KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kybernetická bezpečnosť vo verejnej správe

Pavol Sokol

KCKB UPJS CSIRT UPJS

Bezpečnosť verejnej správy (I.)

košice:dnes

Košice

18.02.2022 | 13:30

Za útok na počítačové siete Úradu KSK môžu hackeri, potvrdilo to CSIRT

Košický samosprávny kraj po predošlom útoku prijal opatrenia, vďaka ktorým zvyšuje kybernetickú bezpečnosť. Vyšetrenie Národného bezpečnostného úradu a vládnej jednotky pre riešenie počítačových incidentov (CSIRT) ukázalo, že za znefunkčnením informačných systémov sú práve hackeri.

Zdroj: ilustračné/pixabay.com

Košický samosprávny kraj po predošlom útoku prijal opatrenia, vďaka ktorým zvyšuje kybernetickú bezpečnosť. Vyšetrenie Národného bezpečnostného úradu a vládnej jednotky pre riešenie počítačových incidentov (CSIRT) ukázalo, že za znefunkčnením informačných systémov sú práve hackeri. **V súčasnosti sú informačné weby plne funkčné.**

aktuality.sk

Predplatné

Zdieľať článok | Diskusia / 32 | Uložiť článok

navyše Slovensko | 12. jan. 2025 o 19:15

Útok na kataster: Hlavný systém nepôjde ešte dlho, do riešenia zapojili zahraničných expertov

Útok

Útok na kataster (ilustračná fotografia)
Zdroj: iStock / redakcia

redakcia Živé.sk

Samuel Migaľ
about 4 months ago

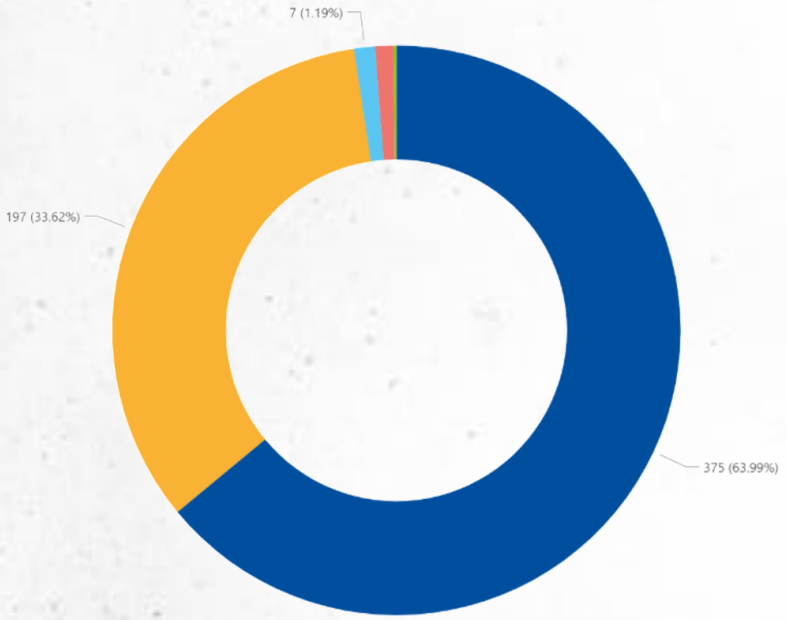
Vládna kybernetická jednotka CSIRT v spolupráci s SK-CERT zasahuje na Ministerstve hospodárstva SR, pre kybernetický útok na servery ministerstva. Momentálne nemôžeme informovať bližšie, aby sme neohrozili prebiehajúce vyšetrovanie.

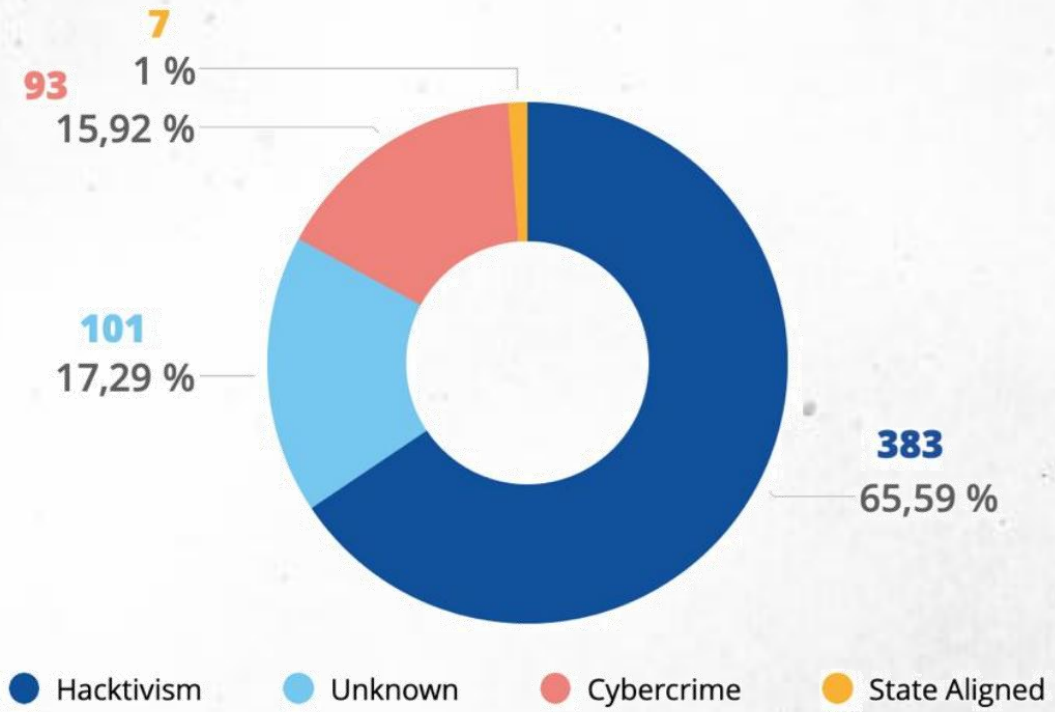
22 52 Share

Zdroj: https://www1.pluska.sk/spravy/kyberneticky-utok-ministerstvo-hospodarstva-v-ohrozeni-co-bude-dalej, https://www.aktuality.sk/clanok/cnFY4sp/utok-na-kataster-hlavny-system-nepojde-este-dlho-do-riesenia-zapojili-zahranicnych-expertov/,, https://kosicednes.sk/spravy/za-utok-na-pocitacove-siete-uradu-ksk-mozu-hackeri-potvrdilo-to-csirt/

Bezpečnosť verejnej správy (II.)

