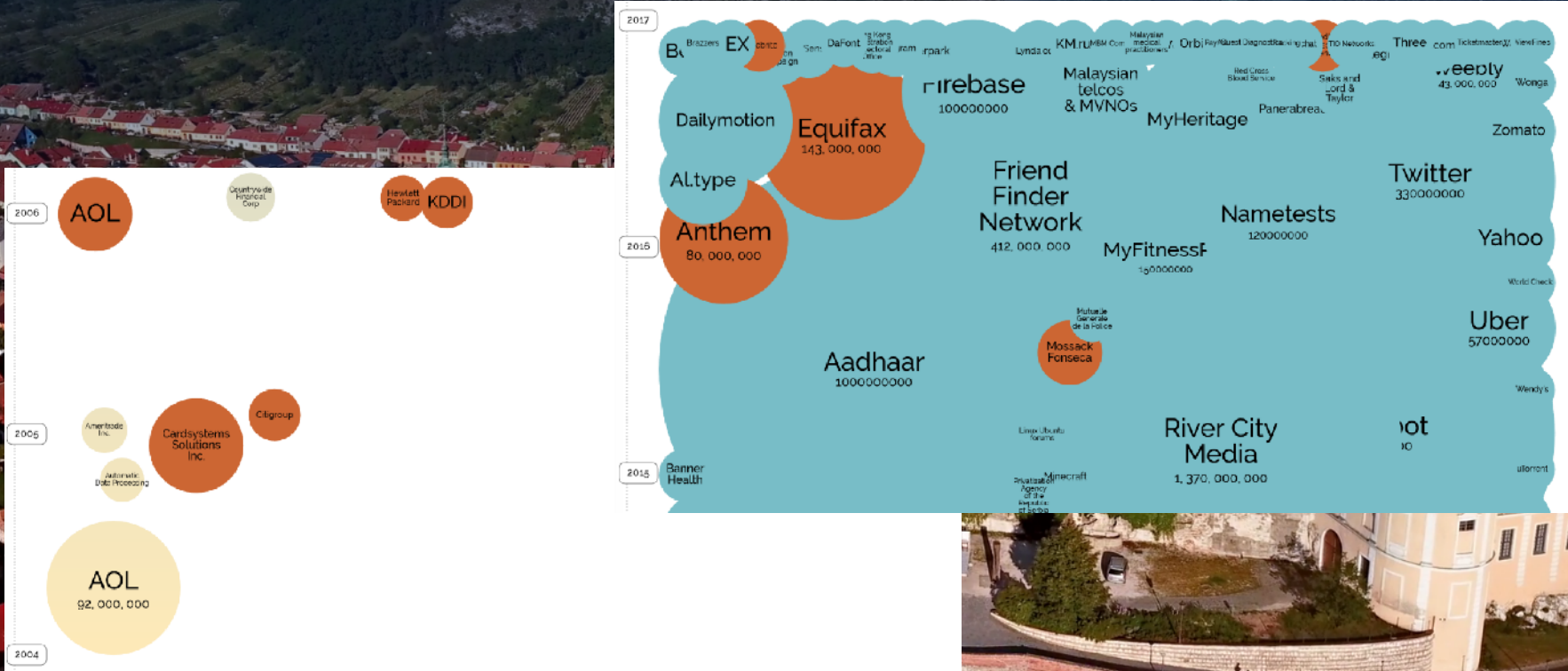
Ohrožení citlivých dat
2017  **Deloitte**

143 milionů ohrožených uživatelů
2017  **EQUIFAX**

57 milionů ohrožených uživatelů
2017  **UBER**

Pro ty, kdo mají raději grafickou formu...

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks>

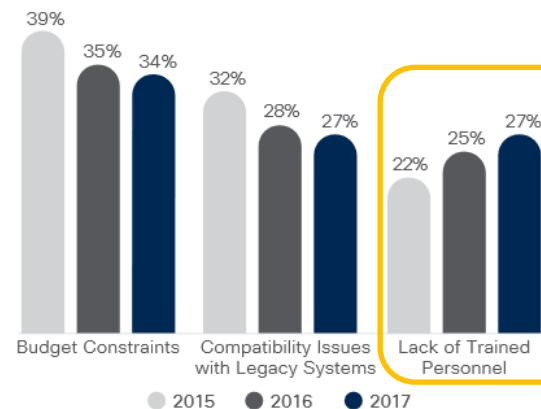


V roce 2021 bude globální ekonomice chybět 1,8 milionu pracovníků v kybernetické bezpečnosti

„Není zkrátka dost lidí. Nemohu najít dost zájemců. Nemůžu je dostatečně zaplatit. Nemůžu je udržet.“

