Kybernetická bezpečnost ve veřejné správě

nutné zlo nebo příležitost?

Tomáš Hlavsa

Atos CYBER security

Atos

Cyber hrozby? Reálné, nebo virtuální téma?

Kolik notebooků / tabletů / mobilních telefonů Vaše firma za poslední rok ztratila?

…….a více jistě co všechno na nich bylo?

Evidujete USB flash disky? Máte na ně bezpečnostní politiku?

…… kolik reklamních Flash disků v práci používáte?

Kolik stojí hodina provozu Vaší firmy, Vašeho úřadu?

…… Business Impact Analýza

Kolik zakázek jste za poslední dobu „o chlup" prohráli?

…… náhoda?

Unikl Vám na veřejnost interní dokument?

…..a tušíte, jak opustil organizaci?

Ochrana dat x Ochrana procesu x Ochrana Vás

BYOD
Vnášení soukromých zařízení zaměstnanci / dodavateli / partnery …..máte tušení co si na soukromých zařízeních zaměstnanci odnášejí domů…….

ICS / SCADA
Máte kontrolu nad periferiemi Vašich řídících prvků?

Pohyb dokumentů v organizaci
Neopouštějí interní dokumenty Vaší organizaci?
Víte kdo, kdy a na jakém zařízení otevírá důležitý dokument?

…a trápí Vás to vůbec?

Normy, zákony, regulace

Zákon o kybernetické bezpečnosti – ?????????

Norma pro systém řízení bezpečnosti informací - ISO 27001

Zákon o ochraně osobních údajů - 122/2013 Zb.

Zákon o Slobodnom prístupe k informáciám - 211/2000 Zb., o

Co mi soulad se cyber zákonem/standardy přinese?

……. jinými slovy, stojí to vůbec za to?

Ochrana informací
- Nebo máte snad v organizaci něco cennějšího?
- Ceníky, výkresy, finanční systém, HR systém…

Garance výkonu / dostupnosti

Na kolik si ceníte hodinu/den výpadek běhu Vaší organizace?

Snížení nákladů na IT
- Budujete si vlastní bezpečnostní oddělení ?
- Jak často obměňujete své bezpečnostní technologie?
- Nešlo by bezpečnostní dohled řešit službou?

Pojištění vůči kybernetickým hrozbám
- požární řád, směrnice
- evakuační plán
- povodňové plány

…..ohodnocení informačních aktiv -> Analýza rizik

Bavme se o penězích

Cyber security compliance jako **přidaná hodnota** Vaší organizace
ISO kvality má každý, ISO 27001 skoro každý, soulad se cyber zákonem bude výhodou…….minimálně vůči státní správě

Vzdělávání zaměstnanců ohledně informačních rizik je nutná součást opatření. Proč z toho neučinit **zaměstnanecký benefit**.

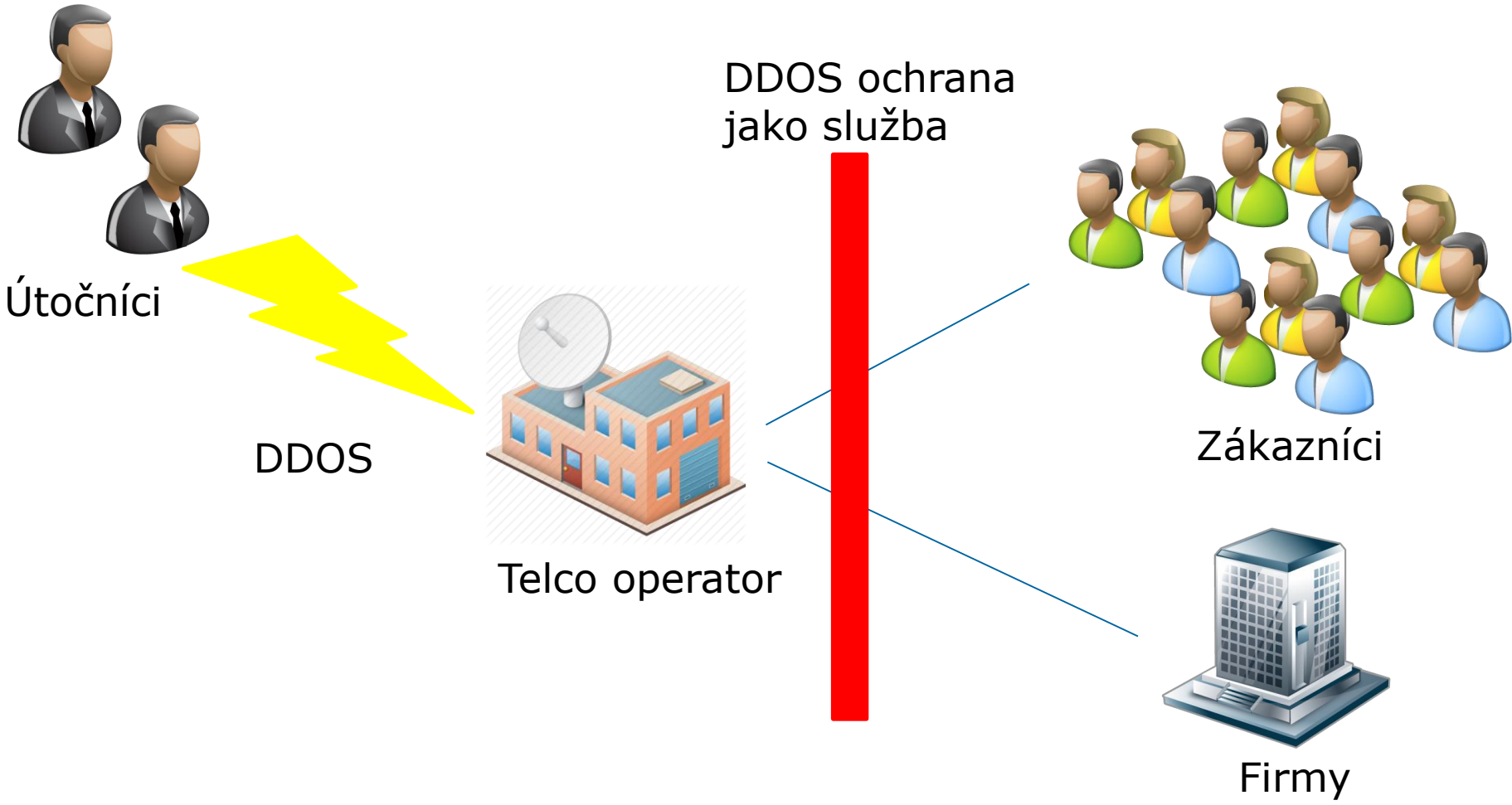
Dodavatelé IT / síťových technologií / infrastruktury – mohou přeci řadu opatření vyřešit za Vás

– síťové prvky mohou generovat netflow
- dodavatelé aplikací mohou upravit logy aby je Váš SIEM lépe parsoval
- dodavatelé firmwarů Vašich zařízení garantují jejich odolnost vůči penetračnímu testování?