- typy hrozieb pozorované v sektore verejnej správy v EÚ v roku 2024
- kľúčoví útočníci zaznamenaní ako aktívni proti sektoru verejnej správy v EÚ v roku 2024

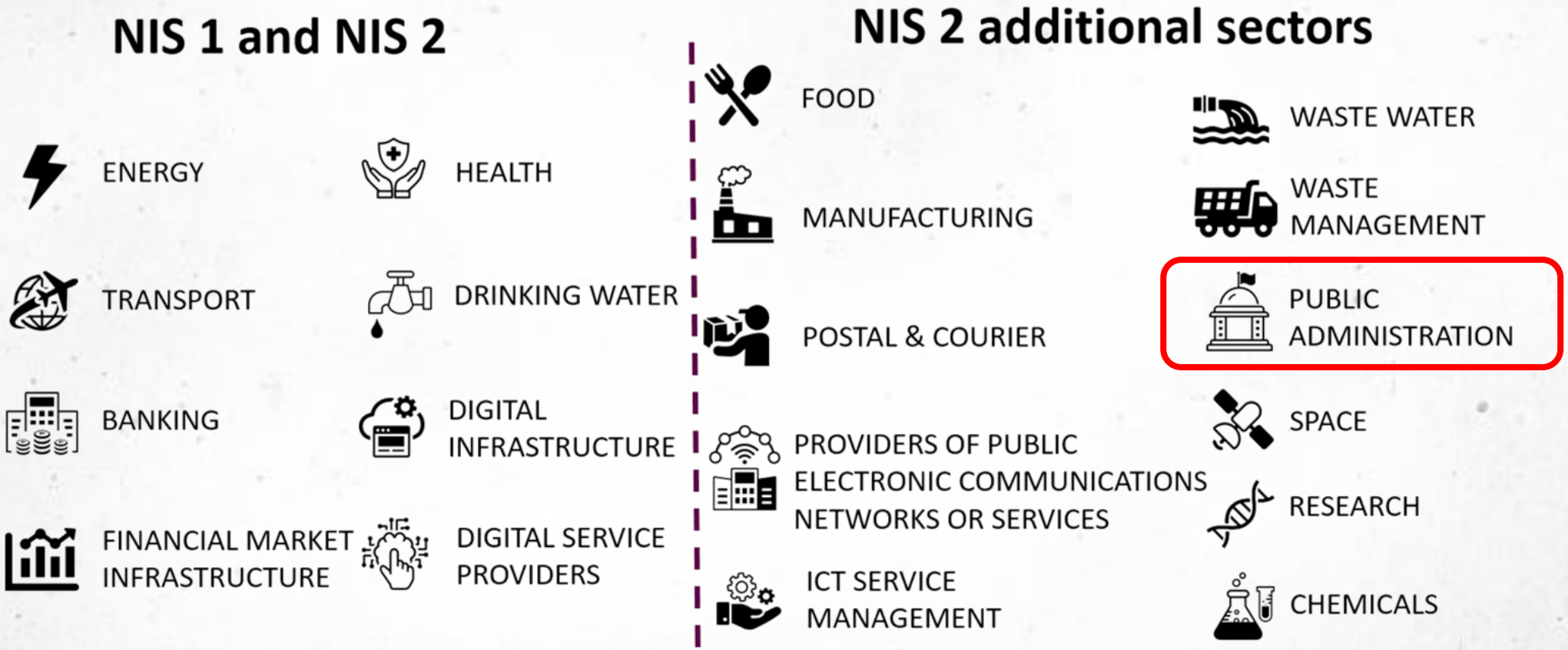




Zdroj: European Union Agency for Cybersecurity (ENISA). (2025). *ENISA sectorial threat landscape: Public administration 2024* (Version 1.2). https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf

Sektor verejnej správy (I.)

- smernica NIS2 – pridanie sektora verejnej správy
- sektor verejnej správy – v SR už od 2018



Zdroj: https://www.fieldfisher.com/en-be/locations/belgium/insights/nis2-directive

Sektor verejnej správy (II.)

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti – príloha č. 1 – sektory s vysokou úrovňou kritickosti

Sektor	Podsektor	Typ subjektu	Ústredný orgán	Poznámka
8.1 Verejná správa		**subjekty verejnej správy na úrovni ústredného orgánu štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou**	Ministerstvo vnútra Slovenskej republiky	zákon č. 302/2001 Z. z. o samospráve vyšších územných celkov (zákon o samosprávnych krajoch) v znení neskorších predpisov zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov zákon č. 596/2003 Z. z. o štátnej správe v školstve a školskej samospráve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
		subjekty verejnej správy na regionálnej úrovni okrem oblasti finančnej správy		

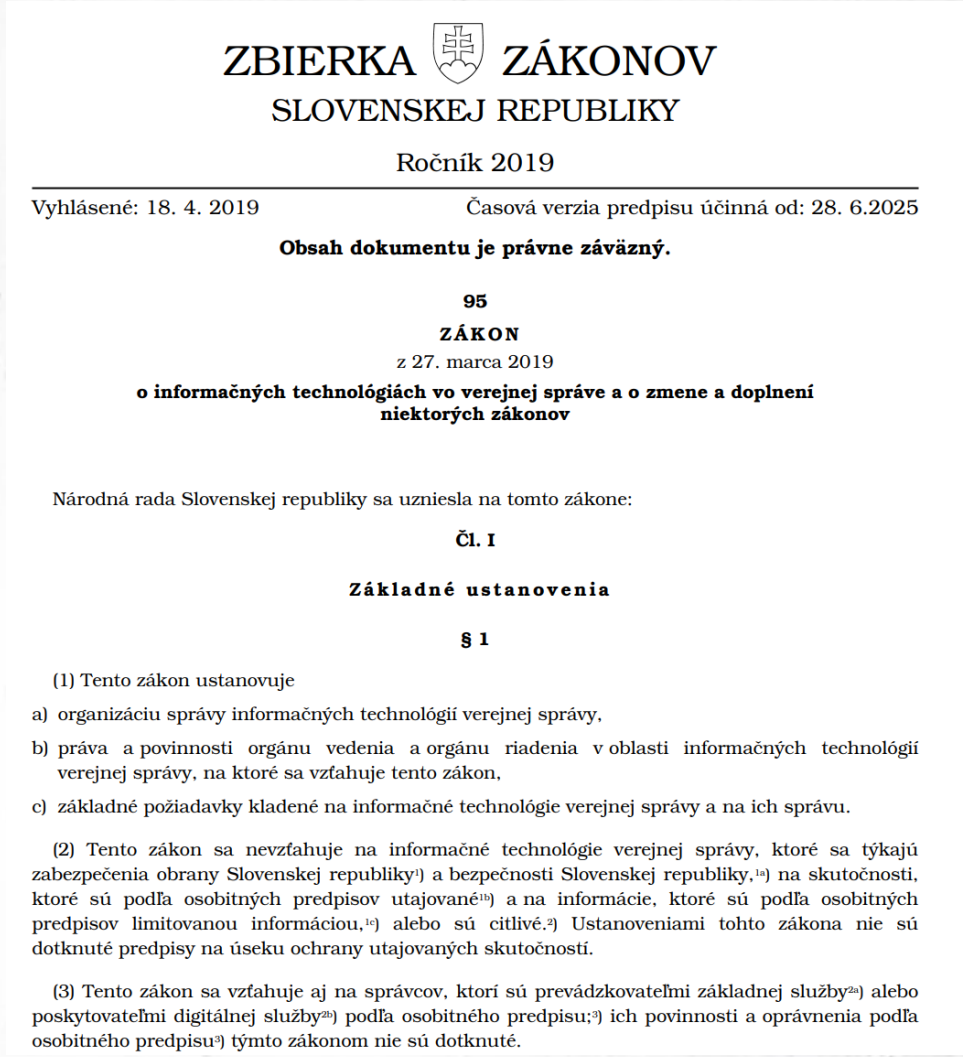
Sektor verejnej správy (III.)