Zdroj: Frost & Sullivan

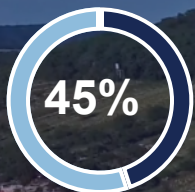
Figure 42 The greatest obstacle to security: budget constraints



2015 (n=2432), 2016 (n=2912), 2017 (n=3651)

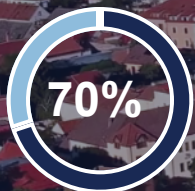
Source: Cisco 2018 Security Capabilities Benchmark Study

Problém je zřejmý z řady průzkumů



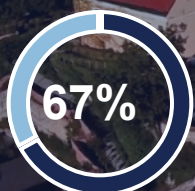
organizací

Problematický nedostatek znalostí a zkušeností v kybernetické bezpečnosti



profesionálů

Nedostatek znalostí a zkušeností v KB má významný dopad na jejich organizaci



profesionálů

Pracovní vytížení nedovoluje dostatečně se vzdělávat a udržovat krok z vývojem na poli KB

Cisco příspěvek: Networking Academy

- Globální vzdělávací program zaměřený na IT, počítačové sítě a profesionální dovednosti
- Partnerství s vládními i nevládními organizacemi a 9,500 školami a univerzitami
- Kurzy probíhají v učebnách i online (bezplatné licence pro neziskové organizace)



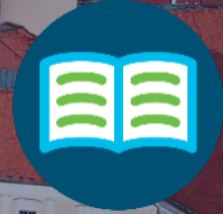
180
zemí



10,000+
akademii



22,000+
instruktorů



19
výukových
jazyků



1.3 milionu
studentů
(aktuálně)



7.8 milionu
studentů od
1997 (celkem)

Portfolio kybernetické bezpečnosti

Možnost certifikace,
perspektivní pracovní
příležitosti

Bezpečnost sítí,
jejich návrh,
implementace a
ochrana

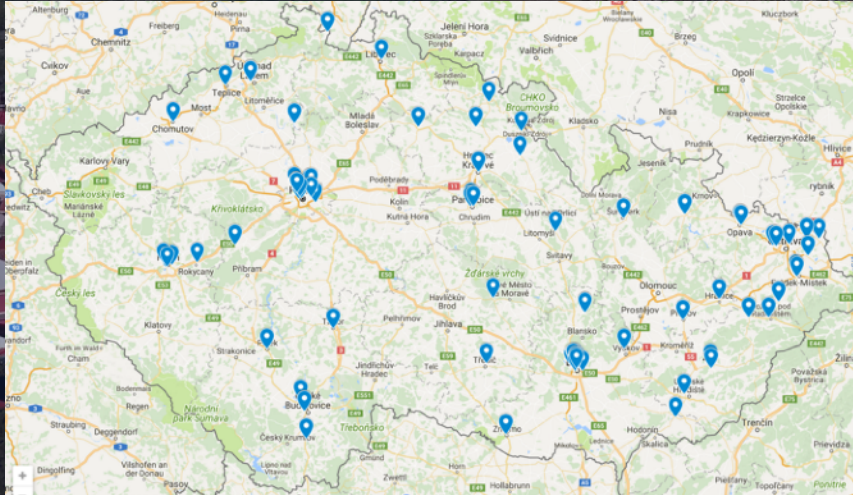


Osobní bezpečnost,
kariérní možnosti

Základní principy,
procedury, postupy

Detekce incidentů,
podpora síťových a
koncových systémů

Kde začít?



<https://www.netacad.cz>
<https://www.netacad.com>

84 akademií

- 58 střední školy
- 26 vysoké školy

Volně dostupné online:

Úvod do KB: <http://cs.co/csintro>

Základy KB: <http://cs.co/csessen>



**Sedli byste do stroje
smontovaného z 50
jiných letadel?**

65%
Organizací používá 6 až
50+ dodavatelů
bezpečnostních produktů

500+ Dodavatelů bezpečnostních produktů

This infographic displays 500+ cybersecurity vendors organized into 14 categories:

