
KYBER2025
09. 06. 2025
Hotel Chopok
ČO SA DEJE
A ČO NÁS ČAKÁ?
PLÁN OBNOVY
ECCC

ČO PRINÁŠA NOVÁ VYHLÁŠKA O BEZPEČNOSTNÝCH OPATRENIACH

Kyber 2025 – konferencia NBÚ
Demänovská dolina, 9. 6. 2025

Nový regulačný rámec kybernetickej bezpečnosti

NIS2 Smernica (EU) 2022/2555
- účinná 17.10.2024

Akt o kybernetickej bezpečnosti (CSA)
Nariadenie (EU) 2019/881

Akt o kybernetickej odolnosti
Nariadenie (EU) 2024/2847
– účinné 11.12.2027

Akt o kybernetickej solidarite
Nariadenie (EU) 2025/38 –
účinné 5.2.2025

DORA nariadenie (EU) 2022/2554
– účinné 17.1.2025

Delegované a vykonávacie nariadenia EK k DORA

Vykonávacie nariadenie Komisie (EÚ) 2024/2690 pre digitálny sektor
- účinné 17.10.2024

Zákon č. 95/2019 Z. z. o ITVS
– novela v LP/2025/226 – po MPK

Vyhláška ÚPVSRpII č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení ITVS
- novela v LP/2025/226 – po MPK

Sektorová regulácia

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- novela účinná od 1.1.2025

Vyhláška NBÚ o bezpečnostných opatreniach
– v LP/2025/194 – po MPK

Ďalšie vyhláška NBÚ k ZoKB (napr. oznamovaní incidentov)
– v príprave

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Vyhláška NBÚ o bezpečnostných opatreniach

- **V legislatívnom procese** pod č. LP/2025/194 – vyhodnotenie pripomienok po MPK

- **Ruší vyhlášku NBÚ č. 362/2018 Z. z.**

- **Upravuje:**
  - Obsah bezpečnostných opatrení
  - Rozsah ich aplikácie pre IKT a pre OT technológie
  - Obsah a štruktúru bezpečnostnej dokumentácie

Slov-Lex.sk
právny a informačný portál

SPOLU SO ZÁKONOM O KB URČUJE RÁMEC PRE RIADENIE KYBERNETICKEJ BEZPEČNOSTI V ORGANIZÁCII

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Obsah a štruktúra bezpečnostných opatrení

Všeobecné bezpečnostné opatrenia:

- ***17 oblastí***
- ***150 opatrení***
- ***relevancia pre IKT a OT a pre PZS a PKZS***

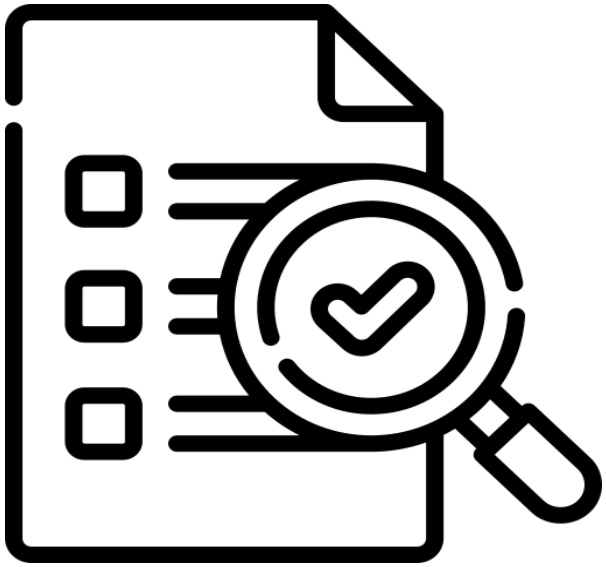
Vyhláška rozlišuje:

- **všeobecné bezpečnostné opatrenia (§20 ZoKB)**
  - Minimálne (povinné) opatrenia (§20 ods. 4 ZoKB)
  - Bezpečnostné opatrenia aplikované na základe analýzy rizík (§20 ods. 2 ZoKB a príloha č. 1 vyhlášky)
- **sektorové bezpečnostné opatrenia (osobitný predpis)**

Základné zložky systému riadenia kybernetickej bezpečnosti

- **Bezpečnostná dokumentácia**
  - Stratégia
  - Bezpečnostné politiky
  - Analýzy rizík
  - Zdokumentované bezp. opatrenia
  - Audity
  - Iné dokumenty

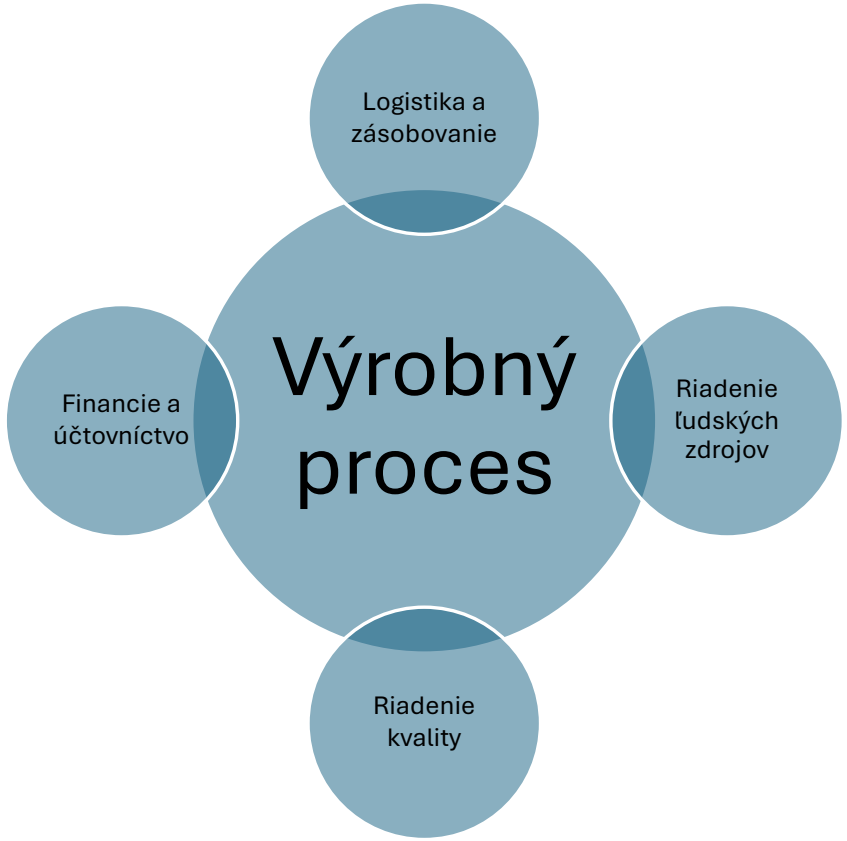
- **Riadenie rizík**
  - riadenie aktív
  - identifikácia rizík (s už prijatými opatreniami)
  - analýza a hodnotenie rizík + BIA
  - mitigácia vyhodnotených rizík/ výber vhodných opatrení
  - revízia



Riadenie aktív

- **Definícia** – dáta, informácie, služby, procesy
  - primárne a podporné aktíva

- **Riadenie aktív**
  - identifikácia
  - centralizovaná evidencia
  - rozlíšenie primárneho a podporného aktíva
  - určenie vlastníka
  - aktualizácia a revízia



Riadenie rizík

- **Analýza rizík**
  - Odporúčaná metodika NBÚ
  - Vlastná metodika – mapovanie rizika v súlade s metodikou NBÚ
  - určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnymi hrozbami v spojitosti s existujúcimi bezpečnostnými opatreniami

Pravdepodobnosť	Následok				
	Zanedbateľný	Malý	Stredný	Závažný	Katastrofický
Veľmi vysoká	Stredné	Stredné	Vysoké	Veľmi vysoké	Veľmi vysoké
Vysoká	Nízke	Stredné	Vysoké	Vysoké	Veľmi vysoké
Stredná	Nízke	Stredné	Stredné	Vysoké	Vysoké
Nízka	Veľmi nízke	Nízke	Stredné	Stredné	Stredné
Veľmi nízka	Veľmi nízke	Veľmi nízke	Nízke	Nízke	Stredné

VÝSLEDKY ANALÝZY RIZÍK MUSIA BYŤ SCHVÁLENÉ URČENOU OSOBOU (§20 ods. 4 písm. h) ZoKB), AK TAKÁ NIE JE, TAK ŠTATUTÁROM.

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Aplikácia bezpečnostných opatrení

- už existujúce (zavedené) bezpečnostné opatrenia sa berú do úvahy už pri identifikácii rizík ako aj pri analýze rizík

- po analýze rizík **sa bezpečnostné opatrenia „navrhujú, prijímajú a vykonávajú tak, aby ošetrili všetky riziká identifikované v rámci vykonanej analýzy rizík a naplnili bezpečnostné ciele určené v stratégii kybernetickej bezpečnosti a ciele bezpečnostných opatrení.“**

- prijatie bezpečnostných opatrení musí byť primerane zadokumentované a musí obsahovať aj vyhlásenie o opatreniach, ktoré neboli prijaté s príslušným zdôvodnením (SoA)

Riedenie tretích strán

Povinnosť uzatvoriť s treťou stranou osobitnú zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (§19 ods. 2 ZoKB).

Podľa návrhu vyhlášky:

- Zmluva musí obsahovať záväzok dodávateľa dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi

- Zmluvy uzatvorené do účinnosti vyhlášky zostávajú v platnosti po dobu určenú zmluvou. Pri predlžovaní účinnosti musí byť daná do súladu so zákonom a touto vyhláškou.

Jaroslav Ďurovka CISM
Riaditeľ Národného centra kybernetickej bezpečnosti

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

STAV KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE

Kyber 2025 – konferencia NBÚ
Demänovská dolina, 9. 6. 2025

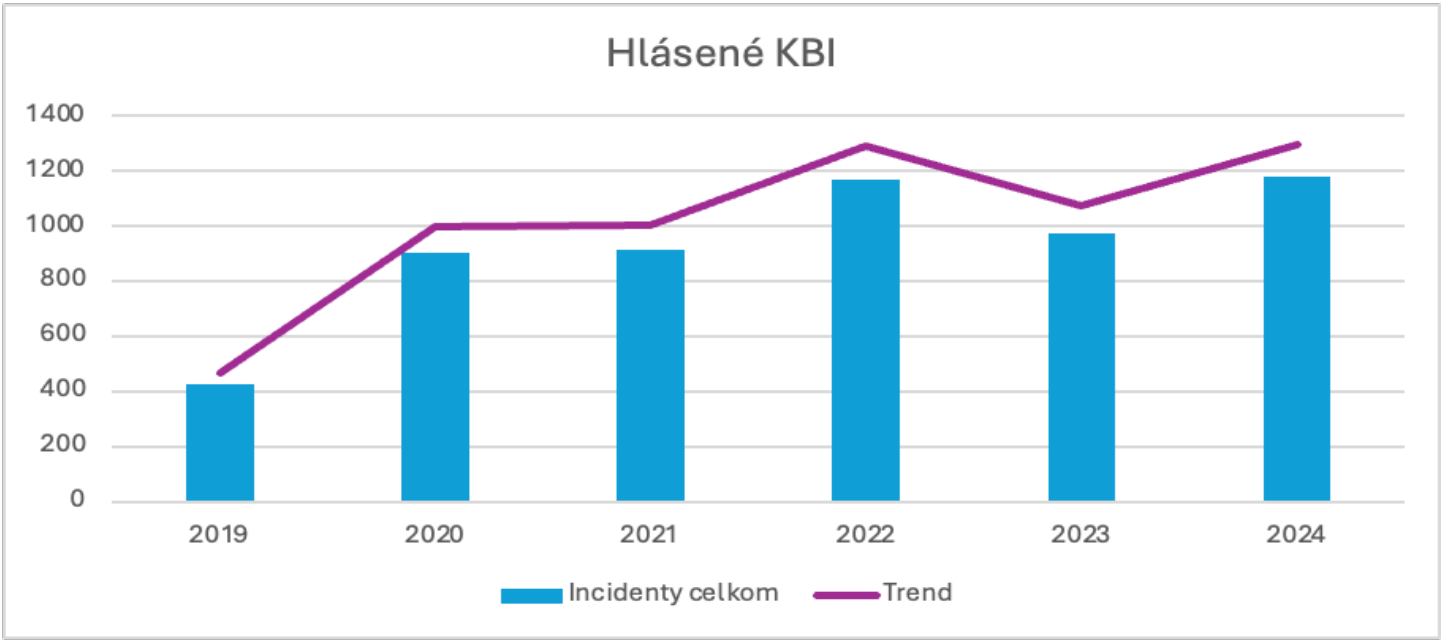
Stav kybernetickej bezpečnosti v SR za rok 2024 – vývoj hrozieb

- **Ovplyvňujúce faktory:**
  - Geopolitický vývoj
  - Vojenské konflikty, najmä na Ukrajine
  - Ransomware – zdroj obrovských nelegálnych príjmov
  - AI v rukách hackerov
  - Šírenie dezinformácií a obáv

- **Vývoj hrozieb:**
  - Pôsobenie štátmi sponzorovaných APT skupín
  - Pôsobenie hacktivistiských a kyber. zločineckých skupín
  - Hybridné hrozby
  - Komercializácia hackerských nástrojov a „služieb“ – napr. RaaS, Phishing
  - Zvyšovanie kvality útokov