……. a dále? Lze na povinnosti vydělat?

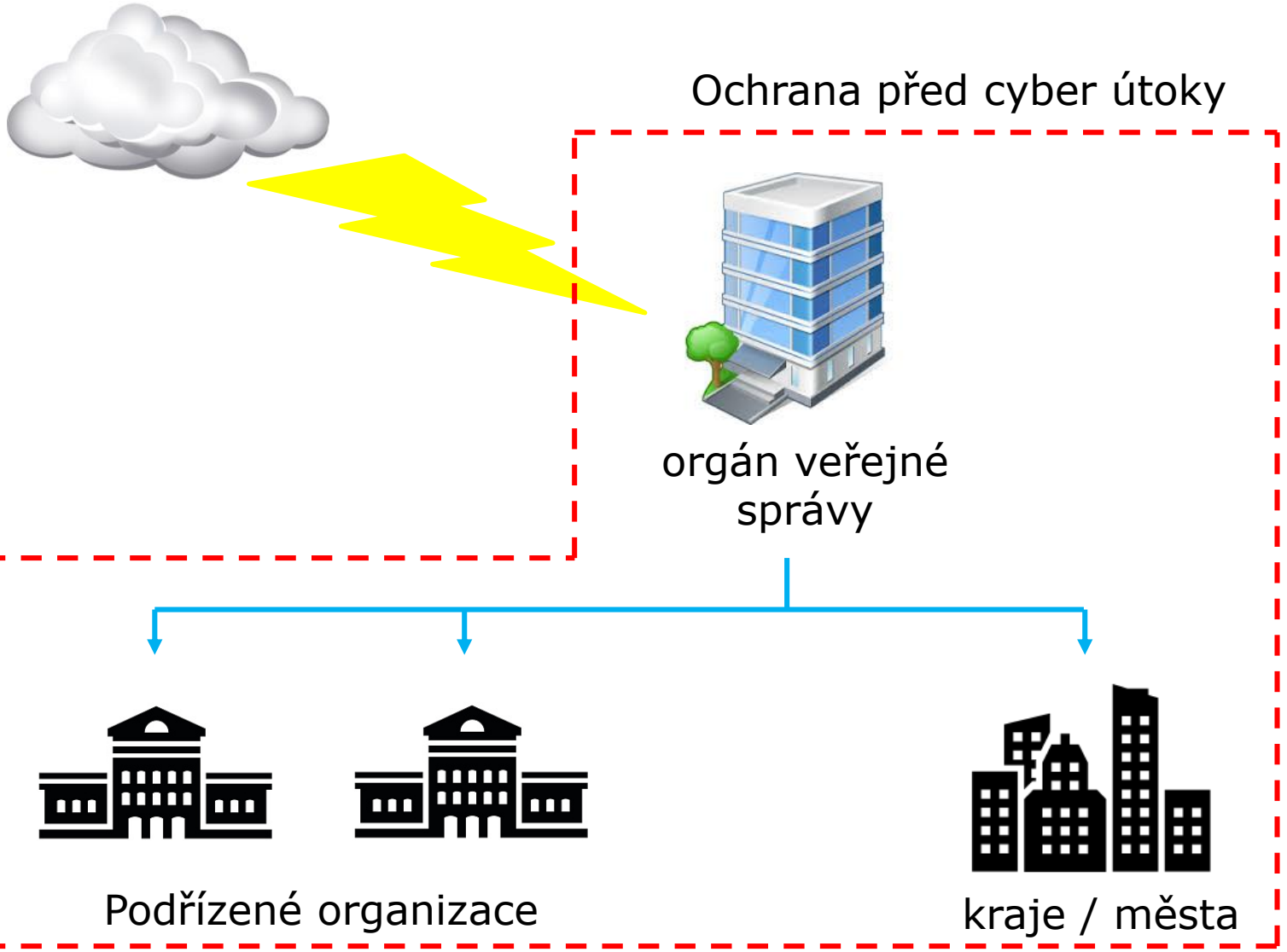
Povinnost přetvořená do obchodní příležitosti

