Kybernetická odolnost: Pilíř stability a růstu v nové regulatorní realitě

Pro vrcholové vedení (CEO, CFO, CTO, COO, CSO, apd.)

Miroslav Hanus, Business Line Auditor, Information Security Services

Ostrava, 24. 6. 2026

Add value.
Inspire trust.

Ing. Miroslav Hanus, LL.M., MBA

Manažer, architekt a auditor kybernetické bezpečnosti

- **Hutní průmysl** (Nová huť Ostrava / ArcelorMittal / Liberty)

U zrodu budování ICT infrastruktury a datových center v náročném průmyslovém prostředí.

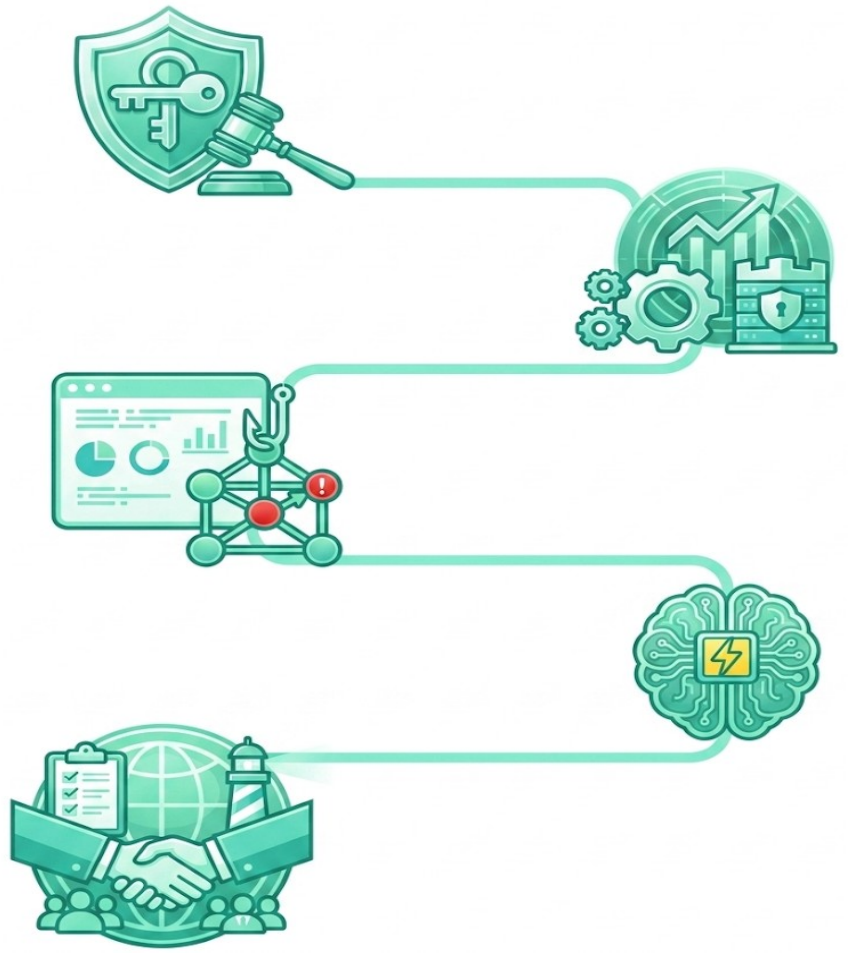
- **Státní správa** (Moravskoslezské datové centrum)

CISO a budování ICT infrastruktury a datových center pro odbory sociální, školství, kultury, dopravy a zdravotnictví, především pro 7 nemocnic a záchrannou službu.

- **TÜV SÜD Czech** auditor a lektor pro certifikační orgán

Agenda dnešního setkání

- LEGISLATIVNÍ RÁMEC A ODPOVĚDNOST
- ŘÍZENÍ RIZIK A BUSINESS KONTINUITA
- NEJČASTĚJŠÍ ÚTOKY A SCÉNÁŘE
- UMĚLÁ INTELIGENCE A NOVÁ RIZIKA
- AKTIVNÍ ROLE MANAGEMENTU A SHRNUTÍ



BUDOUCNOST LEGISLATIVNÍ RÁMEC A ODPOVĚDNOST

Proč je problematika kybernetické bezpečnosti důležitá?

- Celosvětové náklady na kyberkriminalitu v roce 2025 jsou na astronomické částce **10,5 bilionu dolarů**, rostou okolo 15 % ročně. Průměr na jeden KBI 53t $.

- Česká republika v roce 2025 zaznamenala meziroční nárůst kybernetických bezpečnostních incidentů o **30%**, s celkem 3005 registrovanými případy (csirt.cz).