Stav kybernetickej bezpečnosti v SR za rok 2024 – Incidenty

Typ hlásenia	2019	2020	2021	2022	2023	2024
Závažný KBI	13	33	34	35	26	23
Dobrovoľné hlásenia	411	871	879	1135	948	1155
Incidenty celkom	**424**	**904**	**913**	**1170**	**974**	**1178**



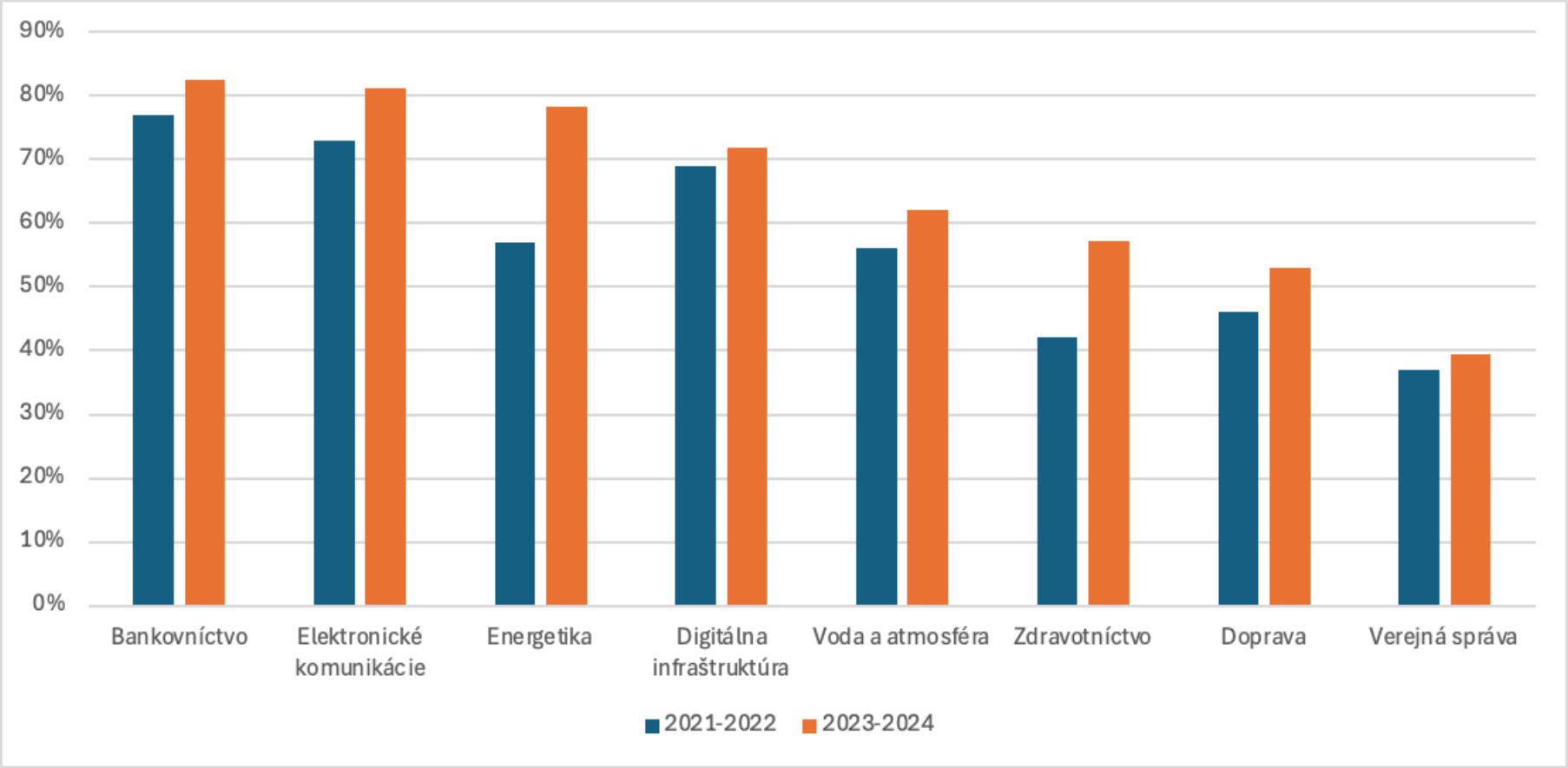
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Stav kybernetickej bezpečnosti v SR za rok 2024 – Incidenty

Všeobecné trendy:

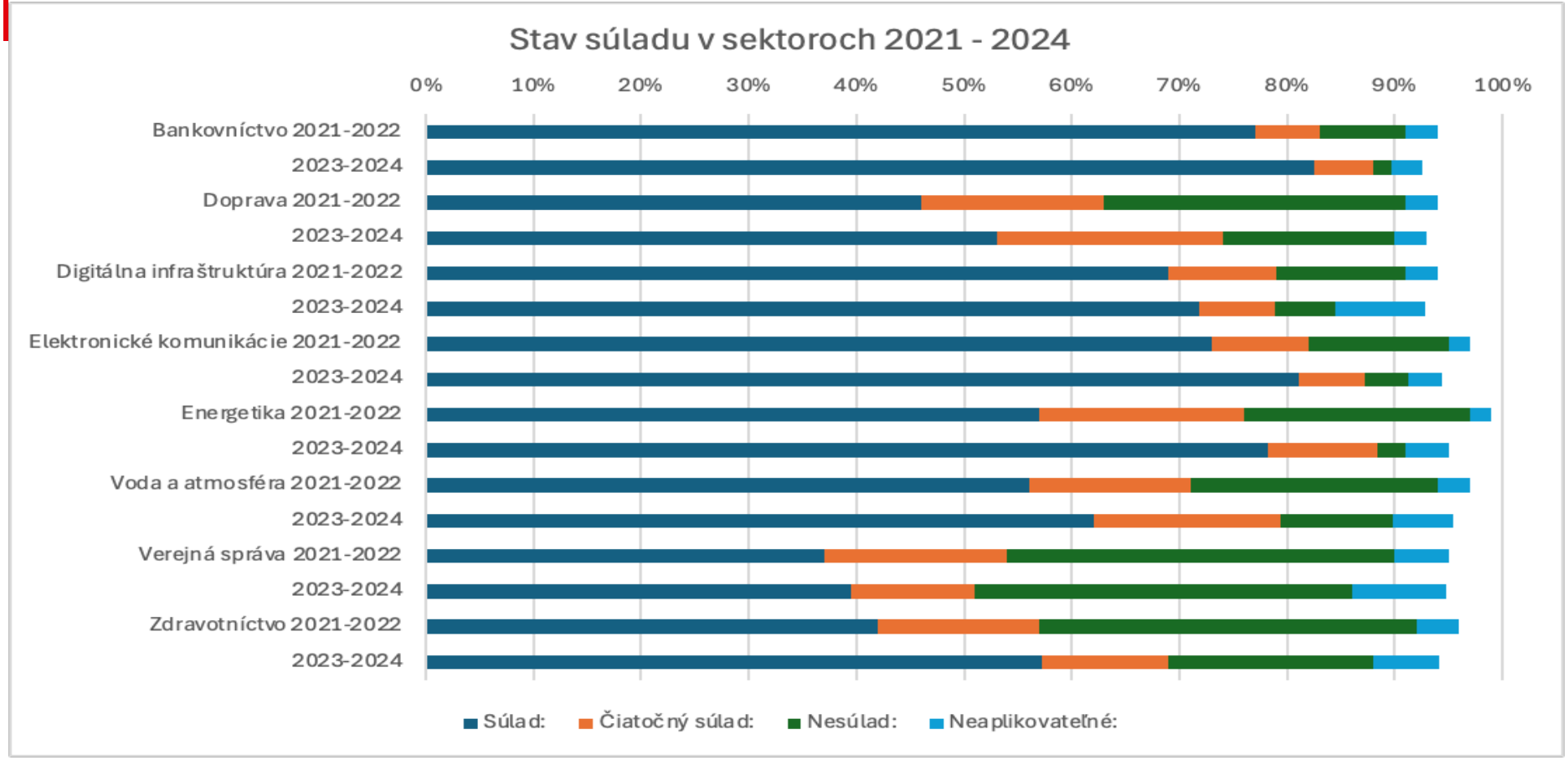
- **Počet incidentov rastie -** nárast medzi rokmi 2023 – 2024: **+204 hlásení**
- **Nerastie počet hlásení závažných KBI (v roku 2024 iba 23)**
- **Najväčší nárast – prienik do systému: + 75%** (úspešný phishing a potvrdené infiltrácie)
- **Malvérové infekcie (resp. útoky s použitím malvéru): +8,2%**
- **Incidenty týkajúce sa získavania informácií (najmä všetky druhy phishingu): +8%** (až 660 hlásení)
- **Najväčší počet incidentov je hlásený sektorom Verejná správa: 703 hlásení** (+ 47%)
- **Najväčší nárast hlásení v sektore Zdravotníctvo: +135%** (61 hlásení)

