Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Kybernetická bezpečnosť vo verejnej správe

Úvod do KB (Blok I)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

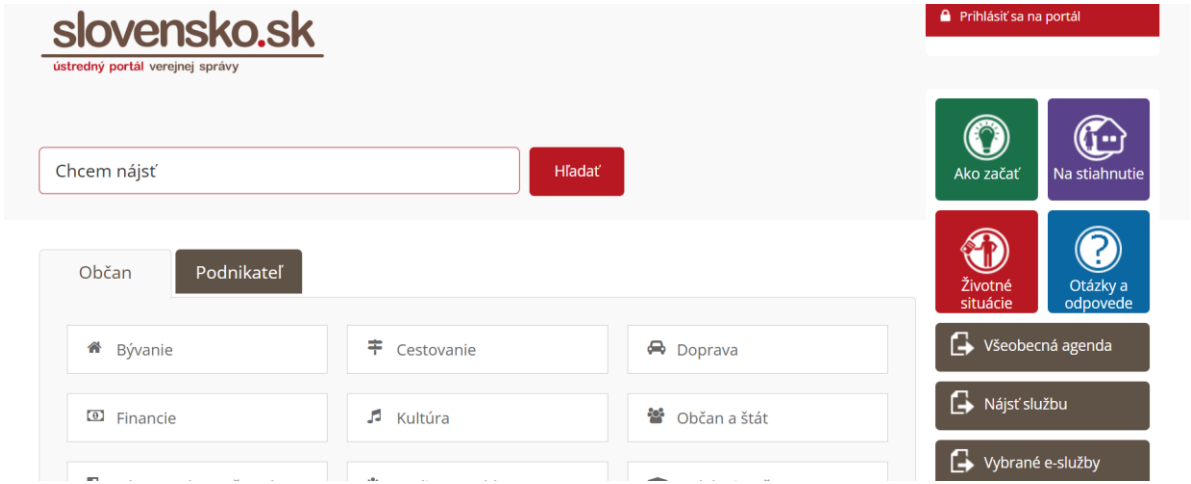
Katarina.kampova@uniza.sk

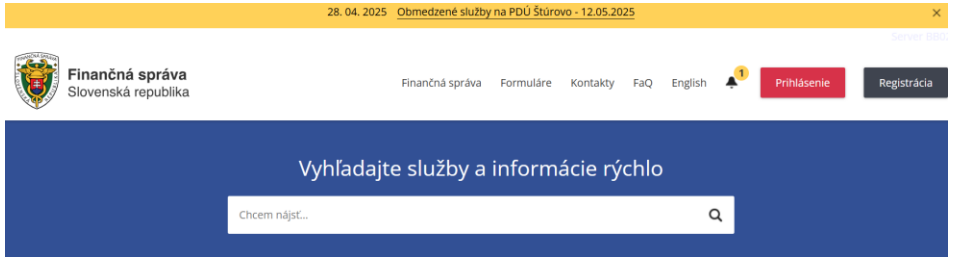
Význam digitalizácie verejnej správy v SR

- **Digitalizácia verejnej správy je kľúčovým nástrojom pre zvyšovanie efektívnosti, transparentnosti a dostupnosti služieb pre občanov aj podnikateľov.** Moderné technológie umožňujú zefektívniť administratívne procesy a zároveň znižovať zaťaženie používateľov.
  - **Zvyšovanie efektívnosti a transparentnosti procesov:** Elektronické formuláre, automatizácia a prepojené registre skracujú dobu vybavenia a minimalizujú priestor pre chyby či manipuláciu.
  - **Skracovanie lehôt a znižovanie byrokracie:** Občan alebo firma nemusí opakovane predkladať tie isté údaje, čím sa znižuje administratívna záťaž a urýchľuje komunikácia s úradmi.
  - **Prístup k službám 24/7:** Vďaka e-schránkam, elektronickým podaniam či dostupnosti elektronických výpisov je možné vybaviť mnoho úradných záležitostí bez návštevy úradu – kedykoľvek a odkiaľkoľvek.
  - **Podpora dátovo riadeného rozhodovania štátu:** Digitalizácia umožňuje štátu získavať a analyzovať relevantné dáta pre lepšie plánovanie verejných politík a služieb.
  - **Výzvy:** S narastajúcou digitalizáciou prichádza aj potreba budovania dôvery používateľov, zaistenia kybernetickej bezpečnosti a jednotného systému správy údajov.