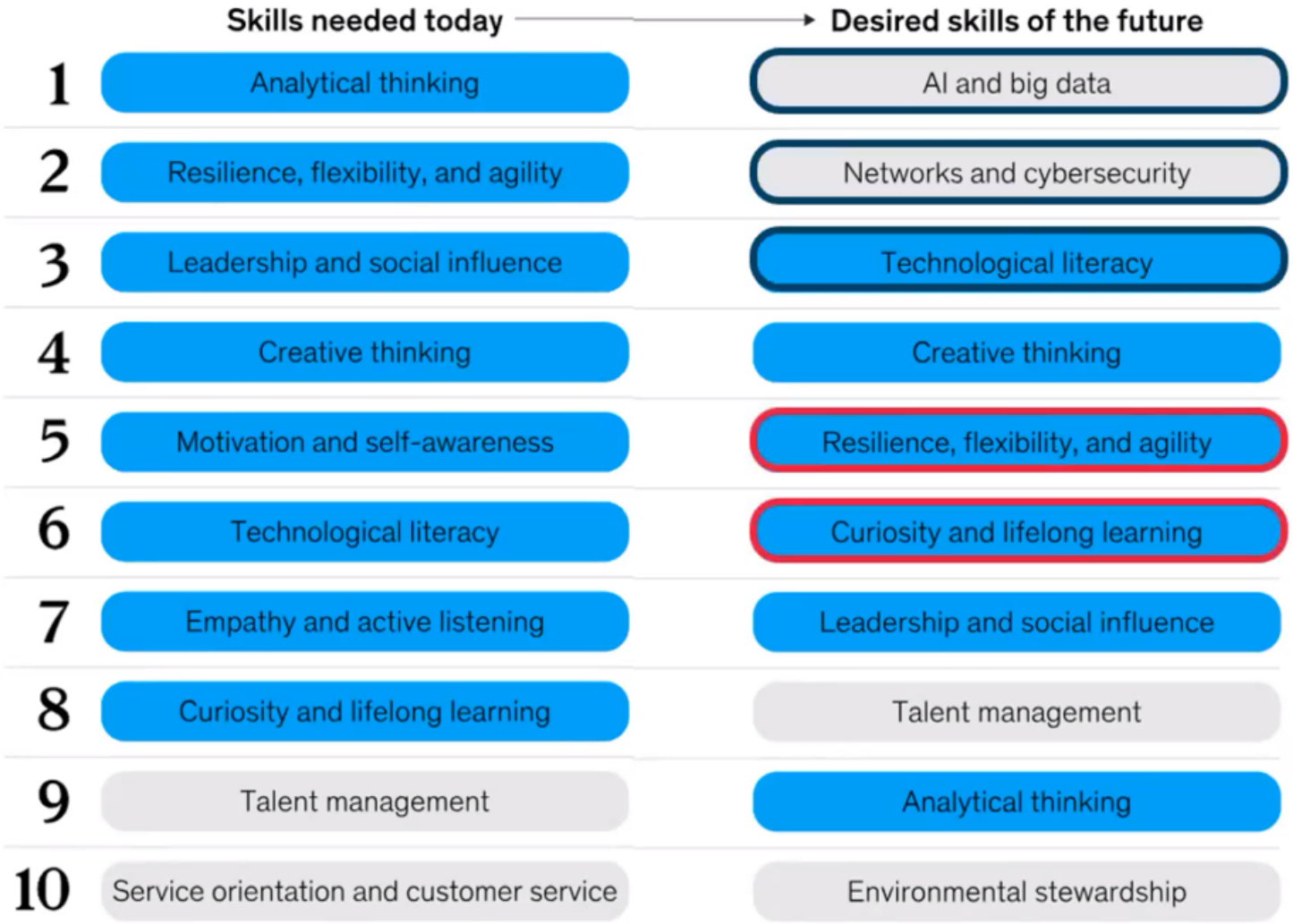
- **AI v útocích:** Pachatelé stále častěji využívají umělou inteligenci pro sofistikovanější oslovování obětí a útoky.

- **Máte s kyberšmejdem nějaké zkušenosti…**

Náhled do budoucnosti

V roce 2030 budou požadavky na konkurenceschopné pracovní dovednosti tkz. Brainskills přeskočí Hardskills orientace v technologiích.

- Celoživotní vzdělávání, adaptabilita, flexibilita, odolnost a vytrvalost.