……. komerční sféra

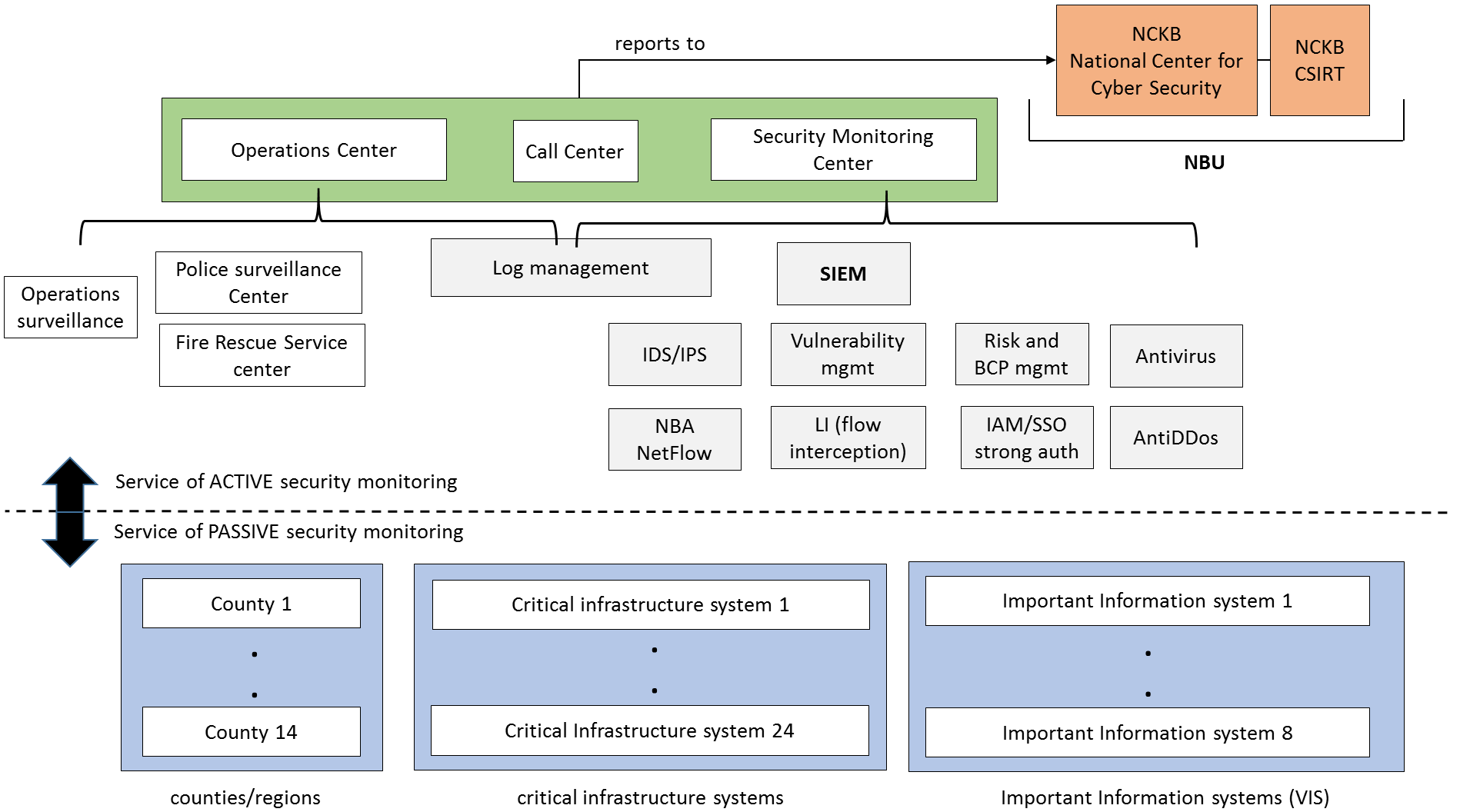


Povinnost přetvořená do obchodní příležitosti

……. veřejná správa

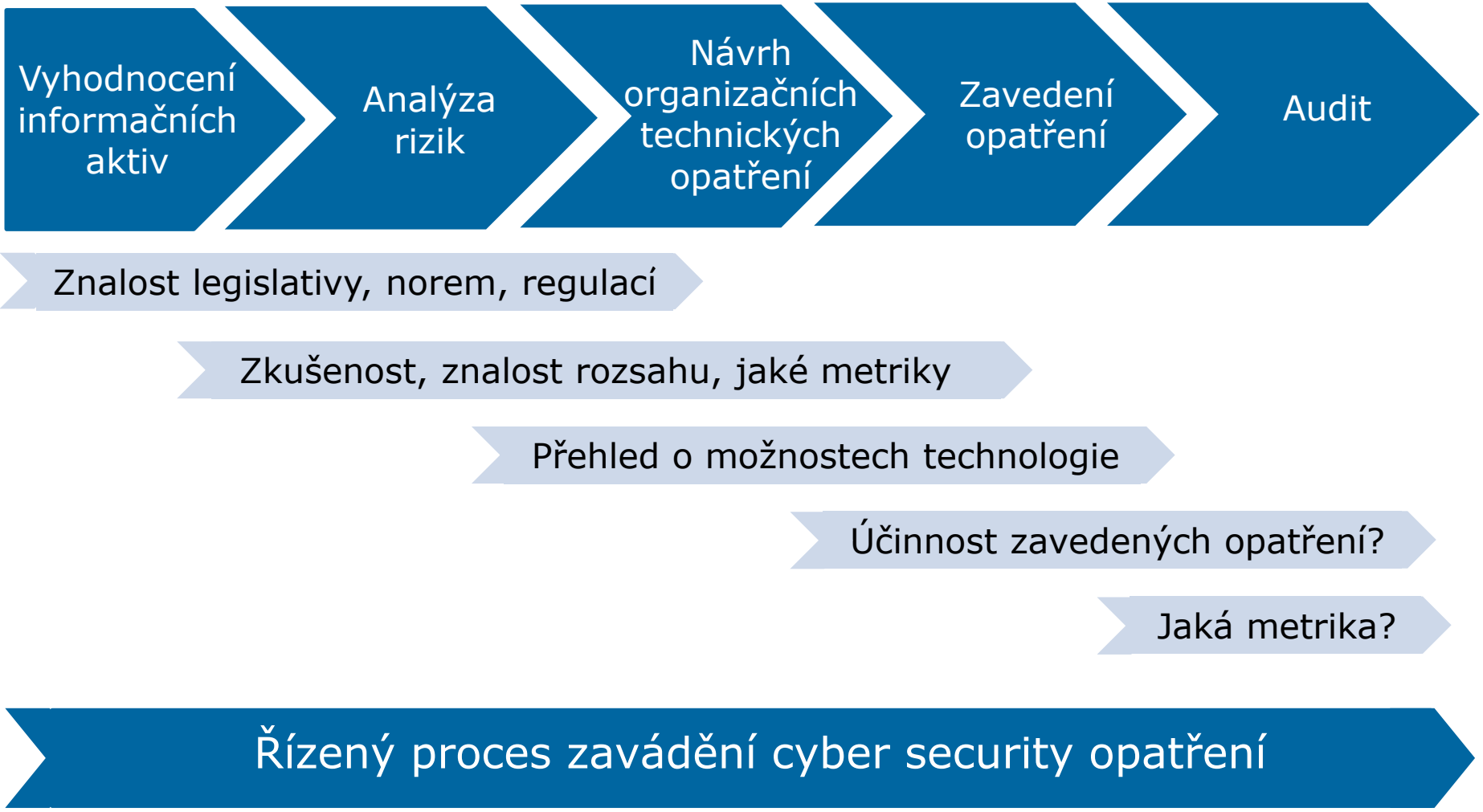


Jaký je na začátku plán

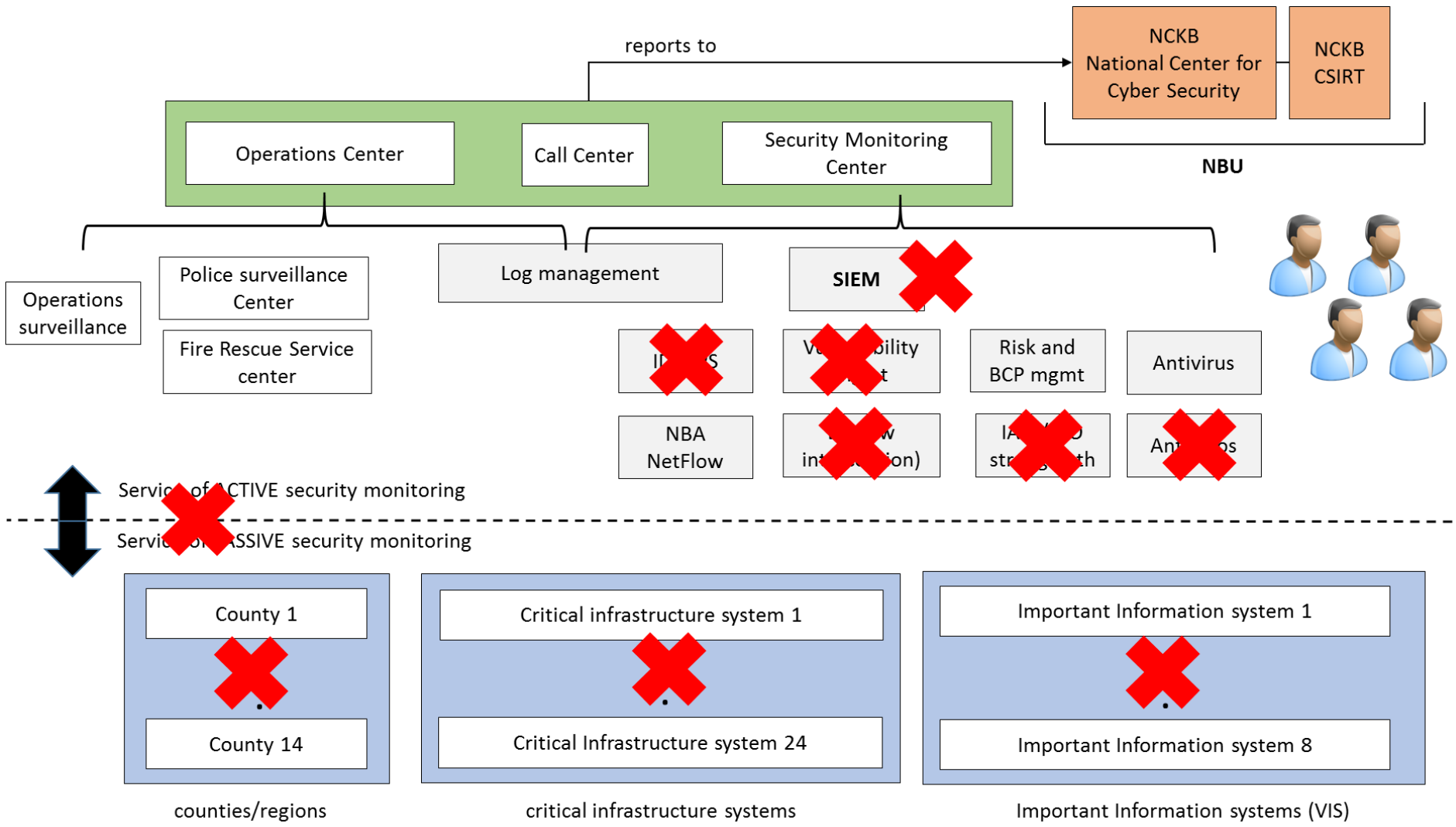


