



# Informační systémy a bezpečnost

Kybernetická a informační bezpečnost I

Vladimír Lazecký

[vladimir.lazecky@viavis.cz](mailto:vladimir.lazecky@viavis.cz)

- ✓ Kde začít s KB:

- ✓ Otevřené kurzy, základní informace:

- ✓ [www.nukib.cz](http://www.nukib.cz)

- ✓ <https://www.isaca.org/>

- ✓ <https://www.cisa.gov/>

- ✓ Pozor na produktové komerční weby a služby

- ✓ Pozor na akademické weby

- ✓ Nabídky certifikačních orgánů

- ✓ <https://www.tuv.com/czech-republic/en/governance-strategy.html?verbid=128>

- ✓ Information Security Management System – ISO/IEC 27000
- ✓ Common Criteria (ISO/IEC 15408)
- ✓ ISO/IEC 18043 – implementace IDS – Intrusion Detection System do IT infrastruktury
- ✓ Center of Internet Security, CIS (<https://www.cisecurity.org/>) – bezpečnostní benchmarky
- ✓ ISO 22301:2012 – Business Continuity
- ✓ National Information Security Technology (NIST) Standard Specification
- ✓ SANS Security Policy Resource – templates pro technické konfigurace
- ✓ ISO 28000 – řízení bezpečnosti dodavatelského řetězce
- ✓ OWASP Foundation
- ✓ ISO/IEC 27037 – digitální důkazy

# Standardy a best practices

4 / 36

- ✓ Payment Card Industry Data Security Standard (PCI DSS)
- ✓ Cloud Security Alliance (CSA)
- ✓ ISO/SAE 21434 KB v automotive
- ✓ ISO/IEC 29147 management zranitelností

Nejde o úplný výčet....

- ✓ NIS2 – nový zákon k kybernetické bezpečnosti č. 264/2025 sb. a navazující vyhlášky
- ✓ DORA - Digital Operational Resilience Act a navazující RTS
- ✓ GDPR...

✓ Pro začátek:

✓ <https://thehackernews.com/>

✓ <https://cybersecuritynews.com/>

✓ <https://www.infosecurity-magazine.com/>

✓ <https://www.altair.blog/>

✓ <https://www.root.cz/>

- ✓ Co je bezpečnostní certifikát
- ✓ Účel:
  - ✓ Formální:
  - ✓ Kvalifikační předpoklady VZ
  - ✓ Požadavek subjektu na dodavatele
- ✓ Pragmatický
  - ✓ Vysoká míra záruky znalostí
- ✓ Porovnatelnost

- ✓ „Národní“ certifikáty manažera a auditora IB/KB ve schématu ČIA
- ✓ Certifikace mimo schéma ČIA např. MKB od NÚKIB
  
- ✓ Mezinárodní certifikáty
  - ✓ GIAC, OSWE,
  - ✓ Certifikace SNAS institutu
  - ✓ ISACA



# Typy certifikátů

9

Certification	LinkedIn	Indeed	Simply Hired	Total
CISSP	34,343	6,976	7,512	48,831
CISA	7,778	2,851	3,085	13,714
Security+	7,366	546,990	16,979	571,335
CEH	9,805	1,300	1,205	12,310
CISM	4,676	1,825	2,248	8,749
GSEC	3,342	1,720	1,743	6,805
SSCP	3,495	3,013	1,799	8,307
CASP	2,026	911	921	3,858
GCIH	1,957	991	1,078	4,026
OSCP	2,194	552	565	3,311

<https://www.coursera.org/articles/popular-cybersecurity-certifications>

# Certifikace - bezpečnostní role

10



## CISA

The Certified Information Systems Auditor® certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems. The recent quarterly IT Skills and Certifications Pay Index (ITSCPI) from Foote Partners ranked CISA among the most sought-after and highest-paying IT certifications. This certification is a must have for mid to advanced-career IT professionals looking for leverage in career growth.

**US\$149,000+** average annual salary | **151,000+** professionals hold CISA

**GET STARTED >**



## CISM

ISACA's Certified Information Security Manager® certification indicates expertise in information security governance, program development and management, incident management and risk management. If you are a mid to advanced-career IT professional aspiring to senior management roles in IT security and control, CISM can get you the visibility you need.

**US\$149,000+** average annual salary | **48,000+** professionals hold CISM

**GET STARTED >**

# Certifikace – bezpečnostní role

11



## CRISC

Our Certified in Risk and Information Systems Control™ certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. You'll gain instant recognition and credibility with CRISC and boost your career. If you are a mid to advanced-career IT professional with a focus on IT and cyber risk and control, CRISC can get you the leverage you need to grow in your career.

