



Digitálna  
koalícia

# DIGITÁLNA BUDÚCNOSŤ



Spolufinancovaný  
Európskou úniou



PROGRAM  
SLOVENSKO



MINISTERSTVO  
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA  
A INFORMATIZÁCIE  
SLOVENSKEJ REPUBLIKY



# Kybernetická bezpečnosť

Michal Ohrablo

29.09.2026, Piešťany

**Tento seminár je súčasťou  
národného projektu Digitálna  
budúcnosť.**



# RIS3 – Stratégia výskumu a inovácií pre inteligentnú špecializáciu SR 2021- 2027

- Spolupráca **podnikateľov, výskumných inštitúcií a štátu**
- Kombinácia priorít **akademickej obce** a strategických **záujmov firiem**
- Zameranie na oblasti s vysokou pridanou hodnotou pre ekonomiku SR
- **Cieľ:** Podpora hospodárskeho rastu cez výskum a inovácie
- Financovanie výhradne pre domény definované v RIS3:
  - **Doména 1: Inovatívny priemysel pre 21. storočie**
  - Doména 2: Mobilita pre 21. storočie
  - **Doména 3: Digitálna transformácia Slovenska**
  - Doména 4: Zdravá spoločnosť
  - Doména 5: Zdravé potraviny a životné prostredie

Naskenujte QR kód  
pre bližšie informácie



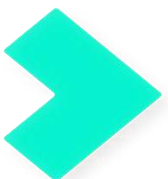
# Agenda



1. Ciele seminára vo väzbe na RIS3 2021+
2. Špecifiká DT pre prioritnú oblasť *Kybernetická bezpečnosť*
  - a) existujúce ohrozenia, urgentnosť ich riešenia formou DT
  - b) hlavné zmeny vyvolané realizáciou DT



3. Šesť pilierov transformácie prioritnej oblasti
4. Digitálne a zelené zručnosti pre kľúčové povolania



5. Zhrnutie cieľov seminára – odporúčenia ďalšieho postupu



## Ciele seminára vo väzbe na RIS3 2021+



## Cieľ seminára

- Pochopenie KB prostredia (Cybersecurity Landscape)
- Poskytnutie základných informácií ohľadom integrácie KB do iniciatív digitálnej transformácie
- Ukázanie prepojenia digitálnych zručností s KB



# Špecifiká digitálnej transformácie pre kybernetickú bezpečnosť

## *Existujúce ohrozenia, urgentnosť ich riešenia*

*„Kybernetická bezpečnosť nie je problém IT oddelenia. Je to podnikateľské riziko, ktoré patrí na stôl vedenia.“*



# Prečo by útočili práve na nás?

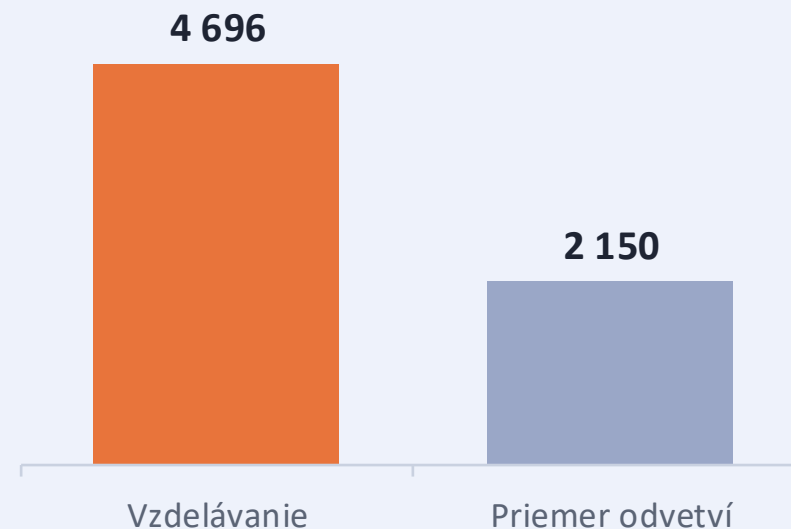
- Útočník si nevyberá firmu – vyberá si **slabé miesto**. Väčšina útokov je automatizovaná.
- Menšie organizácie majú menej zdrojov na obranu → pre útočníka **efektívnejší cieľ**.

*„Nás si nikto nevšimne“ je najčastejší mýtus.*

**+18 %**

medziročný nárast pokusov o útok na vzdelávanie v Európe

Pokusy o útok týždenne na jednu organizáciu (jan – júl 2026)



Vzdelávanie je celosvetovo **najčastejšie napádaný sektor** – viac než dvojnásobok priemeru.

Zdroj: Check Point Research, Back-to-School Cyber Risks (2026). Počítajú sa pokusy o útok zachytené senzormi, nie úspešné incidenty.



# Kto útočí a čo chce



## Zisk

- Krádež dát: osobné údaje, know-how, klientske databázy
- Finančné podvody
- Vydieranie



## Sabotáž

- Vyradenie systémov
- Nedostupnosť služieb
- Zašifrovanie dát (ransomvér)



## Moc a vplyv

- Štátni aktéri a hacktivistí
- Špionáž
- Dezinformácie, geopolitika

**Organizovaný kyberzločin je profesionálne odvetvie: deľba práce, zákaznícka podpora, výskum a vývoj.**



# Mapa hrozieb 2026: šesť vstupných brán



č. 1



## Nezáplatované systémy

VPN, router, NAS či web vystavené do internetu.



## Heslá bez MFA

Ukradnuté alebo slabé heslá k e-mailu, cloudu, sieťam.



## Phishing a podvodné weby

E-mail, SMS a falošné prihlasovacie stránky.

č. 2



## Telefonát a deepfake

„Šéf“ alebo „IT podpora“ žiada prístup či platbu.



## Dodávatelia

IT správca, platforma či agentúra s prístupom k vám.



## Chybné nastavenie

Verejne zdieľané súbory, dáta vložené do AI.

**1 650**

nahlásených incidentov na Slovensku v roku 2025 – medziročne približne +40 %.

Zdroj: NBÚ, Správa o kybernetickej bezpečnosti v SR v roku 2025; Mandiant M-Trends 2026 (poradie vstupných vektorov: č. 1, č. 2).

**DIGITÁLNA  
BUDÚCNOSŤ**



# Anatómia útoku: ako to reálne prebieha



1

## Prienik

Ukradnuté heslo,  
zneužitá zraniteľnosť  
alebo telefonát.

2

## Odovzdanie

Prístup sa predá  
alebo odovzdá  
špecializovanej  
skupine.

3

## Prieskum

Mapovanie siete,  
hľadanie záloh a  
citlivých dát.

4

## Krádež dát

Kópia dát odchádza  
von ako páka na  
vydieranie.

5

## Úder

Zašifrovanie  
systémov, výkupná  
správa.

**22 sekúnd**

krok 2

medián času od prieniku po odovzdanie prístupu  
ďalšej skupine (v roku 2022 to bolo vyše 8 hodín)

**44 %**

krok 5

obetí ransomvéru sa o útoku dozvedelo až od  
útočníka – menej ako polovica ho odhalila sama

Zdroj: Mandiant, M-Trends 2026 (dáta za rok 2025).

**DIGITÁLNA  
BUDÚCNOSŤ**



# Čo incident skutočne stojí



Nad hladinou  
výkupné • obnova IT • forenzná analýza

## Pod hladinou – väčšina nákladov

- Výpadok prevádzky a ušlé tržby
- Pokuty a právne náklady
- Odchod klientov
- Strata reputácie a dôvery
- Dopad na zamestnancov

*Zdroj: IBM / Ponemon, Cost of a Data Breach 2025 a 2026 (priemer, prevažne väčšie firmy).*



# Regulácia: už sa vás to (pravdepodobne) týka



## Zákon o KB (NIS2)

Novela 366/2024 Z. z., účinná od 1. 1. 2025. Zásadné rozšírenie regulovaných subjektov (predtým cca 1 800, odhad nových 3 380 – 16 849). Sankcie do 10 mil. EUR / 2 % obratu, osobná zodpovednosť štatutárov.



## Cyber Resilience Act

Ak vyvíjate softvér alebo aplikácie: od 11. 9. 2026 povinnosť hlásiť aktívne zneužívané zraniteľnosti a závažné incidenty (24 h / 72 h), od 11. 12. 2027 plné požiadavky vrátane CE.



## GDPR

Trvalá povinnosť pri údajoch klientov, študentov a zamestnancov.

1. 1. 2025

NIS2 novela

11. 9. 2026

CRA hlásenia

DNES

29. 9. 2026

11. 12. 2027

CRA naplno

**Self-check:** Ste dodávateľom regulovaného subjektu? Požiadavky vás zasiahnu cez zmluvy, aj keď nie ste regulovaní priamo.

Zákon č. 69/2018 Z. z. v znení zákona č. 366/2024 Z. z.; vyhláška NBÚ 226/2025 Z. z.; nariadenie (EÚ) 2024/2847 (CRA).