Zdroj: WEF – Future of jobs report 2025

EU Digitalní regulativní rámce

Odpovědnost

Auditovatelnost

Vysoké sankce

Ochrana dat

- GDPR (2016/679) - osobní data
- DGA (2022/868) - sdílení dat
- Data Act (2023/2854) - využití dat
- AI Act (2024/1689) - řízení rizik AI

Ochrana spotřebitele / trhu

- DMA (2022/1925) - Big Tech
- DSA (2022/2065) - online obsah
- eIDAS 2 (2024/1183) - digitální identita

Kybernetická bezpečnost

- CSA (2019/881) – ENISA certifikace
- DORA (2022/2554) - finanční sektor
- CRA (2024/2847) - digitální produkty
- CER (2022/2557) - odolnost KI
- NIS2 (2022/2555) - organizace

Nařízení => přímá aplikovatelnost v celé EU

Směrnice => transpozice legislativy do člen.států

Regulace nebude méně

- CRA (2027 co musí produkt splnit)
- CSA2 (2028 jak to certifikovat, ENISA „architekt“ certifikace, ECCF)
- DNA (2028 digitální sítě a telekomunikace v EU)
- NIS3 (2030 proaktivní nařízení kybernetické odolnost pro všechny)
- GDPR 2.0 (203? evoluce méně byrokracie, více AI-ready pravidel)

Digital Omnibus = zjednodušení a propojení existujících EU digitálních regulací

Celosvětové standardy: ISO/IEC 27001:2022 KB, ISO/IEC 42001:2023 AI

Zákon č. 266/2025 Sb. O Kritické infrastruktuře

- Účinnost zákona od 19.8.2025

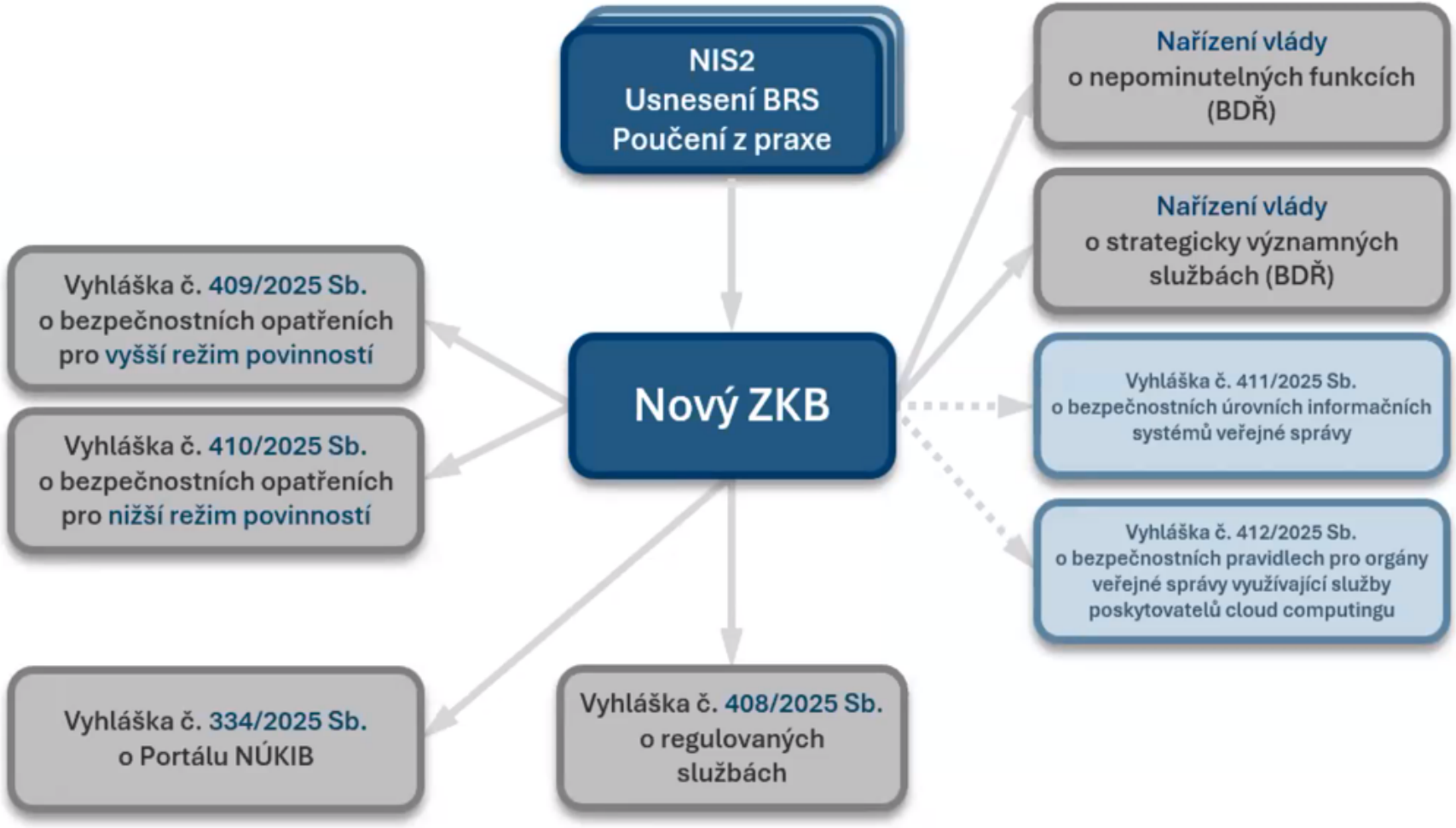
- Je navázán na směrnice EU zejména NIS2 a CER (Critical Entities Reselience Directive). Všechny členské státy EU musí vytvořit národní strategii odolnosti, AR, identifikovat a dohlížet na kritické subjekty (do 17.7.2026).