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti – príloha č. 1 – sektory s vysokou úrovňou kritickosti

Sektor	Podsektor	Typ subjektu	Ústredný orgán	Poznámka
8.2 Verejná správa		**subjekty verejnej správy na úrovni ústredného orgánu štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou pre oblasť finančnej správy**	Ministerstvo financií Slovenskej republiky	zákon č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
		subjekty verejnej správy na regionálnej úrovni pre oblasť finančnej správy		
8.3 Verejná správa		**správcovia a prevádzkovatelia informačných systémov verejnej správy** podporujúcich služby verejnej správy, služby vo verejnom záujme a verejné služby podľa zákona č. 95/2019 Z. z.	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky	zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon o ITVS (I.)

- **zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a** o zmene a doplnení niektorých zákonov (**ZoITVS**)
- je sektorová právna úprava (lex specialis)
- cieľom zákona o ITVS je komplexné a jednotné riadenie IT - od plánovania a organizácie cez implementáciu a prevádzku až po monitoring a hodnotenie
- zákon sa nezameriava výlučne na kybernetickú bezpečnosť, ale na celý životný cyklus riadenia ITVS
- ustanovuje jednotné vedenie a riadenie IT vo verejnej správe



ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2019

Vyhlásené: 18. 4. 2019 Časová verzia predpisu účinná od: 28. 6.2025

Obsah dokumentu je právne záväzný.

95

ZÁKON

z 27. marca 2019

o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

Základné ustanovenia

§ 1

(1) Tento zákon ustanovuje

a) organizáciu správy informačných technológií verejnej správy,

b) práva a povinnosti orgánu vedenia a orgánu riadenia v oblasti informačných technológií verejnej správy, na ktoré sa vzťahuje tento zákon,

c) základné požiadavky kladené na informačné technológie verejnej správy a na ich správu.

(2) Tento zákon sa nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky[1]) a bezpečnosti Slovenskej republiky,[1a]) na skutočnosti, ktoré sú podľa osobitných predpisov utajované[1b]) a na informácie, ktoré sú podľa osobitných predpisov limitovanou informáciou,[1c]) alebo sú citlivé.[2]) Ustanoveniami tohto zákona nie sú dotknuté predpisy na úseku ochrany utajovaných skutočností.

(3) Tento zákon sa vzťahuje aj na správcov, ktorí sú prevádzkovateľmi základnej služby[2a]) alebo poskytovateľmi digitálnej služby[2b]) podľa osobitného predpisu;[3]) ich povinnosti a oprávnenia podľa osobitného predpisu[3]) týmto zákonom nie sú dotknuté.

Vykonávacie právne predpisy

Vykonávacie právne predpisy:

- Vyhláška ÚPVII **č. 78/2020 Z. z.** o štandardoch pre informačné technológie verejnej správy,
- Vyhláška ÚPVII **č. 179/2020 Z. z.**, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- Vyhláška MIRRI **č. 333/2022 Z. z.** o elektronizácii agendy verejnej správy,
- Vyhláška MIRRI **č. 401/2023 Z. z.** o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

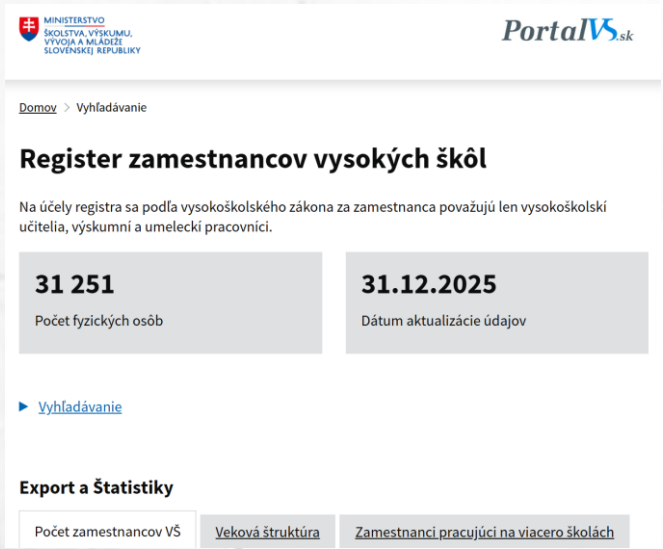
Informačná technológia

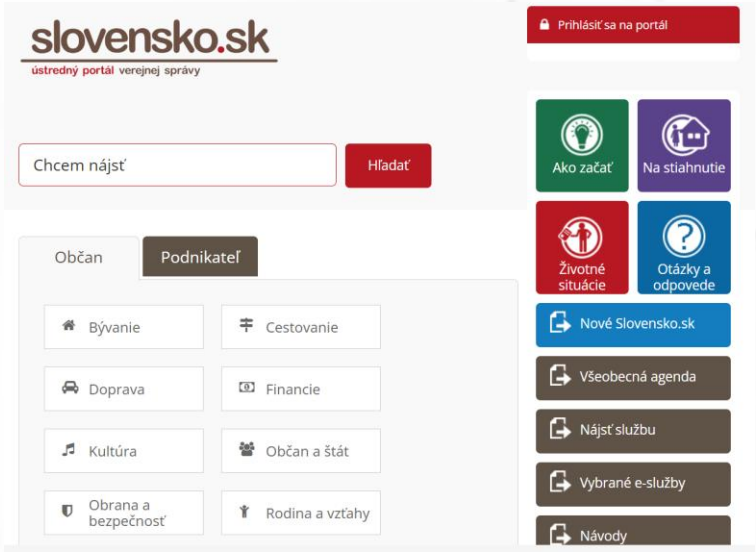
- **Informačná technológia (IT)**
  - prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby (§ 2 ods. 1 ZoITVS)

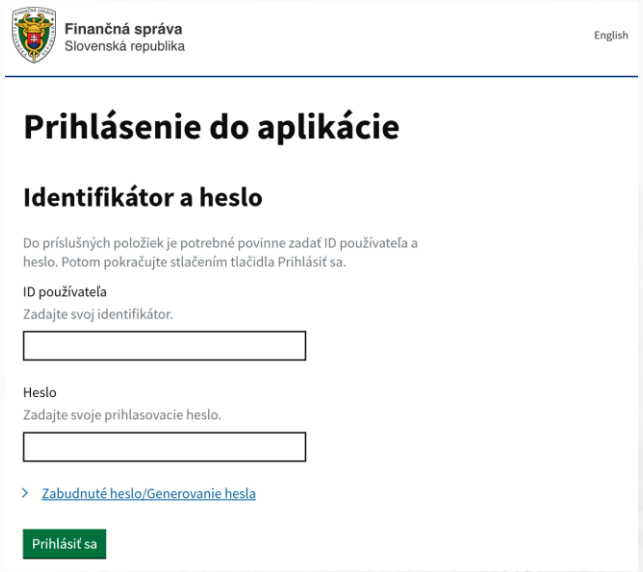
- **Informačná technológia verejnej správy (ITVS)**
  - informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe (§ 2 ods. 3 ZoITVS)

Informačný systém

- **Informačný systém**
  - funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov (§ 2 ods. 2 ZoITVS)
- **Informačný systém verejnej správy**
  - informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby (§ 2 ods. 4 ZoITVS)







Zdroj: https://www.slovensko.sk/sk/titulna-stranka, https://www.portalvs.sk/regzam/, https://pfs.iam.financnasprava.sk/PREZ/idp/authn/lp?authnGuid=4b2f1717-ffb4-4698-a959-4ea38529fc66

Subjekty (I.)