**DIGITÁLNA  
BUDÚCNOSŤ**



# Špecifiká digitálnej transformácie pre kybernetickú bezpečnosť

## Hlavné zmeny vyvolané realizáciou DT

*„Digitálna transformácia posúva IT z pozície pomocníka do pozície najkritickejšej súčasti fungovania organizácie. Tým sa mení celý váš rizikový profil.“*



# Zmena 1: Rozšírená útočná plocha a koniec „hradieb“



## Predtým

- Kancelária a firemné počítače
- Jedna sieť
- Jasná hranica – „hradby“



## Dnes

- Cloud, SaaS
- Práca z domu, vlastné zariadenia
- Integrácie s partnermi, sociálne siete



**Aj výroba a budovy (OT):** riadiace systémy boli izolované, dnes sú pripojené kvôli dátam a servisu.

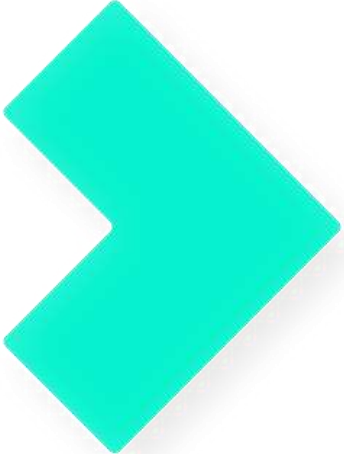
Útok tu nekončí únikom dát – môže **poškodiť stroje a ohroziť zdravie a životy.**

**Novou hranicou organizácie je identita používateľa.**

Minimum: MFA, správa prístupov, princíp „nikomu automaticky never“ (zero trust).



## Zmena 2: Závislosť od technológií a dodávateľov

- 
- Výpadok systému = výpadok prevádzky, služby, výučby, kampane.
  - Rastie závislosť od externých poskytovateľov: cloud, IT správca, platformy.
  - Riziko sa presúva do **dodávateľského reťazca**.

**30 %**

únikov súviselo s dodávateľom – jeho prístupmi, platformou alebo chybou v produkte (2× viac než rok predtým)

**< 20 %**

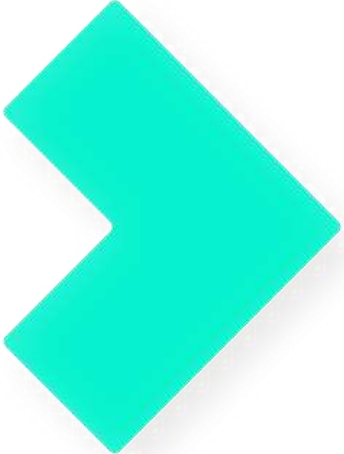
slovenských MSP malo plán kontinuity; z nich necelých 60 % ho overuje aspoň raz ročne

**Dôsledok: kontinuita činností a bezpečnostné požiadavky na dodávateľov patria do každého DT projektu.**

*Zdroj: Verizon DBIR 2025; KCCKB, prieskum stavu KB v MSP (2023).*



# Zmena 3: Dáta a umelá inteligencia

- 
- Viac dát = väčšia hodnota aj **väčší záväzok** (osobné údaje, know-how, dáta klientov).
  - AI je nástrojom útočníka aj obrancu.
  - Nové riziko „**tieňová AI**“ – firemné dáta vkladane do verejných AI nástrojov bez pravidiel.



## AI útočí

phishing v perfektnej slovenčine, deepfake hlas a video



## AI bráni

detekcia, automatizácia, triedenie upozornení

**Dôsledok: klasifikácia dát, zálohy oddelené od siete, jasné pravidlá používania AI.**

Zdroj: IBM / Ponemon, Cost of a Data Breach 2025 a 2026.



# Zmena 4: KB sa stáva manažérskou disciplínou

**Zodpovednosť za KB sa nedá delegovať ani outsourcovať. Začína u štatutára.**

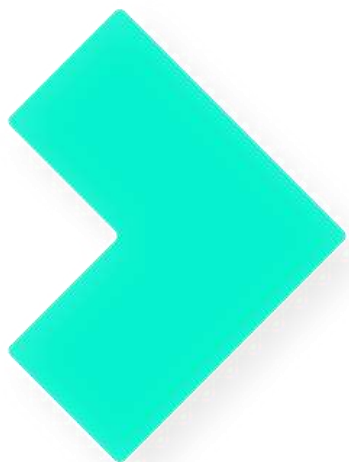
Päť zásad integrácie KB do digitálnej transformácie

- 1 **KB v stratégii** ako financie či obchod: zodpovednosť, ukazovatele, rozpočet.
- 2 **Mapa závislostí:** ktoré procesy stoja na ktorých systémoch.
- 3 **Zabezpečená expertíza:** manažér KB – aj externý.
- 4 **Posúdenie bezpečnosti** pred spustením každého digitálneho projektu.
- 5 **Riadenie rizík a plán reakcie** vrátane externých strán (NBÚ, polícia, klienti).

*Podľa Metodického rámca prípravy seminárov (NP Digitálna budúcnosť), kap. 3.10.2.*



## Zmena 5: Ľudia a kultúra bezpečnosti



Človek zostáva najčastejšou vstupnou bránou – aj po digitalizácii.



DT mení pracovné návyky: nové nástroje, spôsoby komunikácie, riziká.



Nové roly a zodpovednosti: manažér KB, vlastníci procesov a dát.



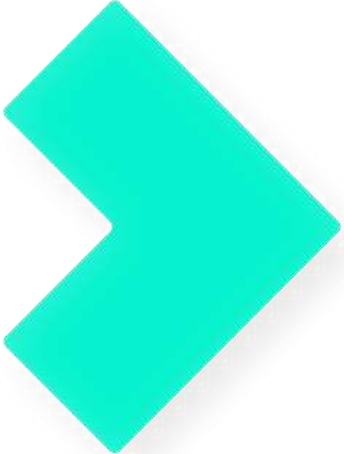
Povedomie od vedenia po každého zamestnanca – **systematicky**, nie jednorazovým školením.



Znalostné štandardy pre roly: vyhláška NBÚ č. 492/2022 Z. z.



# Zhrnutie: prínosy a riziká v jednom obraze



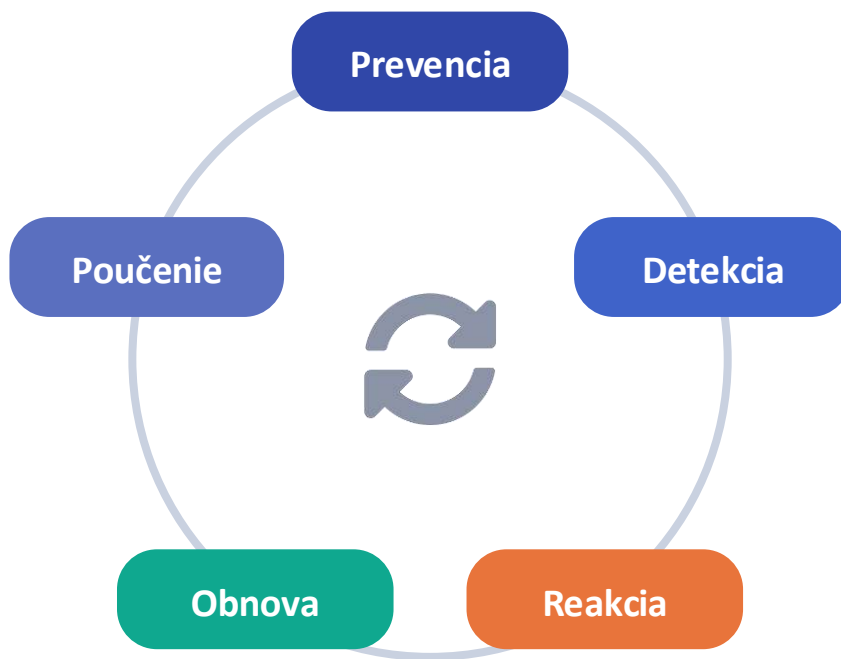
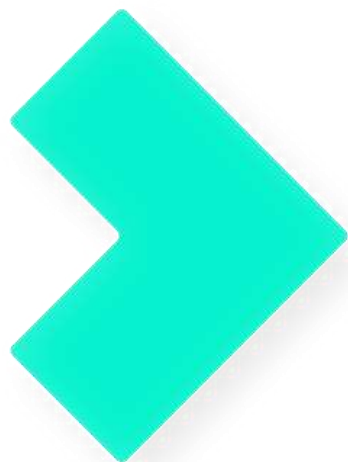
| Zmena                    | Prínos                            | Nové riziko                 |
|--------------------------|-----------------------------------|-----------------------------|
| Rozšírená útočná plocha  | Flexibilita, práca odkiaľkoľvek   | Viac vstupných brán         |
| Závislosť od technológií | Efektivita, škálovanie            | Výpadok = zastavenie        |
| Dáta a AI                | Lepšie rozhodovanie, produktivita | Úniky, deepfake, tieňová AI |
| Manažérska disciplína    | Systematické riadenie             | Osobná zodpovednosť         |
| Ľudia a kultúra          | Odolnejší tím                     | Ľudská chyba ako brána      |

**Žiadna zmena nie je dôvodom DT brzdiť. Každá je dôvodom zabudovať bezpečnosť od začiatku.**



# Cieľ: kybernetická odolnosť

Cieľom nie je nikdy nebyť napadnutý. Cieľom je útok ustáť a rýchlo sa zotaviť.