Dosiahnutý súlad s požiadavkami zákona o KB a vyhlášky NBÚ - sektory



Zdroj: Doručené správy z auditov KB – 2021-2024, NBÚ

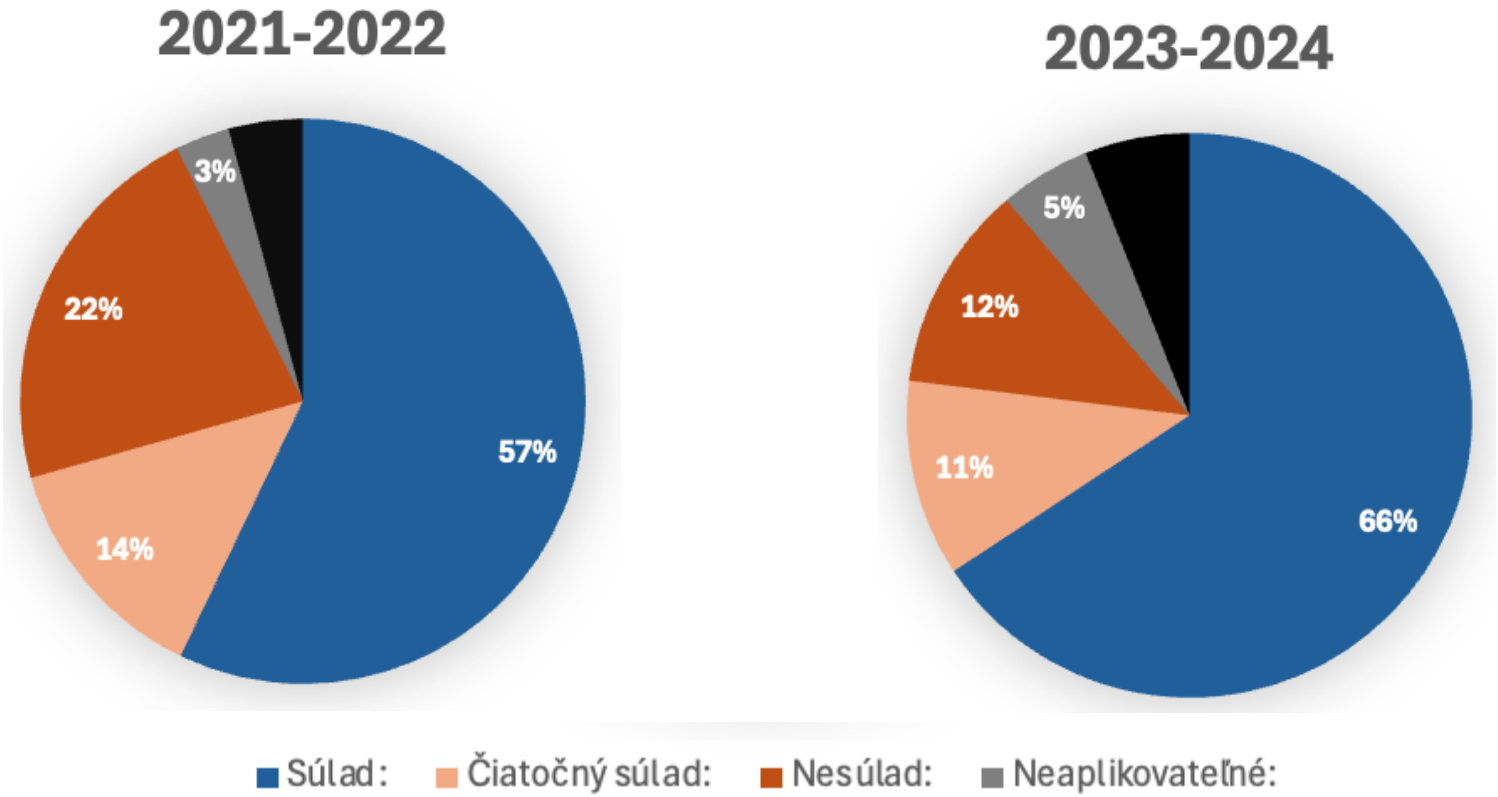
Komplexné porovnanie súladu v sektoroch



Zdroj: Doručené správy z auditov KB – 2021-2024, NBÚ

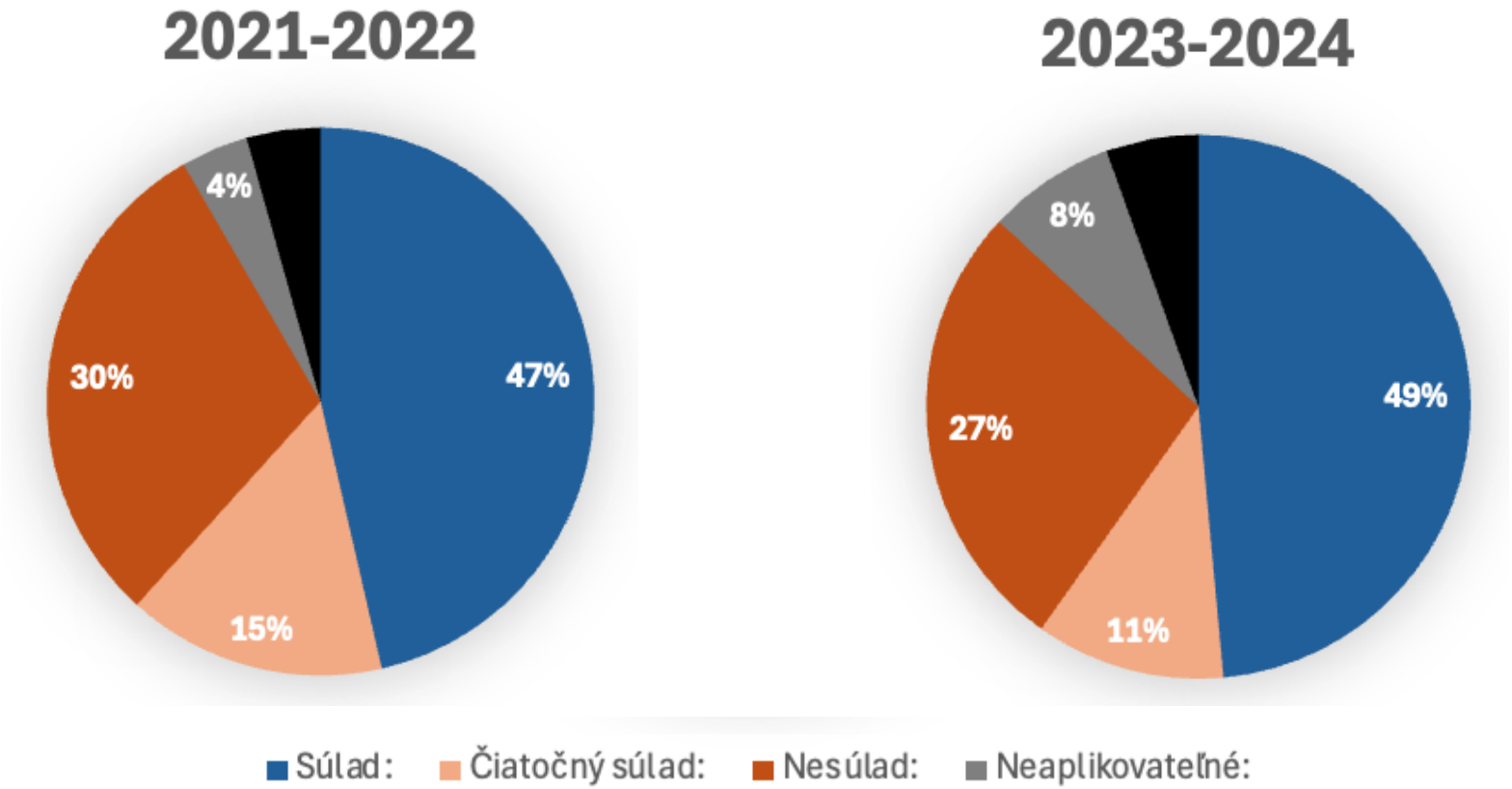
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Porovnanie celkového súladu – jednoduchý priemer podľa sektorov



Zdroj: Doručené správy z auditov KB – 2021-2024, NBÚ

Porovnanie celkového súladu – vážený priemer podľa počtu auditov



Zdroj: Doručené správy z auditov KB – 2021-2024, NBÚ

Ponaučenia (nielen) pre sektory s nízkou úrovňou súladu

1. Kybernetická bezpečnosť je zodpovednosťou každého z nás !
2. Za kybernetickú bezpečnosť v organizácii je zodpovedný štatutár, nie (iba) MKB a už vôbec nie dodávateľ !
3. Dobre riadená kybernetická bezpečnosť je priamo závislá na dobre riadenom IT/OT !
4. Systematické a udržateľné zvyšovanie kybernetickej odolnosť nemôže byť financované výlučne z projektových výziev EÚ !
5. Odborníkov na kybernetickú bezpečnosť nikdy nie je dosť !
6. Dobrého manažéra kybernetickej bezpečnosti nevyrobíte jedným školením !
7. Na dosiahnutie primeranej bezpečnosti nestačí chrániť iba perimeter !
8. Hlásenie incidentov na NBÚ nie je samobičovanie a ani priznanie viny !

Jaroslav Ďurovka CISM
Riaditeľ Národného centra kybernetickej bezpečnosti

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD


KYBER2025
09. 06. 2025
Hotel Chopok
ČO SA DEJE
A ČO NÁS ČAKÁ?
PLÁN OBNOVY
ECCC

TLP:CLEAR

čo robiť pri ransomvérovom útoku

Milan Pikula
National Cyber Security Center
National Security Authority, Slovakia

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

TLP:CLEAR

Čo je ransomvér?

Ransomvér je škodlivý softvér, ktorý šifruje.
Pomôže antivírus, XDR a kópia súborov na USB kľúči.

TLP:CLEAR

Čo je ransomvér?

Dlhodobá aktivita odhodlanej skupiny útočníkov, ktorí rutinne vypínajú XDR a vedia o mojom zálohovaní viac než ja.

TLP:CLEAR

Ransomvérový útok z pohľadu útočníka

TLP:CLEAR

Výber cieľa

Skupina	Stratégia cielenia	Významné ciele
Lockbit	oportunistický, sieť partnerov (affiliates)**, RaaS**. RDP, slabé heslá, zraniteľnosti, Initial Access Brokers.	Boeing, Industrial and Commercial Bank of China, Accenture, … Vyhýba sa Rusku.
Clop	Zneužíva zero day zraniteľnosti. Občas krádež bez šifrovania.	MOVEit Transfer (tisíce firiem, desiatky miliónov obetí), Shell, Qualys, PWC, Ernst & Young, …
~~Conti~~ → ~~Royal~~ → BlackSuit	Pracujú sami za seba. Phishing (aj callback), RDP, známe zraniteľnosti, IAB.	Brazílska vláda, … Vyhýba sa Rusku.

TLP:CLEAR

Výber cieľa

Skupina	Stratégia cielenia	Významné ciele
Vice Society	Slabo zabezpečené sektory (vzdelávanie, zdravotníctvo, výroba). Dvojité vydieranie.	Medical University of Innsbruck, … Vyhýba sa Rusku.
Scattered Spider	Distribuovaní, mladí, technicky zdatní, UK+US. Publicita nad ziskom, komplexné útoky, MFA bypass, bez preferencií.	Marks & Spencer, MGM Resorts, ...
Dragon Force	Poskytuje nástroje partnerom. Retail, komerčné firmy, organizácie s politickým dosahom.	Vyhýba sa Rusku, spolupracuje s FSB?

O výbere cieľa a prieskume

TLP:CLEAR

- Pasívny prieskum
  - verejne dostupné informácie z webov (nie vašich)
  - sociálne siete a médiá
  - historické dáta
  - služby
    - online skenery
    - informácie o IP, passive DNS a passive TLS služby
    - certificate transparency logs
  - leaky hesiel, dark web fóra, nákup prístupov
- Aktívny prieskum
  - skenovanie otvorených portov a hľadanie služieb – aj dopredu
  - hádanie hesiel
  - phishingové kampane

TLP:CLEAR

Úvodný vstup do siete

- útok na
  - technológie
  - ľudí (údajne až 74%)

- ukradnuté prihlasovacie údaje
- škodlivé URL linky a stránky
- ľahké heslá (aj s MFA, napr. Scattered Spider)
- zraniteľnosti
  - známe a nepatchované
  - zero days
- využitie insiderov na získanie prístupu

Mapovanie, rast, rozťahovanie sietí

- viac možností ako na to
  - nahranie a spustenie skenovacích nástrojov
  - vpn, proxy, socks proxy
  - LOTL
- laterálne šírenie
  - služby RDP, SSH, WinRM…
  - zložitejšie, s využitím už dostupných / napadnutých služieb
- prístup
  - rovnaké heslá, zneužiteľné hashe, mimikatz
  - slabé heslá
  - napadnutá doména / ldap
  - ďalšie zraniteľnosti

Mapovanie, rast, rozťahovanie sietí

- eskalácia práv
  - lokálne zraniteľnosti
  - získanie prístupových údajov
- perzistencia a záložné vstupné body
  - autorun, dll hijacking, …
  - nové účty
  - RAT
  - RMM (AnyDesk, TeamViewer, LogMeIn, ConnectWise, Atera, **Kaseya**, …)

TLP:CLEAR

Kde sme sa to ocitli?

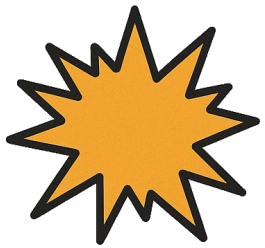
- topológia siete, operačné systémy a aplikácie
- kľúčové informácie na exfiltráciu
- zálohovacie riešenia
- monitorovacie prvky
  - SIEM
  - antivírus
  - logovací systém
  - sieťový monitoring a analytika
  - externé služby (SOC as a service)
  - …

TLP:CLEAR

Príprava na hlavnú aktivitu

- deaktivácia monitoringu a obranných prvkov
- exfiltrácia dát
- deaktivácia, zničenie záloh
- nasadenie šifrovacieho softvéru

- príprava ešte pred vstupom
  - vývoj a prevádzka infraštruktúry
  - príprava nástrojov



Šifrovanie

- voliteľné
- simultánne spustenie na viacerých počítačoch
- rýchlosť vs. dôslednosť
  - čiastočné šifrovanie
  - šifrovanie podľa typu obsahu
    - zakázané typy obsahu
    - kritické typy obsahu
  - limity na dĺžky súborov
- kryptografická kvalita
  - využitie symetrickej a asymetrickej kryptografie
- prevencia obnovy: vypnutie VSS, zmazanie snapshotov
- ransomnote a prípona súboru

TLP:CLEAR

Komunikácia a vydieranie

- komunikácia
- monetizácia (typicky v kryptomene)
  - single extortion: zaplať a dostaneš dáta nazad
  - double extortion
    - šifrovanie + krádež dát
    - zaplať a zmažeme / nevypustíme do sveta
    - prípadne prednostný predaj konkurencii
  - triple extortion: kontaktujeme tvojich známych, partnerov, **regulátorov**, médiá
  - quadruple extortion: pridáme k tomu DDoS zdarma
- CRI, https://www.counter-ransomware.org/
  - výkupné **neplatíme** – a keby to bolo viac známe, mali by sme menej prípadov
  - https://cri.sk-cert.sk/

TLP:CLEAR

čo robiť
keď všetko horí

SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

TLP:CLEAR

Úplne prvé kroky (ale to trošku preskakujeme)

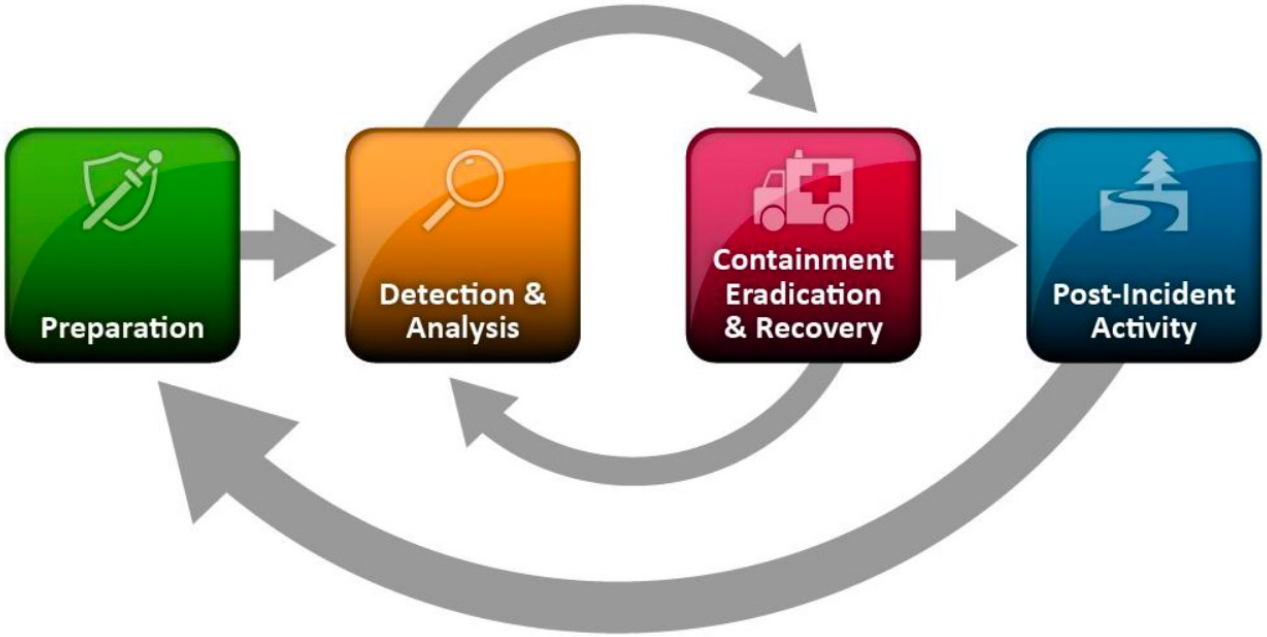
- 🖐️ Zachovajte chladnú hlavu
  - 🐢 spomaľte
  - 🧠 rozmýšľajte
- 🔗 Containment – zamedzenie šírenia
  - siete a pripojenia
  - VM
  - fyzické servery
  - notebooky a desktopy
- 💬 Interná koordinácia, krízový plán
- 📣 Hláste incident na SK-CERT