Investice do lidí x Investice do technologií

…… nezačínejte prosím technickým opatřením ……

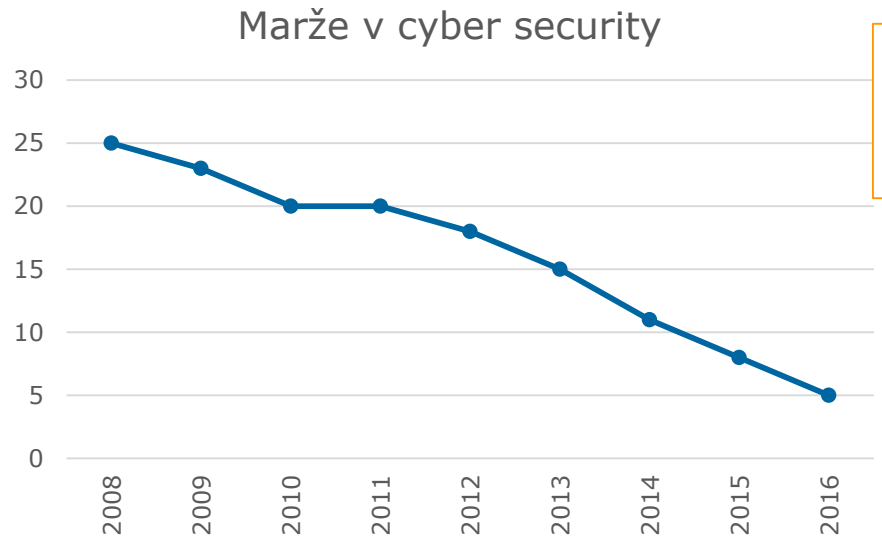


A po pár letech.....



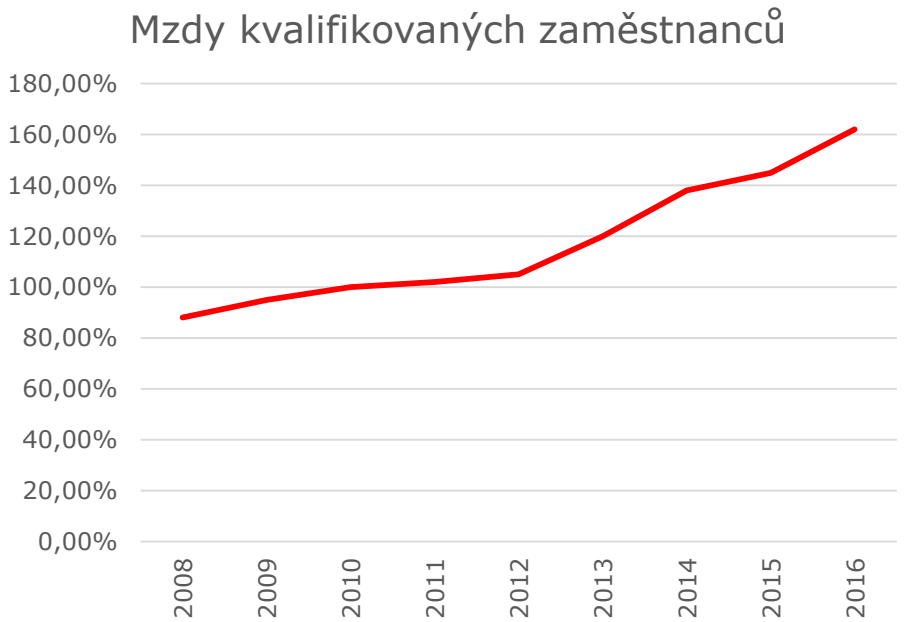
Pohled systémového integrátora

..... trendy .....