Tri otázky, ktoré si odnesiete domov

Viete, ktoré sú vaše kritické systémy?

Viete, komu zavoláte, keď sa to stane?

Viete, ako dlho bez nich vydržíte?

*Ako odolnosť budovať systematicky? Cez šesť pilierov digitálnej transformácie →*



# Šesť pilierov transformácie DT z pohľadu kybernetickej bezpečnosti

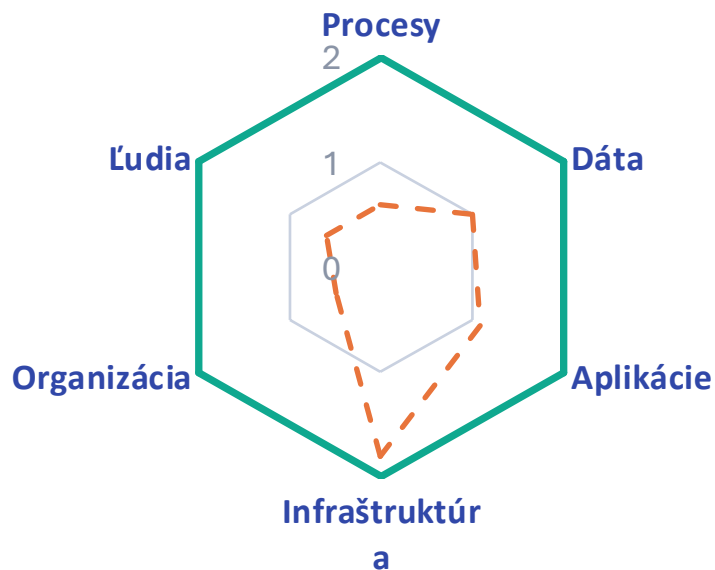
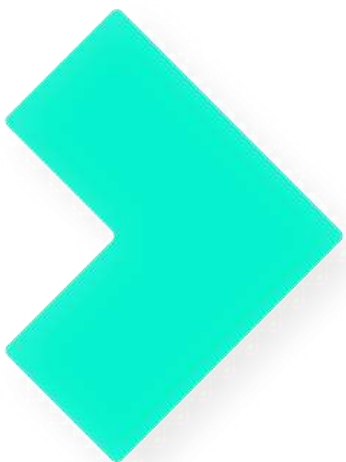
*„Bezpečnosť nevzniká nákupom technológie. Vzniká súhrou procesov, dát, aplikácií, infraštruktúry, organizácie a ľudí.“*



# Rámec P-D-A-I-O-L z pohľadu kybernetickej bezpečnosti

P D A I O L

ŠEŠŤ PILIEROV



— Štandard odvetvia  
- - Typický MSP dnes (ilustračne)

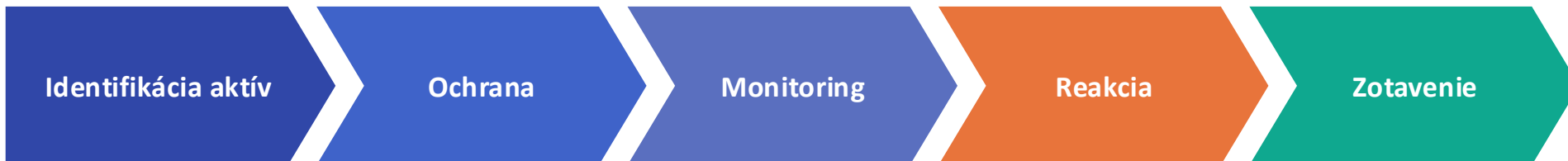
- P** **Procesy** – riadenie rizík a reakcia na incidenty ako opakovaná činnosť s vlastníkmi
- D** **Dáta** – vieme, čo máme, kto k tomu má prístup, kam to odchádza (aj do AI) a či to vieme obnoviť
- A** **Aplikácie** – softvér, ktorý kupujeme, používame a vyvíjame, je aktualizovaný a bezpečný od návrhu
- I** **Infraštruktúra** – siete, zariadenia a cloud sú oddelené, chránené a viditeľné
- O** **Organizácia** – roly, zodpovednosti a pravidlá; zodpovednosť začína u vedenia
- L** **Ľudia** – kompetencie a kultúra; človek ako najčastejšia brána aj najlepší senzor

Nevyvážený radar = zmarená investícia. Útočník prejde najslabšou osou.



# Procesy: KB je cyklus, nie projekt

P D A I O L  
PROCESY



↺ opakovane pri každej digitálnej zmene: nový LMS, CRM, dodávateľ, AI nástroj

Každý proces má vlastníka



**Vedenie**  
rozhodnutia a zdroje



**Manažér KB**  
riadenie



**IT**  
realizácia



**Všetci zamestnanci**  
hlásenie

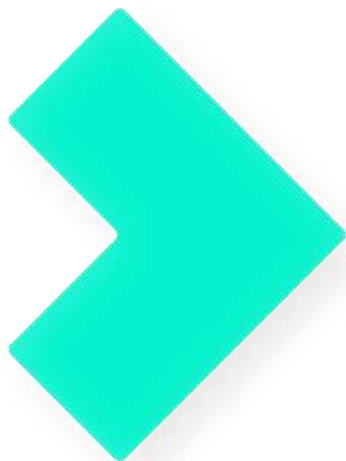


**Opačný pohľad:** zvýšiť úroveň KB je vždy projekt – s rozpočtom, termínom a vlastníkom. Popri bežnej prevádzke sa neudeje.

„Firma, ktorá má bezpečnosť ako projekt, ju má hotovú presne do prvej zmeny.“



# Procesy – štandard: tri dokumenty pre každú firmu



## Register aktív a rizík

Čo máme, čo je kritické, čo hrozí. Na začiatok stačí jedna tabuľka.



## Plán reakcie na incident

Kto čo robí v prvej hodine, koho voláme, kto rozhoduje o odpojení a komunikácii.



## Plán kontinuity a obnovy

Ako dlho vydržíme bez systému X, odkiaľ obnovíme, v akom poradí.



**„Netestovaný plán je hypotéza.“** Cvičenie aspoň raz ročne – tabletop, 2 hodiny, vedenie pri stole.



### AI ako riziko

Útoky s využitím AI medziročne +56 % (najmä deepfake a AI malvér). Plán reakcie musí obsahovať aj overenie hovoru „od šéfa“.

### AI ako nástroj

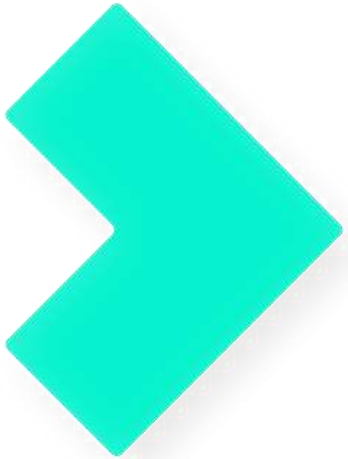
Pomocník pri prvom návrhu politík, plánov a scenárov cvičení – obsah a zodpovednosť zostávajú na vedení.



# Procesy – otázka pre vedenie



PROCESY



Kto u nás v sobotu o tretej ráno rozhodne, že vypneme server?



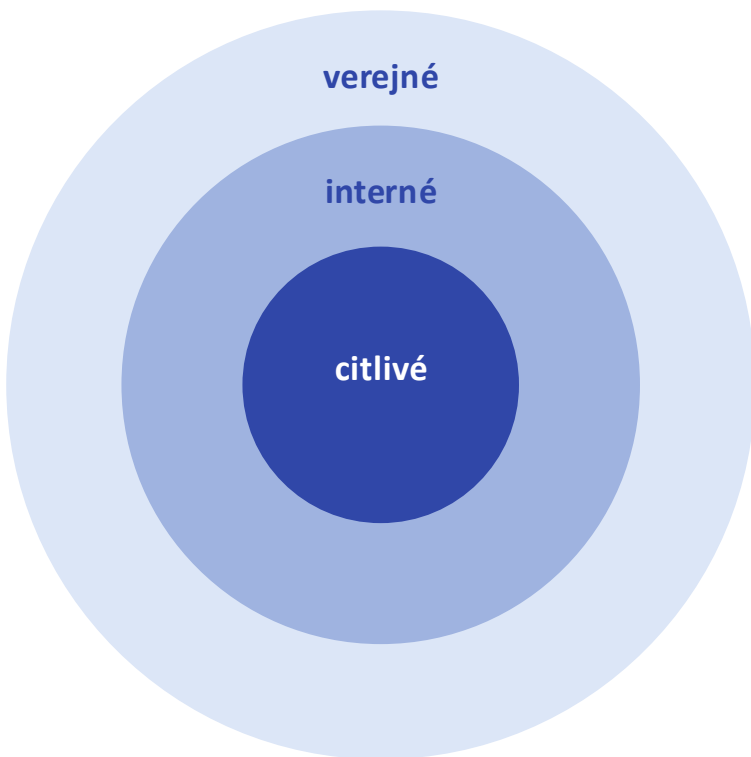
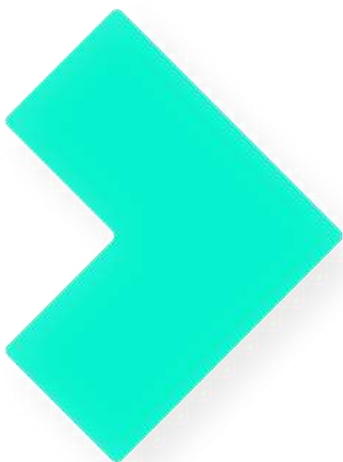
**Vo výrobe:** vypnúť nemusí byť bezpečné. Kto rozhodne o bezpečnom odstavení linky a ručnej prevádzke?