Subjekty podľa ZoITVS:

- Správu informačných technológií verejnej správy vykonávajú:
  - **orgán vedenia**, ktorým je MIRRI
  - **orgán riadenia** vo vzťahu k informačným technológiám verejnej správy v jeho pôsobnosti

- **Správca ITVS**
- **Prevádzkovateľ ITVS**

- **Vládna jednotka CSIRT**

Subjekty (II.)

- **Orgán riadenia** vo vzťahu k informačným technológiám verejnej správy v jeho pôsobnosti
  - **ministerstvo** a ostatný **ústredný orgán** štátnej správy,
  - Generálna prokuratúra SR, NKÚ SR, Úrad pre dohľad nad zdravotnou starostlivosťou, ÚOOÚ SR, ...
  - **obec a vyšší územný celok**,
  - Kancelária NRSR, Kancelária prezidenta SR, Kancelária Ústavného súdu SR, Kancelária Najvyššieho súdu SR, Kancelária Najvyššieho správneho súdu SR, Sociálna poisťovňa, zdravotné poisťovne, TASR, RTVS,
  - **právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti** orgánu riadenia uvedeného vyššie
  - **komora** regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,
  - **osoba neuvedená vyššie**, na ktorú je **prenesený výkon verejnej moci** alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,
  - záujmové združenie právnických osôb **DataCentrum** elektronizácie územnej samosprávy Slovenska,

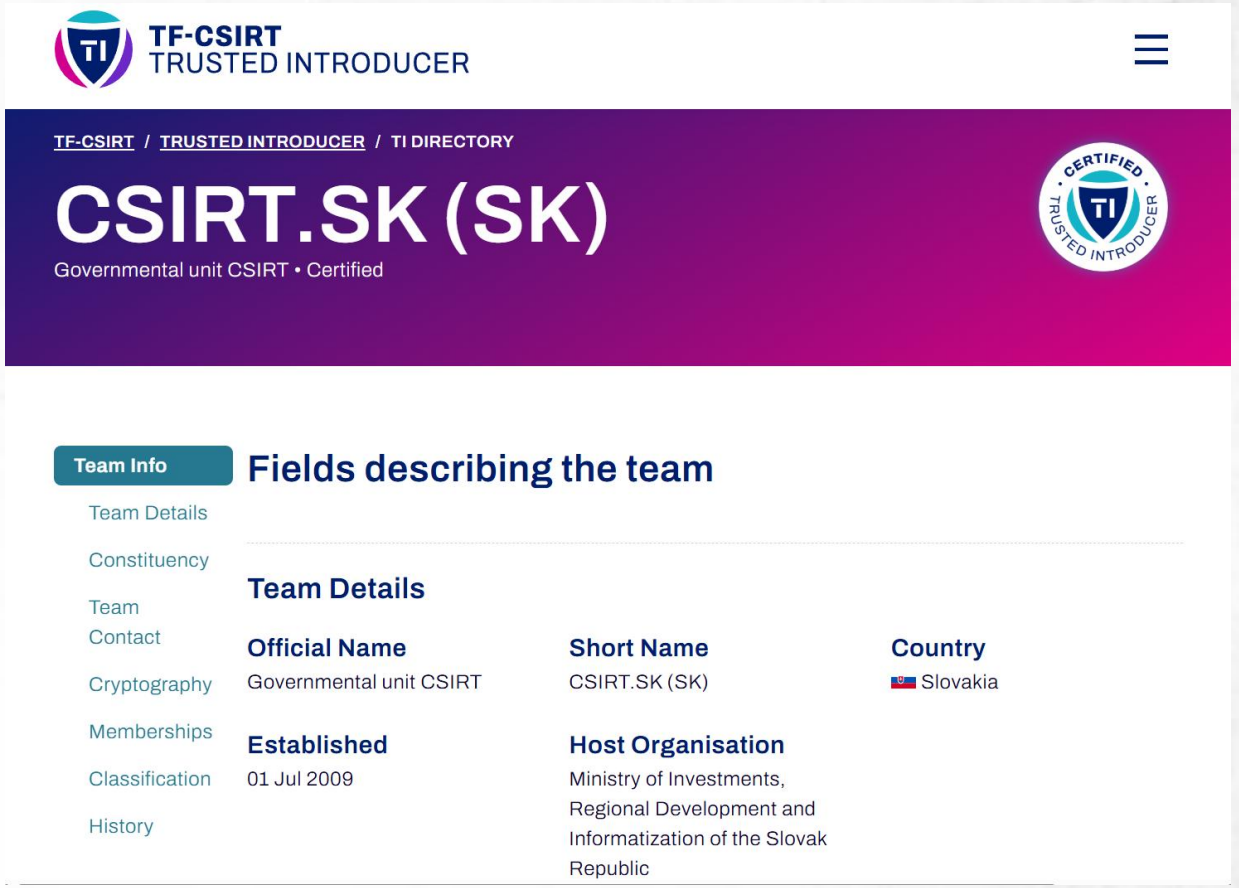
Subjekty (III.)

- **Správca ITVS** (§ 2 ods. 5 ZoITVS)
  - je ten orgán riadenia, ktorého za správcu ITVS ustanoví zákon alebo je ustanovený na základe ZoITVS.
  - ak zákon vo vzťahu k ITVS správcu neustanovuje, je správcom na účely ZoITVS ten orgán riadenia, ktorý ITVS používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby
  - ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.

- **Prevádzkovateľ ITVS** (§ 2 ods. 3 ZoITVS)
  - osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba.
  - správcom určený alebo osobitným predpisom ustanovený prevádzkovateľ vykonáva, v rozsahu povinností správcu, činnosti, ktoré mu určí správca alebo ustanoví tento osobitný predpis
  - ak tento osobitný predpis rozsah činností prevádzkovateľa neustanovuje, vykonáva ich v celom rozsahu činností správcu.
  - určením alebo ustanovením prevádzkovateľa nie je dotknutá zodpovednosť správcu za plnenie povinností podľa ZoITVS