SIEM byl v roce 2011 „niche business“

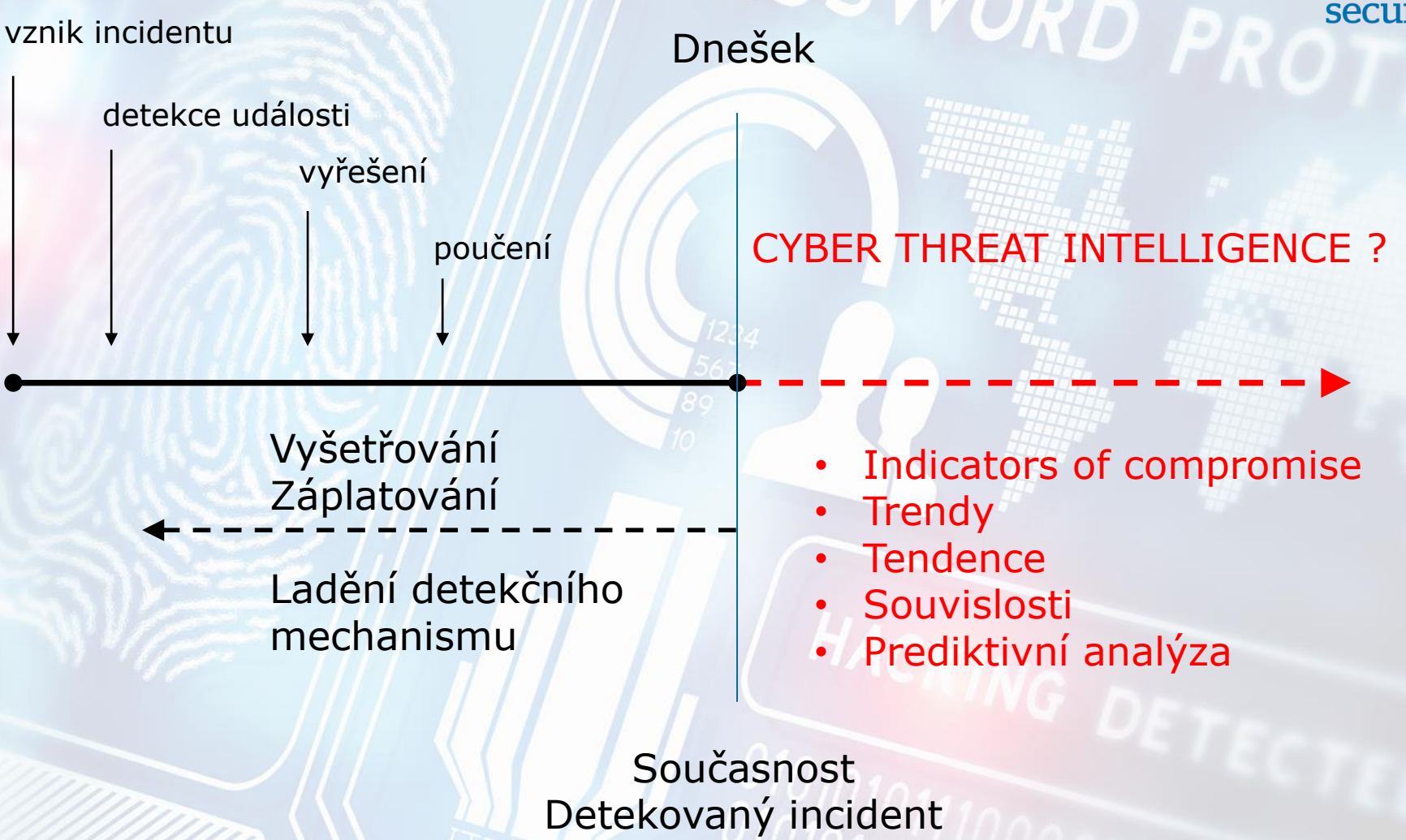
…dnes je to komodita s <5% marží



Dnešní absolvent je o 60% dražší

než konzultant s praxí před 6ti lety

Příliš se díváme do minulosti



Co tedy ATOS odlišuje od desítek CYBER zaměřených firem?

Atos CYBER security

Schopnost přenosu zkušeností ze zahraničí

(Polsko, Izrael, Francie …….)

(SOC centra, informační zajištění Olympijských her ….)

Věda a výzkum

Bezpečnostní výzkum, H2020 ……

Vzdělávání

(eLearning, kontinuální vzdělávání …)

Síla největší evropské IT firmy

Kapacitní pokrytí,
expertiza, partnerská síť

Bezpečnostní řešení nejen v oblasti CYBER

Národní bezp. integrátor (Švýcarsko, Francie ….)