# Dáta: najcennejší majetok a najväčší záväzok

P D A I O L

DÁTA



## Štyri otázky vedenia



Čo máme?



Kto k tomu má prístup?



Vieme to obnoviť?



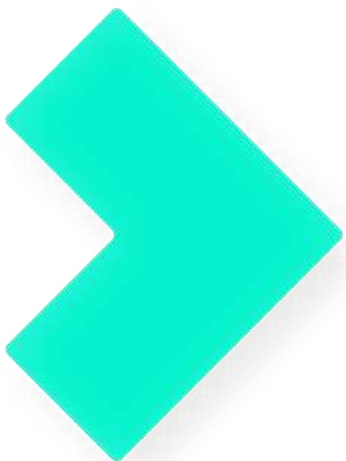
Kam to odchádza? – aj do AI nástrojov



# Dáta – štandard odvetvia: klasifikácia, prístup, zálohy



DÁTA



## Klasifikácia

Tri stupne; citlivé dáta šifrované (notebooky, prenosné zariadenia, cloud).



## Prístup

Najmenšie oprávnenia; pridávanie a odoberanie v HR procesoch; pravidelná revízia.



## Zálohy 3-2-1

3 kópie, 2 médiá, 1 mimo siete / nemenná. **Obnovu testovať.**



## Pravidlá pre AI

Ktoré dáta sa nikdy nevkladajú do nástrojov bez firemnej zmluvy.



### AI ako riziko

Tieňová AI – dáta účastníkov a klientov v nástrojoch, ktoré na nich môžu trénovať alebo ich uchovávať mimo EÚ.

### AI ako nástroj

Automatická klasifikácia a ochrana pred únikom dát (DLP) – dnes súčasť vyšších edícií kancelárskych cloudov.

Zdroj: Sophos, State of Ransomware 2026.

DIGITÁLNA  
BUDÚCNOSŤ



# PQC: kedy prestane fungovať zámok internetu?



VSUVKA • PQC

- HTTPS, elektronický podpis, VPN, internetbanking a eID stoja na matematike (RSA, eliptické krivky), ktorú dostatočne výkonný **kvantový počítač** dokáže prelomiť.
- **Nevieme kedy.** Vieme však: útočníci už dnes zbierajú šifrovanú komunikáciu („harvest now, decrypt later“), dnešné zariadenia zostanú v prevádzke roky a migrácia trvá dlho.

2024



NIST štandardy PQC

koniec 2026



národné plány, inventár

koniec 2030



vysoko rizikové použitia

Q-day?

koniec 2035



všetko prakticky možné

## Podceňovaná téma.

Nemusíte migrovať zajtra – ale musíte vedieť, kde kryptografiu používate a kto ju vymení.

## Postkvantovo chránené HTTPS (4/2026)

67 %



prevádzka celkovo

9 %



servery firiem

Zdroj: EK / NIS Cooperation Group, Coordinated Implementation Roadmap for the Transition to PQC (6/2025); ENISA; NIST FIPS 203–205; Cloudflare Radar 2026.

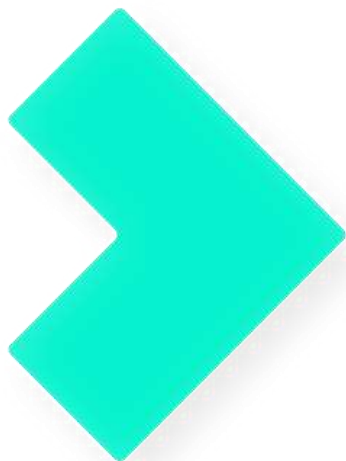
DIGITÁLNA  
BUDÚCNOSŤ



# PQC: čo môže vedenie urobiť už dnes



VSUVKA • PQC



## 1 Inventár kryptografie



Web, VPN, e-mail, elektronické podpisy, archívy, vlastné aplikácie. Presne to je prvý krok aj v pláne EÚ.

## 2 Dáta s dlhou životnosťou



Čo musí zostať tajné aj po roku 2030 (osobné údaje detí, zmluvy, výskum, archívy).

## 3 Otázka dodávateľom



„Aký máte plán prechodu na postkvantovú kryptografiu?“ – do výberových konaní a zmlúv (kryptoagilita).

## 4 Aktualizácie a koniec podpory



Väčšinu prechodu urobia výrobcovia. Úlohou firmy je nezablokovať ho starými systémami.



**Ktoré naše dáta by nesmeli uniknúť ani o desať rokov?**



# Súkromnosť dát pri používaní AI: od zmluvy po vlastný model

P D A I O L

DÁTA

viac kontroly → vyššie náklady a náročnosť

## Úroveň 0 Súkromné účty

**Garantuje:** nič; dáta môžu slúžiť na tréningovanie

**Náklad:** „zadarmo“ – s právnym rizikom

## Úroveň 1 Firemné predplatné

**Garantuje:** netrénuje sa na dátach, zmluva (DPA), správa prístupov

**Náklad:** desiatky EUR / osoba / mesiac

## Úroveň 2 Enterprise / Edu / API (BYOK)

**Garantuje:** dáta v EÚ, obmedzená retencia, vlastné kľúče

**Náklad:** vyššia cena, často cez dodávateľa

## Úroveň 3 Vlastný hostovaný model

**Garantuje:** dáta neopustia naše prostredie

**Náklad:** hardvér, prevádzka, nižšia kvalita

67 %

zamestnancov používa AI cez nefiremné účty

## Na ktorom schode sme dnes – a vieme to vôbec?

Nemusíte prestať používať AI. Musíte vedieť, kde vaše dáta končia.

Zdroj: Verizon DBIR 2026. Bez odporúčania konkrétnych nástrojov.

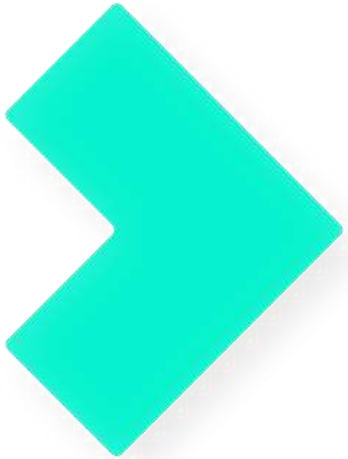
DIGITÁLNA  
BUDÚCNOSŤ



# Aplikácie: softvér, ktorý používame, kupujeme a vyvíjame



APLIKÁCIE



## Používateľ

LMS, CRM, kancelársky balík,  
sociálne siete

Je aktualizovaná?

Kto je admin?



## Zákazník

SaaS nástroje a pluginy s  
prístupom k dátam

Kde sú naše dáta?

A po ukončení zmluvy?



## Výrobca

vlastná platforma, aplikácia alebo  
plugin pre klienta

Testujeme pred nasadením?

Ako opravíme chybu?

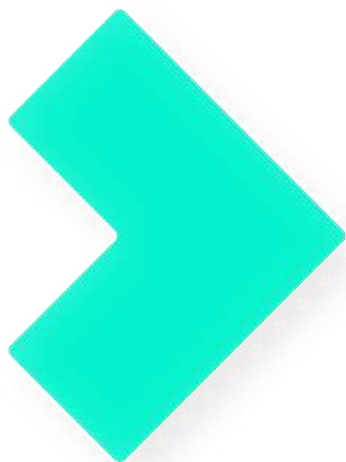
„Každá aplikácia sú dvere. Otázka je, kto má kľúč a či sa dvere opravujú.“



# Aplikácie – štandard: aplikácie, o ktorých neviete



APLIKÁCIE



## Tieňové SaaS

Nástroje zaplatené kartou alebo „zadarmo“ – s firemnými dátami.



## Prístupy tretích strán

„Prihlásiť cez Google / Microsoft“, pluginy s prístupom k e-mailu, disku, sieťam klientov.



## Rozšírenia prehliadača

Vidia všetko, čo používateľ robí na webe.



## Softvér po konci podpory

Napr. Windows 10 bez bezplatných aktualizácií od 14. 10. 2025.



**Štandard:** zoznam aplikácií s vlastníkom · schvaľovanie nových · pravidelná revízia prístupov · plán výmeny pred koncom podpory



## AI ako riziko

AI asistenti a agenti napojení na e-mail, disk a kalendár – s rovnakými právami ako používateľ.