**US\$151,000** average annual salary | **30,000+** professionals hold CRISC

**GET STARTED >**



## CDPSE

Modern privacy laws and regulations require organizations to implement privacy by design and by default into IT systems, networks, and applications. To do so, privacy professionals must partner with software developers, system and network engineers, application and database administrators, and project managers to build data privacy and protection measures into new and existing technology environments.

**US\$150,000** average annual salary | **16,000+** professionals hold CDPSE

**GET STARTED >**

<https://www.isaca.org/credentialing/certifications>

## CEH certification: Everything you need to know to get certified as an ethical hacker

Written by [Steven Bowcut](#) – Last updated: November 2, 2023

### In this guide

[What is the CEH cert?](#)

[CEH exam requirements](#)

[Cost of CEH certification](#)

[Bootcamp overview](#)

[Deep dive into the CEH exam](#)

[CEH salary information](#)

The Certified Ethical Hacker (CEH) certification is a globally recognized credential in the cybersecurity field that can open doors to a number of career opportunities.

<https://cybersecurityguide.org/programs/cybersecurity-certifications/ceh/>

## A deep dive on the OSCP certification aka the Offensive Security Certified Professional

<https://cybersecurityguide.org/programs/cybersecurity-certifications/oscp/>

Written by [Steven Bowcut](#) – Last updated: April 4, 2024

### In this guide

[What is an OSCP certification?](#)

[Certification cost](#)

[OSCP versus CEH](#)

[Exam overview](#)

[Exam requirements](#)

[FAQs](#)

If you have a career in Information Security and are intrigued by defensive and offensive techniques, consider becoming an **Offensive Security Certified Professional (OSCP)**.

# Cíl přednášky – informační systémy

- ✓ Bezpečnostní pohled na informační systémy
  - ✓ Liší se od funkčního – leckdy podstatně, *proč?*
  - ✓ Informační systém je subjektem ochrany

## ✓ Cílem útoků:

- ✓ Informace (reprezentována daty)
- ✓ Informační systém (v celém kontextu)
- ✓ Lidé informační systém využívající
- ✓ Sociální systémy (stát, komunita...)

## ✓ Dopady útoků – mohou být extrémní:

- ✓ Politická rozhodnutí
- ✓ Likvidace firem
- ✓ Likvidace osob

- ✓ Incidenty – nejen útoky:
  - ✓ Informace – nedostupnost, prolomení důvěrnosti, narušení integrity
  - ✓ Informační systém – nedostupnost, neoprávněné vytěžování
  - ✓ Lidé informační systém využívající – lidská selhání, nedostupnost
  
- ✓ Dopady incidentů – obdobné, jako u útoků
  - ✓ Selhání klíčových činností
  - ✓ Vznik škod
  - ✓ Reputační dopady



- ✓ Informační systém x ICT systém
- ✓ Možné pohledy na ICT systém
- ✓ Mikro IT x makro IT
- ✓ Architektura, vrstvy, provoz

- ✓ Informační systém – systém, který:
  - ✓ Sbírá informace
  - ✓ Transformuje informace na data
  - ✓ Zajišťuje přenos, zpracování a uchování dat
  - ✓ Data prezentuje a interpretuje
  - ✓ Zajišťuje archivaci nebo ničení dat
  
- ✓ Je informační systém vždy ICT (počítačový) systém?
  - ✓ Kartotéka u lékaře
  - ✓ Pořadač vizitek

- ✓ ICT systém - informační a komunikační systém využívající IT techniku
- ✓ Komunikační a informační systémy splývají
- ✓ Komunikační systémy jsou samy informačními systémy
- ✓ **ICT systém je pouze podmnožinou informačního systému**
- ✓ Je chybou zužovat bezpečnostní aspekty pouze na ICT systém

- ✓ Manažerský pohled, Business pohled
- ✓ Black Box x Crystal Box
- ✓ Mikro ICT systémy x makro ICT systémy
- ✓ Funkční pohled
- ✓ Procesní pohled
- ✓ Architektonický pohled
- ✓ Pohled dle rolí
  
- ✓ **Bezpečnostní přístup – musí zahrnovat všechny pohledy a aspekty**

- ✓ Do jaké míry IS ovlivňuje chod organizace?
  - ✓ Jak je organizace na IS závislá?
  - ✓ Existují alternativy?
  - ✓ Jaká je hodnota IS?
- ✓ Odpovědi dává analýza rizik

- ✓ Rozhodnutí k neznalosti:
  - ✓ „Jsem přetížen, zahlcen, nechci tomu rozumět“
  - ✓ „Od toho mám ajťáky“
- ✓ Iluze znalosti:
  - ✓ Čtenář časopisů a účastník konferencí
  - ✓ Znalost detailu bez nadhledu
  - ✓ Znalost minulosti
  - ✓ Mikromanagement