Informačné systémy verejnej správy

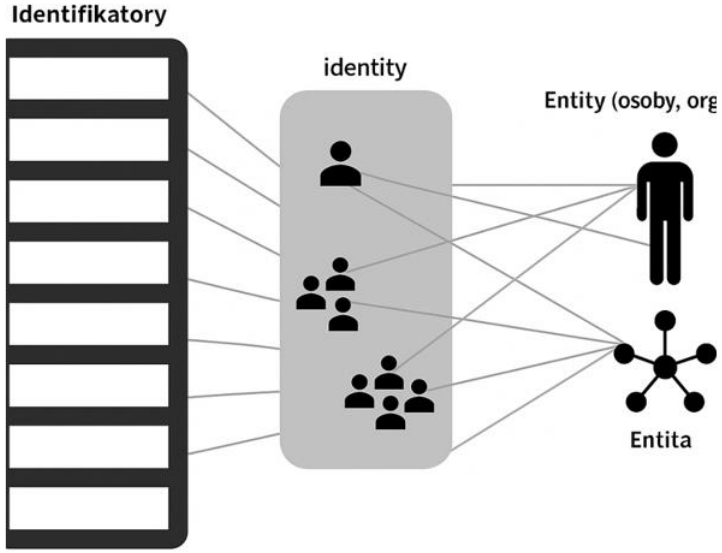
- **Verejná správa používa množstvo centrálnych a špecializovaných IS na poskytovanie služieb občanom a organizáciám.**
  - ÚPVS (Slovensko.sk) – hlavný prístupový bod.
  - Referenčné registre: obyvateľov, právnických osôb, adries.
  - DCOM – riešenie pre obce a mestá.
  - IS sociálneho a zdravotného systému, kataster.
  - Dôležitá je integrita, dostupnosť a dôvernosť údajov.





Ochrana údajov a digitálna identita

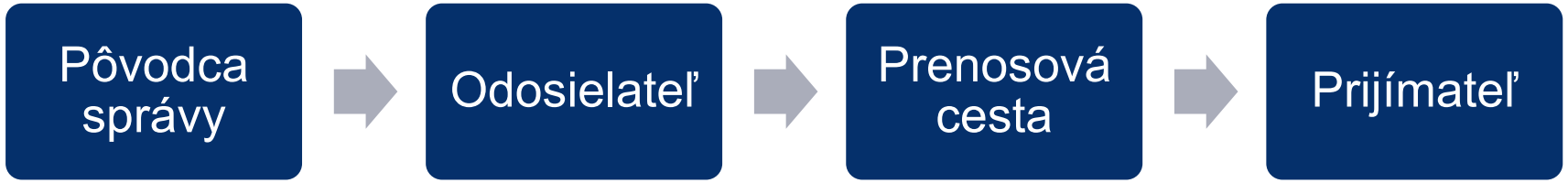
- **Bezpečnosť údajov je základným predpokladom dôvery v e-Government.**
  - Ochrana osobných údajov v zmysle GDPR.
  - Elektronická identita a autentifikácia (eID).
  - Elektronický podpis a časová pečiatka.
  - Viacfaktorová autentifikácia ako štandard.
  - Riziká: neoprávnený prístup, zneužitie identity, phishing.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Čo je cieľom digitálnej identity?

- Cieľom identifikácie je zabezpečiť, že každá digitálna identita je jednoznačná, t. j. že žiadne dve entity (osoby alebo systémy) nemajú rovnakú identitu.
- Jedná entita môže mať v rôznych kontextoch viacero identít, pričom každá z nich je reprezentovaná vlastným súborom identifikátorov.
- Každý prvok, ktorý sa zúčastňuje komunikácie v kybernetickom priestore, musí byť **jednoznačne identifikovateľný.**



- **Identita musí byť určiteľná pre všetky body v komunikačnom reťazci,** nielen pre odosielateľa a prijímateľa.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kybernetická bezpečnosť vo verejnej správe

- Kybernetická bezpečnosť je nevyhnutná pre funkčnosť a dôveryhodnosť štátnych systémov.
  - Verejná správa je cieľom aj garantom bezpečnosti.
  - Povinnosť mať riadenie rizík a incidentov.
  - Dôležitosť školení a bezpečnostného povedomia.
  - Spolupráca medzi štátom, samosprávami a odbornou komunitou.
  - Súlad s NIS2, ISO/IEC normami a zákonom o kybernetickej bezpečnosti.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kybernetická bezpečnosť SR v kontexte Európskej únie

- **Kybernetická bezpečnosť vo verejnej správe SR je úzko prepojená s politikami a reguláciami Európskej únie, ktoré formujú spoločné požiadavky na ochranu informačných systémov:**
  - **Smernica NIS2 (2022/2555)**: stanovuje povinnosti pre verejné inštitúcie a kritické subjekty členských štátov v oblasti kybernetickej bezpečnosti – SR ju transponuje do zákona o kybernetickej bezpečnosti.
    - **Agentúra ENISA**: Európska agentúra pre kybernetickú bezpečnosť poskytuje usmernenia a podporuje výmenu najlepších praktík medzi členskými štátmi.
  - **GDPR (2016/679)**: nariadenie o ochrane osobných údajov platné v celej EÚ, kľúčové aj pri spracúvaní údajov vo verejnej správe.