## AI ako nástroj

Vývoj vlastných aplikácií s AI, AI-native nástroje

*Microsoft: koniec podpory Windows 10 (14. 10. 2025).*

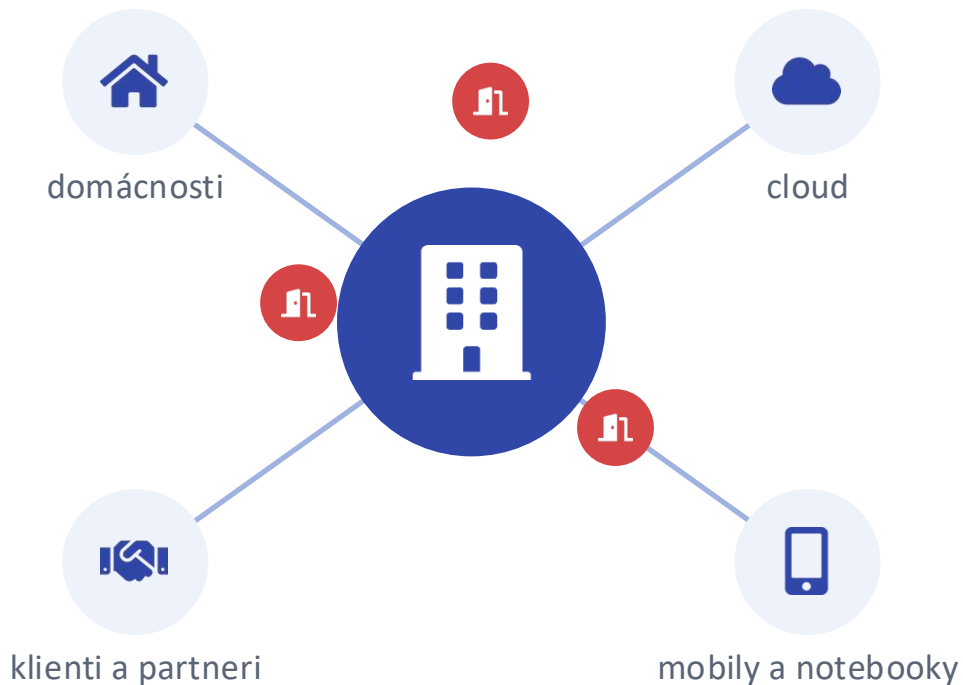
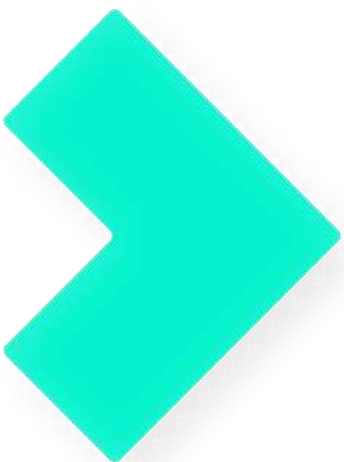
**DIGITÁLNA  
BUDÚCNOSŤ**



# Infraštruktúra: hranicou už nie je budova

P D A I O L

INFRAŠTRUKTÚRA



červené = „dvere do internetu“

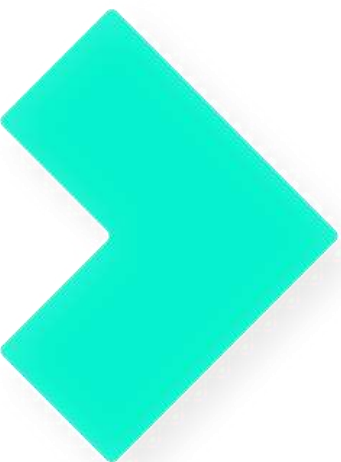
- Typická infraštruktúra MSP: notebooky a mobily (aj súkromné), Wi-Fi, server alebo NAS, kancelársky cloud, tlačiarne, kamery, prístup z domácností a od klientov.
- Útoky na MSP najčastejšie zneužijú to, čo je **vystavené do internetu a neaktualizované**: router, VPN, vzdialená plocha, NAS, webová aplikácia.
- V cloude platí zdieľaná zodpovednosť: poskytovateľ dátové centrum, firma nastavenia, prístupy a zálohy.

„Infraštruktúru dnes neriadime tým, čo vlastníme, ale tým, čo vidíme.“



# Infraštruktúra – päť vecí, ktoré má vedenie vyžadovať od IT

P D A I O L  
INFRAŠTRUKTÚRA



- **Segmentácia**  
hostia, kamery a IoT, interná sieť oddelene; kritické systémy zvlášť
- **MFA všade**  
e-mail, cloud, VPN, platby; admini: kľúče, passkeys
- **Ochrana zariadení (EDR)**  
nie len antivírus; šifrovanie diskov, vzdialená správa
- **Nič otvorené bez dôvodu**  
žiadna otvorená vzdialená plocha; prístup cez overenú identitu
- **Prehľad a záznamy**  
vieme, čo sa v sieti deje → SIEM



**Výroba (OT):** IT a OT oddelené, PLC nikdy z internetu, servis dodávateľov cez kontrolovaný bod. Kde aktualizácia nejde: oddelenie a dohľad.



## AI ako riziko

Útočník s AI automaticky vyhľadáva slabé miesta a prispôsobuje útok konkrétnej infraštruktúre.

## AI ako nástroj

AI v EDR a SIEM: odhaľovanie neobvyklého správania, triedenie upozornení, otázky v prirodzenom jazyku.

*Pre OT referenčne IEC 62443 (bezpečnosť priemyselných automatizačných a riadiacich systémov).*

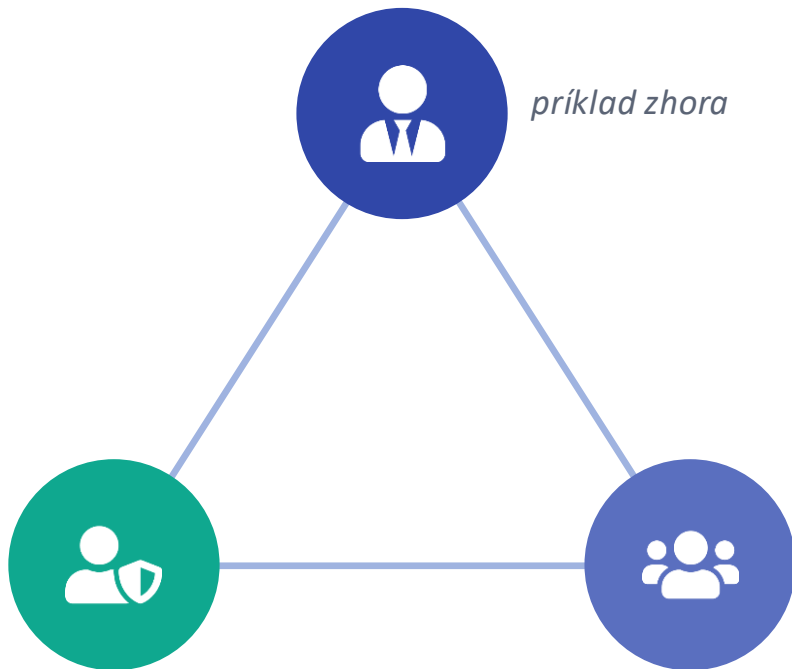
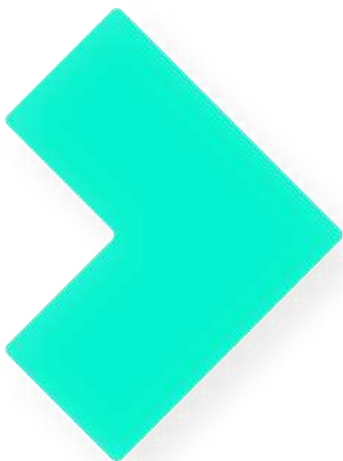
**DIGITÁLNA  
BUDÚCNOSŤ**



# Organizácia: tri roly, ktoré musia spolupracovať



ORGANIZÁCIA



## Vedenie / štatutár

Zodpovednosť, zdroje, osobný príklad. Nedá sa preniesť na tretiu stranu.

## Manažér KB

Riadi procesy; oddelený od prevádzky IT (bezpečnosť vs. pohodlie a rozpočet); môže byť externý.

## Používatelia

Každý vo svojej roli – sloboda + zodpovednosť.

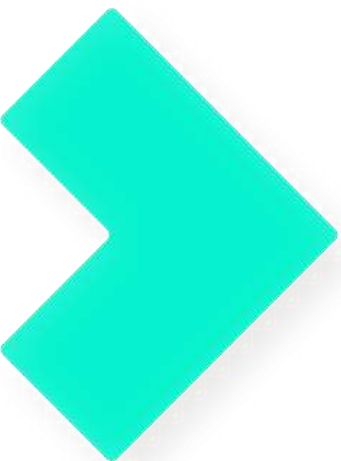
„Nedisciplinovanosť šéfa je najspoľahlivejší spôsob, ako poslať investíciu do bezpečnosti hore komínom.“



# Organizácia – štandard: pravidlá, ktoré fungujú aj bez IT



ORGANIZÁCIA



## Bezpečnostná politika na 2 – 3 strany

Heslá a MFA, zariadenia, dáta, **AI nástroje**, hlásenie incidentov; podpísaná vedením.