## ✓ Manažerský nadhled a manažerská pokora:

- ✓ Přehled základních principů a jejich pochopení
- ✓ Umění naslouchat a hodnotit
- ✓ Schopnost dělat správné závěry a rozhodnutí
- ✓ Schopnost nést odpovědnost

## ✓ Proč manažerský pohled:

- ✓ Manažer rozhoduje, manažer bezpečnosti přesvědčuje a argumentuje
- ✓ Srozumitelný jazyk
- ✓ Využití sociotechnik – manažer bezpečnosti musí mít povědomí o psychologii

- ✓ Manažerský problém:
  - ✓ Jak se orientovat, kde získat relevantní informace a nadhled?
  - ✓ Manažeři jsou přehlčeni informacemi/šumem
  - ✓ Problém nutnosti rychlých rozhodnutí/žádné podklady
  
- ✓ Experti mluví nesrozumitelným jazykem
- ✓ Bez elementárních znalostí nelze vypěstovat manažerský cit
  
- ✓ **PROČ - manažerský pohled je zdrojem vážných incidentů**



[↗ Sdílet článek](#) ▾

## Útok na ŘSD nabývá rozsáhlých rozměrů: Úřad zvažuje, zda hackerům za data zaplatit

**Ekonomika**

10. 6. 2022 11:06

Ředitelství silnic a dálnic zvažuje, zda má zaplatit výkupné ve výši desítek milionů korun, které po něm požadují hackeri. Státní organizace se v květnu stala terčem kybernetického útoku a přišla o celé účetnictví a všechny smlouvy uložené na discích. Hackeri výměnou za peníze nabízejí, že ŘSD odblokují přístup do jeho systémů a úložišť.

reklama



<https://zpravy.aktualne.cz/ekonomika/doprava/rsd/r~c124bcbee89011ec9ae20cc47ab5f122/>

## System veřejné správy napadli hackeři, útok se týkal Prahy i ministerstva práce

 AKTUALIZOVÁNO 5. 3. 2021

System veřejné správy napadli ve čtvrtek hackeři. O masivním kybernetickém útoku informoval na Twitteru pražský primátor Zdeněk Hřib (Piráti), data magistrátu podle něj nebyla poškozena. Jedním z cílů

[https://ct24.ceskatelevize.cz/domaci/3278730-system-verejne-spravy-napadli-hackeri-utok-se-tykal-prahy-i-mpsv?fbclid=IwAR2KTRD0o4re2rGio-hplqQmROzmk\\_NVMVaV47pCdDK\\_D-3wZQ-k7AmBcqA](https://ct24.ceskatelevize.cz/domaci/3278730-system-verejne-spravy-napadli-hackeri-utok-se-tykal-prahy-i-mpsv?fbclid=IwAR2KTRD0o4re2rGio-hplqQmROzmk_NVMVaV47pCdDK_D-3wZQ-k7AmBcqA)

## 6 000 českých firem bude muset řešit kybernetické zabezpečení

Je bláhové si myslet, že hackerské útoky se soustředí pouze na úřady či nemocnice. Ve stejném ohrožení jsou i soukromé firmy. Zde je problém o to větší, že většinou nejsou na podobné útoky připraveny a dosud je vůbec neřeší.

Bezpečné, dvoufaktorové přihlášení do důležitých systémů, zavedení odolné kryptografie, zálohování dat či řízení rizik je pro ně zcela neznámá oblast.

Přitom útoky na ně mohou způsobit daleko větší škody, než útoky na běžné úřady. Hackeři dnes dokážou na dálku ovládnout dávkovače chemických látek či výrobní linky potravinářských firem.

Směrnice NIS 2 bude povinná a bude se týkat jen v ČR tisíců nových subjektů. Přitom maximální pokuta za její nedodržení bude 10 000 000 Kč, nebo 2 % z celkového celosvětového ročního obrátu společnosti.

<https://proid.cz/smernice-nis-2-koho-se-tyka-a-jak-ji-aplikovat-v-praxi/>

- ✓ Black box – interní architektura systému se nezkoumá, pouze jsou definovány:
  - ✓ Vstupy
  - ✓ Transformace - funkce, vlastnosti (neřeší se jak)
  - ✓ Výstupy
  
- ✓ Typický pohled uživatele, managera
- ✓ Prvky systému typu black box – např. komerční software
- ✓ Co dělá excel?
  