- Network Security:** Network Firewall (Infoblox, Cisco, Palo Alto Networks, Juniper, Fortinet, etc.), Network Monitoring/Forensics (NetScout, XDR, etc.), Intrusion Prevention Systems (Cisco, Snort, etc.), Unified Threat Management (Cisco, Palo Alto Networks, etc.).
- Endpoint Security:** Endpoint Prevention (McAfee, Symantec, etc.), Endpoint Detection & Response (CrowdStrike, SentinelOne, etc.).
- Application Security:** WAF & Application Security (Akamai, Cloudflare, etc.), Vulnerability Assessment (Bugcrowd, Checkmarx, etc.).
- Managed Security Service Provider:** Various MSSP providers like Trustwave, Optiv, etc.
- Web Security:** Web Application Security (Veracode, Acunetix, etc.), Web Protection (Cisco, etc.).
- Messaging Security:** Email Security (Mimecast, Proofpoint, etc.), Instant Messaging Security (Cisco, etc.).
- Risk & Compliance:** GRC solutions (PwC, Deloitte, etc.).
- Security Operations & Incident Response:** SIEM (Splunk, IBM, etc.), Security Incident Response (Palo Alto Networks, etc.).
- Threat Intelligence:** Threat detection and analysis (Anomali, etc.).
- Specialized Threat Analysis & Protection:** Advanced threat hunting (Recorded Future, etc.).
- Data Security:** Data loss prevention (Symantec, etc.), Data protection (Veritas, etc.).
- Mobile Security:** Mobile device management (VMware, etc.), Mobile threat defense (Bitdefender, etc.).
- Identity & Access Management:** IAM solutions (Okta, etc.).
- Cloud Security:** Cloud workload protection (CrowdStrike, etc.), Cloud access security (Zscaler, etc.).
- Industrial / IoT Security:** OT security solutions (Siemens, etc.).
- Fraud Prevention / Transaction Security:** Fraud detection (FICO, etc.).

