Ministerstvo zdravotnictví České republiky, Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Kybernetická bezpečnost resortu zdravotnictví 2021-2025

Informační bulletin 1/11-2021

NÁRODNÍ CENTRUM
ELEKTRONICKÉHO
ZDRAVOTNICTVÍ

Úvodník

Tento dokument je první souhrnnou informací poskytovanou v návaznosti na zpracovanou Strategii KB MZ ČR a je určen pro seznámení se s postupem prací na realizaci Strategie KB v resortu.

Dnešní informace je zaměřena především na seznámení se se základními fakty a dokumenty souvisejícími s metodickým řízením problematiky kybernetické bezpečnosti v resortu MZ ČR, vybranými událostmi, se zainteresovanými subjekty, osobami, legislativou a zdroji informací.

Co se odehrálo

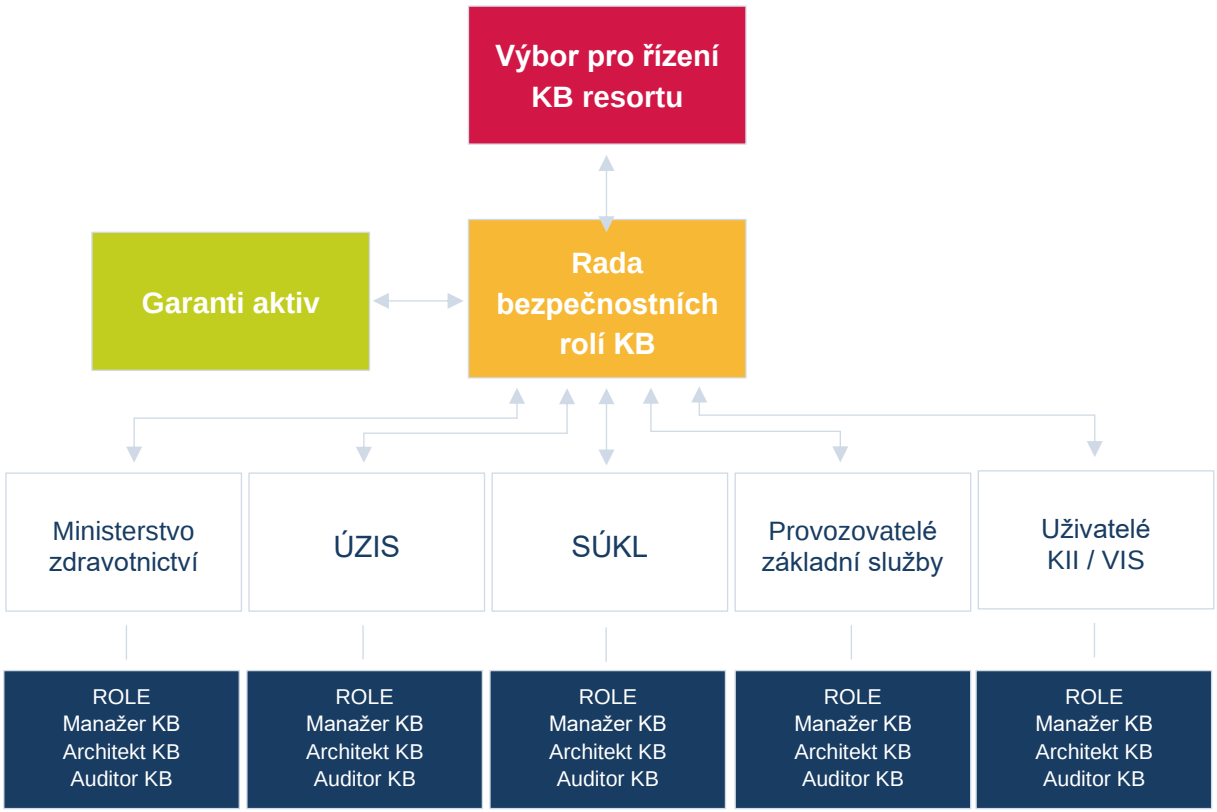
V rámci již proběhlých aktivit:

- **Byla vytvořena a aktualizována vzorová základní dokumentace bezpečnosti informací připravená pro použití resortními organizacemi a poskytovateli zdravotních služeb, vycházející z požadavků zákona č. 181/2014 Sb., vyhlášky č. 82/2018 Sb. a dalších právních předpisů pro budování informačních systémů veřejné správy (zákon č. 365/2000 Sb., vyhláška č. 529/2006 Sb.):**

    - Strategie kybernetické bezpečnosti organizace
    - Bezpečnostní politika informací organizace
    - Politika bezpečnosti lidských zdrojů
    - Politika klasifikace informačních aktiv
    - Politika provozní bezpečnosti
    - Politika řízení dodavatelů
    - Politika systému řízení bezpečnosti informací
    - Metodika analýzy a řízení rizik
    - Metodika identifikace a správy informačních aktiv
    - Metodika pro výkon auditu kybernetické bezpečnosti
    - Metodika pro výkon auditu kybernetické bezpečnosti (pověření)
    - Metodika pro výkon auditu kybernetické bezpečnosti (etický kodex)
    - Metodika pro výkon auditu kybernetické bezpečnosti (zpráva z auditu)
    - Metodika řízení dodavatelů
    - Plán rozvoje bezpečnostního povědomí

    Dokumentace umístěné na stránkách ncez.mzcr.cz/cs/kyberneticka-bezpecnost/kyberneticka-bezpecnost, aktuálně připravujeme její další aktualizaci. Metodický pokyn pro jejich používání byl zveřejněn ve Věstníku č. 7/2019.