## Prístupy ako súčasť HR

Nástup → zmena pozície → odchod: odobrať prístupy v deň odchodu, aj ku klientskym účtom.



## Kultúra, nie len pravidlá

Vedenie ide príkladom, KB je v onboardingu aj hodnotení, bezpečné správanie sa oceňuje.



## Reporty vedeniu – 5 čísel štvrťročne

Zálohy a čas obnovy, incidenty od používateľov, privilegované účty, aktualizácie, výsledky testov.



## AI ako riziko

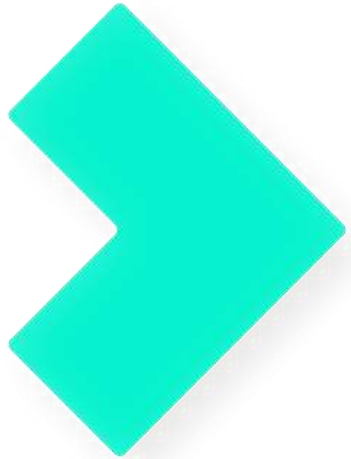
Každý si vie AI nástroj zaviesť sám – bez pravidiel vzniká tieňová AI.

## AI ako nástroj

AI Akt (čl. 4): podporovať AI gramotnosť zamestnancov – platí od 2/2025. V SR dozor MIRRI, zákon v parlamente (od 1/2027).



# Organizácia – otázka pre vedenie



Keby dnes odišiel váš správca IT, kto má heslá?



**Jeden človek, všetky kľúče**  
choroba, odchod, spor



**Tím so zdieľaným trezorom**  
funguje, aj keď niekto chýba

## Minimum

- správca hesiel s núdzovým prístupom vedenia
- základná dokumentácia systémov
- **dva** ľudia s admin právami
- zmluvné odovzdanie pri ukončení spolupráce s dodávateľom

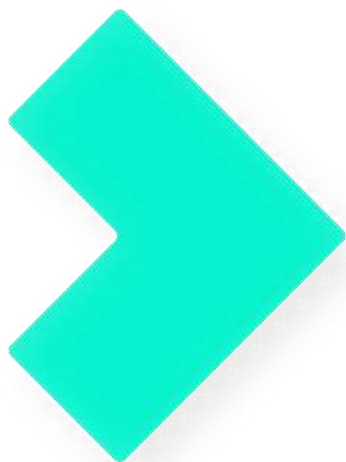
**Kultúra: nahlásenie chyby bez trestu = rýchlejšie odhalenie. Ľudia sú senzory, nie len riziko.**



# Ľudia: najčastejšia brána a najlepší senzor

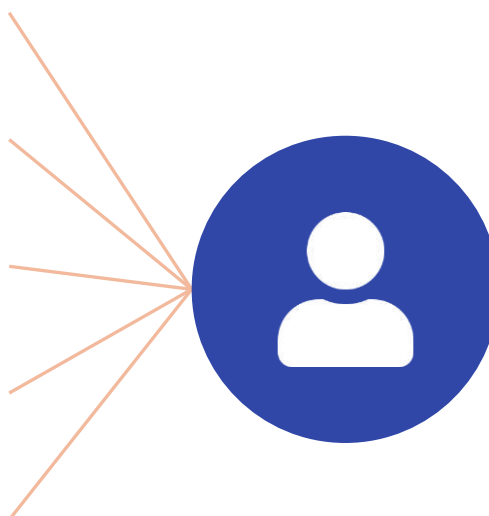
P D A I O L

ĽUDIA



vektory útoku

- e-mail
- SMS
- hovor
- video
- heslo



čo môže urobiť

- overiť
- nahlásiť
- nezdieľať

62 %

únikov – ľudský faktor zohral úlohu

+40 %

vyššia úspešnosť sociálneho inžinierstva cez mobil (SMS, hovory) oproti e-mailu

Útočníci sa presúvajú z e-mailu do telefónu, SMS a chatu – konverzácia v reálnom čase. E-mail pritom nezmizol.

„Cieľom nie je zamestnanec, ktorý sa bojí kliknúť. Cieľom je zamestnanec, ktorý vie, čo urobiť potom.“

Zdroj: Verizon DBIR 2026; Sophos, State of Ransomware 2026.

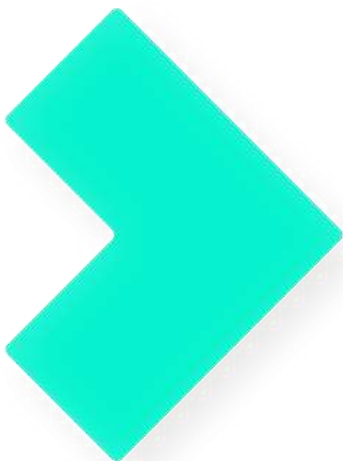
DIGITÁLNA  
BUDÚCNOSŤ



# Ľudia – štandard odvetvia: kompetencie podľa rolí



ĽUDIA



## Vedenie

rozhodovanie pri incidente, cvičenie 1× ročne

## Špecialisti

manažér KB ≠ správca IT (vyhláška 492/2022)

## Všetci zamestnanci

krátke moduly priebežne + simulované útoky



### AI ako riziko

Phishing v bezchybnej slovenčine, deepfake hlas či video „šéfa“, ktorý žiada platbu alebo prístup.

### AI ako nástroj

Simulácie a mikroškolenia pripravené s AI; AI gramotnosť pre každú rolu.

Zdroj: IBM / Ponemon, Cost of a Data Breach 2026; vyhláška NBÚ č. 492/2022 Z. z.

**DIGITÁLNA  
BUDÚCNOSŤ**



# Ľudia – otázka pre vedenie

P D A I O L  
ĽUDIA



Kedy naposledy niekto u vás nahlásil podozrivý e-mail – a čo sa stalo potom?

## Tri znaky funkčnej kultúry



Hlásenie je jednoduché – jedno tlačidlo, jedna adresa, jedno číslo.



Nahlásenie sa nikdy netrestá – ani keď človek predtým klikol.



Spätná väzba do 24 hodín.

nahlásené / kliknuté



Počet nahlásení je lepší ukazovateľ kultúry než počet kliknutí v simulácii.

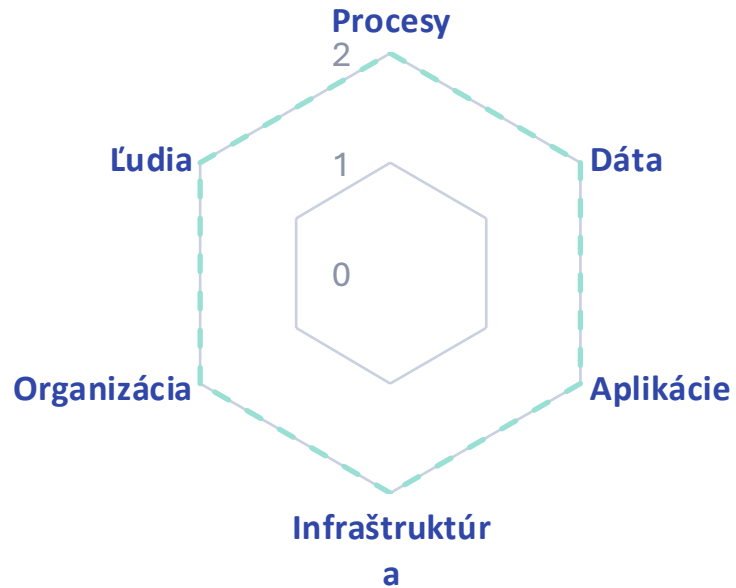
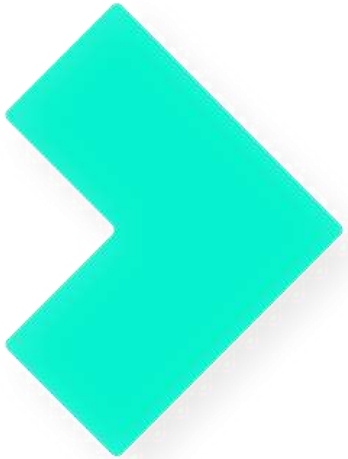
→ Aké digitálne zručnosti potrebujú vaše kľúčové povolania, aby toto fungovalo?