----- *AŽ POTOM ČOKOĽVEK ĎALŠIE* ----------

- ⚒️ Celý zvyšok riešenia incidentu až po obnovu

TLP:CLEAR

Čo hovoria metodiky: NIST SP 800-61 rev2



TLP:CLEAR

Čo hovoria metodiky: ISO 27035-1:2023

- Plan and Prepare (plánuj a pripravuj)

- Detect and Report (odhaľ a nahlás)
- Assess and Decide (posúď a rozhodni)
- Respond (reaguj)

- Learn Lessons (ponaučenia)

TLP:CLEAR

Čo hovoria metodiky: SANS Incident Handler's handbook

- Preparation (príprava)

- Identification (identifikácia)
- Containment (zamedzenie šírenia)
- Eradication (odstránenie)
- Recovery (obnova)

- Lessons Learned (poučenie)

TLP:CLEAR

Čo hovoria metodiky: ENISA Incident Management Guide

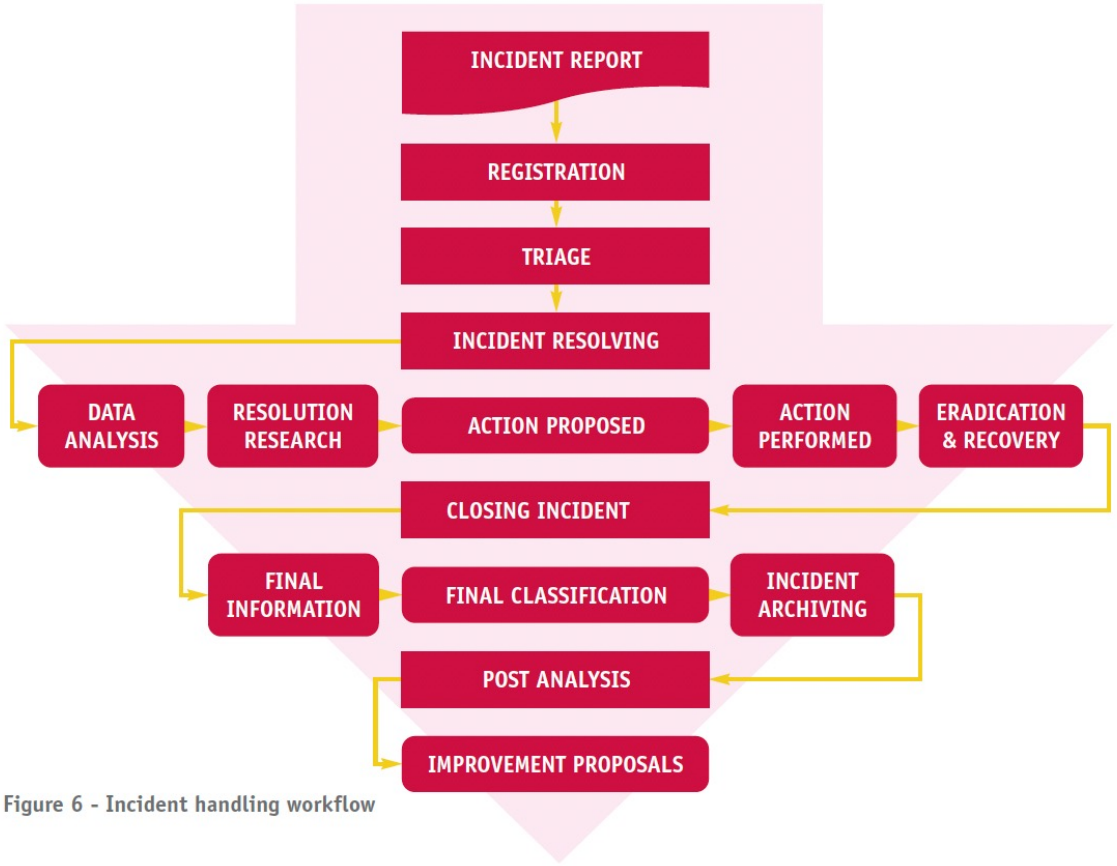
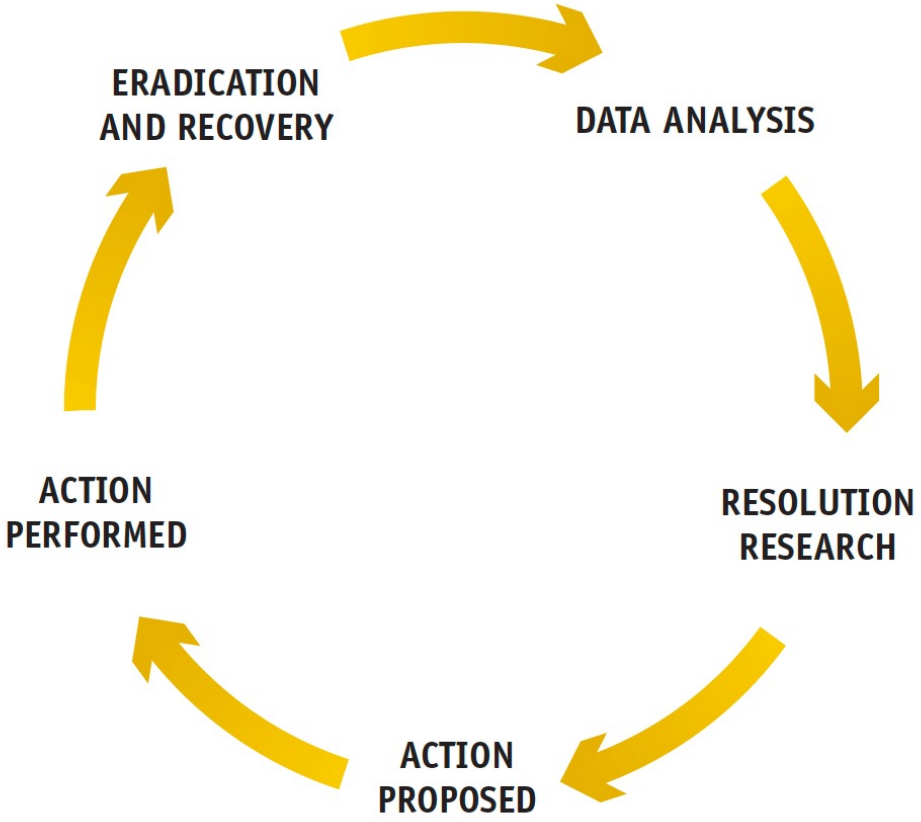


Figure 6 - Incident handling workflow

- hlásenie incidentu, registrácia, triáž
- riešenie incidentu
- dátová analýza, hľadanie riešenia, navrhované akcie, vykonané akcie
- odstránenie a obnova
- zatvorenie incidentu, finálna klasifikácia, archivovanie incidentu
- post analýza, zlepšováky

Čo hovoria metodiky: ENISA Incident Management Guide



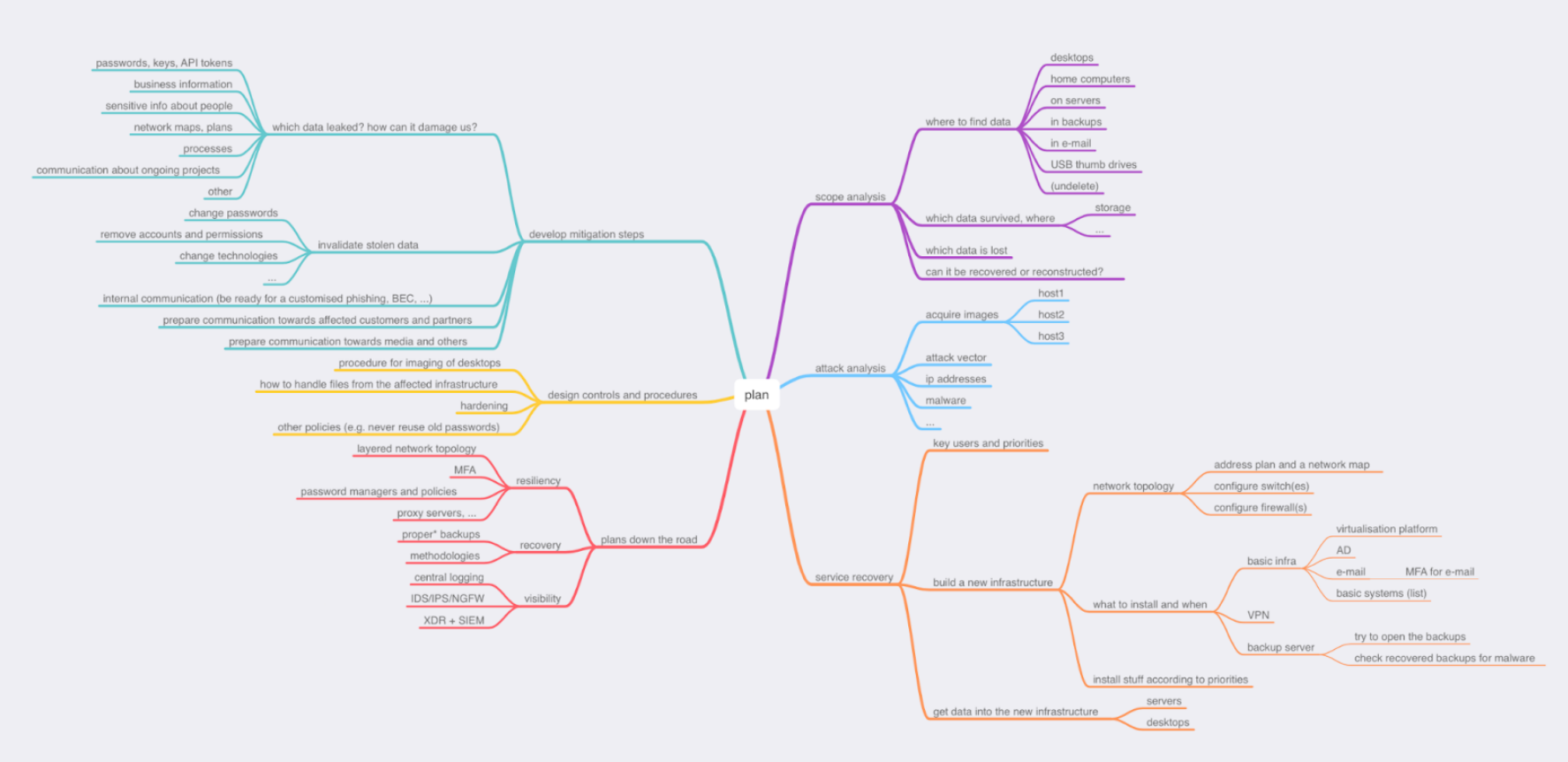
- odstránenie a obnova
- analýza dát
- hľadanie riešenia
- navrhnuté akcie
- vykonané akcie

TLP:CLEAR

Čo hovoria metodiky: SK-CERT ransomware plán

TLP:CLEAR

Čo hovoria metodiky: SK-CERT ransomware plán



TLP:CLEAR

Takže poďme po krokoch

- rýchly containment
- zachovať stopy, forenzné kópie
- analýza rozsahu
- analýza útoku
- obnova služieb
- sprievodné aktivity
  - mitigácia pre ukradnuté dáta
  - návrh procedúr na čiastkové aktivity
  - vylepšenia súčasného stavu

Zamedzenie šírenia / containment

- siete a pripojenia
  - odpojiť zasiahnutý počítač, počítače, sieťový segment
    - fyzicky vytiahnutím kábla do switchu
    - vypnutím sieťového adaptéru na počítači alebo vo virtualizácii
    - vypnutím portov na switchi
  - odstrihnúť od Internetu
  - odstrihnúť externé integrácie
  - rozpojiť LAN – občas aj vypnutie wifi pomôže
- VM – len ak virtualizácia nie je zasiahnutá útokom
  - pozastaviť (suspend)
  - a potom znemožniť prístup k manažmentu virtualizácie
  - ako zistím, či je virutalizácia zasiahnutá?