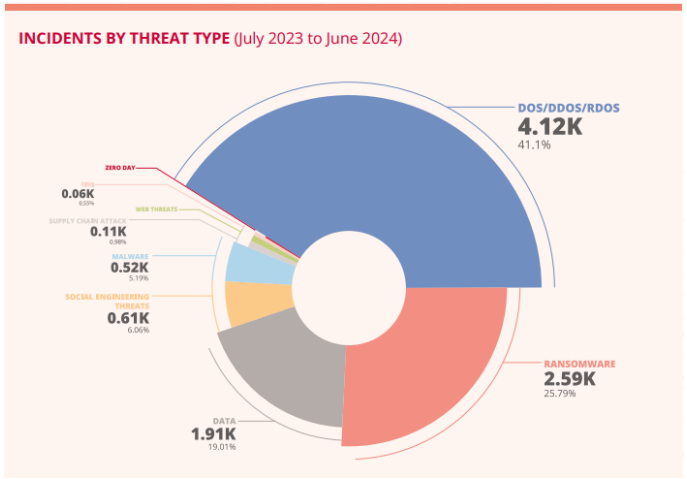
ORGANIZÁCIA ENISA

- 7 Strategických cieľov ENISI vo vzťahu ku kybernetickej bezpečnosti

Posilnenie komunít	+
Predvídavosť	+
Vedomosti	+
Politika kybernetickej bezpečnosti	+
Operatívna spolupráca	+
Budovanie kapacít	+
Overené riešenia	-

ENISA a je základné úlohy

- **Základné úlohy:**
  - **Podpora a koordinácia** – ENISA pomáha členským štátom pri vypracovávaní a implementácii politiky kybernetickej bezpečnosti.
  - **Posilnenie kapacít** – Agentúra prispieva k rozvoju národných kapacít na ochranu pred kybernetickými hrozbami.
  - **Rýchla reakcia na incidenty** – ENISA zaisťuje efektívnu koordináciu pri riešení kybernetických incidentov a krízových situácií.
  - **Legislatívna podpora** – Pomáha pri harmonizácii právnych rámcov a implementácii európskych nariadení a smerníc.
  - **Osveta a školenia** – Podporuje šírenie povedomia o kybernetickej bezpečnosti prostredníctvom školení a kampaní.
  - **Analýzy a správy** – ENISA poskytuje pravidelné správy o aktuálnych trendoch v oblasti kybernetických hrozieb, ktoré slúžia na podporu rozhodovania v členských štátoch.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

CSIRT - Computer Security Incident Response Team

- Čo je CSIRT?
  - Špecializovaný tím na monitorovanie, detekciu a riešenie kybernetických incidentov.
  - Zodpovedný za rýchlu a koordinovanú reakciu na bezpečnostné hrozby.
  - Posilňuje kybernetickú bezpečnosť a odolnosť kritickej infraštruktúry a iných subjektov.
- Kľúčové úlohy CSIRT
  - Monitorovanie a analýza incidentov – Sleduje hrozby a identifikuje bezpečnostné incidenty v sieťach a informačných systémoch.
  - Reakcia a zmiernenie následkov – Poskytuje technickú podporu a koordinuje riešenie incidentov s cieľom minimalizovať škody.
  - Koordinácia a výmena informácií – Spolupracuje s národnými a medzinárodnými CSIRT tímami pre efektívnejšiu prevenciu a riešenie hrozieb.
  - Podpora tvorby bezpečnostných štandardov – Prispieva k vývoju národných a medzinárodných postupov na zvýšenie bezpečnosti.

- CSIRT je kľúčovým článkom kybernetickej obrany EÚ!