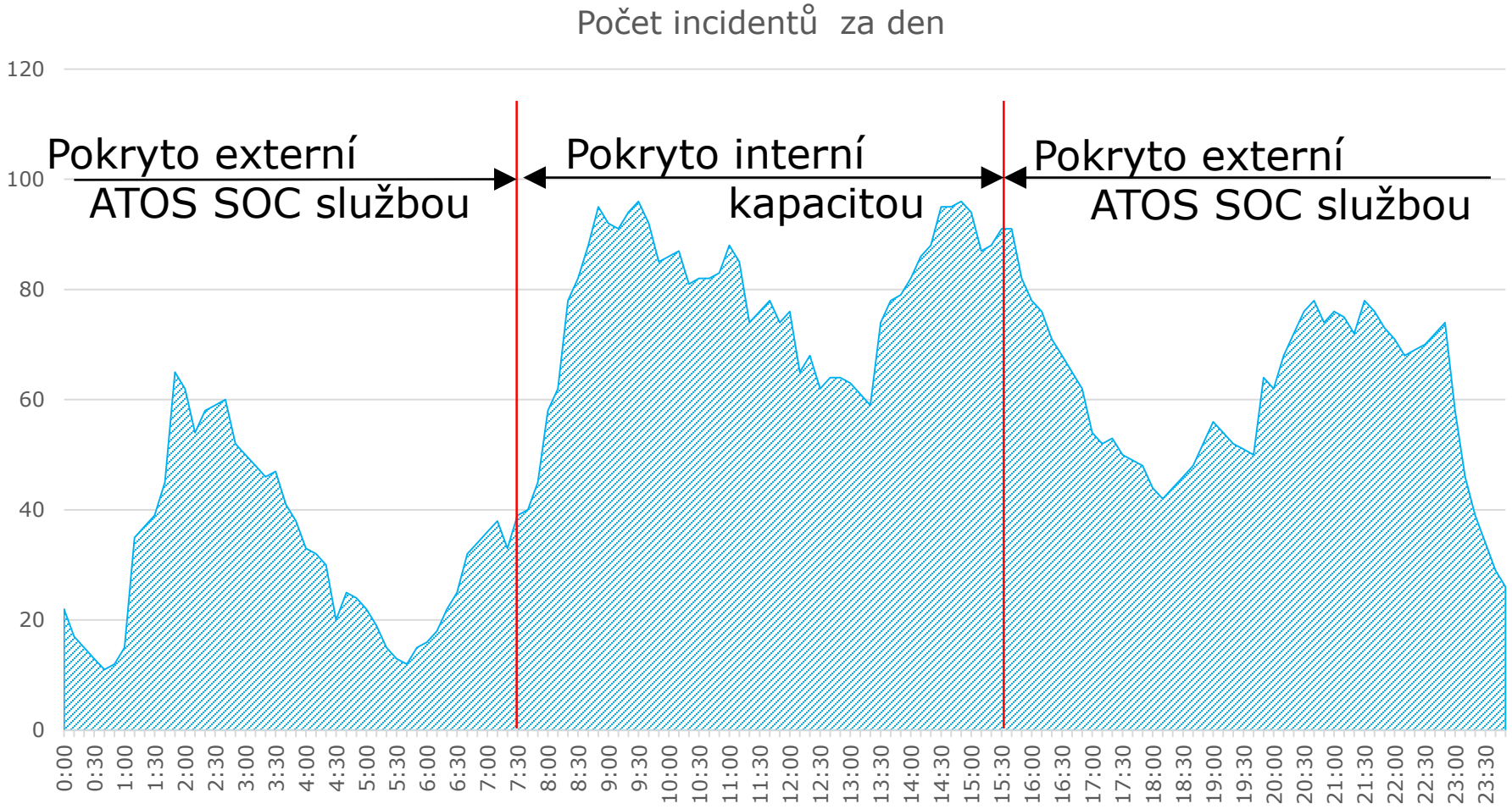
Financování

Fondy, dotace, rozvojové programy

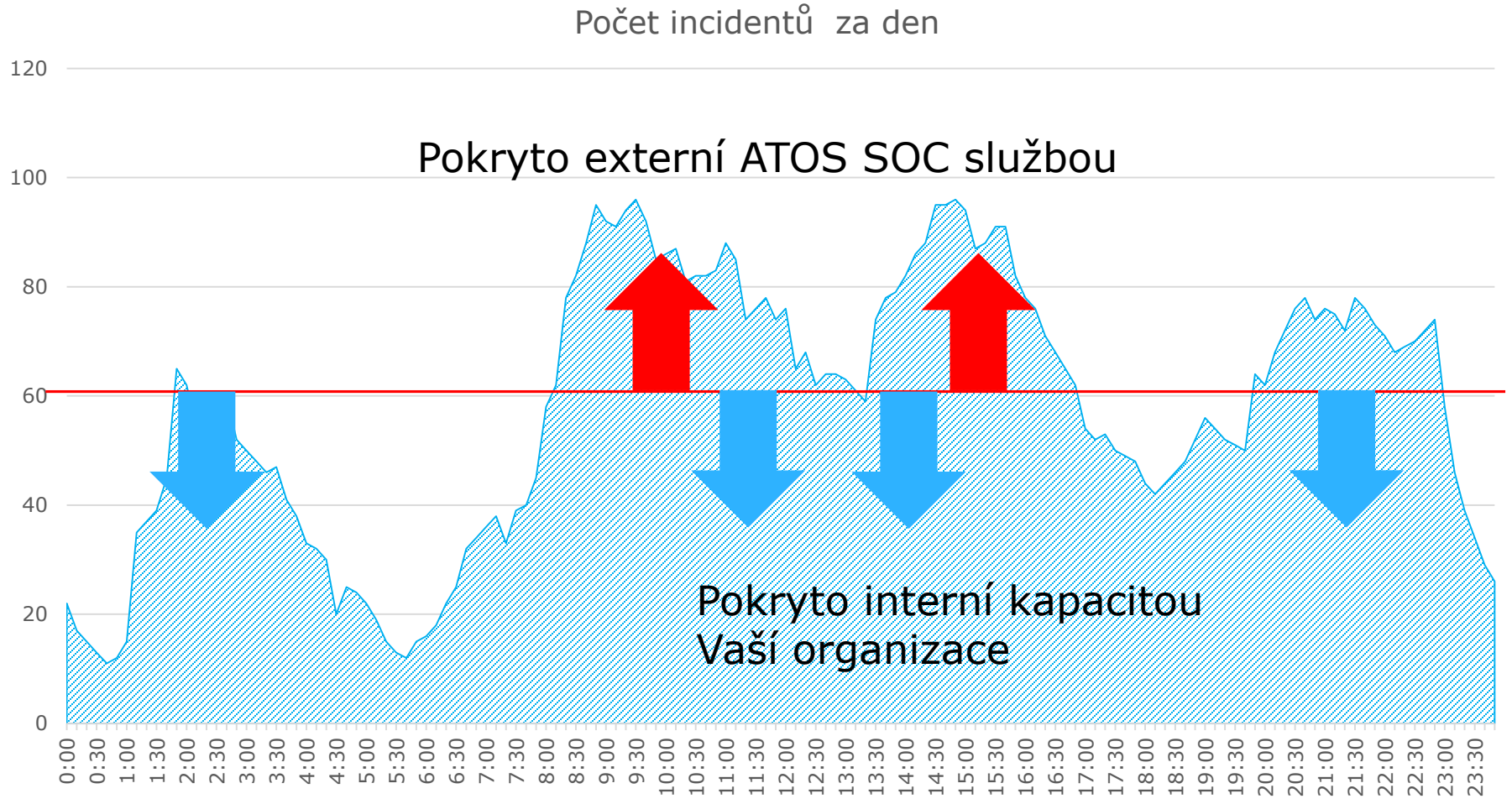
? Existuje vzájemně udržitelná spolupráce?

Atos

Řešíte incidenty 24 x 7?
… a dovoláme se k Vám v sobotu dopoledne?



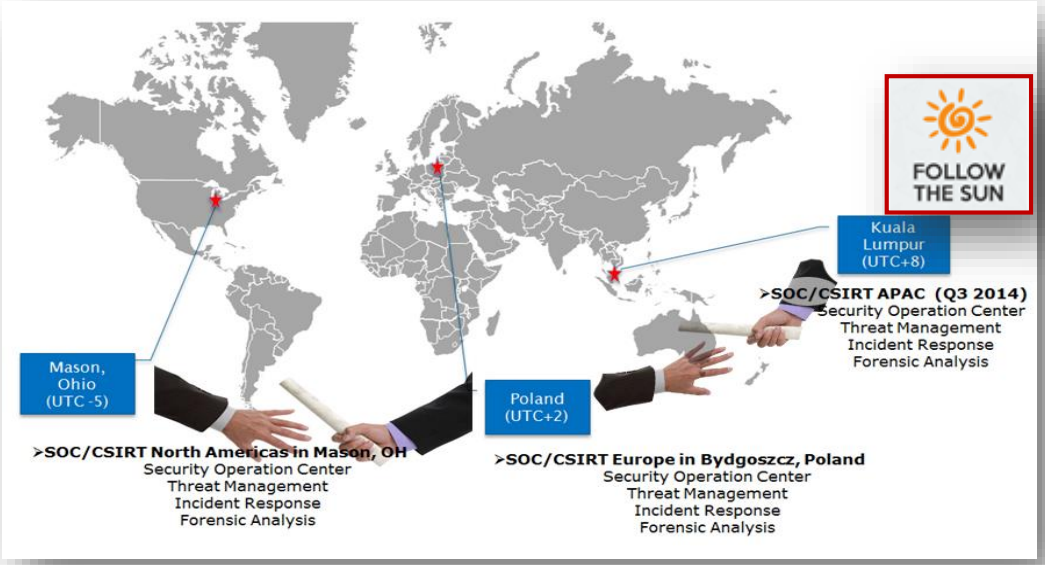
Pokryjete dnes incidenty vlastními silami?
…… a zítra?