TLP:CLEAR

Zamedzenie šírenia / containment

- fyzické servery
  - odpojiť od siete – rozhodne!
  - vypnúť či nevypnúť? (nemám odpoveď)
  - nezabudnúť odpojiť aj manažmenty (ilo, idrac, ipmi, …)
  - SAN: snapshot diskov
- notebooky a desktopy
  - odpojiť od siete
  - uspať - nevypínať (vždy môžete vypnúť neskôr)

Zachovať stopy, forenzné obrazy disku, pamäti

- neznažte sa príliš skúmať incident – kazí to možné stopy
- nerobte obrazy disku / pamäti sami, ale keby…
  - hodnoverná dokumentácia zdroja dát
  - zber forenzne správnym postupom
  - typicky Expert Witness Format (EWF, E01)
- poradie akvizície
  - počítač je živý: najskôr RAM, potom DISK (pre toto ste nevypínali)
  - počítač bol vypnutý: najskôr DISK, potom RAM
  - všetko na čisté externé médiá, správnym softvérom
  - dokumentácia celého procesu
- zabráňte rotovaniu logov, vykopírujte logy z kľúčových prvkov
- ochráňte existujúce zálohy

TLP:CLEAR

Analýza rozsahu

- napadnuté služby, softvér, zariadenia, lokality
  - pochopiť dopady, závislosti, priority
- dáta
  - o čo sme asi prišli
  - kde dáta hľadať a ako ich dostať nazad
    - v zálohách
    - na serveroch
    - na pracovných staniciach, domácich počítačoch, USB kľúčoch, v e-mailoch
    - obnova (viacero stupňov vrátane undelete, carving, až po rekonštrukciu “z papiera”)

Analýza útoku

- paralelne s obnovou, vzájomne sa ovplyvňujú
- analyzovať získané logy, obrazy diskov, pamäti
- útočný vektor
- IP adresy, DNS mená, URL adresy a ďalšie
- malvér
- TTP, ideálne mapovateľné na MITRE ATT&CK maticu

TLP:CLEAR


MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
ATT&CK®
Get Started
Take a Tour
Contribute
Blog
FAQ
Random Page
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (4)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (8)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (7)
Stage Capabilities (6)
Initial Access
11 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Wi-Fi Networks
Execution
16 techniques
Cloud Administration Command
Command and Scripting Interpreter (12)
PowerShell
AppleScript
Windows Command Shell
Unix Shell
Visual Basic
Python
JavaScript
Network Device CLI
Cloud API
AutoHotKey & AutoIT
Lua
Hypervisor CLI
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (3)
User Execution (4)
Windows Management Instrumentation
Persistence
23 techniques
Account Manipulation (7)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Cloud Application Integration
Compromise Host Software Binary
Create Account (3)
Create or Modify System Process (5)
Event Triggered Execution (17)
Exclusive Control
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (9)
Modify Registry
Office Application Startup (6)
Power Settings
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (6)
Software Extensions (2)
Traffic Signaling (2)
Valid Accounts (4)
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (5)
Domain or Tenant Policy Modification (2)
Escape to Host
Event Triggered Execution (17)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)
T1547
Defense Evasion
45 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification (2)
Email Spoofing
Execution Guardrails (2)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (14)
Hijack Execution Flow (12)
Impair Defenses (11)
Impersonation
Indicator Removal (10)
Indirect Command Execution
Masquerading (11)
Modify Authentication Process (9)
Modify Cloud Compute Infrastructure (5)
Modify Cloud Resource Hierarchy
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (17)
Plist File Modification
Pre-OS Boot (5)
Process Injection (12)
Credential Access
17 techniques
Adversary-in-the-Middle (4)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (9)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (5)
Steal Web Session Cookie
Unsecured Credentials (8)
Discovery
33 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Location Discovery (1)
System Network Configuration Discovery (2)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtual Machine Discovery
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Adversary-in-the-Middle (4)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Screen Capture
Video Capture
Command and Control
18 techniques
Application Layer Protocol (5)
Communication Through Removable Media
Content Injection
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Tools (3)
Traffic Signaling (2)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (4)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
15 techniques
Account Access Removal
Data Destruction (1)
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Email Bombing
Endpoint Denial of Service (4)
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking (4)
Service Stop
System Shutdown/Reboot
https://attack.mitre.org/techniques/T1547

Obnova

- kľúčoví používatelia, služby, priority
- obnova nemôže byť “do pôvodného stavu”
- stavba novej infraštruktúry
  - “na zelenej lúke”
  - navrhnúť
  - zabezpečiť potrebný hardvér, softvér, ľudí
  - postaviť
- riadený presun dát do novej infraštruktúry
- kontrola integrity dát
- zavedenie nových opatrení a monitoringu
- mitigácia pre ukradnuté dáta

TLP:CLEAR

dalo sa to čakať, alebo
čo u obetí často vidíme

TLP:CLEAR

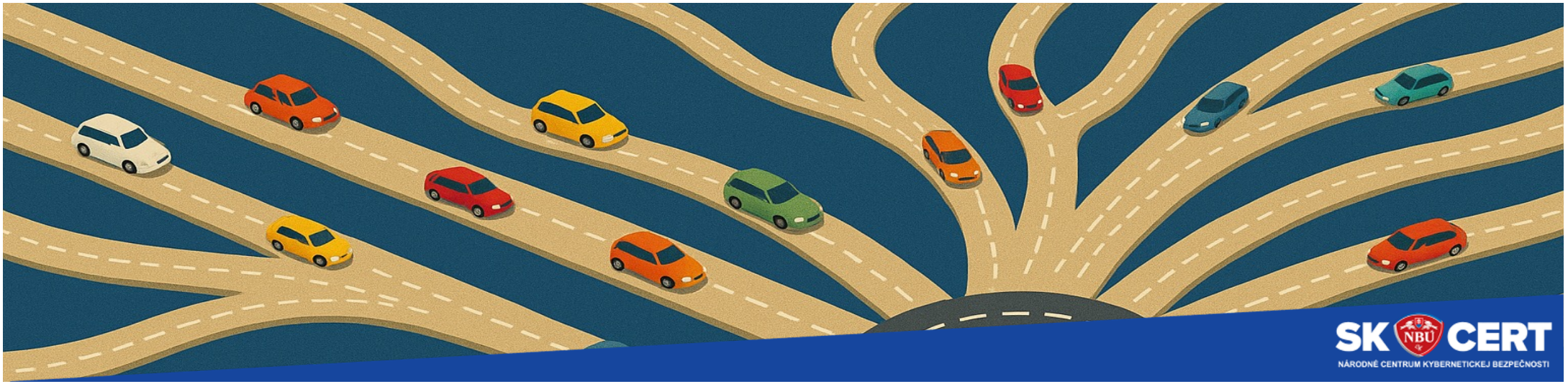
Chýbajúci patch manažment

- 💀 zraniteľné verzie aplikácií na verejnom internete
- zastaralé OS a aplikácie
  - ⚠️ **Windows 10 – október 2025**
    - **ESU (extended security update) pre VM pod Windows 365, Azure Virtual Desktop**
  - ❌ **SQL server 2012, 2012 R2 – október 2023**
    - **ESU do októbra 2026**
  - ❌ Windows 8.1 – január 2023, Windows 8 – január 2016, Windows 7 – január 2020
  - ❌ Windows Vista – Apríl 2017, Windows XP – Apríl 2014, Windows 2000 – Júl 2010
- hardvér – serverový bios (a CPU mikrokód), storage, firewally, switche
- špeciálne zariadenia (telefóny, tlačiarne, senzory, manažmenty)
- virtualizácia, docker
- vlastné aplikácie a aplikačné závislosti

TLP:CLEAR

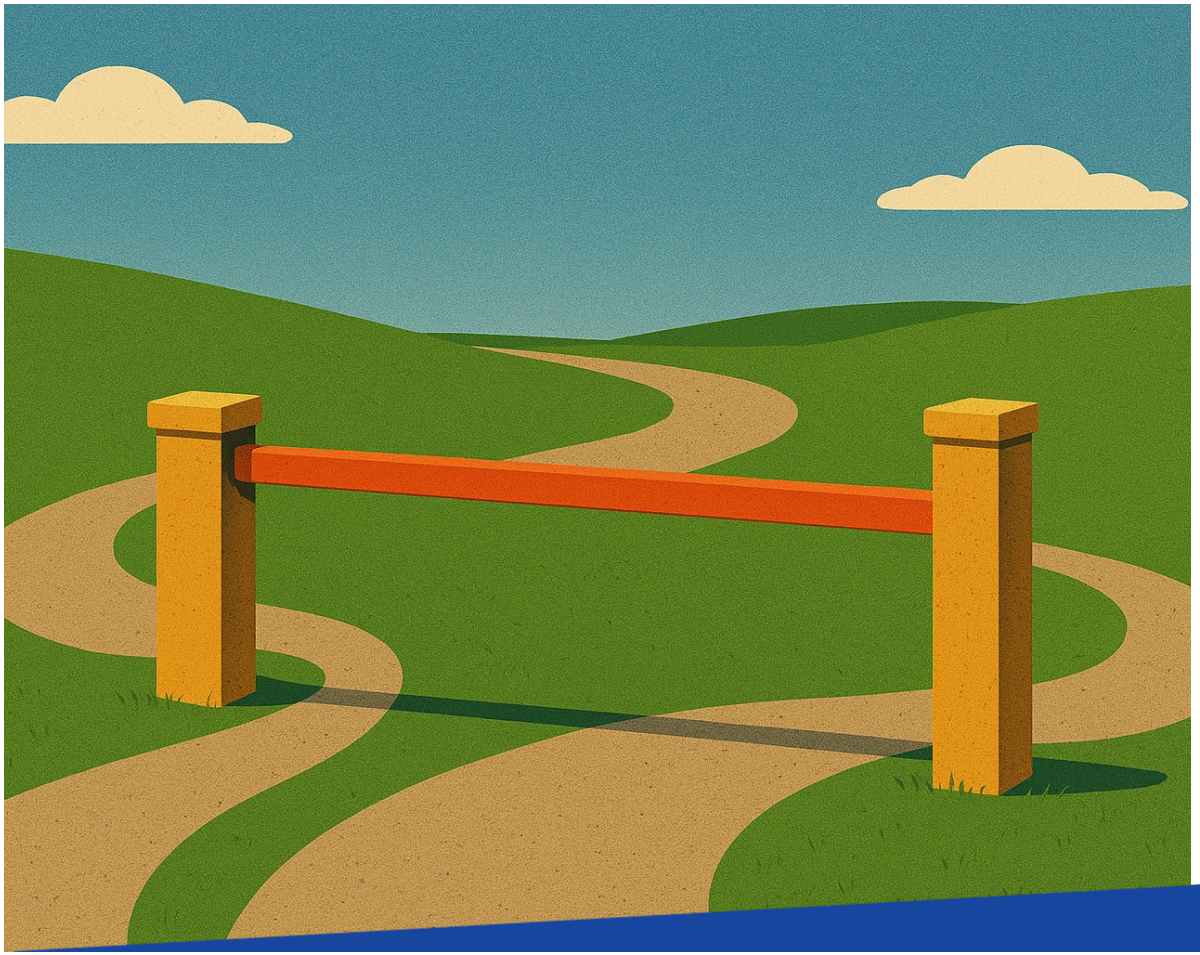
Žiadna alebo slabá segmentácia siete

- jedna plochá sieť
- sieť má čiastočnú segmentáciu
  - oddelenie A, oddelenie B
  - IP telefóny
  - všetky servery
- sieť má dobrú segmentáciu, ale zlé firewallové pravidlá



TLP:CLEAR

Mizerné riadenie prístupov



- ľahko uhádnuteľné heslá
- slovníkové heslá
- chýbajúce viacfaktorové overenie
- viacfaktor cez nezabezpečený kanál

TLP:CLEAR

Žiadny monitoring

- nakúpený antivírus, SIEM, EDR/XDR, IPS vo firewalli, sieťový monitoring
- nikto sa neunúva čítať
- útočníci mesiace až roky slobodne behajú infraštruktúrou, generujú alerty
- napokon monitoring vypnú

TLP:CLEAR

čo robiť pri ransomvérovom útoku

Milan Pikula
National Cyber Security Center
National Security Authority, Slovakia

SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI


KYBER2025
09. 06. 2025
Hotel Chopok
ČO SA DEJE
A ČO NÁS ČAKÁ?
PLÁN OBNOVY
ECCC

Čo nové v certifikácii?

por. Ing. Anna Kováčiková, PhD.
Orgán pre bezpečnostnú certifikáciu
Budatínska 30 | 85106 Bratislava | Slovenská republika
ncca@nbu.gov.sk | https://ncca.nbu.gov.sk

Obsah

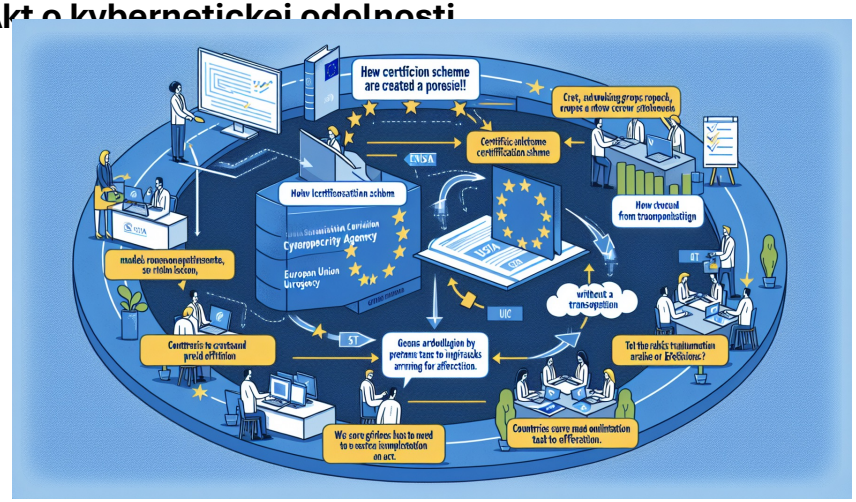
Národná autorita pre certifikáciu kybernetickej bezpečnosti

Certifikácia kybernetickej bezpečnosti

Certifikácia kybernetickej bezpečnosti - Projekty

Certifikácia kybernetickej bezpečnosti - Školenia

Akt o kybernetickej odolnosti



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

NCCA

Vytvorenie štruktúr

Legislatíva a ZoKB

Nový web

Quo vadis?