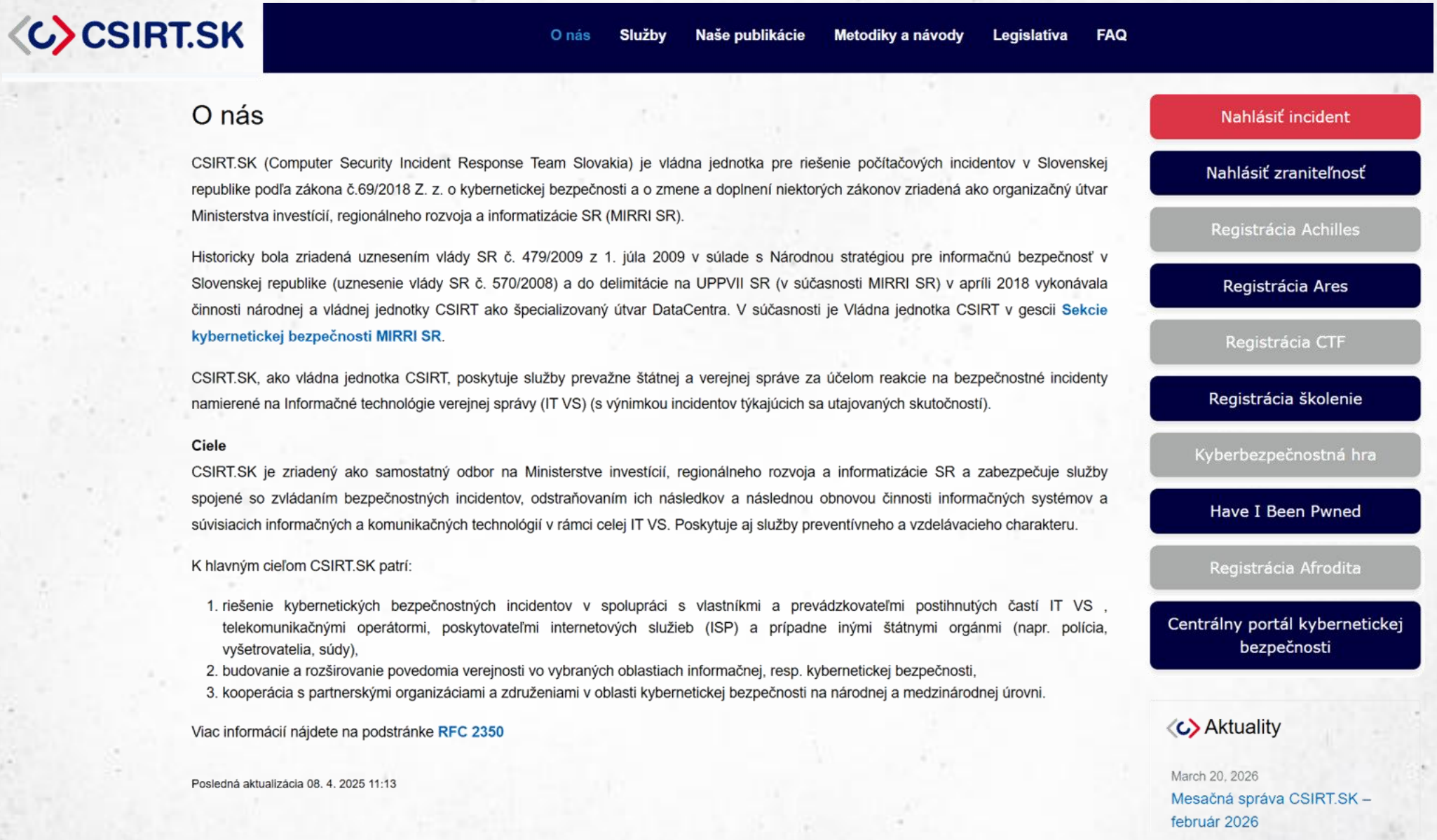
Vládna jednotka CSIRT (I.)

- **Vládna jednotka CSIRT (§ 11 ZoKB)**
  - CSIRT.SK
  - v pôsobnosti MIRRI
  - zaraďuje do zoznamu akreditovaných jednotiek CSIRT.



Zdroj: https://www.trusted-introducer.org/trusted-introducer/directory/teams/csirtsk-sk/

Vládna jednotka CSIRT (II.)



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. V súčasnosti je Vládna jednotka CSIRT v gescii **Sekcie kybernetickej bezpečnosti MIRRI SR**.

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**

Posledná aktualizácia 08. 4. 2025 11:13

Nahlásiť incident
Nahlásiť zraniteľnosť
Registrácia Achilles
Registrácia Ares
Registrácia CTF
Registrácia školenie
Kyberbezpečnostná hra
Have I Been Pwned
Registrácia Afrodita
Centrálny portál kybernetickej bezpečnosti

Aktuality

March 20, 2026
Mesačná správa CSIRT.SK – február 2026

Vládna jednotka CSIRT (III.)

- Orgán vedenia prostredníctvom **vládnej jednotky CSIRT** (§ 23a ods. 2 ZoITVS)
  - na žiadosť správcu vykonáva činnosti nepretržitého monitorovania ITVS v jeho správe (**monitoring**),
  - vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy ... (**hodnotenie zraniteľností**)
  - s predchádzajúcim súhlasom správcu vykonáva hodnotenie zraniteľnosti služby verejnej správy, ... ktoré boli zistené pri pravidelnom neinvazívnom hodnotení zraniteľnosti (**hodnotenie zraniteľností**)
  - zbiera, spracúva a vyhodnocuje systémové informácie ITVS (**zber aktív**)
  - môže na žiadosť orgánu riadenia vykonávať činnosti na účely riešenia KBI, jeho predchádzania alebo odstraňovania a hodnotenia zraniteľnosti (**reakcia na KBI a zraniteľnosť**).
    - je len sektorový CSIRT, nie interný

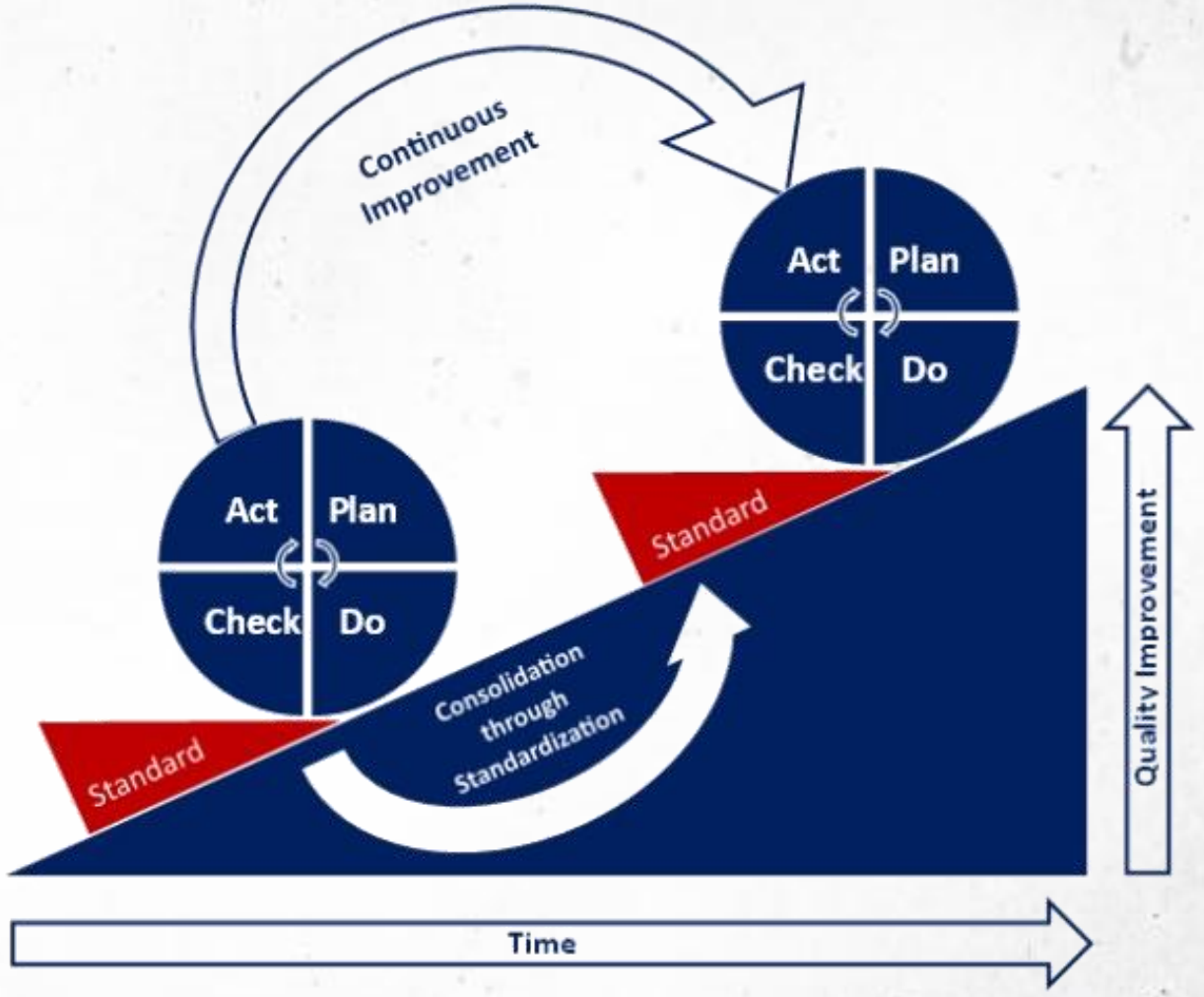
Bezpečnosť ITVS (I.)