- ✓ **Praxe víry – existuje cesta limitace rizik?**

- ✓ Black box - diskuse:
  - ✓ WIN, Mac OS, iOS, Android – jaká je jejich míra bezpečnosti?
  - ✓ Bezpečnostní aspekty black box, výhody, nevýhody
  - ✓ Kdy je možné z bezpečnostního hlediska využít black box?
  - ✓ Čím je dána bezpečnost systému black box
  - ✓ Jak lze ošetřit bezpečnostní aspekty systému black box
  - ✓ Kyber bezpečnost x právní instrumenty – smlouvy, odpovědnost

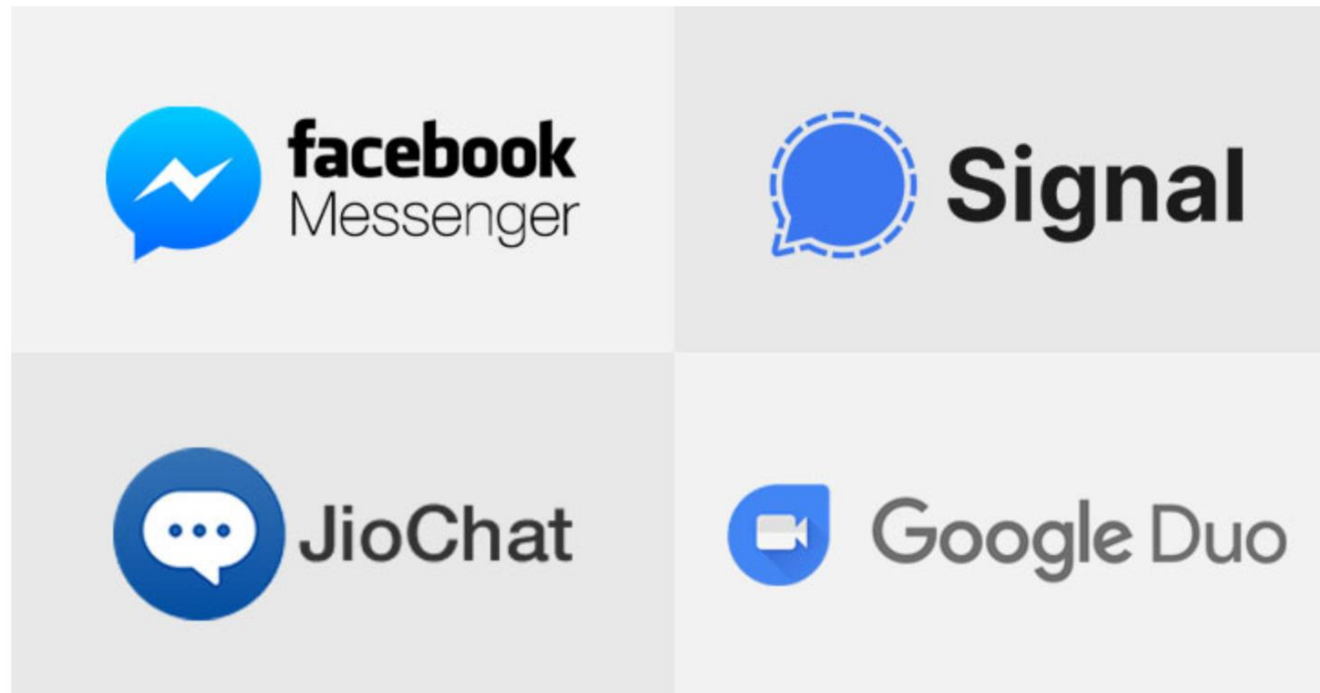
- ✓ Crystal Box – je známa podrobná architektura a všechny prvky systému:
  - ✓ Vstupy
  - ✓ Transformace - funkce, vlastnosti:
  - ✓ Prvky systému, jejich vlastnosti, funkce
  - ✓ Vazby mezi nimi – funkční, bezpečnostní
  - ✓ Interní architektura
  - ✓ Výstupy
- ✓ Pohled architekta, designéra, správce, auditora
- ✓ Pohled manažera – opět důvěra k profesionálovi
- ✓ Prvky systému – např. Open Source software

## ✓ Diskuse o Crystal Box:

- ✓ Bezpečnostní aspekty, výhody, nevýhody
- ✓ Čím je dána míra bezpečnosti?
- ✓ Kdy je výhodné použít crystal box x black box
- ✓ Kritické místo?
- ✓ Právní aspekty
- ✓ Vynutitelnost odpovědnosti za open source SW

## Google Details Patched Bugs in Signal, FB Messenger,

📅 January 20, 2021 👤 Ravie Lakshmanan



<https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html>



- **Signal** (fixed in September 2019) - A audio call flaw in Signal's Android app made it possible for the caller to hear the callee's surroundings due to the fact that the app didn't check if the device receiving the connect message from the callee was the caller device.
- **JioChat** (fixed in July 2020) and **Mocha** (fixed in August 2020) - Adding candidates to the offers created by Reliance JioChat and Viettel's Mocha Android apps that allowed a caller to force the target device to send audio (and video) without a user's consent. The flaws stemmed from the fact that the peer-to-peer connection had been set up even before the callee answered the call, thus increasing the "remote attack surface of WebRTC."
- **Facebook Messenger** (fixed in November 2020) - A **vulnerability** that could have granted an attacker who is logged into the app to simultaneously initiate a call and send a specially crafted message to a target who is signed in to both the app as well as another Messenger client such as the web browser, and begin receiving audio from the callee device.
- **Google Duo** (fixed in December 2020) - A race condition between disabling the video and setting up the connection that, in some situations, could cause the callee to leak video packets from unanswered calls.