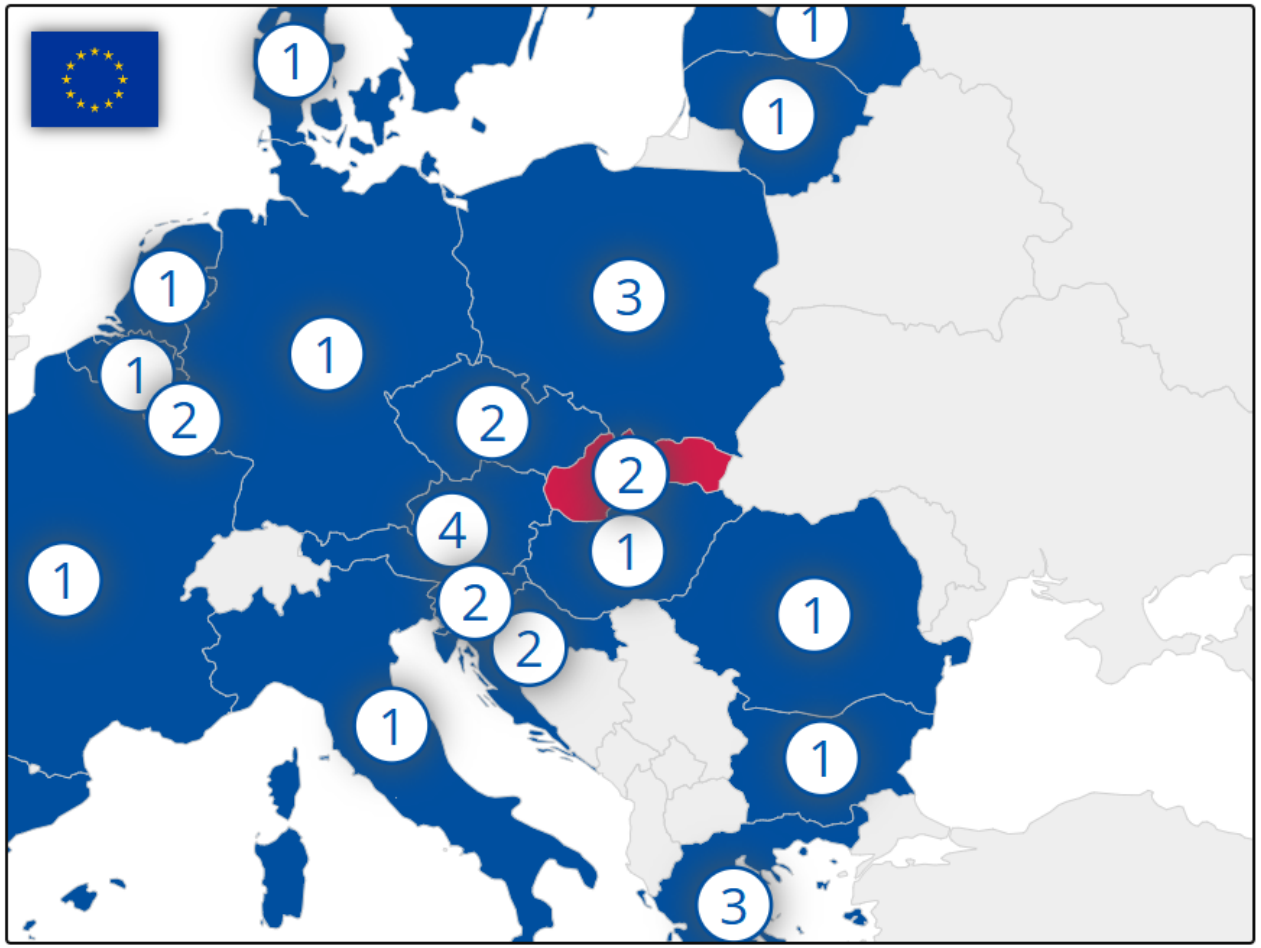
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sieť CSIRT - Computer Security Incident Response Team

- Sieť CSIRT bola zriadená smernicou **NIS** a neskôr posilnená smernicou **NIS2**.
- Cieľom siete je **budovanie dôvery a sebadôvery** a **posilňovanie operačnej spolupráce** medzi členskými štátmi.
- Hlavné činnosti siete:
  - Výmena informácií
  - Koordinácia pri reakcii na incidenty
  - Pomoc členským štátom pri cezhraničných incidentoch
  - Podpora koordinovaného odhaľovania zraniteľností s vplyvom na viac členských štátov
  - Uľahčovanie spolupráce a poskytovanie osvedčených postupov
- **Čo tvorí sieť CSIRT?**
  - Tímy CSIRT vymenované členskými štátmi EÚ
  - CERT-EU
  - Európska komisia ako pozorovateľ
  - Agentúra ENISA:
    - Poskytuje sekretariát siete
    - Aktívne podporuje spoluprácu medzi CSIRT
    - Podporuje koordináciu incidentov

Sieť CSIRT - Computer Security Incident Response Team

Search by country or CSIRT Team



Slovakia

SK-CERT	CSIRT.SK
www.sk-cert.sk	www.csirt.gov.sk
sk-cert@nbu.gov.sk	incident@csirt.gov.sk
CIIP	Government
National	