Ministerstvo zdravotnictví řídí bezpečnost informací a koordinuje implementaci bezpečnostních opatření v dotčených organizacích resortu MZ ČR dle stanovené působnosti a odpovědnosti vedoucích zaměstnanců a dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. K naplnění cílů MZ ČR v oblasti bezpečnosti informací byl vydáním příkazu ministra ustanoven Výbor pro řízení kybernetické bezpečnosti, který je vrcholovým koordinačním orgánem kybernetické bezpečnosti v resortu MZ ČR. Pracovním orgánem v oblasti kybernetické bezpečnosti je Rada bezpečnostních rolí. Byla nastavena organizační struktura pro Systém řízení bezpečnosti informací (SŘBI) v rámci resortu zdravotnictví, jak je uvedeno v následujícím obrázku.



- **V průběhu tohoto roku byla dokončena příprava Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025, strategie byla schválena Výborem pro řízení kybernetické bezpečnosti resortu MZ ČR, přijata vedením MZ ČR a 3. 8. 2021 byla schválena ministrem zdravotnictví. V rámci této strategie jsou definovány následující globální cíle:**
  - GC1 Zavedení řízení bezpečnosti informací jako mandatorního procesu všech poskytovatelů zdravotních služeb
  - GC2 Zajištění minimálního technického standardu kybernetické bezpečnosti
  - GC3 Zvyšování bezpečnostního povědomí
  - GC4 Kybernetická bezpečnost elektronického zdravotnictví
  - GC5 Kybernetická bezpečnost zdravotnických prostředků

Na ně navazující specifické cíle budeme, po jejich stanovení, postupně představovat v následujících informačních bulletinech.

- **Pro zajištění financování KB:**

  - Proběhla přípravná jednání k NPO na projektu KB na pracovní úrovni s MPO a NAKIT.
  - 30. 3. 2021 proběhla osvětová schůzka k tématu financování KB pro nemocnice v Praze.
  - MZ ČR připravilo materiály, které slouží pro identifikaci připravenosti organizace na zavedení KB a pro specifikaci jejich požadavků tak, aby mohla požádat o finanční podporu na zavedení kybernetické bezpečnosti. Těmito materiály jsou:
    - Vzor Studie proveditelnosti rozvoje systému řízení kybernetické bezpečnosti zpracovaná ve spolupráci s vybranou organizací.

      Účelem Studie proveditelnosti je zpracování strukturovaného zhodnocení potřeb v oblasti kybernetické bezpečnosti a racionální posouzení investičních aktivit pro organizace resortu Ministerstva zdravotnictví žádající o přidělení finančních prostředků z programu Národní plán obnovy na rozvoj kybernetické bezpečnosti.

    - Kontrolní seznam zavedení systému řízení kybernetické bezpečnosti.

      Účelem Kontrolního seznamu je zjištění stavu připravenosti organizace na zavedení kybernetické bezpečnosti.

  Každý žadatel o finanční podporu zpracuje tyto dokumenty dle vzorů tak, aby mohl zažádat o finanční prostředky.

  - Proběhlo jednání zástupců MZČR s platformou hSOC včetně zástupců CESNET.
  - Proběhla jednání s MPO a MV ČR ohledně zajištění financování programu.

Co připravujeme

- Probíhá zpracování Akčního plánu pro realizaci Strategie KB pro období 2021 – 2025.
- Probíhá ověření vzorových dokumentů Studie proveditelnosti a Kontrolního seznamu ve vybrané organizaci.
- Ve spolupráci zejména s NÚKIB a CESNET připravujeme:
  - Metodiky hodnocení důležitosti informačních systémů ve zdravotnictví (stanovení primárních aktiv).
  - Standard zálohování a obnovy informací (Proces Disaster Recovery).

Seznamte se

V rámci této části vás budeme postupně seznamovat (1) s organizacemi podílejícími se na zavádění kybernetické bezpečnosti v rámci resortu Ministerstva zdravotnictví ČR, (2) s osobami, které se na realizaci budou podílet a jejich rolemi.