<https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html>

- ✓ Mikro ICT systémy:
  - ✓ Zjednodušeně – lze definovat jejich perimetr
  - ✓ Interní ICT systémy korporací, firem, organizací veřejné správy, domácností
  - ✓ Feudální charakter řízení – vlastníkem
  - ✓ Větší možnosti vynucení bezpečnostní politiky
- ✓ Častý cíl interních útoků
- ✓ Rychlá reakce na incident
- ✓ Omezené zdroje (opravdu?)
  
- ✓ **Výhody?**

## ✓ Perimetr:

- ✓ Definované rozhraní
- ✓ Odděluje různé bezpečnostní úrovně
- ✓ Řízené a kontrolované prostupy

## ✓ Výhody?

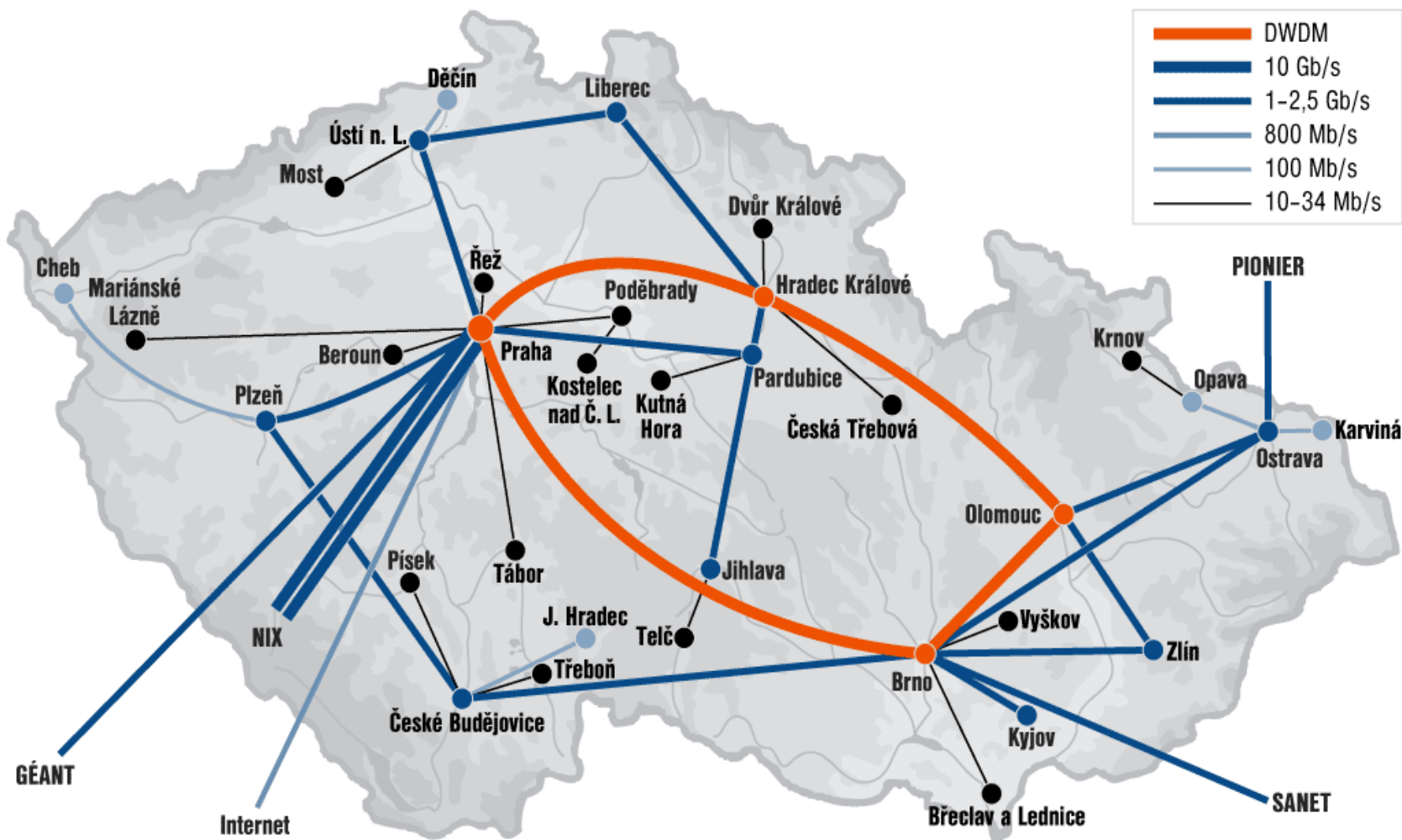
## ✓ Nevýhody?