EU-CyCIONe - European Cyber Crisis Liaison Organisation Network

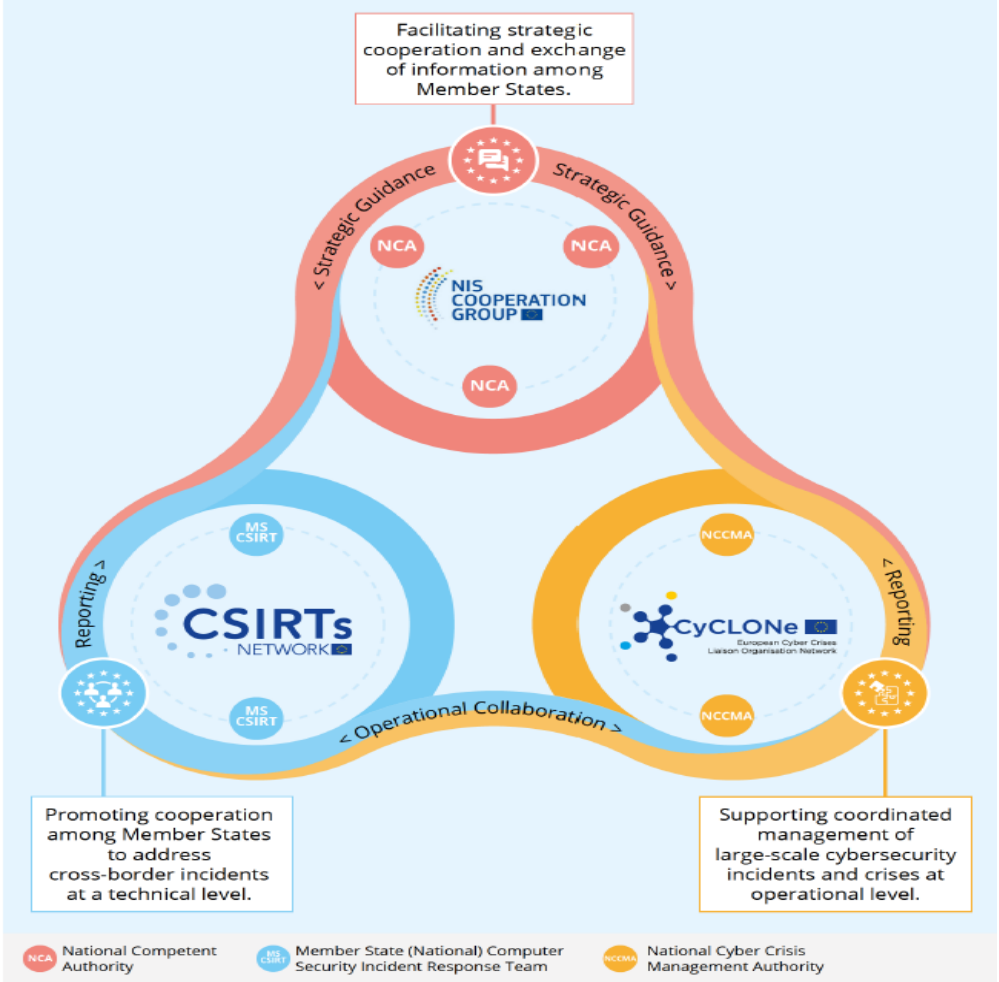
- Čo je EU-CyCLONe? - Európska sieť styčných organizácií pre kybernetické krízy
  - Sieť EÚ na koordináciu reakcie na veľké kybernetické incidenty.
  - Funguje na strategicko-operačnej úrovni.
  - Pomáha pri rozhodovaní medzi národnými orgánmi kybernetickej bezpečnosti.
- Hlavné úlohy
  - Strategická koordinácia medzi členskými štátmi.
  - Podpora pri rozhodovaní na vládnej úrovni.
  - Výmena informácií medzi CSIRT a strategickými orgánmi.
  - Synchronizácia národných opatrení v reakcii na incidenty.
  - Zvyšovanie pripravenosti a odolnosti voči kybernetickým hrozbám.

Vzťah EU-CyCLONe, CSIRT a ENISA

- **Vzťah s CSIRT, EU-CyCLONe a ENISA**
  - CSIRT rieši incidenty na technickej úrovni.
  - EU-CyCLONe sa zameriava na strategické rozhodovanie a koordináciu.
  - ENISA poskytuje odbornú podporu a plánovanie.

- **Členovia siete**
  - Predstavitelia národných kybernetických bezpečnostných agentúr.
  - Európska komisia a ENISA ako podporné inštitúcie.

- **Podpora koordinovaného zverejňovania zraniteľností (CVD - Coordinated Vulnerability Disclosure) agentúrou ENISA**
  - Proces zodpovedného nahlasovania zraniteľností pred ich verejným zverejnením.
  - Hlásia ho bezpečnostní výskumníci, etickí hackeri alebo organizácie.
    - Cieľ: poskytnúť čas na opravu a minimalizovať riziko zneužitia.
    - Zahrnuté v smernici NIS 2, ktorá zaväzuje štáty k efektívnym opatreniam.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Národný bezpečnostný úrad a kybernetická bezpečnosť

- **Národný bezpečnostný úrad (NBÚ)** – kľúčový orgán pre riadenie kybernetickej bezpečnosti v SR
- **Hlavné úlohy NBU**:
  - Riadenie a metodická podpora – stanovuje štandardy, operačné postupy a zásady prevencie kybernetických incidentov
  - Stratégia a krízové riadenie – vypracúva Národnú stratégiu kybernetickej bezpečnosti, zabezpečuje reakciu na kybernetické krízy
  - Medzinárodná spolupráca – národný kontaktný bod, výmena informácií s EÚ, zastúpenie v CSIRT sieti
  - Spolupráca na národnej úrovni – štátna správa, CSIRT jednotky, prevádzkovatelia základných služieb, akademické inštitúcie
  - Dohľad a audity – kontrola dodržiavania pravidiel, audity, vydávanie certifikátov kybernetickej bezpečnosti
  - Reakcia na kybernetické hrozby – koordinovaná odpoveď na incidenty, varovania, výstrahy, stav kybernetickej krízy

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

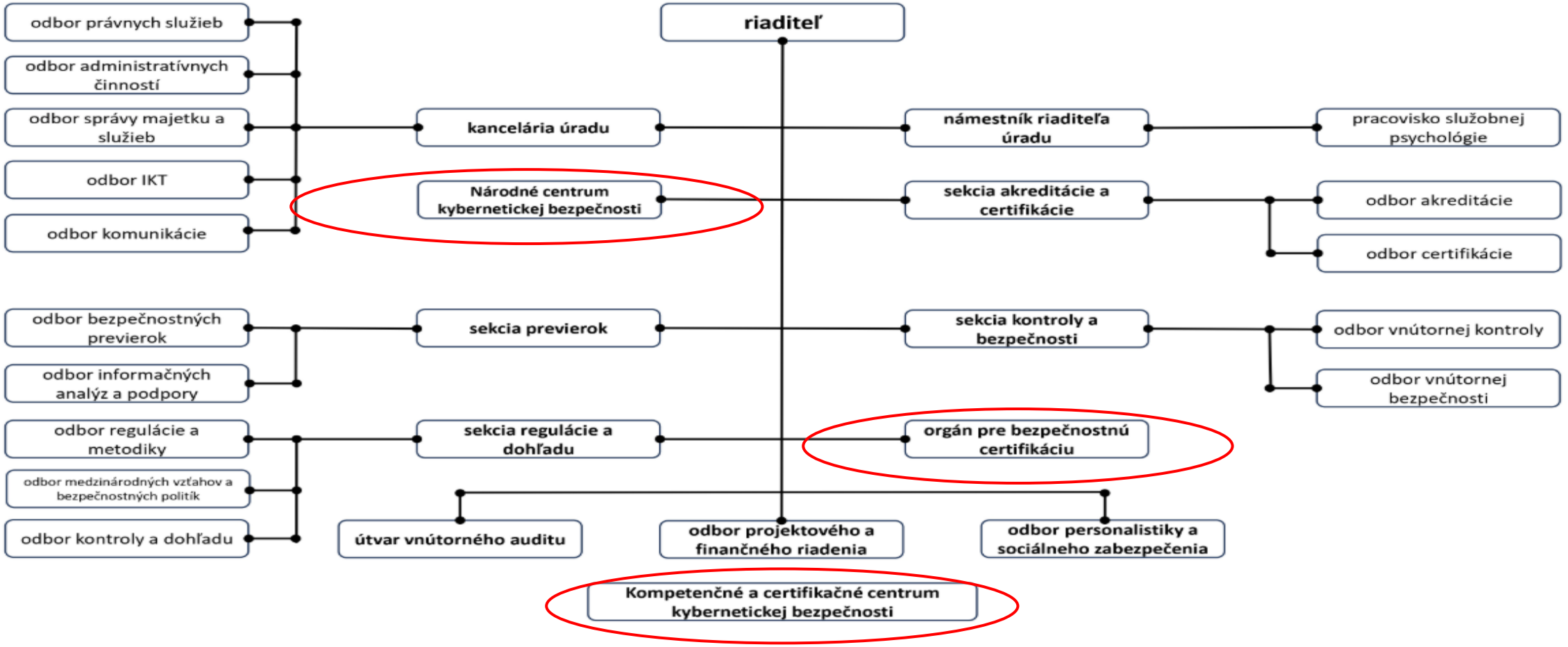
Zadajte hľadaný výraz

ÚRAD | OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ | ŠIFROVÁ OCHRANA INFORMÁCIÍ | DÔVERYHODNÉ SLUŽBY | KYBERNETICKÁ BEZPEČNOSŤ

- Národná stratégia a akčný plán kybernetickej bezpečnosti
- Jednotný informačný systém kybernetickej bezpečnosti
- Hlásenie kybernetických bezpečnostných incidentov
- Národná jednotka CSIRT
- Prevádzkovatelia základných služieb
- Metodiky
- Akreditácia jednotky CSIRT
- Bezpečnostné opatrenia
- Riadenie rizík
- Certifikácia
- NCCA - Národná autorita pre certifikáciu kybernetickej bezpečnosti
- Audit
- Krátky slovník hybridných hrozieb
- Organizácie a partneri
- Samohodnotenie účinnosti prijatých bezpečnostných opatrení v zmysle zákona o kybernetickej bezpečnosti