- **Cíl zákona:** zvýšit odolnost státu a zajistit nepřerušené fungování klíčových služeb pro společnost (např. energetika, doprava, zdravotnictví, ICT, apd.).

- Rostoucí komplexita prostředí (hyperfragilita), digitalizace a automatizace AI FOMO.

Zákon č. 264/2025 Sb. O kybernetické bezpečnosti

- Účinnost od 1.11.2025
- Samoidentifikace (březen 2026)
- Plnění do 1 roku



Zdroj: NÚKIB Portál (TLP:GREEN)

Nové povinnosti zákona o kybernetické bezpečnosti

2025

- § 6 Registrovat regulovanou službu => do 60 dnů od naplnění identifikačních kritérií
- § 9 Hlásit změny regulované služby
- §11 Hlásit kontaktní a další údaje => do 14 dní změny údajů
- §12 Stanovit rozsah řízení kybernetické bezpečnosti

2026

- §13 §14 Zavádět bezpečnostní opatření => do 1 roku od zařazení do evidence
- §15 Hlásit kybernetické bezpečnostní incidenty => do 1 roku od zařazení do evidence
- §19 Plnit informační povinnost poskytovalete reg.služby => ihned podle zav.opatření a incidentů
- §20 Reagovat na protiopatření => ihned podle lhůt stanovených v protiopatření

Osobní odpovědnost statutárů a ředitelů

- **§ 13:** Stanovení rozsahu řízení kybernetické bezpečnosti.
- **§ 14:** Odpovědnost za zavedení bezpečnostních opatření.
- **Důsledek:** Vedení už nemůže říct "já tomu nerozumím, to řeší CISO". Musíte rozumět dopadům na podnikání.
- **Důraz:** Zákon je přísnější než směrnice EU. Definuje jasné lhůty pro hlášení (24/72 hodin) a povinnost vzdělávání vedení.

Sankce a následky nesouladu

Př. Obrat 1,33 mla EUR, max. pokuta 2% = 26,6 mlo EUR

- **§ 59 Pokuty:** Do 250 mil. Kč nebo 2 % z obratu.
- **§ 57 Reputace:** Ztráta důvěry u dodavatelů a bank.
  (Pozastavení platnosti certifikace nejméně na 6 měsíců).
- **§ 58 Osobní dopad:** Dočasný zákaz výkonu funkce člena statutárního orgánu.
  (V extrémním případě).

Vyhláška č. 408/2025 Sb. O regulovaných službách

- **Regulované služby**:

  1.Veřejná správa, 2.Energetika

  7.Výrobní, potravinářský a chemický průmysl

  10.Vodní a odpadové hospodářství

  12.Letecká, drážní, vodní a silniční doprava

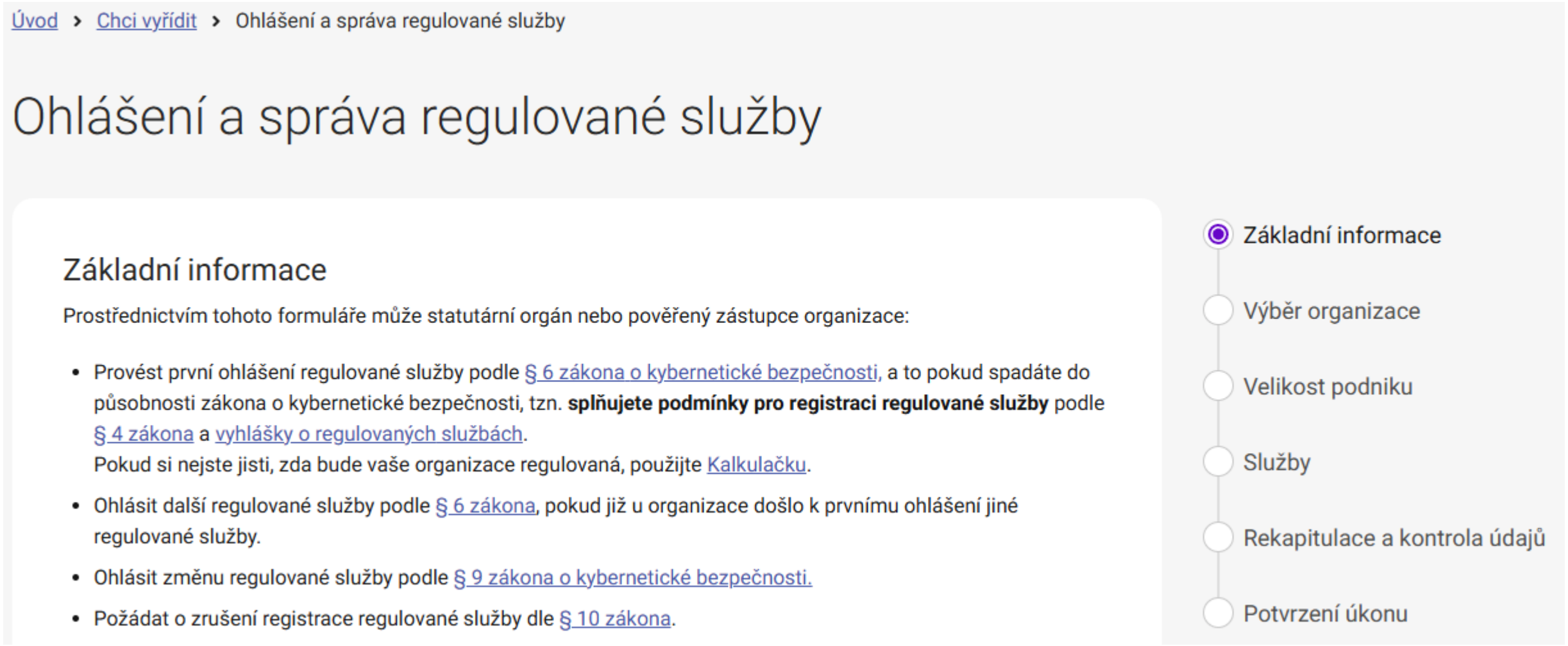
  16.Digitální infrastruktura a služby, 20.Poštovní a kurýrní služby

  17.Finanční trh, 18.Zdravotnictví, 19.Věda a výzkum

  21.Obranný a vesmírný průmysl

- **Režim vyšších povinností:** pro velký podnik nad 250 zaměstnanců a nebo obrat nad 1,25 miliardy Kč, případně pro strategicky významné subjekty

Vyhláška č. 334/2025 Sb. O portálu NÚKIB



Zdroj: https://portal.nukib.gov.cz

Upozornění na smishingovou kampaň, ve které se útočníci vydávají za Policii České republiky

Upozorňujeme na smishingovou kampaň, v rámci které se útočníci prostřednictvím SMS zpráv vydávají za Policii České republiky s cílem získat platební údaje obětí.

Číst více

20. 5. 2026

Upozorňujeme na sérii zranitelností v Linuxovém kernelu

Během přelomu dubna a května 2026 byly zveřejněny hned čtyři závažné zranitelnosti v Linuxovém jádře. Copy Fail (CVE-2026-31431), Dirty Frag (CVE-2026-43284 + CVE-2026-43500), Fragnesia (CVE-2026-46300) a ssh-keysign-pwn.

Číst více

15. 5. 2026

Podpůrné materiály

Podpůrné materiály k legislativě, technická doporučení a další užitečné dokumenty z oblasti kybernetické bezpečnosti.

Zobrazit všechny podpůrné materiály

Rychlé přehledy

Informativní články s hlubším kontextem

Metodiky a doporučení s praktickými postupy

Zdroj: https://portal.nukib.gov.cz

Vyhláška č. 410/2025 Sb. Režim nižších povinností

Určuje mírnější sadu pravidel pro zajišťování kybernetické bezpečnosti pro méně kritické subjekty.