Certifikácia kybernetickej bezpečnosti

- ENISA ✓
- NCCA ✓
- NAB ✓
- CAB

Od 15.4.2025 je možné žiadať SNAS (NAB) o akreditáciu CAB

Certifikácia kybernetickej bezpečnosti - Projekty a výzvy

ncca.nbu.gov.sk

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Certifikácia kybernetickej bezpečnosti - Projekty a výzvy

Výzvy:

Podpora certifikácie CAB

Podpora vzdelávania hodnotiteľov

Podpora auditov IT

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

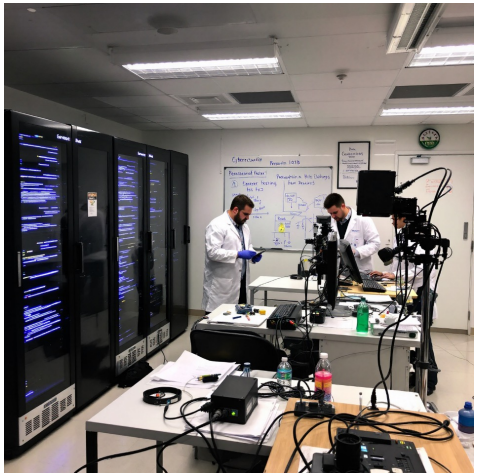
Certifikácia kybernetickej bezpečnosti - Projekty a výzvy

Podpora vzdelávania

Tvorba stratégií

Vytvorenie platformy

Pilotná certifikácia produktu



Certifikácia kybernetickej bezpečnosti - Školenia a vzdelávanie

Online školenia:

17.,18.10.2024
Vzťah medzi CSA a CRA (NSAI)

29.,30.10.2024
EUCS (NSAI)

7.,8.11.2024
ISO/IEC 17025, ISO/IEC 17065 (NSAI)

12.,13.11.2024
Common Criteria vs EUCC (NSAI)

29.4.2025
Seminár certifikácia KB pre IKT produkty (NCCA)

3.6.2025
Vzťah medzi EUCC a nariadením CRA (ENISA)

Zdroj: ncca.nbu.gov.sk

Prezenčné školenie:

3.-7.2.2025
Common Criteria (CCLab)

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Certifikácia kybernetickej bezpečnosti - Školenia a vzdelávanie

Online školenia:
https://ncca-certifikacia-ikt-foau28u.gamma.site/

17.6.2025
Analýza hodnotiacej správy podľa Common Criteria

30.6.2025
Metodika EUCC a tvorba Bezpečnostného zámeru ST

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Akt o kybernetickej odolnosti CRA

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

ĎAKUJEM ZA POZORNOSŤ

por. Ing. Anna Kováčiková, PhD.
Orgán pre bezpečnostnú certifikáciu
Budatínska 30 | 85106 Bratislava | Slovenská republika
ncca@nbu.gov.sk | https://ncca.nbu.gov.sk


KYBER2025
09. 06. 2025
Hotel Chopok
ČO SA DEJE
A ČO NÁS ČAKÁ?
PLÁN OBNOVY
ECCC

Manažérsky pohľad na ransomvér

(je to vlastne nárast kybernetického vydierania)

Rastislav Janota

styčný dôstojník pre oblasť kybernetickej bezpečnosti vo Washingtone D.C.

Úvod – prečo ransomware nie je len IT téma

- Ransomware je jednou z najväčších hrozieb nie pre IT ale pre fungovanie celej organizácie
- Nie je to otázka technológie, zasahuje celú organizáciu vrátane reputácie voči externému prostrediu, partnerov/zákazníkov
- Reakcia na útok si vyžaduje dobre koordinovanú (natrénovanú) reakciu celej organizácie (vedenie, právne, komunikačné, IT, bezpečnosť, financie, prevádzka...)
- Manažéri organizácie musia chápať riziko ransomware ako problém manažmentu s veľmi kritickými reálnymi dopadmi
- Kvalitná prevencia / odolnosť začína zhora – bez silného zapojenia najvyššieho vedenia sa nevytvoria procesy, kultúra bezpečnosti ani nenastavia priority
- CEO (ale nie len) musí byť schopný odpovedať na otázku: “Viem ako by sme zareagovali keby nás to zasiahlo zajtra?"

Štatistiky: nárast incidentov globálne + EÚ

Štatistika SOPHOS:

- 59% organizácii postihnutých
  - 32% využitie zraniteľnosti
  - 29% kompromitované credentials
- 94% postihnutých povedalo, že útočník cielil na ich backup, 57% úspešne
- 32% postihnutým so zašifrovanými údajmi boli dáta aj exfiltrované
- 70% postihnutým boli dáta zašifrované (98% postihnutým v sekt. verejnej správy)
- $2mil priemerná suma ransomu
- $2.73mil priemerné náklady na recovery
- 34% organizácii potrebovalo >30 dní

Štatistika IBM:

- Výroba je najzraniteľnejší sektor
- Nárast útokov s použitím AI
- Nárast útokov s použitím “Persistent Infostealers“
- Európa – 23% svetových útokov
- 70% útokov na kritickú infraštruktúru

Iné:

- Počet ransomvér incidentov globálne prekročil 190tis ročne (SonicWall 2024).
- V EÚ narástol počet incidentov za 3 roky o viac než 50 % (ENISA 2023).
- Zasiahnuté sú zdravotníctvo, logistika, energetika, aj verejná správa.
- Iba 63 % organizácií, ktoré zaplatili, skutočne získali všetky dáta späť.

Ransomvér ako služba (RaaS) – trhová realita

- Ransomware ako služba (RaaS) označuje systém ransomvéru založený na predplatnom, ktorý umožňuje aj neskúseným kybernetickým zločincom spúšťať útoky ransomvéru.
- Programy RaaS eliminujú potrebu útočníkov písať škodlivý kód.
- RaaS môže používať ktokoľvek jednoduchým zaregistrovaním sa na predplatné. Existuje kompletný čierny trh s podporou, outsourcingom a reputáciou “dodávateľov“.
- Tento model znižuje bariéru vstupu a zvyšuje objem útokov – útok môže uskutočniť aj neskúsený útočník.

- RaaS vytvára dynamický ekosystém, kde sa ransomvér šíri ako bežný obchodný model.

Geopolitika a tolerancia útokov

- Aktivity súvisiace s ransomvérom sú čoraz viac prepojené s geopolitikou
- Ransomware presahuje čisto finančné motivácie a slúžia ako nástroj politického tlaku, špionáže a dokonca aj kybernetickej vojny.
- Kybernetická kriminalita je často sponzorovaná štátmi, kde vlády využívajú ransomvér na presadzovanie svojich záujmov.
- Mnohé ransomvér skupiny pôsobia z krajín, kde majú tichú toleranciu alebo aj podporu.
- V čase geopolitického napätia sú kybernetické útoky používané ako nástroj asymetrického nátlaku.
- Niektoré štáty útočníkov nevyšetrujú alebo ich dokonca využívajú ako 'proxy' operácie.
- Útoky teda nie sú len kriminálne, ale často majú politické a strategické pozadie.
- Manažér musí počítať s tým, že útočník je motivovaný inak, než len ziskom.

CEO pohľad – dopady na biznis, reputáciu, operácie, právo

- Ransomvér nie je technická udalosť – je to krízová situácia s priamym dopadom na biznis.
- CEO/riaditeľ/prezident firmy zodpovedá za kontinuitu prevádzky, dôveru trhu, reputáciu a právne dôsledky.
- Útok môže zastaviť výrobu, e-shopy, služby, logistiku – s okamžitým dopadom na tržby.

- Strata dôvery partnerov/investorov sa nedá vyriešiť zálohovacím softvérom.
- Zlyhanie v pripravenosti môže mať následky na osobnú aj reputačnú úroveň vrcholového vedenia.
- Preto CEO potrebuje rámec rozhodovania: čo sa deje, kto rozhoduje, aké sú alternatívy.

- V mnohých incidentoch práve absencia tohto rámca spôsobila najväčšie škody.

Odolnosť – ako vzniká, ako sa buduje, čo ju podkopáva

„Kybernetická odolnosť je schopnosť organizácie odolávať kybernetickým útokom, reagovať na ne a zotaviť sa z nich a zároveň zachovať obchodné operácie.“

- Vzniká kombináciou plánovania, výcviku, testovania, technickej pripravenosti a vedomostí.
- Každý útok preveruje praktickú schopnosť konať: kto rozhoduje, aké máme limity, čo sú priority.
- Odolná organizácia nielen zvláda incident – ale sa z neho aj poučí a zlepší.
- Budovanie odolnosti musí byť strategická priorita – nie len 'projekt IT‘.

=> Kľúčové aspekty odolnosti:
Predvídanie a prevencia, detekcia a reakcia, obnova, adaptácia, kontinuita podnikania

Bezpečnostná kultúra – ako sa líši od „školení“

Silná kybernetická kultúra v organizácii zahŕňa angažovanosť vedenia, povedomie a školenie zamestnancov, jasné zásady a pozitívny postoj ku kybernetickej bezpečnosti.

- Mala by obsahovať návyky ako: hlásenie podozrení, preverovanie požiadaviek (nie len neobvyklých), opatrnosť pri kliknutí a pod.
- Bezpečnostná kultúra nie je náklad – je investícia do odolnosti a dôvery.
- Manažéri musia ísť príkladom – ak sa zaujímajú, zamestnanci tiež.
- Vedomosti sa musia dať preniesť aj domov – to je znak toho, že kultúra funguje.

Ale: skutočná kultúra je to, čo ľudia robia, keď ich nikto nevidí.

Regulácia

- NIS2 nastavuje jasné pravidlá a zodpovednosti pre rôzne typy subjektov.
- Slovenský zákon o kybernetickej bezpečnosti patrí medzi najpokrokovejšie v EÚ.
- Zavádza zodpovednosť vedenia, minimálne štandardy a povinnosti v oblasti prevencie a hlásenia.
- Nejde len o súlad – ale o rámec, ktorý pomáha organizácii systematicky budovať odolnosť.
- Správna implementácia zákona = vyššia pripravenosť, nie len 'compliance‘.

Pre väčšinu organizácii reálne nestačí spraviť len to, čo zákon požaduje

Prvé odporúčania

1. Začnite tam, kde sa dá konať hneď: ľudia a procesy.
2. Overte si, kto v organizácii má aké role počas incidentu.
3. Zapojte všetkých manažérov v organizácii.
4. Cvičte incidenty aspoň raz ročne – aj netechnicky.
5. Vyhodnoťte najslabší článok: je to vedomosť, proces, alebo technológia?
6. Nebojte sa začať „zľahka“ – aj malá zmena správania má veľký dopad.
7. Zapojte partnerov, dodávateľov, regulačné orgány – bezpečnosť nie je izolovaná.

Technické:

1. Kvalitné riadenie zraniteľností: Identifikujte a riešte zraniteľnosti v systémoch a softvéri s cieľom znížiť počet útokov.
2. Zálohovanie a obnova: Pravidelne zálohujte dáta a testujte procesy obnovy, aby ste zabezpečili dostupnosť dát v prípade útoku.

ĎAKUJEM

Rastislav Janota

rastislav.janota@nbu.gov.sk

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD


KYBER2025
09. 06. 2025
Hotel Chopok
ČO SA DEJE
A ČO NÁS ČAKÁ?
PLÁN OBNOVY
ECCC

Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

AUDIT
A IMPLEMENTÁCIA POŽIADAVIEK

Kyber2025 Roadshow, 9.6.2025

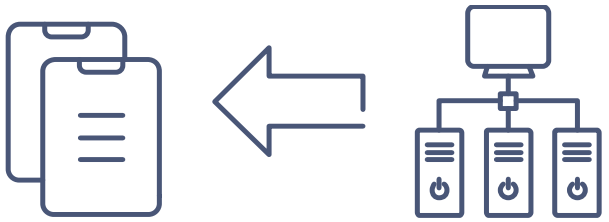
Tomáš Hettych, CISA, CISM, CGEIT, CRISC, CDPSE, ITIL4 Master

Certifikovaný audítor a manažér KB, COO KCCKB

PREČO AUDIT?

AUDIT

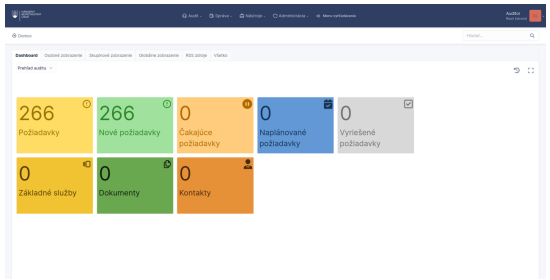
- Systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky
- **Typické metódy:**
  - Auditné rozhovory a dotazníky
  - Porovnávanie deklarovaného a skutkového stavu
  - Preskúmanie zdokumentovaných informácií
  - Vzorkovanie (vykonáva sa, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu)

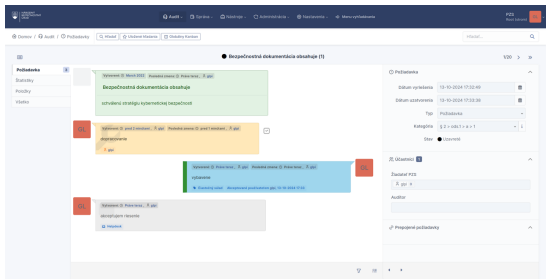


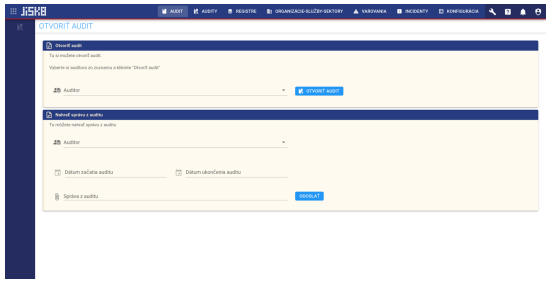
- **Primárny účel:**
  - Získanie informácie o nezhodách a rizikách formou konsolidovanej správy
  - Iniciácia návrhov na zmenu jestvujúcich resp. Implementáciu ďalších bezpečnostných opatrení

Pre audit je typická požiadavka na nestrannosť

AUDIT VS. SAMOHODNOTENIE







- Podľa novelizovaného znenia Zákona:
  - Prevádzkovateľ základnej služby, **ktorý nie je prevádzkovateľom kritickej základnej služby**, môže zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti – **JISKB**
  - Samohodnotenie vykonáva **manažér kybernetickej bezpečnosti**
  - Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti **do piatich rokov** odo dňa zaradenia do registra prevádzkovateľov základnej služby

NAJČASTEJŠIE RIZIKÁ A NÁLEZY AUDITU

- **Riadenie bezpečnosti (Security governance):**
  - Nedostatočná podpora vedenia ústavu
  - Nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti kybernetickej bezpečnosti
  - Zodpovednosť za identifikáciu a evidenciu aktív, hrozieb a rizík
  - Neexistencia analýzy rizík a analýzy dopadov
  - Nedostatočná, alebo stále chýbajúca bezpečnostná dokumentácia
  - Nezávislosť riadenia bezpečnosti od riadenia IT
  - Vzdelávanie v oblasti informačnej bezpečnosti
  - Neformálne riadenie prevádzky

- **Výkon bezpečnosti (Security operations):**

  - Chýbajúci bezpečnostný monitoring
  - Nesystematické riešenie incidentov
  - Vzdialený prístup do interných sietí a IS nie je zabezpečený
  - Chýbajúca topológia, segmentácia, zoznamy portov
  - Neexistencia procesov riadenia kontinuity činností
  - Nejasné a neformálne postupy zálohovania a obnovy
  - PZS nedostatočne rieši šifrovú ochranu informácií

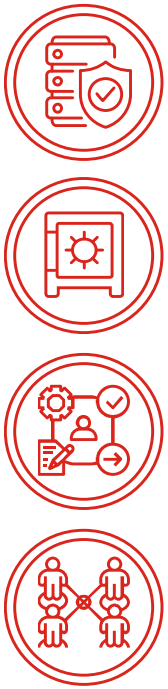
Spolufinancovaný Európskou úniou

AKÝ MÁTE AKČNÝ PLÁN?

BEZPEČNOSTNÉ OPATRENIA

TYPY OPATRENÍ

- **TECHNOLOGICKÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov technologickej povahy
- **FYZICKÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej povahy
- **ORGANIZAČNÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie
- **PERSONÁLNE OPATRENIA**
  - organizačné opatrenia týkajúce sa riadenia ľudských zdrojov



Efektívnu bezpečnosť je možné dosiahnuť
LEN POMOCOU KOMBINÁCIE
rôznych kategórií opatrení

PREVENTÍVNE OPATRENIA (výber)

- Aktualizácia a záplaty (Patch management) – aktualizácia firmvérov, operačných systémov, aplikácií
- Ochrana pracovných staníc (Endpoint security) – antivírus, antispam, antimalvér
- Silné heslá (Password management) – rôzne heslá pre rôzne systémy, komplexné heslá, špeciálne znaky, časté zmeny
- Viacstupňové prihlasovanie (Multifactor authentication) – používanie kombinácie viacerých spôsobov prihlasovania
- Zálohovanie a kontrola obnovy (Backup and recovery) – pravidelne, rôzne miesta a spôsoby
- Vzdelávanie, šifrovanie komunikácie, atď.

REAKTÍVNE OPATRENIA (výber)

- Plány kontinuity a obnovy
  - Business Continuity Plan (BCP)
  - Disaster Recovery Plan (DRP)
- Riadenie incidentov (Incident management) – komplexný systém pre identifikáciu, klasifikáciu, riešenie a reporting incidentov
- Analýza rizík (Risk analysis)
- Analýza dopadov (Business Impact Analysis)
- Zverejňovanie zraniteľností
- Pravidelný audit

IMPLEMENTÁCIA POŽIADAVIEK, KDE ZAČAŤ?

INFORMAČNÉ AKTÍVA

- **Informačné aktíva** sú všetky objekty a komponenty:
  - podieľajúce sa na dodávke IT produktov, alebo IT služieb,
  - ktoré pre organizáciu priamo, alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu,
  - ktorých narušenie integrity, dôvernosti a dostupnosti môže mať na organizáciu negatívny dopad

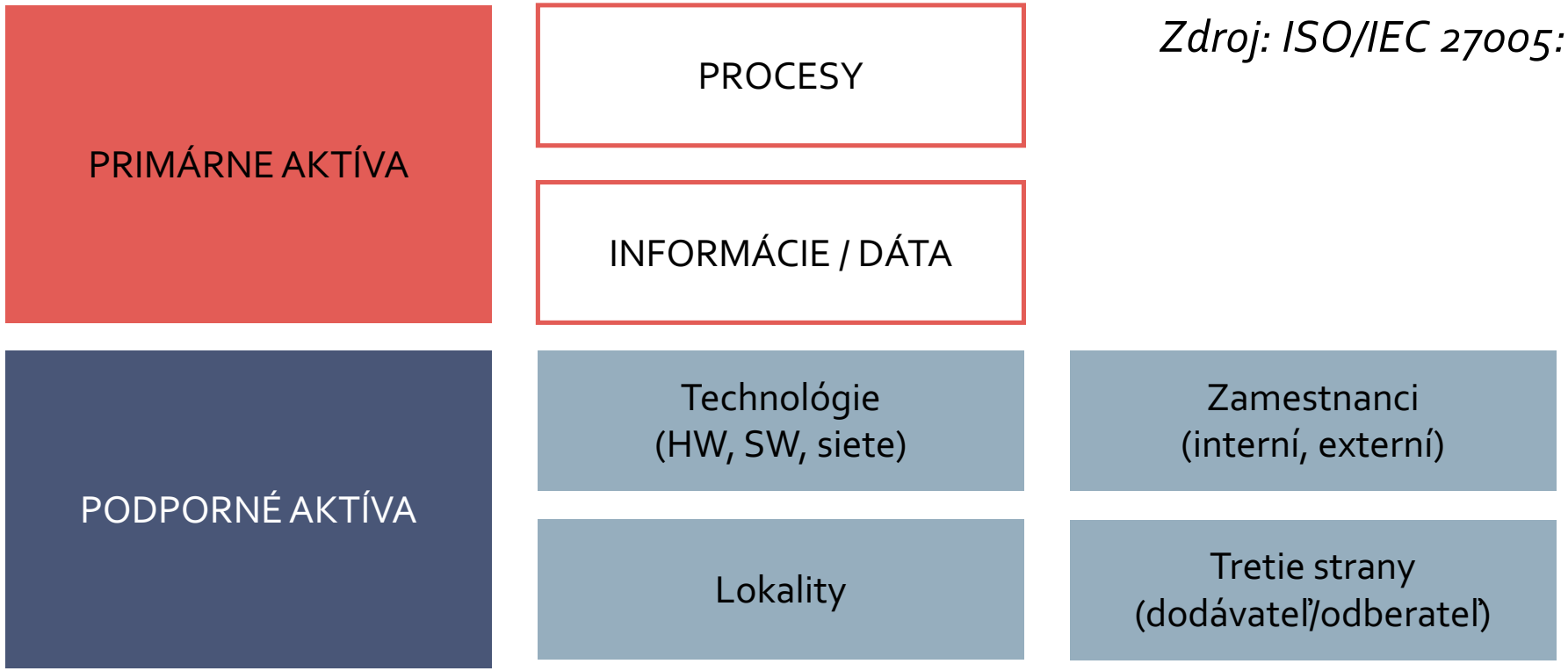
Confidentiality (Dôvernosť)

Integrity (Celistvosť)

Availability (Dostupnosť)

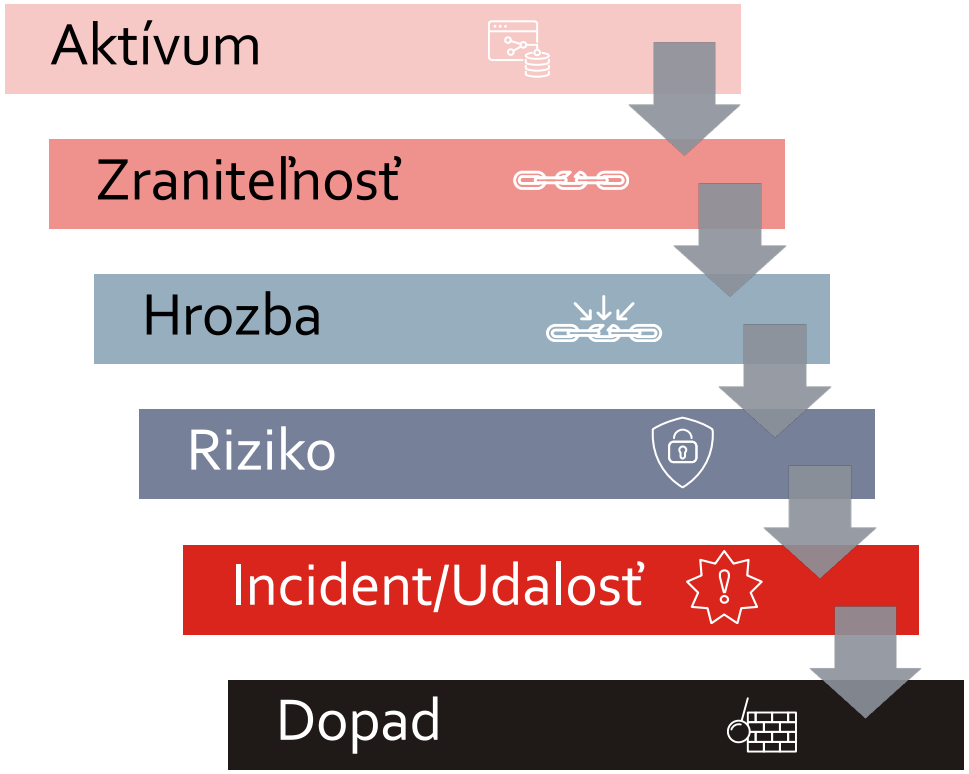
Zdroj: NBÚ - Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

TYPY INFORMAČNÝCH AKTÍV PODĽA VÝZNAMNOSTI



Zdroj: ISO/IEC 27005:2022

ZRANITEĽNOSTI, HROZBY, RIZIKÁ, DOPADY



Zraniteľnosť - slabé miesto informačného aktíva, slabina v informačnom systéme, v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb.

Hrozba - potenciál, že akákoľvek okolnosť či udalosť využije zraniteľnosť informačného aktíva a spôsobí negatívny následok (dopad).

Riziko - funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody.

Dopad - hodnota závažnosti ujmy, resp. rozsah škody, ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou.