Subjekty z pohledu zajišťování kybernetické bezpečnosti

Název subjektu	Role subjektu
MZ ČR	Nositel projektu zavedení KB a povinná osoba dle ZoKB.
NÚKIB	Je správním úřadem pro kybernetickou bezpečnost.
CESNET	Je sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu.
ÚZIS	ÚZIS ČR je správcem Národního zdravotnického informačního systému.
ITEZ	Odbor IT a elektronizace zdravotnictví MZ ČR zabezpečuje působnost ministerstva v oblasti strategického a koncepčního rozvoje digitalizace zdravotnictví a související činnosti např. • Přípravu a správu Informační koncepce ministerstva a dalších resortních informatických koncepcí vydávaných ministerstvem. • Zabezpečuje agendu Národního kontaktního místa pro elektronické zdravotnictví. • Zabezpečuje činnost vnitrostátní sítě pro digitální zdravotnictví. Součástí odboru je Národní centrum elektronického zdravotnictví.

Osoby podílející se na realizaci programu zavádění KB

Jméno	Role osoby
Martin Zeman	ředitel odboru ITEZ předseda Výboru pro řízení kybernetické bezpečnosti MZ ČR digitální zmocněnec MZ ČR
Jiří Borej	hlavní architekt elektronizace zdravotnictví člen Výboru pro řízení kybernetické bezpečnosti MZ ČR vedoucí Národního centra elektronického zdravotnictví.
Tomáš Bezouška	manažer kybernetické bezpečnosti MZ ČR předseda Rady bezpečnostních rolí kybernetické bezpečnosti MZ ČR
Jakub Tomas	architekt kybernetické bezpečnosti MZ ČR
Václav Minářů	vedoucí oddělení IKT a KB MZ ČR Tajemník: • Výboru pro řízení kybernetické bezpečnosti • Rady bezpečnostních rolí kybernetické bezpečnosti

Dalšími klíčovými osobami podílejícími se na realizaci programu jsou další:

- členové Výboru pro řízení kybernetické bezpečnosti MZ ČR.
- členové Rady bezpečnostních rolí kybernetické bezpečnosti.

Bližší informace o obsazení uvedených orgánů KB uvedeme v následujících informačních bulletinech.

Financování projektů KB

Aktuální dostupné informace o připravovaném financování zavádění KB jsou uvedené v následující tabulce a textu.

O aktuálním stavu vás budeme informovat v dalších číslech bulletinu.

Zdroj financování	Předmět financování	Možnost čerpat od
NPO	Specifické oblasti kybernetické bezpečnosti, kterými jsou: • Vícefaktorová autentizace • Antivirové programy • Advanced Threath Protection • Load Balancing • L2/L3 Switches a segmentace sítě • Log Management • NGFW • SandBox • SIEM • Virtualizace • Zálohování	Bude upřesněno

- Podpora kybernetické bezpečnosti z Národního plánu obnovy bude určena poskytovatelům zdravotních služeb v Praze, pro poskytovatele zdravotních služeb mimo Prahu je připravováno financování zavádění kybernetické bezpečnosti z ESIF/IROP.

Zkratky a pojmy

CESNET	sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu pro vědu, výzkum a vzdělávání zahrnující počítačovou síť, výpočetní gridy, datová úložiště, prostředí pro spolupráci a nabízející širokou škálu služeb.
NCKB	Národní centrum kybernetické bezpečnosti je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
ESIF	Evropské strukturální a investiční fondy
hSOC	hospital Security Operation Center - komunitní iniciativ a platforma
HaSIM	Health and Social Insider Monitor.
IROP	Integrovaný regionální operační program
ISMS	Information Security Management System - je mezinárodní zkratka pro systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací např. podle normy ISO27001.
ITEZ	Odbor informačních technologií a elektronizace zdravotnictví MZ ČR
KB	Kybernetická bezpečnost.
MPO	Ministerstvo průmyslu a obchodu České republiky
MZ ČR	Ministerstvo zdravotnictví České republiky.
NAKIT	Národní agentura pro komunikační a informační technologie, s. p.
NCeZ	Národní centrum elektronického zdravotnictví, součást ITEZ.
NPO	Národní plán obnovy
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost.
SOC	Security Operation Center (Operační centrum informační bezpečnosti).

SŘBI	Systém řízení bezpečnosti informací – česká zkratka a význam pro ISMS.
Strategie KB	Dokument Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025.
ÚZIS	Ústav zdravotnických informací a statistiky ČR.
VoKB	Vyhláška o kybernetické bezpečnosti.
ZoKB	Zákon o kybernetické bezpečnosti.

Legislativa

Základní legislativa ke kybernetické bezpečnosti

- Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti

  https://www.zakonyprolidi.cz/cs/2014-181

  NÚKIB vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb.

- Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

  https://www.zakonyprolidi.cz/cs/2018-82

- Vyhláška č. 437/2017 Sb. Vyhláška o kritériích pro určení provozovatele základní služby

  https://www.zakonyprolidi.cz/cs/2017-437

Základní legislativa k informačním systémům veřejné správy

- Zákon 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů

  https://www.zakonyprolidi.cz/cs/2000-365

- Vyhláška č. 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

  https://www.zakonyprolidi.cz/cs/2006-529

- Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů.

  https://www.zakonyprolidi.cz/cs/2020-360
  https://www.zakonyprolidi.cz/cs/2014-317