3. klíčové přílohy

BEZPEČNOSTNÍ OPATŘENÍ (12)

- § 3 Systém zajišťování minimální kybernetické bezpečnosti
- § 4 Požadavky na vrcholné vedení
- § 5 Bezpečnost lidských zdrojů
- § 6 Řízení kontinuity činností
- § 7 Řízení přístupu
- § 8 Řízení identit a jejich oprávnění
- § 9 Detekce a zaznamenávání kybernetických bezp.událostí
- §10 Řešení kybernetických bezpečnostních incidentů
- §11 Bezpečnost komunikačních sítí
- §12 Aplikační bezpečnost
- §13 Kryptografické algoritmy
- §14 Stanovení významnosti dopadu KBI

- Příloha č.1 Přehled bezpečnostních opatření
- Příloha č.2 Požadavky na smluvní ujednání s dodavateli (14)
- Příloha č.3 Témata pro rozvoj bezpečnostního povědomí (25)

Vyhláška č. 409/2025 Sb. Režim vyšších povinností

Stanovuje přísná organizační a technická bezpečnostní opatření i pro strategické a významné subjekty.

ORGANIZAČNÍ OPATŘENÍ (14)

- § 3 Systém řízení bezpečnosti informací
- § 4 Požadavky na vrcholné vedení
- § 5 Stanovení bezpečnostních rolí
- § 6 Řízení bezpečnostní politiky a bezpečnostní dokumentace
- § 7 Řízení aktiv
- § 8 Řízení rizik
- § 9 Řízení dodavatelů
- § 10 Bezpečnost lidských zdrojů
- § 11 Řízení změn
- § 12 Akvizice, vývoj a údržba
- § 13 Řízení přístupu
- § 14 Zvládání kybernetických bezp.událostí a incidentů
- § 15 Řízení kontinuity činností
- § 16 Provádění auditu kybernetické bezpečnosti

TECHNICKÁ OPATŘENÍ (11)

- § 17 Fyzická bezpečnost
- § 18 Bezpečnost komunikačních sítí
- § 19 Správa a ověřování identit
- § 20 Řízení přístupových oprávnění
- § 21 Detekce kybernetických bezpečnostních událostí
- § 22 Zaznamenávání událostí
- § 23 Vyhodnocování kyber.bezpečnostních událostí
- § 24 Aplikační bezpečnost
- § 25 Kryptografické algoritmy
- § 24 Zajišťování dostupnosti regulované služby
- § 27 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Celkem 25 základních opatření.

409 vs 410

Vyhláška č. 409/2025 Sb. Režim vyšších povinností

Stanovuje přísná organizační a technická bezpečnostní opatření i pro strategické a významné subjekty.

6. klíčových příloh

- Příloha č.1 Hodnocení aktiv
- Příloha č.2 Likvidace informací a dat
- Příloha č.3 Zranitelnosti (17) a hrozby (21)
- Příloha č.4 Hodnocení rizik
- Příloha č.5 Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy (18)
- Příloha č.6 Témata pro rozvoj bezpečnostního povědomí (25)

Další požadavky nové regulace

- Princip přiměřenosti pro realnou mitigaci svých rizik
- Nutné změny ve smlouvách (bezp.opatření, hlášení KBI, monitoring, audity a kontroly)
- Certifikace, technické a oborové standardy ? (DORA, ISO27001, 27701, TISAX apod.)
- Incident management (včasné oznámení a spolupráce při řešení)
- Zajištění kontinuity služeb a exit strategie (zvládat bezpečnostní krize a havárie)
- Odpovědnost a sankce
  - Smluvní pokuty za porušení bezpečnostních povinností
- Podmínky pro subdodavatelé
  - Zajištění stejných bezpečnostních standardů, je to opravdu nutné?
- Předávání dat
  - Povinnost informovat o změnách v infrastruktuře

Jak začít

- S rozmyslem a rozumnými náklady princip přiměřenosti pro realnou mitigaci svých rizik
- Analýza poskytovaných služeb a jejich klasifikace podle legislativy
- Analýza rizik, zpracování informací a obchodních tajemství
- GAP analýza bezpečnostních opatření, procesů, evidencí a nástrojů
- Zavedení bezpečnostního standardu (ISMS)
- Vzdělávání zaměstnanců klíčové !

ŘÍZENÍ RIZIK A BUSINESS KONTINUITA

Rizikově orientovaný přístup "Risk-Based Approach"?

- **Definice:** Nechráníme všechno stejně. Chráníme to, co nás nejvíc bolí!
- **Příklad:** Rozdíl v ochraně testovacího prostředí vs platební brány.
- **Hlavní principy rizik**: Identifikace, Hodnocení, Prioritizace, Řízení a Kontrola.
- **Dokumentace:** Metodika řízení rizik, Zpráva o hodnocení rizik, Plán zvládání rizik a Prohlášení o aplikovatelnosti.

Klíčové aktiva

- **Registr aktiv:**
  - Zákaznická databáze
  - Logistický systém
  - Webová platforma
  - Reputace značky

- **Úkol pro účastníky:** Které z těchto 4 aktiv by při výpadku na 24h bolelo nejvíc?

Business Continuity – Plán obnovy

- **Klíčové metriky:**
  - RTO (Recovery Time Objective) – Jak dlouho budeme stát?
  - RPO (Recovery Point Objective) – O kolik dat příjdeme?

- **Scénář:**

  Pokud vám shoří serverovna, za jak dlouho budeme expedovat první balík?

Role managementu v řízení rizik

- Management definuje "apetit k riziku".

- **Rozhodnutí:** Je pro nás levnější riskovat výpadek, nebo investovat 5 milionů do záložního systému? To je manažerské, ne technické rozhodnutí.

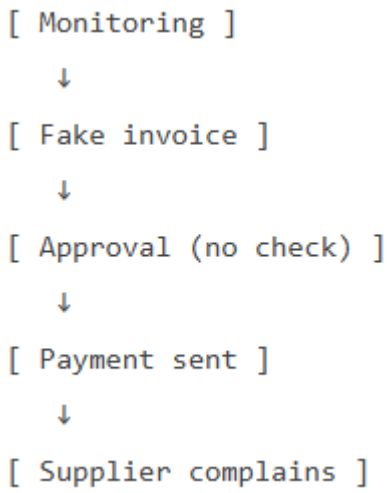
NEJČASTĚJŠÍ ÚTOKY A SCÉNÁŘE

Útok 1: Spear Phishing (Cílený lov)

- **Detail:** Útočník studuje cíle několik týdnů, například LinkedIn apd...
- **Jak to vypadá:** E-mail od "dodavatele", který vypadá naprosto legitimně.
- **Cíl:** Získat přístupové údaje do nákupního portálu.

Scénář: Napadení nákupního procesu

- **Popis kroky:** Útočník změní číslo účtu u faktury. Peníze odcházejí na offshore účet.
- **Zjištění:** Až po měsíci, kdy se ozve skutečný dodavatel, že nemá peníze.
- **Ponaučení:** Chybělo procesní (lidské) ověření mimo e-mail.



Útok 2: Ransomware (Vyděračský software)

- **Mechanismus:** Zašifrování dat a požadavek na výkupné v Bitcoinech.

```
Day 0 → Infection
Day 30 → Silent spread
Day 60 → Backup compromised
Day 90 → ATTACK TRIGGERED 💥
```

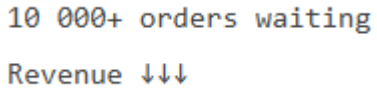
- **Doba nákazy:** Malware může v síti "spát" měsíce a mapovat zálohy.

```
Systems → 🔒 encrypted
Warehouse → STOP
Web → DOWN
```

Scénář: Skladová paralýza

- Skladníci nemohou skenovat kódy. Dopravci nemají štítky. Expedice stojí.

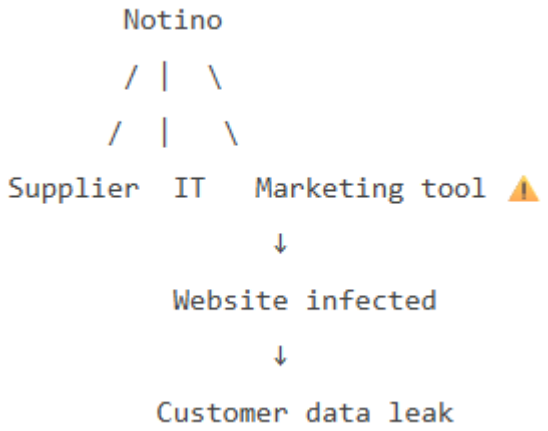
- **Problém:** Zálohy byly napadeny jako první. Obnova trvá týdny.



- **Cena:** Nejde jen o výkupné, ale i o ušlý zisk a penále.

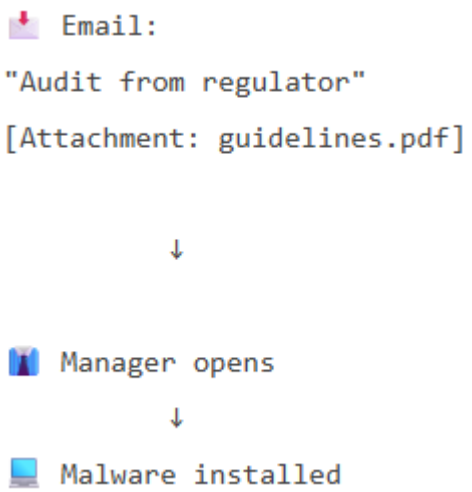
Útok 3: Dodavatelský řetězec

- **Kontext:** Společnost je tak bezpečná, jak bezpečný je jeho nejslabší dodavatel.
- **Příklad:** Útok přes marketingový skript na webu (získání dat o kartách).