## ✓ Realita dnes?

- ✓ Makro systémy:
  - ✓ Systémy na úrovni velkých celků – státu, silových složek, nadnárodních organizací
  - ✓ Velmi obtížně lze definovat jejich perimetr
  - ✓ Jiná architektura a charakter, než mikro ICT systémy
  - ✓ Nelze obvykle uplatnit feudální (hierarchické) řízení
- ✓ Pomalejší reakce
- ✓ Problematická definice odpovědnosti
- ✓ Obtížná vynutitelnost pravidel hry
- ✓ Jakou mají vůbec strukturu? Je hierarchická – pouze u této lze velet...

# Jak lze vypnout internet?

37 / 30



- ✓ Internet byl navržen s odolností vůči útokům zvenčí, **ne zevnitř**
- ✓ Návrh neobsahuje principy pro trasování uživatelů
- ✓ Nemá mechanismy rezistence proti nedůvěryhodným uživatelům
- ✓ **Pokrývá globální prostor – různé jurisdikce**
- ✓ Obrovská míra heterogenity
- ✓ Bezpečnost je na připojeném systému

## ✓ Hlavní výhody:

- ✓ Nízká cena
- ✓ Dostupnost připojení – rozšíření Internetu

## ✓ Problémy k řešení:

- ✓ Řízení kapacity přenosu – QoS
- ✓ Kapacita internetu se sdílí
- ✓ Bezpečnost při sdílené komunikaci – přenos nepřátelským prostředím
- ✓ Kdo komunikace sleduje?
- ✓ Neznámá rizika a vlivy na bezpečnost

- ✓ Klientské systémy – bezpečnostní pohled
  - ✓ K informačnímu systému přistupuje klient:
  - ✓ Vlastní uživatel – lze vynutit pravidla hry
  - ✓ Cizí oprávněný uživatel – vynucení pravidel hry je obtížnější
  - ✓ Anonymní uživatel
  - ✓ Identita uživatele – autentizace, autorizace
  - ✓ Bezpečnost přistupujícího zařízení – různé bezpečnostní úrovně
  - ✓ Právní odpovědnost – bankovní systémy



## ✓ Systémy bez perimetru

- ✓ Zero Trust

- ✓ Identity management

  - ✓ Human identity:

    - ✓ MFA

    - ✓ Behaviour biometrics

- ✓ Non Human Identity

  - ✓ Identita zařízení, služeb, procesů

  - ✓ MFA je obtížně řešitelné

- ✓ Nový přístup k řešení bezpečnosti

- ✓ Informatika je chápána jako množina procesů, kterými je zajištěno zpracování informací
- ✓ Příklady informatických procesů:
  - ✓ Vstupy dat – automatizované, ruční
  - ✓ Správa infrastruktury
  - ✓ Správa uživatelských požadavků
  - ✓ Provoz informačních systémů
  - ✓ Rozvoj informačních systémů
  - ✓ Řízení ICT
  - ✓ Podpůrné procesy – nákup, ekonomika, kontrola
- ✓ Procesní pohled dnes v ICT světě převažuje
- ✓ Velice často ICT procesy neobsahují bezpečnostní aspekty – ona otřepaná hesla v obálkách

- ✓ Risk management – jak identifikovat a zvládat rizika
- ✓ Business continuity – jak co nejefektivněji zvládnou výpadek
  - ✓ Zálohovací schémata
  - ✓ Havarijní plány
  - ✓ Plány obnovy
- ✓ Incident management – jak efektivně identifikovat a zvládnou incident
- ✓ Identity management
  - ✓ Uživatelé a řízení jejich přístupových oprávnění
  - ✓ Procesy zavedení nového, změna, ukončení prac. Poměru
- ✓ Release management
- ✓ Change management

- ✓ Trend – definice **katalogu služeb**
  - ✓ Definice služby, kvalitativní i kvantifikace
  - ✓ Požadavky na službu - SLA
  - ✓ Odpovědnost a role
  - ✓ Způsob poskytování služby
  - ✓ **Bezpečnostní požadavky (důvěrnost, dostupnost integrity...)**
  - ✓ Cena služby

## ✓ Business katalog služeb

- ✓ Definice služby pro management:
  - ✓ Elektronická pošta
  - ✓ Správa uživatelů
  - ✓ Provoz ERP

## ✓ Navrhněte:

- ✓ Odpovědnost a role
- ✓ Způsob poskytování služby
- ✓ Cena služby

## ✓ Technický katalog služeb

- ✓ Pod business katalogem služeb, je na něj navázán
- ✓ Zohledňuje vazby mezi systémy
- ✓ Spojuje technické služby
  - ✓ Server s virtuálem pro více služeb
  - ✓ Sdílení infrastruktury
  - ✓ Provoz ERP