ATOS – mezinárodní SOC centra

ATOS Poland | Bydgoszcz

- **SOC centra v:**
  - **Polsku**
  - **Rumunsku**
  - FRANCII
  - SPOJENÉM KRÁLOVSTVÍ
  - SEVERNÍ AMERICE
  - MALAYSII



Požadavky na vzdělání

... nabídněte svým zaměstnancům růst

Atos CYBER security

Technické znalosti

Zkušenosti z obdobné pozice

Certifikace

CompTIA Security+

Anglický jazyk

B2 – Common European Framework of Reference for Languages

Nástroje

Sentinel Training

NetIQ

NetIQ Sentinel

SIEM McAfee Training

McAfee

IBM Qradar Training

IBM Radar

Jiné podobné nástroje?

Pracovní náplň

ITIL Foundation

- Event Mgmt
- Incident mgmt
- Change mgmt
- Problem mgmt

Interní procesy organizace na zvládání incidentů

Řešení incidentů

Rozsah monitoringu

Security Incident Response proceduresv

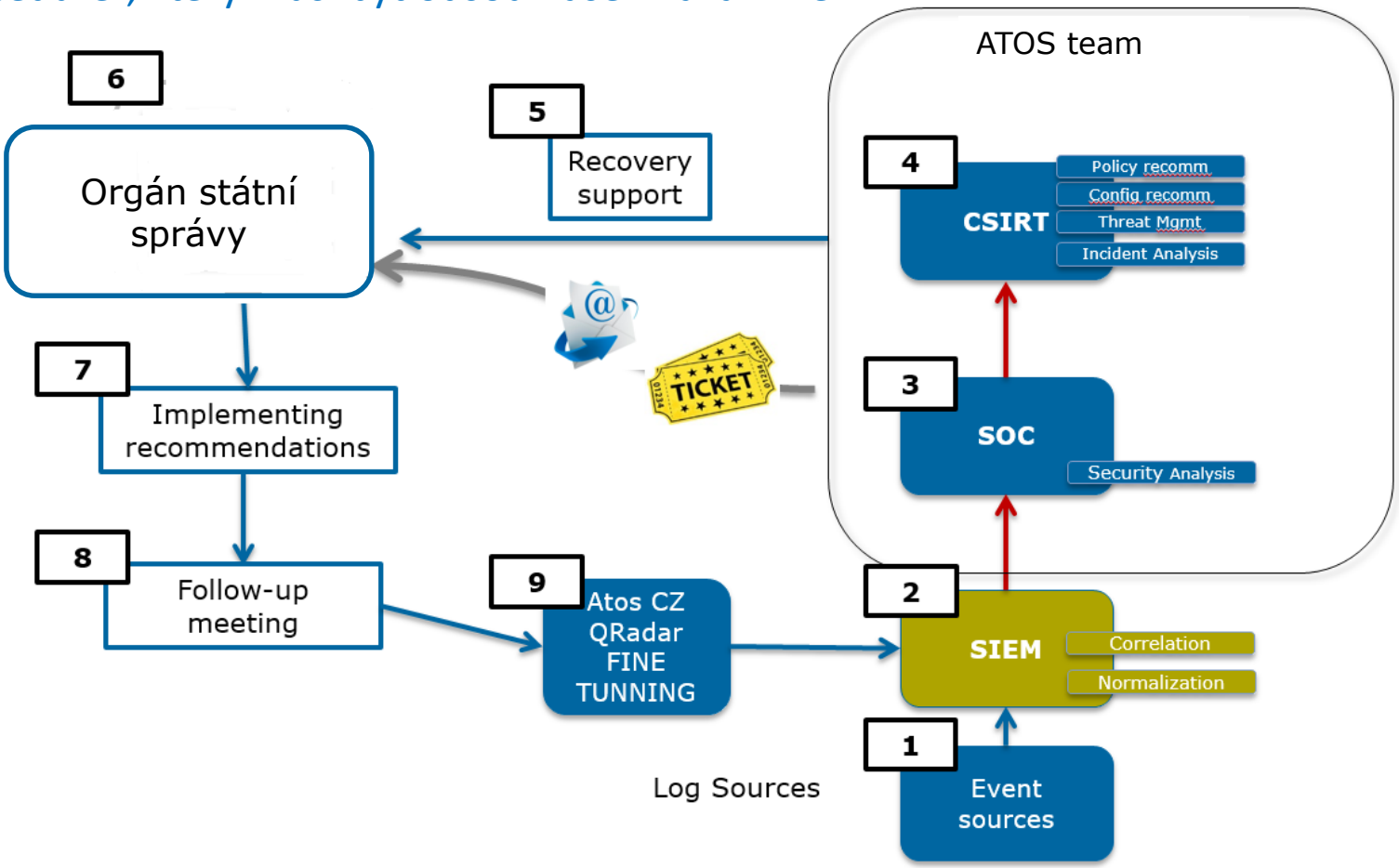
CSIRT Incident Management

Eskalační procedury

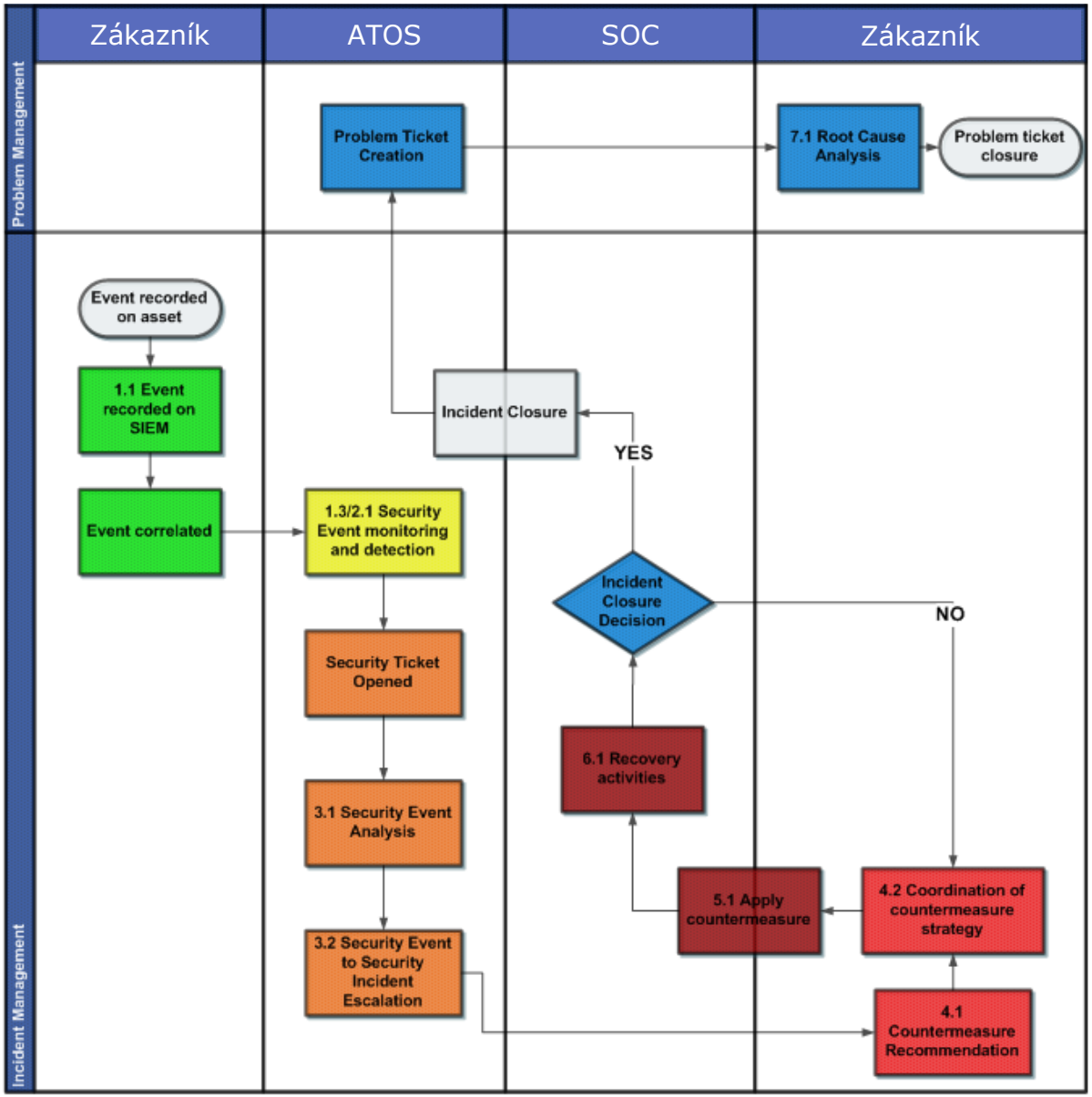
Management

Když už incident nastane a je detekován

Workflow cyber incidentu poskytuje základní informaci o aktivitách provázejících každý incident. Detailní popis workflow ATOS dokumentuje v „Security Incident Response Procedure“, který musí být odsouhlasen Zákazníkem.



Workflow a odpovědnost?



Jasné rozdělení odpovědnosti a návazností v komunikaci.

Každý bezpečnostní incident vychází ze scénáře, který má oporu v bezpečnostní politice organizace.

Budování bezpečnostního povědomí

Atos CYBER security

10 základních bezpečnostních pravidel

1. Buďte odpovědní

Atos zavedl systém řízení bezpečnosti, který zahrnuje aspekty ochrany dat, fyzickou bezpečnost, ochranu zdraví a majetku. Všechna aktiva (data, majetek, dokumenty, výrobní prostředky, intelektuální vlastnictví) Atosu, jakožto aktiva zákazníků, musí být adekvátním způsobem chráněna vůči známým hrozbám. Proto Atos definoval pravidla a směrnice, které byste měli znát a řídit se jimi. Všechny naleznete na Sharepointu v sekci Organization - Support functions - Group security.

2. Hlašte bezpečnostní incidenty

Bezpečnostní incidenty musí být bezodkladně hlášeny. Ať jde o incidenty fyzické bezpečnosti, informační bezpečnosti nebo incidenty ochrany zdraví. Cílem je především bezpečnost a zdraví zaměstnanců. Teprve poté bezpečnost a ochrana majetku společnosti Atos. Seznamte se se směrnicí „Jak hlásit bezpečnostní incidenty".

5. Při používání e-mailu a internetu buďte opatrní