Útok 4: Sociální inženýrství na management

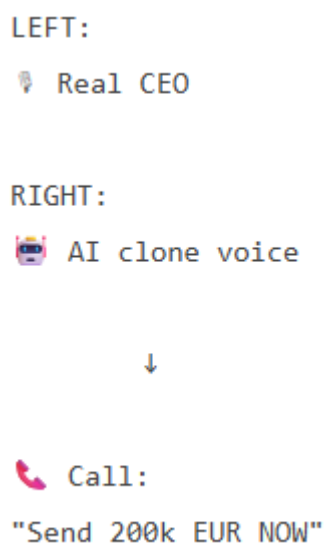
- **Spouštěč:** Útok "na ego" nebo "strach".
- **Příklad:** Falešný e-mail od dozorového úřadu o zahájení kontroly s infikovanou přílohou "Pokyny pro kontrolu".



UMĚLÁ INTELIGENCE A NOVÁ RIZIKA

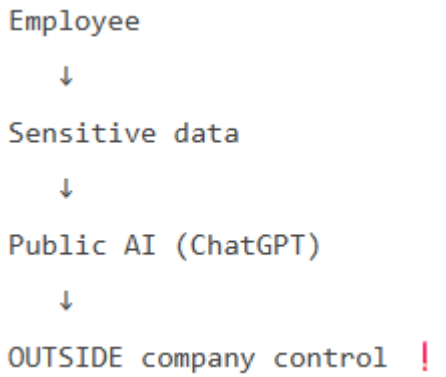
AI jako nástroj útoku: Deepfake 2.0

- **Vizuální podvody:** Vytvoření falešného videa s vedením firmy.
- **Audio podvody:** Hlas šéfa v telefonu, který dává urgentní pokyn k převodu.
- **Realita:** Dnes stojí vytvoření hlasového klonu pár dolarů a pár minut.



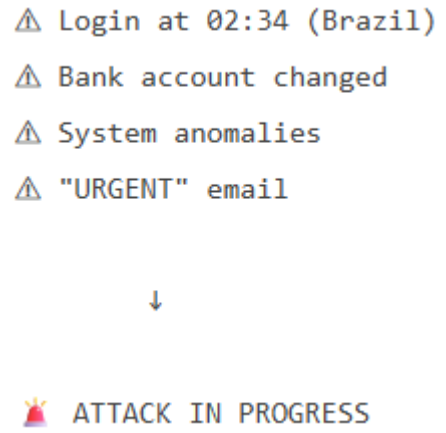
Bezpečné používání AI ve společnosti

- **Riziko úniku dat:** Zaměstnanci vkládají citlivá data do veřejných modelů.
- **Pravidlo:** Co nesmíte říct na veřejnosti, nesmíte napsat do ChatGPT.



AI v obraně (Jak nám pomáhá)

- **Detekce anomálií v reálném čase.**
  - AI pozná, že se uživatel přihlašuje z neobvyklého místa nebo v neobvyklý čas.



AKTIVNÍ ROLE MANAGEMENTU A SHRNUTÍ

5 věcí, které musí vedoucí dělat od pondělí

- Prověřit, zda jeho lidé mají zapnuté MFA (vícefaktor).
- Mít přehled o kritických dodavatelích.
- Podporovat nahlašování chyb (No-blame culture).
- Znát krizový komunikační strom (komu volat ve 2 ráno).
- Být příkladem v digitální hygieně.

Kybernetická hygiena jednotlivce

- Hesla (správci hesel), MFA, aktualizace, bezpečné Wi-Fi na cestách.

- **Důraz:** Útok na firmu začíná u vašeho soukromého Gmailu nebo LinkedInu.

Praktická cvičení a simulace

- **Plánování:** Budete provádět testovací simulaci útoku (v souladu s NZKB).

- **Prosba:** Potřeba vaši součinnosti a účasti, aby to bylo reálné.

Shrnutí

- **Klíčové sdělení**:

  Bezpečnost společnosti je týmový sport, kde management je v první linii.

- Kontakty na CISO / Bezpečnostní tým.

Prostor pro vaše dotazy

Děkuji za pozornost.

Ing. Miroslav Hanus, LL.M., MBA

Business Line Auditor

Information Security Services

Email: miroslav.hanus@tuvsud.com

Follow us on:

tuvsud.com
info@tuvsud.com