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 2/6-2022

NÁRODNÍ CENTRUM
ELEKTRONICKÉHO
ZDRAVOTNICTVÍ

Úvodník

Tento dokument přináší informace v návaznosti na zpracovanou Strategii KB MZ ČR a je určen pro seznámení se s postupem a aktualizací prací na zavádění KB v resortu MZ ČR.

Dnešní informace je zaměřena na aktuality za posledních 6 měsíců a zajištění financování aktivit Strategie KB MZ ČR prostřednictvím dotačních prostředků z Národního plánu obnovy.

Co se odehrálo

V rámci již proběhlých aktivit:

- Na základě schválené **Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025** zveřejněné na webu Národního centra elektronického zdravotnictví (https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/strategie-kyberneticke-bezpecnosti) byla tato strategie rozpracována do podoby **Akčního plánu**, který obsahuje jednotlivé globální, strategické a specifické cíle. Tento Akční plán byl v dubnu 2022 schválen Výborem pro řízení kybernetické bezpečnosti a následně byl schválen poradou vedení Ministerstva zdravotnictví. Po schválení **Akčního plánu došlo také k jeho zveřejnění na stránkách ncez.mzcr.cz** (https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/akcni-plan-strategie-kyberneticke-bezpecnosti-2021-2025).

- V rámci **aktualizace prvků Kritické informační infrastruktury v resortu zdravotnictví** probíhá redefinice těchto prvků ve spolupráci s NÚKIB. Bližší informace budou zveřejněny po schválení aktualizovaného Seznamu prvků kritické infrastruktury Bezpečnostní radou státu.

- **Podporujeme vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti prostřednictvím online kurzu Dávej Kyber!, který připravil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).**
    - Tento kurz absolvovali s kladnou odezvou všichni zaměstnanci MZČR, a tak bude tento kurz přístupný pro všechny nově nastoupivší zaměstnance a také pro všechny zaměstnance přímo řízených organizace MZČR.
    - Absolvováním kurzu všemi zaměstnanci přispělo Ministerstvo zdravotnictví k ochraně informačních aktiv a zvýšilo tak bezpečnostní povědomí zaměstnanců v oblasti kybernetické bezpečnosti. Povinnost zvyšování bezpečnostního povědomí zaměstnanců vyplývá také ze zákona č. 181/2014 Sb. ve znění pozdějších předpisů.

- **Došlo ke změně Manažera kybernetické bezpečnosti resortu.** Nové obsazení bezpečnostních rolí je uvedeno níže. Změny nastaly rovněž ve Výboru pro řízení kybernetické bezpečnosti v rámci běžné obměny zaměstnanců.

- Ministerstvu zdravotnictví se podařilo uzavřít **veřejnou zakázku na výběr dodavatelů za účelem poskytování auditu kybernetické bezpečnosti**. Tato veřejná zakázka proběhla v rámci Dynamického nákupního systému a zdravotnická zařízení, která se přihlásila k této veřejné zakázce, mají nyní možnost uspořádat „minitender" mezi dodavateli, kteří splnili zadaná kritéria, na uskutečnění auditu kybernetické bezpečnosti ve svých organizacích. Zástupcům těchto organizací byl zaslán podrobný návod, jak postupovat za účelem vyhlášení „minitenderu" v prostředí systému TENDERARENA.

- V souvislosti s vydáním **ochranného opatření ze strany NÚKIB**, které se týká **zabezpečení e-mailové komunikace**, proběhlo na Ministerstvu zdravotnictví nastavení e-mailové komunikace v souladu s požadavky NÚKIB. Zároveň byla zajištěna koordinace s přímo řízenými organizacemi v rámci provedení nastavení konfigurace jejich emailových prostředků. **Zvýšené zabezpečení e-mailové komunikace je platné od 1.7.2022** a týká se především nastavení šifrované komunikace mezi poštovními servery.

Co připravujeme

- Připravujeme **finanční podporu projektů** pro zajištění **řešení kybernetické bezpečnosti poskytovatelů zdravotních služeb na území Hlavního města Prahy**. Podporovány budou následující oblasti:
    - systém řízení bezpečnosti informací a báze znalostí v oblasti kybernetické bezpečnosti,
    - nástroje pro zálohování a archivaci,
    - L2/L3 switche a nástroje pro segmentaci datové komunikační sítě, NAC, 802.1X,
    - NGFW vč. IPS/IDS,
    - Antivirus, Endpoint protection apod.,
    - nástroje pro load balancing,
    - nástroje pro analýzu a monitoring síťového provozu,
    - nástroje pro Multifaktorovou autentizaci,
    - nástroje pro LogManagement,
    - nástroje pro SandBoxing,
    - dodávka a implementace služeb SIEM, služby SOC,
    - nástroje z kategorie Advanced Threat Protection,
    - nástroje pro řízení přístupů a identit (PIM/PAM atp.),
    - nástroje pro Mobile/Enterprise device management,
    - nástroje pro správu aktiv a řízení rizik a zranitelností.

- Finanční prostředky z národního plánu obnovy bude možné **využít na investice i vybrané typy služeb.**
- MZČR v rámci prostředků Národního plánu obnovy na kybernetickou bezpečnost poskytovatelů zdravotních služeb v Praze **následující subjekty**:
    a. Poskytovatele základní služby podle zákona o kybernetické bezpečnosti nebo
    b. Poskytovatele zajišťující urgentní příjem I. Typu nebo
    c. Poskytovatele zajišťující urgentní příjem II. Typu nebo
    d. Poskytovatele zajišťující vysoce specializované centrum nebo
    e. Poskytovatele poskytující službu v obecném hospodářském zájmu

- Koordinujeme a realizujeme projekty v rámci **Národního plánu obnovy, Výzva 09, v pilíři 1.2. Digitální transformace,** která se zabývá Kybernetickou bezpečností. Zmíněná výzva zahrnuje předem definované projekty, jejichž cílem je zvýšení počtu informačních systémů a posílení jejich kybernetické bezpečnosti v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti:
    - 1.6.5. Posílení kybernetické bezpečnosti resortní infrastruktury,
    - 1.6.6. Posílení kybernetické bezpečnosti infrastruktury SÚKL,
- V rámci projektů připravujeme žádosti včetně návazných výběrových řízení a realizace projektů.

Seznamte se

Osoby podílející se na realizaci programu zavádění KB

Jméno	Role osoby
Vít Lidinský	Manažer kybernetické bezpečnosti MZ ČR Předseda Rady bezpečnostních rolí kybernetické bezpečnosti
Jakub Tomas	Architekt kybernetické bezpečnosti MZ ČR
Václav Minářů	Tajemník: • Výboru pro řízení kybernetické bezpečnosti • Rady bezpečnostních rolí kybernetické bezpečnosti

Dalšími klíčovými osobami podílejícími se na realizaci programu jsou:

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

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)
ESF	Evropský sociální fond
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 - mezinárodní zkratka pro systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací podle normy ISO27001
IKT	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
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 ČR	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