# Radar: kde ste dnes?

P D A I O L

SEBAHODNOTENIE



0 – nič · 1 – čiastočne · 2 – štandard odvetvia

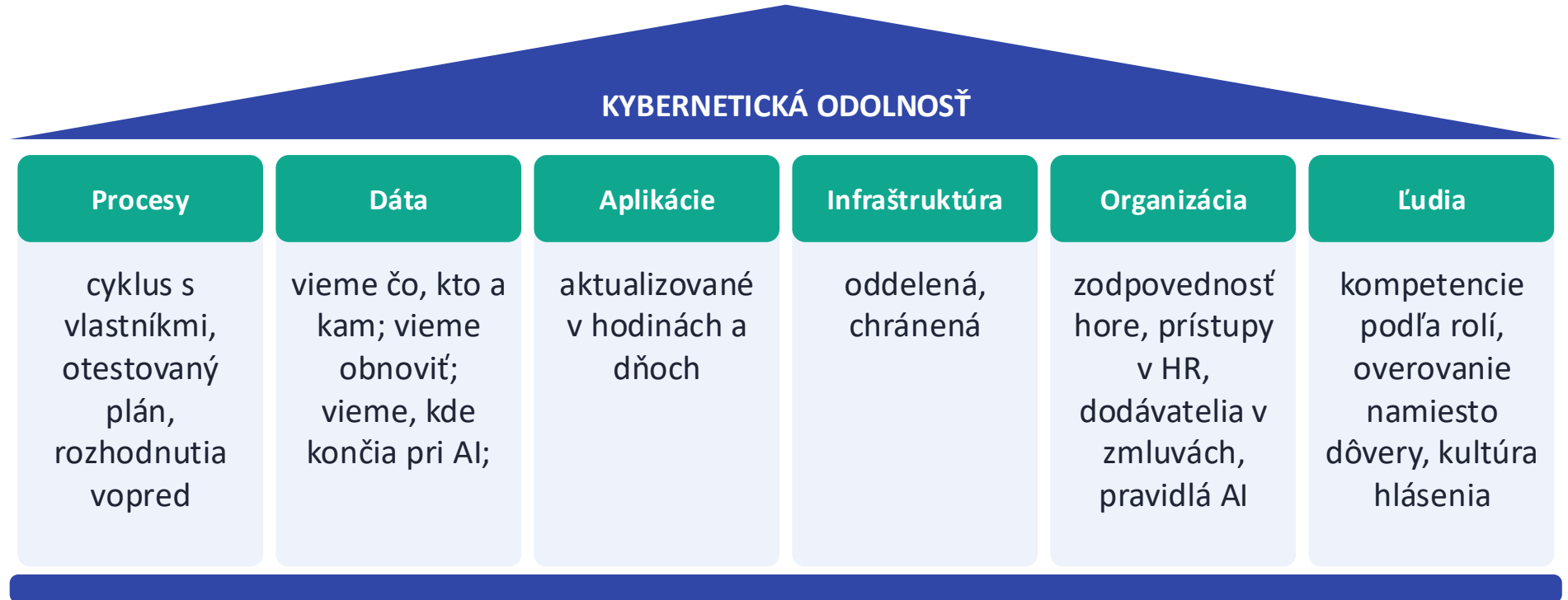
- P** Kto rozhodne o vypnutí servera v sobotu o tretej?
- D** Na ktorom schode súkromnosti dát pri AI sme? Ktoré dáta nesmú uniknúť ani o 10 rokov?
- A** Dodávame niekomu softvér? Do kedy dostávajú aktualizácie produkty, ktoré používame?
- I** Kto by si všimol nočné sťahovanie databázy?
- O** Kto má heslá, keby odišiel správca IT?
- L** Čo sa stalo po poslednom nahlásení?

**Neriešte všetko naraz. Riešte najkratšiu os.**



# Zhrnutie: šesť pilierov, jedna odolnosť

P D A I O L



Odolnosť stojí na všetkých šiestich stĺpoch – o nej rozhoduje ten najslabší. AI je novou vrstvou každého z nich.

→ Ktoré z toho vedia vaši ľudia urobiť dnes – a ktoré zručnosti im chýbajú?



# Digitálne a zelené zručnosti pre klúčové povolania vo vzťahu ku kybernetickej bezpečnosti



# REFERENČNÉ RÁMCE

- Transformácia začína **pri ľuďoch**
- Je kľúčové vedieť, **koho zamestnať, rekvalifikovať a ako rozvíjať potenciál.**
- **Riešenie:** Jasný systém hodnotenia zručností
- Vytvárajú **jednotný jazyk** medzi zamestnávateľmi a zamestnancami
- Fungujú podobne ako **Cambridge systém pre jazyky**
- Stanovujú **úroveň zručností** pre každé povolanie
- Už aplikované na **1800 povolaní** v rámci Národnej sústavy povolaní

## Systém určovania úrovne zručností:

A – základná úroveň (začiatocníci, menej skúsení pracovníci)  
B – samostatný používateľ  
C – expert

Naskenujte QR kód  
pre bližšie informácie



# TESTOVANIE

- Potrebné sú **implementačné nástroje** – prepojenie teórie s praxou
- **Riešenie:** Testovanie digitálnych a zelených zručností
- Test hodnotí **schopnosť konať v kontexte dvojitej transformácie**
  - Spôsob myslenia, rozhodovania a komunikácie
  - Silné a slabé stránky – priestor na rozvoj
- Dostupné pre **riadiacich pracovníkov firiem, samospráv, orgánov verejnej moci**

Informácie o zapojení sa do testovania poskytuje konzultant, ktorý je prítomný na konferencií a je označený červenou šnúrkou.

Naskenujte QR kód  
pre bližšie informácie



# Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

**Odborný zamestnanec** - používateľ, ktorý pri výkone povolania využíva sieť alebo informačný systém (úroveň B1.1)

- porozumieť vybraným základným pojmom kybernetickej bezpečnosti
- porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti
- chápať význam informačných aktív s ktorými zamestnanec pracuje
- porozumieť potrebe ochrany informácií a informačných aktív
- osvojiť si základné pravidlá bezpečnej práce s IKT
- rozpoznať incident a vedieť naň správne reagovať
- porozumieť bezpečnostným politikám a používaniu bezpečnostných mechanizmov v pracovných procesoch



# Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

**Informatik - zamestnanec** zodpovedný za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT (úroveň B2.2)

- doplniť vlastné odborné znalosti špecificky pre oblasť kybernetickej bezpečnosti
- porozumieť podstate bezpečnostných požiadaviek na IKT a IT služby
- porozumieť zraniteľnostiam, hrozbám a rizikám spojeným s používanými IKT a IT službami
- nadobudnúť schopnosť navrhnuť, implementovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IKT a IT služby
- nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať so špecialistami kybernetickej bezpečnosti, formulovať problémy, posudzovať a implementovať navrhované opatrenia.



# Digitálne zručnosti pre kľúčové povolania

## Informatik

| <b><i>Rola/povolanie</i></b>                                 | <b><i>Spracovanie dát a práca s informáciami – úroveň/popis</i></b>                                                                                 | <b><i>Komunikácia a spolupráca – úroveň/popis</i></b>                                                                                                                                                                        | <b><i>Tvorba digitálneho obsahu – úroveň/popis</i></b>                                                                                                              | <b><i>Kybernetická bezpečnosť – úroveň/popis</i></b>                                                                                                                                                                       | <b><i>Stratégie riešenia problémov – úroveň/popis</i></b>                                                                                                                                                             | <b><i>Celková minimálna požadovaná úroveň – digitálne zručnosti</i></b> |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <i>IKT špecialisti (ISCO – Správca informačného systému)</i> | <i>B2.2<br/>Dokáže pri správe a organizácii informácií vo forme štruktúrovaných dát využiť komplexné funkcie relevantného digitálneho nástroja.</i> | <i>B2.1<br/>Dokáže v digitálnom prostredí presvedčivo komunikovať a argumentovať, ako aj organizovať a moderovať pracovné stretnutie a využívať pokročilé funkcie komunikačných nástrojov na účinnú pracovnú interakciu.</i> | <i>B2.2<br/>Dokáže pri tvorbe digitálneho obsahu navrhnuť alternatívne stratégie, pričom si uvedomuje nutnosť overovať dodržiavanie licencií a autorských práv.</i> | <i>B2.2<br/>Dokáže obhájiť stratégie a postupy na predchádzanie bezpečnostným rizikám v digitálnom prostredí a v prípade bezpečnostného incidentu efektívne riadiť komunikáciu v súlade s bezpečnostnými nariadeniami.</i> | <i>B2.2<br/>Dokáže v digitálnom prostredí revidovať zaužívané postupy riešenia problémov a navrhovať stratégie na zefektívnenie pracovných postupov a používania digitálnych technológií a ich prípadnú inováciu.</i> | <i>B2.2</i>                                                             |



# Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

**Manažér kybernetickej bezpečnosti** - riadiaci zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, vlastníci bezpečnostných procesov (úroveň C1)

- vytvoriť rámec riadenia kybernetickej bezpečnosti v organizácii
- riadiť procesy súvisiace s informačnou a kybernetickou bezpečnosťou v organizácii
- formulovať návrhy a odporúčania na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení a navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti
- navrhovať, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia
- znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív,
- navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru
- znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie



# Digitálne zručnosti pre kľúčové povolania

## Manažér kybernetickej bezpečnosti

| <i><b>Rola/povolanie</b></i>                                                            | <i><b>Spracovanie dát a práca s informáciami – úroveň/popis</b></i>                                                                                 | <i><b>Komunikácia a spolupráca – úroveň/popis</b></i>                                                                                                                                                                        | <i><b>Tvorba digitálneho obsahu – úroveň/popis</b></i>                                                                                                              | <i><b>Kybernetická bezpečnosť – úroveň/popis</b></i>                                                                                                                                                               | <i><b>Stratégie riešenia problémov – úroveň/popis</b></i>                                                                                                                                                             | <i><b>Celková minimálna požadovaná úroveň – digitálne zručnosti</b></i> |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <i>Manažér kybernetickej bezpečnosti (ISCO – Špecialista kybernetickej bezpečnosti)</i> | <i>B2.2<br/>Dokáže pri správe a organizácii informácií vo forme štruktúrovaných dát využiť komplexné funkcie relevantného digitálneho nástroja.</i> | <i>B2.1<br/>Dokáže v digitálnom prostredí presvedčivo komunikovať a argumentovať, ako aj organizovať a moderovať pracovné stretnutie a využívať pokročilé funkcie komunikačných nástrojov na účinnú pracovnú interakciu.</i> | <i>B2.2<br/>Dokáže pri tvorbe digitálneho obsahu navrhnúť alternatívne stratégie, pričom si uvedomuje nutnosť overovať dodržiavanie licencií a autorských práv.</i> | <i>C1<br/>Dokáže navrhnúť rôznorodé stratégie a nové postupy na predchádzanie bezpečnostným rizikám, implementovať ich a v prípade potreby iniciatívne komunikovať s príslušnými inštitúciami v tejto oblasti.</i> | <i>B2.2<br/>Dokáže v digitálnom prostredí revidovať zaužívané postupy riešenia problémov a navrhovať stratégie na zefektívnenie pracovných postupov a používania digitálnych technológií a ich prípadnú inováciu.</i> | <i>B2.2</i>                                                             |



# Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

**Audítor a výskumník kybernetickej bezpečnosti** - odborný zamestnanec špecializovaný na oblasť výskumu alebo posudzovania kybernetickej bezpečnosti, analýzy rizík, testovania a vyhodnocovania efektivity bezpečnostných opatrení, posudzovania zhody a súladu (úroveň C1)

- nadobudnúť schopnosti v rozsahu podľa predchádzajúcich cieľov platných pre všetky ostatné kategórie
- vykonať audit kybernetickej bezpečnosti a posúdiť efektívnosť prijatých bezpečnostných opatrení



# Digitálne zručnosti pre kľúčové povolania

## Audítor kybernetickej bezpečnosti

| <b>Rola/povolanie</b>                                                        | <b>Spracovanie dát a práca s informáciami – úroveň/popis</b>                                                                                | <b>Komunikácia a spolupráca – úroveň/popis</b>                                                                                                                                                                | <b>Tvorba digitálneho obsahu – úroveň/popis</b>                                                                                                            | <b>Kybernetická bezpečnosť – úroveň/popis</b>                                                                                                                                                              | <b>Stratégie riešenia problémov – úroveň/popis</b>                                                                                           | <b>Celková minimálna požadovaná úroveň – digitálne zručnosti</b> |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Audítor kybernetickej bezpečnosti (ISCO – Audítor kybernetickej bezpečnosti) | B2.2<br>Dokáže pri správe a organizácii informácií vo forme štruktúrovaných dát využiť komplexné funkcie relevantného digitálneho nástroja. | B2.2<br>Dokáže používať pokročilé funkcie rôznych digitálnych technológií s cieľom zefektívniť procesy spolupráce a účinne predchádzať neprípustným formám správania sa a komunikácie v digitálnom prostredí. | C1<br>Dokáže tvorivo využívať pokročilé funkcie digitálnych nástrojov na tvorbu komplexného obsahu, predkladať nové nápady a navrhovať inovatívne procesy. | C1<br>Dokáže navrhnúť rôznorodé stratégie a nové postupy na predchádzanie bezpečnostným rizikám, implementovať ich a v prípade potreby iniciatívne komunikovať s príslušnými inštitúciami v tejto oblasti. | C1<br>Dokáže používať digitálne nástroje určené na správu a organizáciu komplexných informácií na podporu rozhodovania a riešenia problémov. | B2.2                                                             |



## Zhrnutie prínosov a rizík DT v oblasti KB – návrh ďalšieho postupu



# Prínosy DT v oblasti KB – keď je bezpečnosť jej súčasťou



## A. Bezpečnosť sa stáva riaditeľnou

Jasné roly, tri krátke dokumenty, päť čísel pre vedenie.

„Netestovaný plán je hypotéza.“



## B. Odolnosť je dostupná aj menším

MFA, EDR, zálohy 3-2-1, open-source SIEM so službou.

66 % obetí obnovilo dáta zo záloh



## C. Časť práce urobia za vás iní

CRA, prechod na PQC, garancie Edu/enterprise edícií.

PQC: 67 % prevádzky, servery firiem 9 %



## D. AI a ľudia na strane obrany

AI v detekcii a ľudia, ktorí nahlasujú.

–1,93 mil. USD s AI a automatizáciou

Prínosy aj riziká sú tie isté zmeny. Rozhoduje, či bezpečnosť plánujete od začiatku.



# Riziká DT v oblasti KB – keď bezpečnosť príde až potom



## A. Zodpovednosť končí u vedenia

Zákon o KB, CRA aj AI Akt smerujú k štatutárovi.

**Sankcie do 10 mil. EUR / 2 % obratu**



## B. Viac dverí, žiadne hradby

Hranicou je identita, vstupom nezáplatovaná chyba.

**31 % únikov cez zraniteľnosť**



## C. Závislosť: výpadok = zastavenie

Riziko sa presúva k dodávateľom a jednému človeku.

**< 20 % MSP má plán kontinuity**



## D. Dáta odchádzajú aj bez útoku

Tieňová AI, deepfake „šéfa“, človek ako brána.

**67 % používa AI cez nefiremné účty**

Prínosy aj riziká sú tie isté zmeny. Rozhoduje, či bezpečnosť plánujete od začiatku.



# Jedna minca: čo rozhoduje

| Prínos                      | Rozhoduje                                                                 | Riziko                       |
|-----------------------------|---------------------------------------------------------------------------|------------------------------|
| Bezpečnosť je riaditeľná    | Má každý proces vlastníka a otestovaný plán?<br>(P · O)                   | Zodpovednosť bez riadenia    |
| Odolnosť dostupná aj menším | Vieme, čo je vystavené do internetu a kto si všimne nočné sťahovanie? (I) | Viac dverí, nikto nestráži   |
| Časť práce urobia iní       | Pýtame sa dodávateľov na aktualizácie, dáta a ukončenie zmluvy? (A)       | Závislosť bez záruk          |
| AI a ľudia bránia           | Vieme, kam idú naše dáta pri AI, a čo sa stane po nahlásení? (D · L)      | Dáta odchádzajú, ľudia mlčia |
| Riešte najkratšiu os.       |                                                                           |                              |



# Odporúčania ďalšieho postupu – projekt Digitálna budúcnosť



## Financovanie

Na konferenciách projektu:  
financovanie z Plánu obnovy a  
štrukturálnych fondov – aj pre  
opatrenia KB.



## Zručnosti

Audit zručností: Meranie  
digitálnej zrelosti ľudského  
kapitálu. Čo vaši ľudia vedia a  
čo im chýba?



## Workshop

Popoludní päť situácií z praxe  
MSP: „Kde sa stala chyba?“  
Radar ako pracovný list.

*[OVERIŤ] Aktuálna dostupnosť služby Meranie digitálnej zrelosti ľudského kapitálu (pôvodne „v roku 2025“).*



# Ako začať: nie všetko naraz, ale od najkratšej osi



1

**Zistite, kde ste** · tento týždeň

Radar a pôsobnosť regulácie – nečakajte na štát.

2

**Expertíza a analýza rizík** · do 3 mesiacov

Externý manažér KB, GAP a riziková analýza, roadmapa.

3

**Tri dokumenty, cvičenie, 5 otázok pre IT** · do 6 mesiacov

Plán reakcie a kontinuity, tabletop, „Máme to?“

4

**Pravidlá pre AI a ľudí** · do 6 mesiacov

Politika vrátane AI, prístupy v HR, hlásenie bez trestu.

5

**Investícia, nie náklad** · priebežne

Granty KCCKB: **SIEM** (do 19. 10. 2026), **PQC, CRA**.

Poradie je  
dôležitejšie než  
termíny.



[granty.kcckb.sk](https://granty.kcckb.sk)

[OVERIŤ] Stav výziev KCCKB pred každým behom seminára.

DIGITÁLNA  
BUDÚCNOSŤ



## HODNOTENIE SEMINÁRA





**ĎAKUJEM ZA POZORNOSŤ**

Michal Ohrablo

29.09.2026, Piešťany





Digitálna  
koalícia

# DIGITÁLNA BUDÚCNOSŤ



Spolufinancovaný  
Európskou úniou



PROGRAM  
SLOVENSKO



MINISTERSTVO  
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA  
A INFORMATIZÁCIE  
SLOVENSKEJ REPUBLIKY