- **§ 18 - § 23a ZoITVS**
- Povinnosť správcu, ktorý je prevádzkovateľom základnej služby prijať a realizovať bezpečnostné opatrenia vo vzťahu k ITVS v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov ustanovuje ZoKB (toto už neplatí)
- Správca, ktorý je prevádzkovateľom základnej služby prijíma a realizuje bezpečnostné opatrenia vo vzťahu k ITVS v jeho správe podľa ZoITVS a ZoKB, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje osobitý predpis (čiastočne neplatí, prebiehajúci legislatívny proces)

- § 19 - Bezpečnosť ITVS v oblasti **plánovania a organizácie**
- § 20 - Bezpečnosť ITVS v oblasti **obstarávania a implementácie**
- § 21 - Bezpečnosť ITVS v oblasti **prevádzky, servisu a podpory**
- § 22 - Bezpečnosť ITVS v oblasti **monitoringu a hodnotenia**
- § 23 - **Osobitné opatrenia** na úseku bezpečnosti ITVS
- § 23a - **Vedenie na úseku** bezpečnosti ITVS

Bezpečnosť ITVS (II.)

- § 19 - § 22 ZoITVS
- **PDCA (PLAN-DO-CHECK-ACT) cyklus**



Zdroj: https://www.leanairline.com/blog/standardized-work

Bezpečnosť ITVS (III.)

- **Fáza PLAN**
  - predstavuje základ pre riadenie bezpečnosti informačných technológií verejnej správy
  - zahŕňa definovanie cieľov, rozsahu a organizácie bezpečnosti, ako aj identifikáciu aktív a rizík.
  - § 18 a § 19 ZoITVS.

- § 18 - základná povinnosť správcu prijímať a realizovať bezpečnostné opatrenia
- § 19 ods. 1 písm. a) - rámec riadenia bezpečnosti prostredníctvom definovania cieľov, rozsahu, podmienok a procesov, pričom zahŕňa aj organizačné zabezpečenie, riadenie aktív a rizík,
- § 19 ods. 2 - schvaľovanie opatrení vyplývajúcich z incidentov, analýz, auditov a kontrol,
- § 19 ods. 5 - dodržiavanie bezpečnostnej stratégie, určenie zodpovednej osoby a identifikácia rizík prostredia
- § 23 - identifikácia kritických systémov, evidenciu aktív, reporting a pravidlá pre oznamovanie zraniteľností.

Bezpečnosť ITVS (IV.)

- **Fáza DO**
  - zahŕňa implementáciu navrhnutých bezpečnostných opatrení do praxe
  - § 20 a § 21 ZoITVS

- § 20 ods. 1 - povinnosť určiť bezpečnostné požiadavky na ISVS vrátane podmienok jeho vývoja, testovania a dodania, ako aj zabezpečiť vypracovanie bezpečnostnej dokumentácie vrátane bezpečnostného projektu.
- § 20 ods. 2 - požiadavky na bezpečné vývojové prostredie, dokumentáciu vývoja a testovania, povinnosť mlčanlivosti dodávateľa ...
- § 21 - zavedenie, prevádzku a vyradenie ISVS
- § 23 - prijímanie bezpečnostných opatrení na základe testovania, hodnotenia zraniteľností a incidentov, ako aj o povinnosti súvisiace s ich hlásením.

Bezpečnosť ITVS (V.)

- **Fáza CHECK**
  - je zameraná na overovanie účinnosti bezpečnostných opatrení.
  - § 21 - § 23 ZoITVS

- § 21 ods. 3 - zabezpečenie monitorovania informačných systémov, riadenie konfigurácie a vykonávanie kontrolných a auditných činností.
- § 22 - povinnosť pravidelného monitorovania, testovania a hodnotenia bezpečnosti informačných systémov podľa osobitného predpisu.
- § 23 ods. 5 - evidencia incidentov a realizáciu bezpečnostných opatrení na základe ich vyhodnotenia.
- § 23a ods. 2 - vykonávanie činností na riešenie bezpečnostných incidentov, prevenciu, ako aj hodnotenie zraniteľností.

Bezpečnosť ITVS (VI.)

- **Fáza ACT**
  - predstavuje prijímanie nápravných a preventívnych opatrení. Vychádza z výsledkov monitorovania a auditov.
  - § 19, §21, §23, §23a ZoITVS

- § 19 ods. 2 - prijímanie a schvaľovanie opatrení na základe závažných bezpečnostných incidentov, analýz, auditov a kontrol s cieľom minimalizovať ich opätovný výskyt.
- § 23 ods. 1 - bezpečnostný projekt ako základný nástroj riadenia bezpečnosti
- § 21 ods. 4 - bezpečné vyradenie informačných systémov z prevádzky ako súčasť životného cyklu.
- § 23a - metodické usmerňovanie, zvyšovanie povedomia a vykonávanie činností na riešenie incidentov a hodnotenie zraniteľností.

Bezpečnostné opatrenia (I.)

- Vyhláška ÚPVII **č. 179/2020 Z. z.**, ktorou sa ustanovuje spôsob kategorizácie a obsah **bezpečnostných opatrení** informačných technológií verejnej správy,
  - Aktuálne prebieha legislatívny proces – vyhláška bude nahradená novou vyhláškou

- Bezpečnostné opatrenia informačných technológií verejnej správy tvoria minimálne bezpečnostné opatrenia troch kategórií pre jednotlivé oblasti

- **Minimálne bezpečnostné opatrenia**
  - upravuje príloha č. 2 Vyhlášky 179/2020 Z. z.
  - sú rozdelené do Kategórie I, Kategórie II a Kategórie III v rámci jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti.

Bezpečnostné opatrenia (II.)