Momentum CYBERScape · 2017



Vytrvalí
ÚTOČNÍCI

VS

Neúnavní
OBRÁNCI



Jediná možná cesta

AUTOMATIZOVANÁ BEZPEČNOST

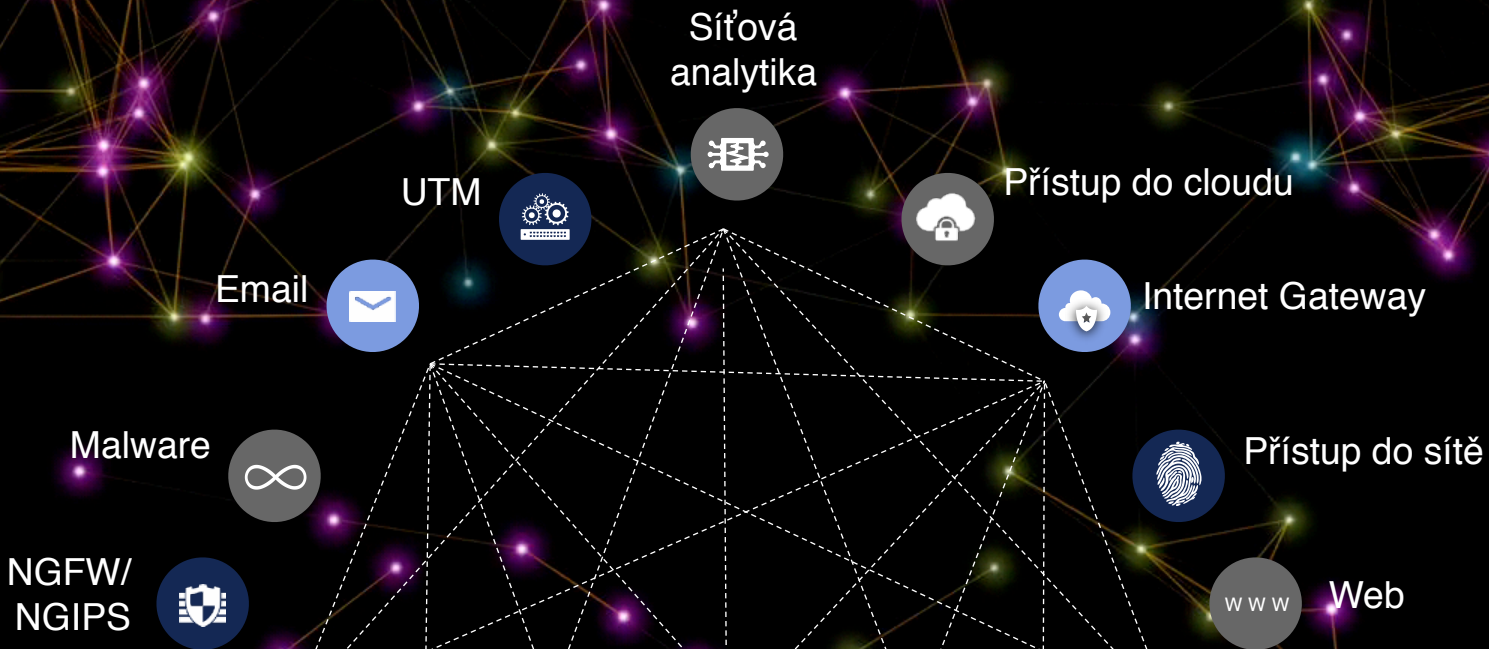
Cisco a kybernetická bezpečnost

Špičkové
PORTFOLIO

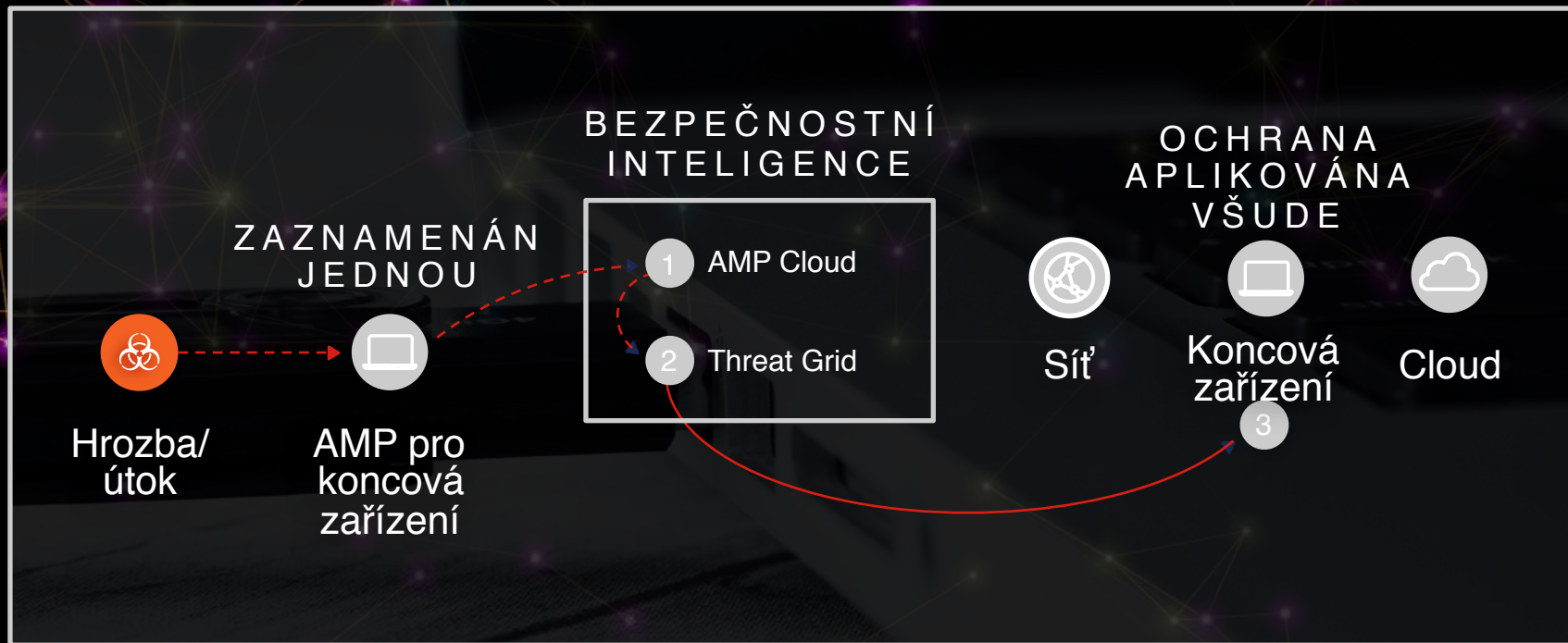
Čas
DETEKCE

Integrovaná
ARCHITEKTURA

Špičkové portfolio



"Výhoda architektury" v akci



CISCO INTEGROVANÁ BEZPEČNOSTNÍ ARCHITEKTURA

Integrovaná obrana proti hrozbám

Znalost a výzkum hrozeb - **TALOS**



Sít'



Koncové zařízení



Cloud

S l u ž b y

Talos: Cisco globální přehled, výzkum hrozeb a analytika – unikátní na trhu



GLOBÁLNÍ

Hrozby v
Internetu



LOKÁLNÍ

Hrozby ve vaší
síti

Stovky tisíc

Zákazníků

**Desítky
milionů**

Uživatelů

100TB

Dat o aktuálních
hrozbách denně

250

Výzkumníků

Stovky

Algoritmů pro
analýzy hrozeb

20 miliard útoků blokových denně (3x více než dotazů Google)

Shrnutí

Nárůst provozu v kybernetickém prostoru zvyšuje rizika

Zajištění bezpečnosti se stává předpokladem dalšího rozvoje

Nedostatek profesionálů vyžaduje pozornost a řešení

Nároky na technologii: Integrace, automatizace, inteligence