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

NBU organizačná štruktúra

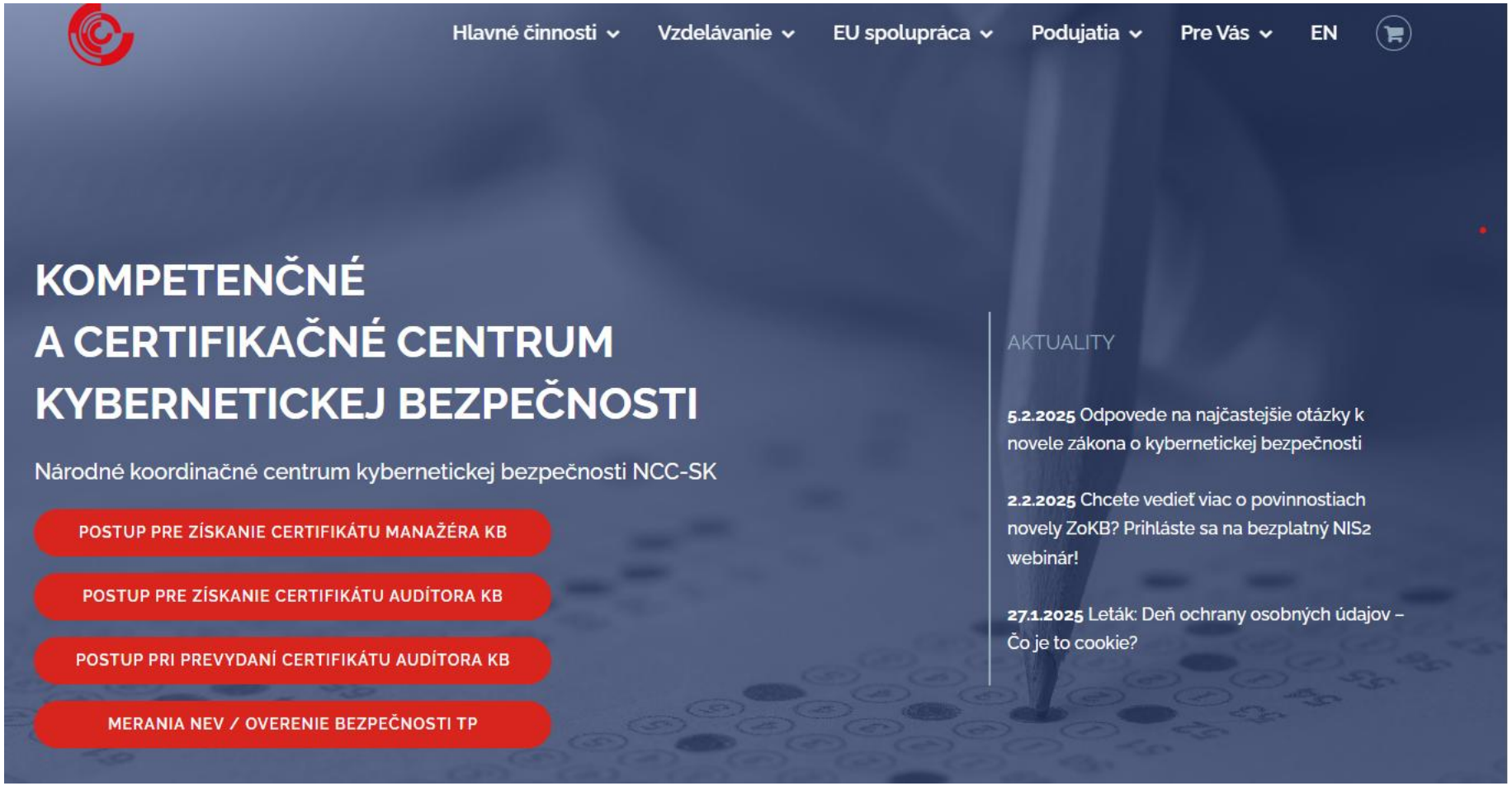


SK-CERT - Národné centrum kybernetickej bezpečnosti SK-CERT

- 1. septembra 2019 bola Národná jednotka kybernetickej bezpečnosti transformovaná na Národné centrum kybernetickej bezpečnosti SK-CERT

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

- príspevková organizácia úradu



CSIRT.SK

O nás | Služby | Naše publikácie | Metodiky a návody | Legislatíva | FAQ

O nás

CSIRT.SK (Computer Security Incident Response Team Slovakia) je vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike podľa zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov zriadená ako organizačný útvar Ministerstva investícií, regionálneho rozvoja a informatizácie SR (MIRRI SR).

Historicky bola zriadená uznesením vlády SR č. 479/2009 z 1. júla 2009 v súlade s Národnou stratégiou pre informačnú bezpečnosť v Slovenskej republike (uznesenie vlády SR č. 570/2008) a do delimitácie na UPPVII SR (v súčasnosti MIRRI SR) v apríli 2018 vykonávala činnosti národnej a vládnej jednotky CSIRT ako špecializovaný útvar DataCentra.

CSIRT.SK, ako vládna jednotka CSIRT, poskytuje služby prevažne štátnej a verejnej správe za účelom reakcie na bezpečnostné incidenty namierené na Informačné technológie verejnej správy (IT VS) (s výnimkou incidentov týkajúcich sa utajovaných skutočností).