## ✓ *Navrhněte:*

- ✓ Technický katalog pro elektronickou poštu

- ✓ Role v ICT procesech:
  - ✓ ICT manager
  - ✓ ICT administrátor
  - ✓ Uživatelská podpora – helpdesk
  - ✓ Solution architekt
  - ✓ Project mnanager
  - ✓ Aplikační správce
  - ✓ Auditor
  - ✓ Zákazník ICT služeb
- ✓ Organizační struktura je optimalizována pro procesní řízení
  - ✓ Podceňované hrozby – socioútoky, útoky „na role“
  - ✓ *Které role lze sdílet jednou osobou? Diskuse*

- ✓ Zaměstnanec v ICT či bezpečnostní roli
  - ✓ Vysoká míra rizika
  - ✓ Omezená možnost kontroly
  - ✓ Kreativita v obcházení pravidel
  - ✓ Zaměstnanec po výpovědi
  - ✓ Rodinní příslušníci



- ✓ Některé nástroje personální bezpečnosti (bude více v KB II)
  - ✓ Zbavení anonymity
  - ✓ Vědomí o hodnotách – přijetí zodpovědnosti
  - ✓ Školení a vzdělávání
- ✓ Definice pravidel hry:
  - ✓ Politiky a směrnice
  - ✓ Etické kodexy
  - ✓ Smlouvy a závazky mlčenlivosti
- ✓ Firemní kultura a prostředí
  - ✓ Sociotechniky
  - ✓ Důsledná kontrola – audit, pen testy

- ✓ Rizikové faktory:
  - ✓ Výpověď
  - ✓ Podcenění výpovědi ne manažerských pozic
  - ✓ Podcenění procesního a technického řešení
  - ✓ Trénink manažerů, jak se rozejít
  - ✓ Pocit křivdy – nespravedlnost, nedodržení podmínek, demotivace
- ✓ Vážná rodinná situace
- ✓ Charakter zaměstnance - chamtivost

- ✓ Infrastruktura
  - ✓ Vše, co je potřeba k provozu aplikací
- ✓ Aplikační vrstva
  - ✓ Aplikační software, ERP systémy...
- ✓ Vrstva služeb
  - ✓ Služby poskytované IS
  - ✓ Řízení, správa a vše okolo

- ✓ Fyzická vrstva:

- ✓ Datové spoje

- ✓ Hardware

- ✓ Software infrastruktury:

- ✓ SW spojený s HW – ovladače, speciální komunikační software, protokoly

- ✓ Operační systémy

- ✓ Databázové systémy

- ✓ Komunikační software

- ✓ Bezpečnostní software

## ✓ Bezpečnostní problémy:

- ✓ Důvěrnost – autentizace, autorizace, nakládání s vadnými díly, otevřené přístupy, infrastrukturní software - zabezpečení
- ✓ Dostupnost – business continuity – zálohování a obnova funkcí, odezvy, přístupy, servisní smlouvy
- ✓ Integrita – nedochází ke změnám uložených dat? Jsou kompletní?

## ✓ Problém dneška:

- ✓ Heterogenní prostředí, mobily, tablety...
- ✓ Neexistence perimetru
- ✓ Cloud

## ✓ *Kde je optimum mezi uživatelským komfortem a náklady na bezpečnost?*

- ✓ Bezpečnostní problémy:
  - ✓ Black Box x Crystal Box
- ✓ Black Box:
  - ✓ Software (ale i hardware) obvykle na komerční bázi, není k dispozici úplná dokumentace, zdrojové kódy
  - ✓ Microsoft, Apple, Oracle, CheckPoint, McAfee, Symantec ...
- ✓ Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit
- ✓ Crystal Box:
  - ✓ Většinou Open Source, je k dispozici zdrojový kód a dokumentace
  - ✓ Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit

- ✓ Zjednodušeně – software, který pracuje nad infrastrukturou, využívá ji a zpracovává data – interpretuje na informace
- ✓ Členění je různé:
  - ✓ Podnikové systémy – ERP, CRM, APS, MES, Document Management, Workflow Management...
  - ✓ Kancelářské systémy – Office, mail...
- ✓ Bezpečnostní problémy:
  - ✓ Důvěrnost – přístupy, způsob uložení dat, přístupy podpory, logy
  - ✓ Dostupnost – SLA, business continuity
  - ✓ Integrita – jsou data korektní, zpracovávají se popsáním způsobem? Je aplikační logika dokumentována a testována?