(2) Minimálne bezpečnostné opatrenia Kategórie I jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na

a) obec do 6000 obyvateľov,

b) obec so štatútom mesta do 6000 obyvateľov,

c) právnickú osobu v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia podľa **§ 5 ods. 2 písm. a) až d) zákona**, ktorá nie je uvedená v odsekoch 3 a 4,

d) osobu podľa **§ 5 ods. 2 písm. g) zákona**,

e) komoru podľa **§ 5 ods. 2 písm. f) zákona**.

(3) Minimálne bezpečnostné opatrenia Kategórie I a Kategórie II jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na

a) obec nad 6000 obyvateľov,

b) obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,[3)]

c) mestskú časť s právnou subjektivitou,[4)]

d) Kanceláriu verejného ochrancu práv,

e) Úrad komisára pre deti,

f) Úrad komisára pre osoby so zdravotným postihnutím,

g) Radu pre vysielanie a retransmisiu,

h) prevádzkovateľa základných služieb podľa osobitného predpisu,[2)] ktorého siete a informačné systémy sú zaradené do Kategórie I alebo Kategórie II podľa osobitného predpisu[1)] neuvedeného v odseku 4.

(4) Minimálne bezpečnostné opatrenia Kategórie I, Kategórie II a Kategórie III jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na

a) obec, ktorá je aj krajským mestom,[3)]

b) samosprávny kraj,

c) ministerstvo a ostatný ústredný orgán štátnej správy,[5)]

d) Úrad pre reguláciu sieťových odvetví,

e) Úrad pre reguláciu elektronických komunikácií a poštových služieb,

f) Najvyšší kontrolný úrad Slovenskej republiky,

g) Úrad pre dohľad nad zdravotnou starostlivosťou,

h) Úrad na ochranu osobných údajov Slovenskej republiky,

i) Generálnu prokuratúru Slovenskej republiky,

j) Dopravný úrad,

k) Ústav pamäti národa,

l) Tlačovú agentúru Slovenskej republiky,

m) Rozhlas a televíziu Slovenska,

n) Kanceláriu Súdnej rady Slovenskej republiky,

o) Kanceláriu Najvyššieho súdu Slovenskej republiky,

p) Kanceláriu Ústavného súdu Slovenskej republiky,

q) Kanceláriu prezidenta Slovenskej republiky,

r) Kanceláriu Národnej rady Slovenskej republiky,

s) Finančné riaditeľstvo Slovenskej republiky,

t) Národnú agentúru pre sieťové a elektronické služby,

u) Zbor väzenskej a justičnej stráže,

v) DataCentrum Ministerstva financií Slovenskej republiky,

w) DataCentrum elektronizácie územnej samosprávy Slovenska,

x) Sociálnu poisťovňu,

y) zdravotnú poisťovňu,

z) Národné centrum zdravotníckych informácií,

aa) prevádzkovateľa základných služieb podľa osobitného predpisu,[2)] ktorého siete a informačné systémy sú zaradené do Kategórie III podľa osobitného predpisu.[1)]

Bezpečnostné opatrenia (III.)

Príklad: G. Hodnotenie zraniteľností a bezpečnostné aktualizácie

- **Kategória I**
  - Nastavenie automatickej aktualizácie operačného systému a aplikácií.

- **Kategória II**
  - V organizácii správcu zaviesť pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.
  - Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.
  - Vykonávanie hodnotenie zraniteľností najmenej raz ročne.
  - ...

- **Kategória III**
  - Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov.
  - Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.

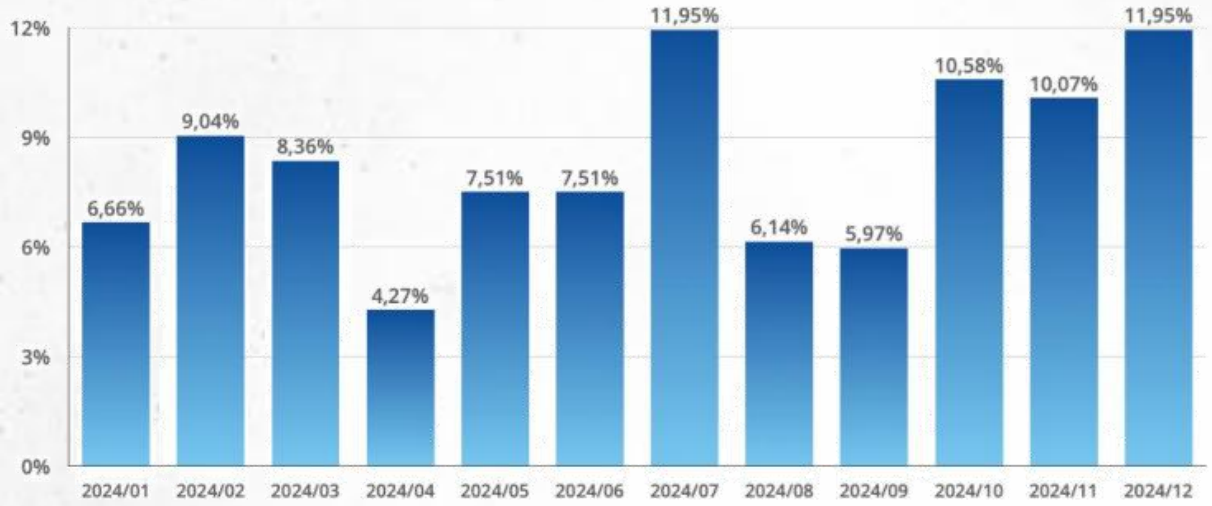
Bezpečnostné opatrenia (IV.)

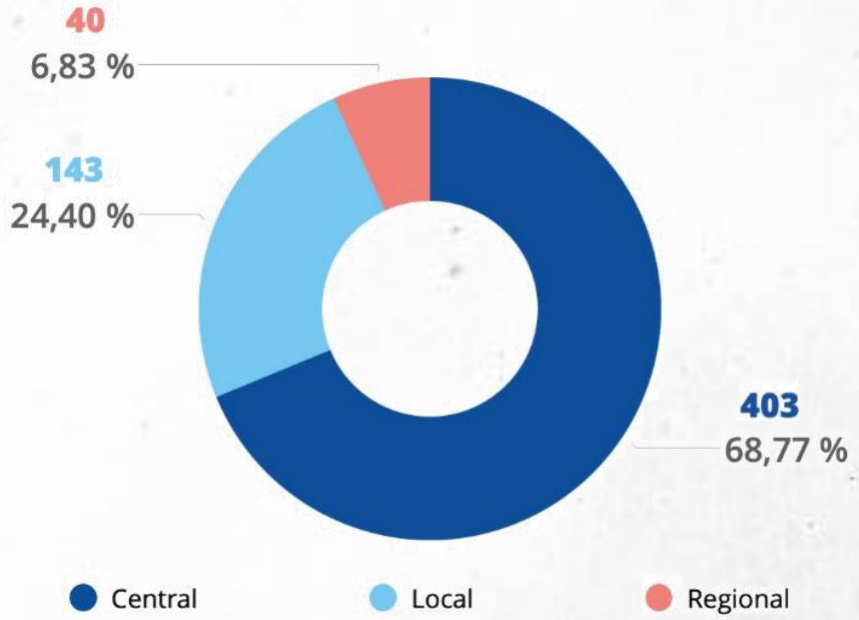
- **nová vyhláška** (v legislatívnom proces)
  - ostávajú minimálne bezpečnostné opatrenia troch kategórií
  - menia sa jednotlivé oblasti (podľa vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach
  - zmena zaradenia subjektov do kategórií

Položka	Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
17.	organizácia získava informácie o zraniteľnostiach všetkých aktív podporujúcich ISVS a ITVS, vrátane hodnotenia do akej miery sú tieto systémy zraniteľné a prijímania vhodných opatrení na ich mitigáciu alebo úplne odstránenie	ÁNO	ÁNO	ÁNO
18.	kontinuálne získava informácie o zraniteľnostiach používaných ISVS a prijíma vhodné opatrenia na ich mitigáciu		ÁNO	ÁNO
19.	najmenej raz ročne je vykonávané pravidelné preskúmanie zraniteľností		ÁNO	
20.	najmenej raz za 6 mesiacov je vykonávané pravidelné preskúmanie zraniteľností			ÁNO
21.	je definovaný a zavedený systém kontroly dostupnosti a inštalovania aktualizácií pre všetky aktíva podporujúce ISVS a ITVS podľa ich technických možností s čo najmenším dosahom na prevádzku systémov organizácie	ÁNO	ÁNO	ÁNO
22.	sú určené priority aktualizácií na základe posúdenia rizík		ÁNO	ÁNO
23.	na webovom sídle sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností			ÁNO

Riešenie incidentov (I.)

- od januára do decembra 2024 ENISA analyzovala celkovo 586 verejne hlásených kybernetických incidentov zameraných na verejnú správu v EÚ.
- incidenty podľa subsektorov verejnej správy v roku 2024





Zdroj: European Union Agency for Cybersecurity (ENISA). (2025). *ENISA sectorial threat landscape: Public administration 2024* (Version 1.2). https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf

Riešenie incidentov (II.)

- **Orgán riadenia** je povinný (§23 ods. 3 ZoITVS):
  - a) ak je zaradený do registra prevádzkovateľov základných služieb nahlasovať cez JISKB aj KBI, na ktorý sa nevzťahuje povinnosť nahlasovania podľa ZoKB
  - b) poskytnúť orgánu vedenia (MIRRI) súčinnosť a spoluprácu pri plnení jeho úloh a plniť jeho pokyny

- **Orgán riadenia,** ktorý **nie je prevádzkovateľom základnej služby** (§23 ods. 5 ZoITVS):
  - nahlasovať KBI vládnej jednotke CSIRT,
  - bezodkladne riešiť KBI a prijať opatrenia na zníženie rizika vyplývajúceho zo zraniteľnosti bezodkladne po tom, ako sa o kybernetickom bezpečnostnom incidente alebo zraniteľnosti dozvedel,
  - poskytnúť orgánu vedenia (MIRRI) súčinnosť a spoluprácu pri plnení jeho úloh a plniť pokyny orgánu vedenia pri výkone jeho oprávnení,
  - viesť evidenciu KBI, postupov na riešenie KBI,
  - určiť a zverejniť na svojom hlavnom webovom sídle kontaktné údaje na kontaktný bod alebo primeraný počet kontaktných bodov na nahlasovanie KBI.

Hodnotenie zraniteľností (I.)

- Orgán riadenia je povinný (§23 ods. 3 ZoITVS):
  - zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív
    - prostredníctvom - VISKB
  - zasielať spôsobom určeným orgánom vedenia vládnej jednotke CSIRT vládnou jednotkou CSIRT určené systémové informácie o aktívach, rizikách, kontaktných bodoch a evidencii kybernetických bezpečnostných incidentov ITVS v rozsahu ustanovenom všeobecne záväzným právnym predpisom vydaným MIRRI a aktualizovať zaslané údaje každých 14 dní
  - zverejniť na svojom webovom sídle **pravidlá na oznamovanie zraniteľností.**
    - nie je prijatá vyhláška, ale sú pravidlá na oznamovanie zraniteľností vydané NBÚ

Hodnotenie zraniteľností (II.)

- **VISKB – informačný systém kybernetickej bezpečnosti pre verejnú správu**

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

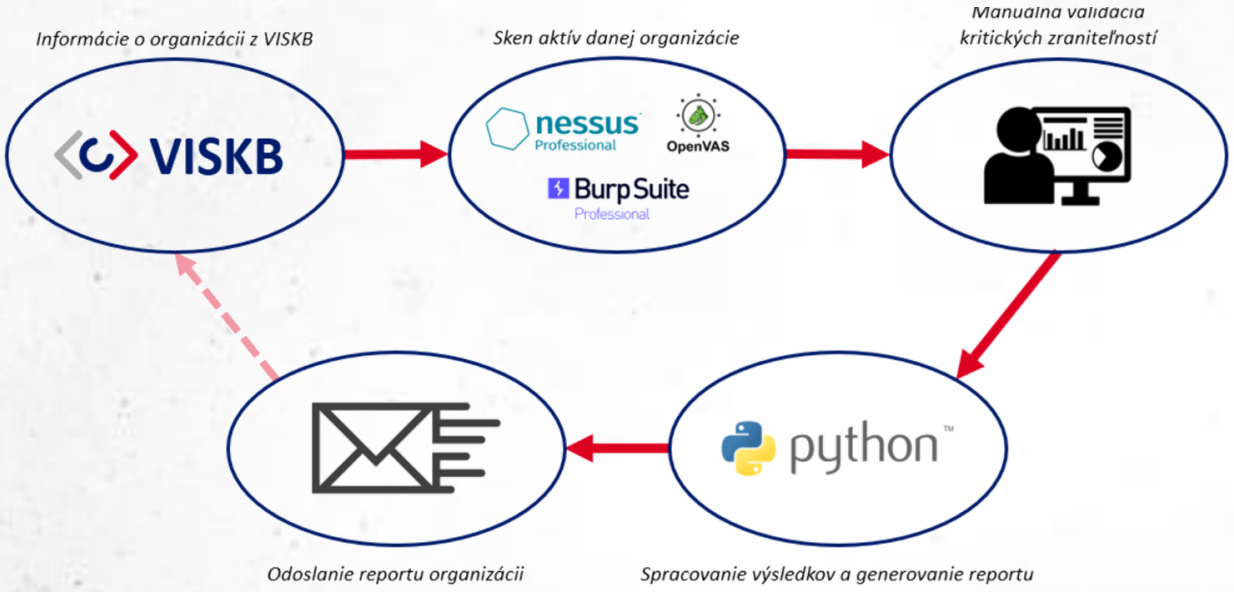
Vitajte v aplikácii Vládnej jednotky CSIRT na registráciu informácií o subjektoch verejnej správy pre systém Achilles.

Ak už máte pre Vašu organizáciu vytvorený používateľský účet, prihláste sa.

Achilles

Hodnotenie zraniteľností (III.)

- **Systém Achilles**
  - report na mesačnej báze
  - údaje z VISKB



Zdroj: https://csirt.sk/wp-content/uploads/2026/02/Achilles_vseobecne_informacie_v1.3.pdf

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

pavol.sokol@upjs.sk

https://cyberawareness.sk