Ciele

CSIRT.SK je zriadený ako samostatný odbor na Ministerstve investícií, regionálneho rozvoja a informatizácie SR a zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci celej IT VS. Poskytuje aj služby preventívneho a vzdelávacieho charakteru.

K hlavným cieľom CSIRT.SK patrí:

1. riešenie kybernetických bezpečnostných incidentov v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí IT VS , telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy),
2. budovanie a rozširovanie povedomia verejnosti vo vybraných oblastiach informačnej, resp. kybernetickej bezpečnosti,
3. kooperácia s partnerskými organizáciami a združeniami v oblasti kybernetickej bezpečnosti na národnej a medzinárodnej úrovni.

Viac informácií nájdete na podstránke **RFC 2350**

Nahlásiť incident | Nahlásiť zraniteľnosť

Registrácia Achilles | Registrácia Pentest

Registrácia CTF | Registrácia školenie

Centrálny portál kybernetickej bezpečnosti

Aktuality

February 21, 2025
Otvorené pozície CSIRT.SK

February 17, 2025
Mesačný prehľad kritických zraniteľností január 2025

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Princíp samoidentifikácie subjektu

Subjekt musí spadať pod kritériá uvedené v § 17 alebo § 18 zákona o kybernetickej bezpečnosti v spojení s prílohou č. 1 alebo prílohou č. 2 zákona o kybernetickej bezpečnosti

Subjekt sa musí podľa týchto príloh aj identifikovať ako typ subjektu

SEKTORY S VYSOKOU ÚROVŇOU KRITICKOSTI

Sektor	Podsektor	Typ subjektu	Ustredný orgán	Poznámka
1. Energetika	a) elektrická energia	**elektroenergetické podniky** - každá osoba, ktorá vykonáva aspoň jednu z týchto činností: výroba, prenos, distribúcia, dodávka alebo nákup elektriny a ktorá je v súvislosti s týmito činnosťami zodpovedná za obchodné a technické úlohy alebo údržbu; nezahŕňa však koncových odberateľov, ktorí vykonávajú predaj elektriny odberateľom vrátane jej ďalšieho predaja	Ministerstvo hospodárstva Slovenskej republiky	zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov zákon č. 251/2012 Z. z. o energetike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov zákon č. 321/2014 Z. z. o energetickej efektívnosti a o zmene a doplnení niektorých zákonov v znení

Identifikácia PZS

- Prevádzkovateľom základnej služby sa identifikuje podľa:
  - podľa § 17 Zákona o kybernetickej bezpečnosti - PZS
  - podľa § 17 Zákona o kybernetickej bezpečnosti - PKZS

SEKTORY S VYSOKOU ÚROVŇOU KRITICKOSTI (príloha 1)	INÉ KRITICKÉ SEKTORY (príloha 2)
Energetika (vykurovanie, chladenie, vodík)	**Poštové a kuriérske služby**
Doprava	Odpadové hospodárstvo
Financie	**Výroba a distribúcia chemických látok**
Zdravotníctvo	Výroba a distribúcia spracovanie potravín
Voda a atmosféra (odpadová voda)	Výroba (zdrav. pomôcky, elektro, výpočtová technika, optika, stroje a zariadenia, motorové vozidlá, iné dopr. prostriedky)
Digitálna infraštruktúra	**Poskytovatelia digitálnych služieb**
Riadenie služieb IKT	Výskum
Verejná správa	
Vesmír	

HRANIČNÉ HODNOTY *(článok 2)*

Kategória podniku	Počet pracovníkov: ročná pracovná jednotka (RPJ)	Ročný obrat	alebo	Celková ročná bilančná suma
Stredné podniky	< 250	≤ 50 miliónov EUR	alebo	≤ 43 miliónov EUR
Malé podniky	< 50	≤ 10 miliónov EUR	alebo	≤ 10 miliónov EUR
Mikropodniky	< 10	≤ 2 milióny EUR	alebo	≤ 2 mil. EUR

Základné lehoty pre prevádzkovateľa základnej služby

Jednotný informačný systém

- **Správa a prevádzka:**
  - Systém je spravovaný a prevádzkovaný úradom
  - Zabezpečuje efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a CSIRT
- **Funkcie systému:**
  - Spracovanie a vyhodnocovanie údajov
  - Komunikačný a varovný systém
  - Obsahuje komunikačný kanál pre hlásenie a riešenie incidentov a centrálny systém včasného varovania
- **Štruktúra systému:**
  - Verejná Časť:
    - Register ústredných orgánov
    - Register prevádzkovateľov základnej služby
    - Zoznam akreditovaných jednotiek CSIRT
    - Metodiky, usmernenia, štandardy, politiky a oznamy
    - Informácie, výstrahy a varovania
    - Nástroj na registráciu a hlásenie zmien
- **Neverejná časť**
  - Interné procesy a doplňujúce nástroje (prístup bezodplatný pre oprávnené subjekty).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Kybernetická bezpečnosť vo verejnej správe

Úvod do KB (Blok I)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Katarina.Kampova@uniza.sk