Víceméně všechny druhy malwaru či virů mohou být součástí e-mailu nebo webových stránek. Nikdy neotevírejte email, či přílohu, která vypadá podezřele. Pozor na sociální sítě, pohyb na nich není anonymní a jste zranitelnější než si myslíte. Nestahujte soubory z nedůvěryhodných, pochybných či neautorizovaných stránek. Mohou obsahovat škodlivý software. Neklikejte na odkazy v nevyžádaných e-mailech, ty mohou obsahovat hrozby typu phishing apod.

6. Chraňte vaše koncová zařízení (notebook, smartphone, tablet)

Zálohy jsou jediným rozumným způsobem, jak obnovit ztracenou, či poškozenou informaci. Ujistěte se, že všechny relevantní informace ukládáte na servery, které jsou automaticky zálohovány. Notebooky, tablety a mobilní telefony, které opouští prostředí Atosu, jsou velmi zranitelné a hodnota ztraceného hardwaru je často mnohem nižší, než hodnota ztracených informací

8. Řiďte se bezpečnostními pravidly Atosu

Seznamte se s bezpečnostními opatřeními platnými na dané pobočce Atosu (například kouření je přísně zakázáno ve všech Atos prostorách). Evakuační pravidla a procedury jsou zde především kvůli ochraně vašeho zdraví a života. Řiďte se evakuačními pokyny v případě poplachu i v případě cvičných poplachů.

9. Respektujte pravidla a opatření v Atos prostorách

Každý zaměstnanec má jeden či více vstupních průkazů opravňující přístup do prostor Atosu. Noste vstupní karty viditelně. Každý zaměstnanec je odpovědný za své návštěvy. Návštěvníci bez řádných vstupních průkazů nezůstávají po dobu svého pobytu v prostorách Atosu bez doprovodu. Neváhejte nabídnout neznámým, či neoznačeným osobám svůj doprovod na recepci.

Atos

Inspirujte se v našem SOC centru

….. pravidelné referenční návštěvy

Referenční návštěva v ATOS Security Operations Center

Agenda

DEN 1

09:30	Zahájení - Představení Atos Big Data & Security Polan *Marcin Lipinski, CEE Hea*
10:00	Atos Security Monitoring and Detection *SOC (Maciej Glama)* *Vulnerability Managem* *AHPS service (Przemek*
12.00	Oběd
13.30	Prohlídka všech oddělení Security Operations Center *Jakub Chmielewski*
14:30	TPS – Organizational Cyber Security
16:00	Atos Security Incident Response - CSIRT *Piotr Chmylkowski*
16:45	Atos Security Prevention – Identity and Access Management *Kamil Jarzembski*
18:00	Individuální konzultace s jednotlivými členy SOC týmu

DEN 2

09:30	Atos Security Prevention – Endpoint perimeter protect *Rafal Grochowski*
10.15	CIC – National Cyber security challenge to country int
12.00	Individuální konzultace s jednotlivými členy SOC týmu

Děkuji za pozornost

Trusted partner for your Digital Journey

Tomáš Hlavsa

tomas.Hlavsa@atos.net
+420 604 290 196