ANALÝZA RIZÍK

- **Kvalitatívna**
  - Použitie **slovných (nečíselných) hodnôt** na vyjadrenie faktorov a úrovní rizika
  - Subjektívne hodnotenie (kvalifikovaný hrubý odhad)
  - Hodnota pravdepodobnosti a dopadu je určená na základe individuálnych odborných znalostí
- **Kvantitatívna**
  - Použitie **numerických hodnôt** na vyjadrenie faktorov a úrovní rizika
  - Objektívne hodnotenie
  - Hodnota pravdepodobnosti a dopadu je určená na základe histórie udalostí
- **Semikvantitatívna (zmiešaná)**
  - Použitie **numerického rozsahu hodnôt** s jedinečným významom a kontextom
  - Kontextové hodnotenie (kvalifikovaný detailný odhad)
  - Hodnota pravdepodobnosti a dopadu sú odvodené z rozsahu číselných hodnôt (stupnice) s priradením príslušného stupňa jedinečného významu

Pravdepodobnosť	Dopad			
	Zanedbateľný	Minimálny	Závažný	Katastrofický
Vysoká	C	B	A	A
Stredná	C	B	B	A
Malá	D	C	B	B
Veľmi malá	D	D	C	C

Exposure Factor -> Single Loss Expectancy

Annualized Loss Expectancy = Single Loss Expectancy * Annualized Rate of Occurrence

$ALE_{(IS)}=ALE_1+ALE_2+...+ALE_n$

Pravdepodobnosť hrozby	Dopad hrozby			
	Zanedbateľný (20)	Minimálny (50)	Závažný (70)	Katastrofický (100)
Vysoká (1)	20*1,0=20	50*1,0=50	70*1,0=70	100*1,0=100
Stredná (0,7)	20*0,7=14	50*0,7=35	70*0,7=49	100*0,7=70
Malá (0,4)	20*0,4=8	50*0,4=20	70*0,4=28	100*0,4=40
Veľmi malá (0,2)	20*0,2=4	50*0,2=10	70*0,2=14	100*0,2=20

ANALÝZA FUNKČNÉHO DOPADU – BIA

1/2

- **Analýza funkčných dopadov** (Business Impact Analysis - BIA) identifikuje, kvalifikuje a kvantifikuje potenciálne dopady a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie s cieľom identifikovať tie procesy, ktoré sú pre organizáciu **kľúčové / kritické**
- Jedná sa o posúdenie ekonomických, reputačných a regulačných vplyvov, hrozieb a nákladov na obnovenie procesu v prípade výpadku v rôznych časových intervaloch od začiatku výpadku

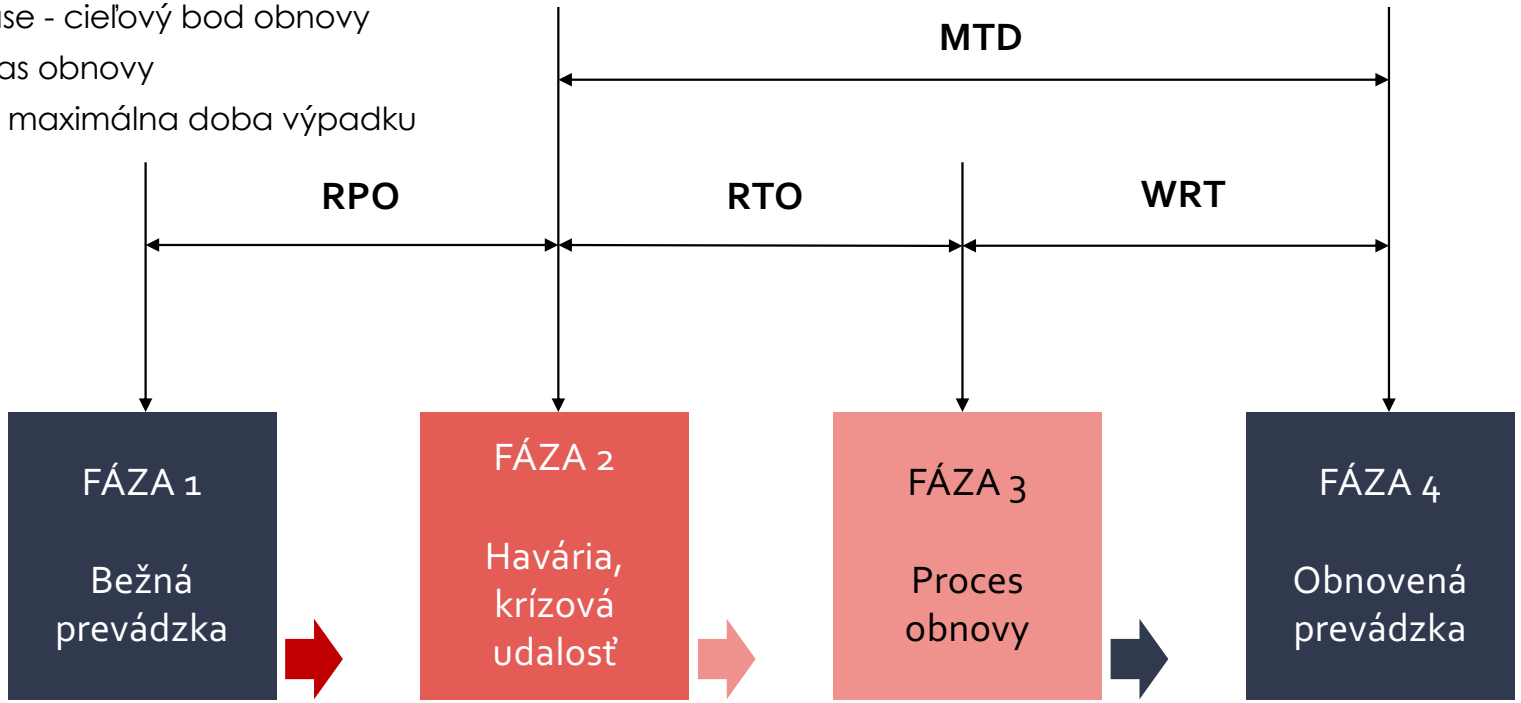
CIEĽOVÁ DOBA OBNOVY (RTO) A CIEĽOVÝ BOD OBNOVY (RPO)

RTO (Recovery Time Objective) - identifikácia maximálne tolerovanej doby
pre obnovenie činnosti na prijateľnej úrovni

RPO (Recovery Point Objective) - identifikácia maximálne prijateľného množstva a straty údajov merané v čase - cieľový bod obnovy

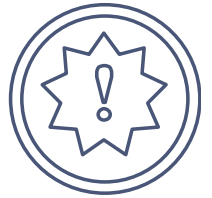
WRT (Work Recovery Time) – celkový čas obnovy

MTD (Maximum Tolerable Downtime) – maximálna doba výpadku



PLÁNY KONTINUITY A KRÍZOVÉ SCENÁRE

- Nevyhnutným predpokladom efektívneho plánovania kontinuity je, aby boli vopred definované scenáre rôznych udalostí, ktoré potenciálne môžu mať negatívny vplyv na bežné činnosti organizácie.
- Typickými kategóriami scenárov BCM sú napr.:
    1. **Náhla nedostupnosť personálu**
    2. **Náhla nepoužiteľnosť pracoviska/budovy**
    3. **Náhla nepoužiteľnosť technológií**
    4. **Náhla nedostupnosť médií.**



- Vedenie podniku by malo formálne rozhodnúť, ktoré scenáre majú byť vzhľadom na obmedzené zdroje predmetom BCM.
- Zvyčajne sú riešené len vyššie uvedené kategórie scenárov, pričom nie sú zahrnuté scenáre ako prírodné katastrofy, vojnové konflikty, občianske nepokoje a podobné, ktoré prekračujú rámec plánovacích možností bežnej organizácie.

TYPICKÉ KRÍZOVÉ SCENÁRE

- **Scenáre náhlej nepoužiteľnosti pracoviska:**
  - Uzatvorenie cesty
  - Únik plynu
  - Požiar
  - Povodeň
  - Obmedzenia v súvislosti s vodovodom a kanalizáciou
  - Rozsiahla porucha infraštruktúry stavebného objektu
  - Štrukturálne poškodenie stavby a objektu
  - Bombový útok
  - Povinná evakuácia oblasti
- **Scenáre náhlej nedostupnosti technologickej infraštruktúry:**
  - Rozsiahly výpadok počítačovej siete
  - Strata údajov
  - Rozsiahly výpadok kritických aplikácií
  - Kybernetický bezpečnostný incident
- **Scenáre náhlej nedostupnosti personálu:**
  - Dopravné obmedzenia a logistické problémy
  - Nákazlivá choroba
  - Poškodenie zdravia, alebo úmrtie kritického personálu
  - Štrajk
  - Úradné uzatvorenie budovy
- **Scenáre náhlej nedostupnosti médií:**
  - Výpadok elektrického napájania
  - Výpadok telekomunikácií
  - Výpadok plynu
  - Nedostatok vody
  - Poškodenie prenosových trás
  - Porucha inžinierskych sietí

ZAPOJENIE VEDENIA ORGANIZÁCIE

MOŽNÉ RIEŠENIA NEDOSTATKU ODBORNÍKOV NA KB

MOŽNÉ RIEŠENIA

- Stredné a vysoké školy
- Zvyšovanie zručností (upskilling)
- Certifikácia
- Hľadanie mladých talentov

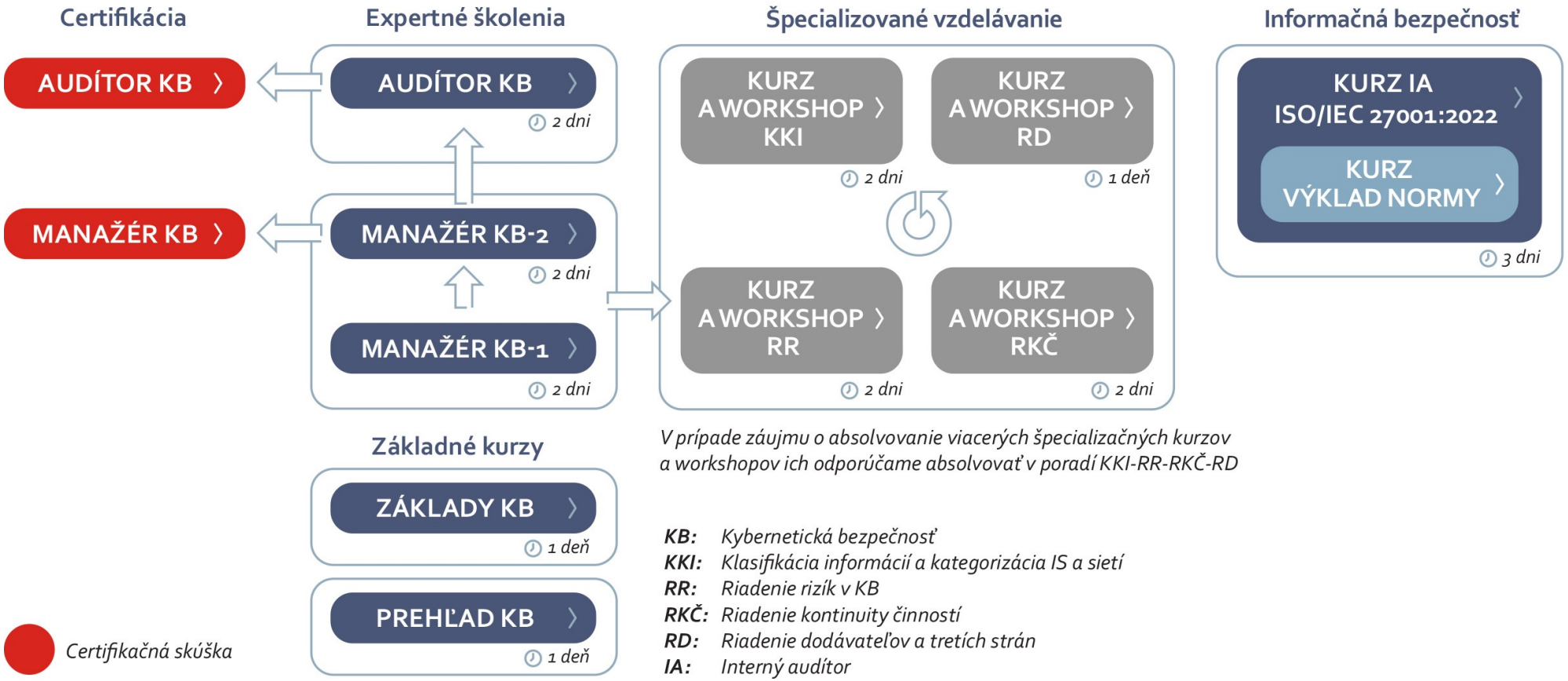
UPSKILLING

- Trend, ktorý uľahčuje ďalšie vzdelávanie poskytovaním školiacich programov a príležitostí na rozvoj
- **Zlepšovanie zručností súčasných profesionálov**
- **Zvyčajné metódy**: školenia a tréningy vo forme ďalšieho vzdelávania
- **Cieľom je najmä**:
  - napredovanie v práci
  - nájdenie nových príležitostí v rámci organizácie
  - zvýšenie disponibilnej kapacity ľudských zdrojov v konkrétnych profesiách a roliach

CERTIFIKÁCIA OSÔB

- Ako potvrdiť získané vedomosti a zručnosti?
  - Vysokoškolské vzdelávanie je po absolvovaní štúdia formálne **ukončené štátnou skúškou a potvrdené vysokoškolským diplomom**
  - Ďalšie vzdelávanie (upskilling) je možné formálne **ukončiť certifikačnou skúškou a potvrdiť certifikátom**
- **<u>Certifikácia je zásadne dobrovoľná !</u>**
- Existujú dve kategórie certifikátov:
  - **Komerčné certifikáty vydávané v neakreditovanom režime** (ISACA, ISC2, CompTIA, GIAC, SANS, a ďalšie)
  - **Certifikáty od akreditovaných vzdelávacích inštitúcií**

CERTIFIKAČNÁ SCHÉMA VZDELÁVANIA V KYBERNETICKEJ BEZPEČNOSTI



V prípade záujmu o absolvovanie viacerých špecializačných kurzov a workshopov ich odporúčame absolvovať v poradí KKI-RR-RKČ-RD

KB: *Kybernetická bezpečnosť*
KKI: *Klasifikácia informácií a kategorizácia IS a sietí*
RR: *Riadenie rizík v KB*
RKČ: *Riadenie kontinuity činností*
RD: *Riadenie dodávateľov a tretích strán*
IA: *Interný audítor*

HĽADANIE MLADÝCH TALENTOV

- **Kybernetická bezpečnosť formou CTF hier a súťaží:**
  - Cybergame (nielen pre mladých)
  - Hackfest
  - Online a onsite CTF turnaje
  - European Cyber Security Challenge (ECSC)

Slovak Cyber Team

ZÁVER

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI


JUST DO IT®

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti


KYBER2025
09. 06. 2025
Hotel Chopok
ČO SA DEJE
A ČO NÁS ČAKÁ?
PLÁN OBNOVY
ECCC