- ✓ Licenční čistota, podmínky rozšíření licencí
- ✓ Vendor Lock
- ✓ Podmínky podpory – SLA, obsah, podmínky, řešení incidentů
- ✓ Práce s datovými médii
- ✓ Know how – dostupnost implementačních konzultantů
- ✓ Vzdálené přístupy – neexistence NDA
- ✓ Stabilita dodavatele
- ✓ Struktura dat
- ✓ Aplikační logika
- ✓ Archivace dat
- ✓ Formát dat
- ✓ Odezva a rychlost



- ✓ Stará myšlenka nově marketingově uchopená
  - ✓ Jak mámit z uživatelů více peněz 😊
  - ✓ Obecně nelze cloud ani zatratit ani nekriticky doporučit
- ✓ Princip:
  - ✓ Sdílení zdrojů je levnější
  - ✓ Platím jen to, co opravdu potřebuji
- ✓ Obsah cloudu:
  - ✓ Uložiště dat
  - ✓ Synchronizace, sdílení dat
  - ✓ Poskytování aplikací
  - ✓ Zajištění provozu – SLA

## ✓ Bezpečnostní rizika:

- ✓ Data nejsou pod kontrolou – i „triviální operace“ (výmaz dat...)
- ✓ Jurisdikce, kde jsou data uložena
- ✓ Bezpečnostní řetězec - kdo má k datům přístup – poskytovatel, telco služby
- ✓ Důvěryhodnost a stabilita poskytovatele

## ✓ Bezpečnostní výhody:

- ✓ SLA
- ✓ Zajištění drahých bezpečnostních služeb (zálohování, incident management)
- ✓ Sdílení drahých technologií (uživatel by si je sám nikdy nekoupil)

- ✓ Pokud uvažuji cloud – co bych měl řešit:
  - ✓ Kupuji si co – ne jak
  - ✓ Obsah služby
  - ✓ Výkon – ne konfiguraci
  - ✓ Rozsah služby – jak bude měřena účtována
  - ✓ SLA
  - ✓ Dostupnost
  - ✓ Business continuity
  - ✓ Management dat, výmaz dat
  - ✓ EXIT služby

- ✓ Služby poskytované IS – návrat ke katalogu služeb
- ✓ Forma poskytování:
  - ✓ Insourcing – realizace vlastními zaměstnanci
  - ✓ Outsourcing – realizace najatými subjekty

# IS = Information Technology + Operational Technology

61 / 30

✓ IT => Information Technology

✓ Standardní IS

✓ ERPP, CRM...

✓ OT => Operational Technology

✓ Technologie

✓ Stroje

✓ Senzory

✓ Řídící jednotky

# IS = Information Technology + Operational Technology

62 / 30

- ✓ IT bezpečnost => CIA Triad = Důvěrnost x Dostupnost x Integrita
- ✓ OT bezpečnost => BOZP x CIA Triad:
  - ✓ Norma ISA / IEC 62443
  - ✓ Security technologies for industrial automation and control systems
  - ✓ Primárně je zaměřena na ochranu OT prostředí
  - ✓ Obsahuje však také částečně ISO 270001

# IS = Information Technology + Operational Technology

63 / 30

- ✓ IT bezpečnost => CIA Triad = Důvěrnost x Dostupnost x Integrita
- ✓ OT bezpečnost => BOZP x CIA Triad:
  - ✓ Norma ISO / IEC 62443
  - ✓ Security technologies for industrial automation and control systems
  - ✓ Primárně je zaměřena na ochranu OT prostředí
  - ✓ Obsahuje však také částečně ISO 270001

- ✓ Architektura IS:
  - ✓ Návrh IS, aby sloužil svému účelu
  - ✓ Aby IS dosáhl stanoveného cíle
  
- ✓ Cíle musí být známy
  
- ✓ Architektura co nejjednodušší
  - ✓ Komplikovanost generuje problémy
  
- ✓ Bez architektury nelze úspěšně řešit bezpečnost



## ✓ Historické architektury:

- ✓ Architektura mainframe (sálové počítače)
- ✓ Architektura sdílení souborů
- ✓ Architektura klient – server
- ✓ Dvouvrstvá architektura (uživatelská a databázová vrstva)
- ✓ Třívrstvá architektura (vrstvy uživatelská, obchodní logiky a datová)
- ✓ MDA – modelově řízená architektura
- ✓ SOA – servisně orientovaná architektura

## ✓ *Kde se nám ztratila bezpečnost?*

- ✓ Bezpečnost je nezbytnou součástí architektonického návrhu
  - ✓ Ex post bezpečnost je obtížná a drahá
  - ✓ Ex post bezpečnost je někdy neřešitelná
- ✓ Řešení:
  - ✓ Přístup založený na managementu rizik
  - ✓ Detekce primárních x business aktiv
  - ✓ Návrh bezpečnostní architektury odolné proti relevantním hrozbám
- ✓ *Kde se nám ztratila bezpečnost?*



Prostor pro vaše dotazy

Prostor pro vaše dotazy...

# Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký