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 4/10-2022

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 výsledky provedeného Proof of Concept (dále jen „PoC“) nástroje pro identifikaci a hodnocení zdravotnických prostředků a dalších technických aktiv v síti, které proběhlo ve Fakultní nemocnici v Plzni (dále jen „FN Plzeň“).

Níže uvádíme výsledky PoC v rámci řešení kybernetické bezpečnosti zdravotnických prostředků na základě výstupů a zkušeností manažera kybernetické bezpečnosti FN Plzeň.

Zdůvodnění potřebnosti

Základním předpokladem pro strategické nastavení a řízení Systému řízení bezpečnosti informací je kompletní přehled o všech primárních a podpůrných aktivech v rozsahu ISMS. Problematickou oblastí jsou technická aktiva zahrnující servery, koncové stanice, aktivní síťové prvky a také zdravotnické prostředky. Evidence o těchto aktivech jsou buď roztříštěny ve statických Office dokumentech nebo zejména o zdravotnických prostředcích nejsou vedeny přehledy v rozsahu informací potřebných pro zajištění kybernetické bezpečnosti. Kromě toho se stala oblast bezpečnosti zdravotnických prostředků jednou z priorit FN Plzeň i v návaznosti na nálezy z auditní činnosti NÚKIB.

Z tohoto důvodu byl ve Fakultní nemocnici Plzeň proveden průzkum trhu a byly identifikovány mezinárodně osvědčené nástroje zajišťující kompletní visibilitu a přinášející dynamický přehled nad všemi technickými aktivity s cílem řízení jejich rizik, zranitelností a změn. Z těchto nástrojů byl vybrán SW nástroj Armis https://www.armis.com/, který byl podroben bezpečnostnímu posouzení, vzhledem k citlivosti informací a dat, a následně byl v omezeném rozsahu odzkoušen v rámci PoC.

Jak nástroj funguje

Cílem je představit způsob fungování nástroje a možnosti implementace.

- Jedná se o zcela pasivní řešení s vyhodnocováním metadat v cloudu, bez nutnosti instalace sw na koncové zařízení.
- Do interní sítě se napojí pouze sondy, které analyzují přijatá data a následně posílají metadata do cloudu (Cloud je umístěn v AWS ve Frankfurtu).

- Sondy sami aktivně nekomunikují s ostatními zařízeními v síti. Celý sběr dat probíhá jen pomocí analýzy kopie datových toků v síti.
- Odeslaná data do cloudu obsahují pouze metadata o zařízeních (IP adresa, MAC adresa, OS, název zařízení, model, atp.) – nikdy se nepřeposílá obsah komunikace koncových zařízení.
- Nedochází k výraznému zatížení sítě. Poměr odeslaných dat vůči těm zpracovaným se pohybuje od 1:1 000 až k 1:10 000.
- Zabezpečení je šifrované po celou dobu komunikace, zároveň i v samotném cloudu (TLS 1.3, vlastní certifikát SHA256, 2048 klíč s ECDHE_RSA).

Co se odehrálo

Rozsah PoC

Cílem projektu bylo zajištění PoC nástroje Armis ve FN Plzeň. **Hlavním úkolem PoC bylo zjistit schopnosti nástroje v oblasti evidence zdravotnických prostředků připojených do sítě a identifikace jejich bezpečnostních nedostatků a známých zranitelností**. Celková doba provozu byla stanovena na **6 týdnů** a probíhala v období července a srpna 2022.

Místo pro zapojení sond bylo zvoleno na základě vlastností a topologie sítě a připojených zařízení, která byla předmětem monitoringu. Celkem byly zapojeny tři 10G sondy do VLAN, kde jsou umístěny zdravotnické prostředky. V rámci PoC nebyla využita žádná jiná doplňková integrace, kromě dvou nezbytně nutných portů pro optimální provoz (SPAN a SNMP).

Během projektu byly provedeny následující činnosti:

- Sběr informací v nástroji Armis
- Kontrola podezřelých aktivit a upozornění na zařízení s velkým rizikem (zranitelnostmi)
- Konfigurace sledovacích sond a vytvoření cloudového prostředí pro sběr a vyhodnocovaní dat
- Porovnání nástroje s konkurenčním řešením
- Vyhodnocování využitelnosti ze strany FN Plzeň
- Vytvoření doporučení pro implementaci v plném rozsahu

Nálezy na základě PoC

6-ti týdenní implementace nástroje Armis do prostředí FN Plzeň proběhla bez jakýchkoliv problémů. Následující provoz splnil očekávaní **v oblastech inventarizace, hlášení alertů a nalezení zranitelností.** V rámci těchto tří oblastí byly definovány níže uvedené závěry:

Inventarizace

Nástroj Armis je schopný rozpoznat jak zdravotnická, tak i IT zařízení a je možné sytém použít k vytvoření IT a zdravotnického dynamického inventáře pro zdravotnické zařízení.

Nástroj Armis dokáže uspokojivě kategorizovat rozpoznaná zařízení a zobrazit jejich detailní parametry v závislosti na informacích poskytnutých v zachyceném datovém provozu.

Ve VLANě bylo rozpoznáno 34 zařízení v kategorii „zdravotnické“ z nichž pouze u 8 nebyl zcela rozpoznán typ z důvodu nedostatečných informací zasílaných v zachycených datech a to z důvodu limitace sledování na dané VLANě a nedostatečné komunikaci zařízeních v síti. U zbylých 26 bylo zjištěno dostatek informací k určení typu zařízení:

- 9x Fluoroskopické zařízení
- 2x MRI
- 6x Systém pro radiologii
- 3x CT
- 1x Rentgen
- 2x Zařízení nukleární medicíny
- 2x Angiografický přístroj
- 1x Medicínský server

Dále bylo ve VLANě rozpoznáno 9 IT zařízení s kategorií a typem a u 19 zařízení nebyla rozpoznána kategorie ani typ z důvodu malé komunikace na síti v průběhu PoC.

Alerty

I přes to, že během PoC **nebyla zaznamenána žádná potvrzená kyberbezpečností hrozba**, tak je nástroj Armis - dle výsledků **PoC - schopný generovat relevantní bezpečnostní alerty** pro ~~jak~~ zdravotnická, tak i IT zařízení v rozsahu, který je očekáván od pasivního nástroje pro bezpečnostní sledovaní provozu.

Nástroj Armis kromě porovnání informací výrobce v rámci CWE rovněž komparuje komunikaci a chování zdravotnického prostředku v síti se shodnými již dříve detekovanými zdravotnickými prostředky a zjišťuje odchylku od běžného chování či komunikace zařízení.

Od počátku sledování bylo **zaznamenáno celkově 3 990 alertů.** 2 733 z nich bylo vygenerováno zdravotnickými prostředky. Alerty jsou rozdělené dle závažnosti na:

- Nízká závažnost - 1 273 alertů

- Střední závažnost - 1 909 alertů
- Kritická závažnost - 809 alertů

Čtyři nejzávažnější druhy alertů jsou:

- Komunikace s externím zařízením
- FTP komunikace s externí IP
- Připojení ke zdravotnickému zařízení na portu 80/8080
- Zdravotnické zařízení používá nešifrované přihlašovací údaje

Nad rámec rozsahu sledování (VLAN) Armis celkově zaznamenal 5 737 alertů, které detekoval.

Zranitelnosti

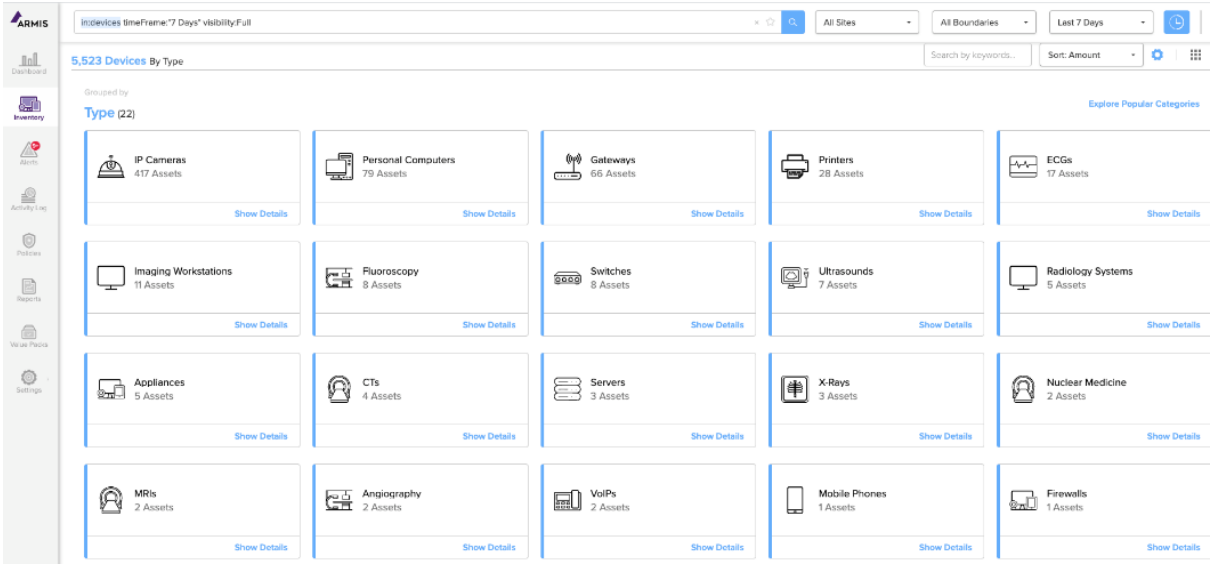
Nástroj Armis je schopen **identifikovat zranitelnosti ze zachyceného provozu, a to nejen pro zdravotnická, ale i pro IT zařízení.** Pomocí Armisu tak FN Plzeň může zavézt řízení zranitelností pro zdravotnická zařízení a tím zamezit hrozbě potencionálního zneužití aktivních zranitelnosti. Tohoto nelze dosáhnout prostřednictvím aktivního skenu, kdy při externí komunikaci ze skenu k zdravotnickému prostředku často dochází k omezení jeho funkčnosti nebo výpadku.

U sledovaných zařízení **bylo zjištěno celkově 332 unikátních zranitelností**. Každá z unikátních zranitelností může být obsažena hned v několika zařízeních. Celkově bylo nalezeno:

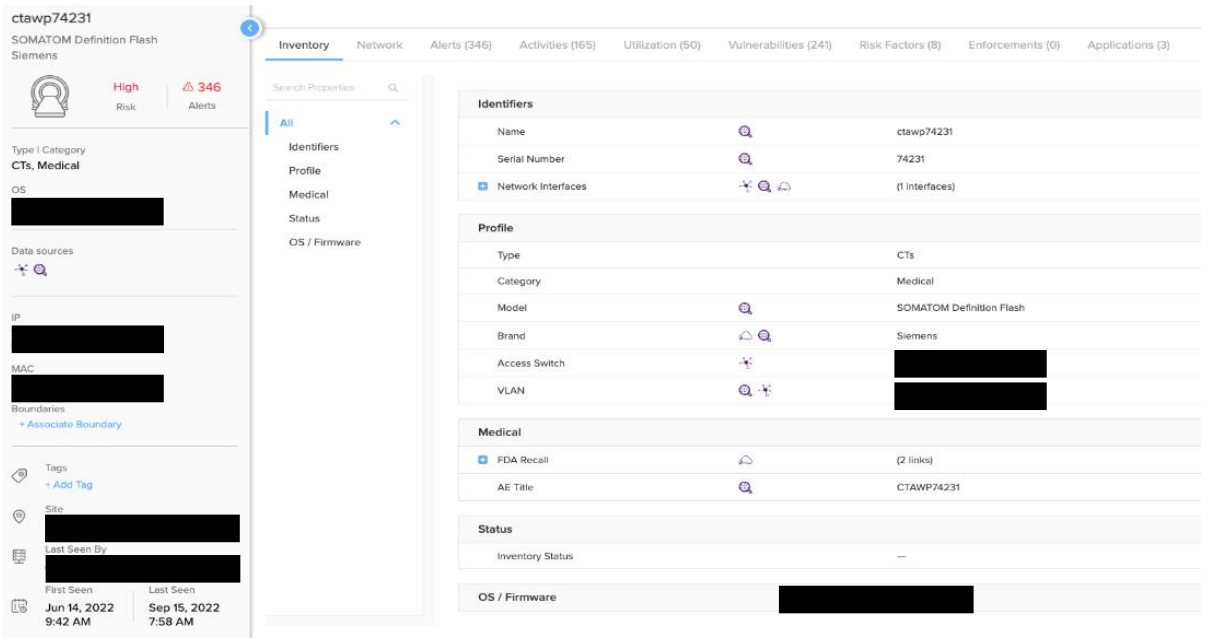
- 118 kritických zranitelností s 326 výskyty
- 73 závažných zranitelností s 163 výskyty
- 141 mírných zranitelností s 347 výskyty
- 199 unikátních zranitelností je hodnoceno jako lehce zneužitelných

Nad rámec rozsahu sledování (VLAN Armis odhalil celkem unikátních 831 zranitelností v 3 170 výskytech.

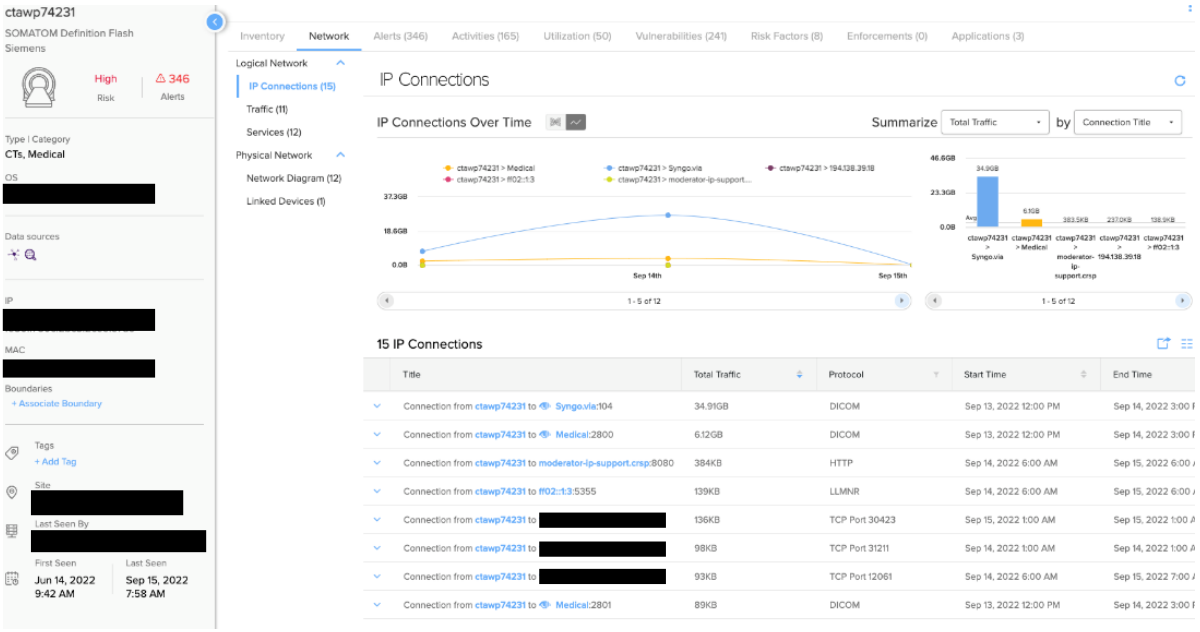
Obrázek č. 1 SW Armis, zobrazení identifikovaných aktiv



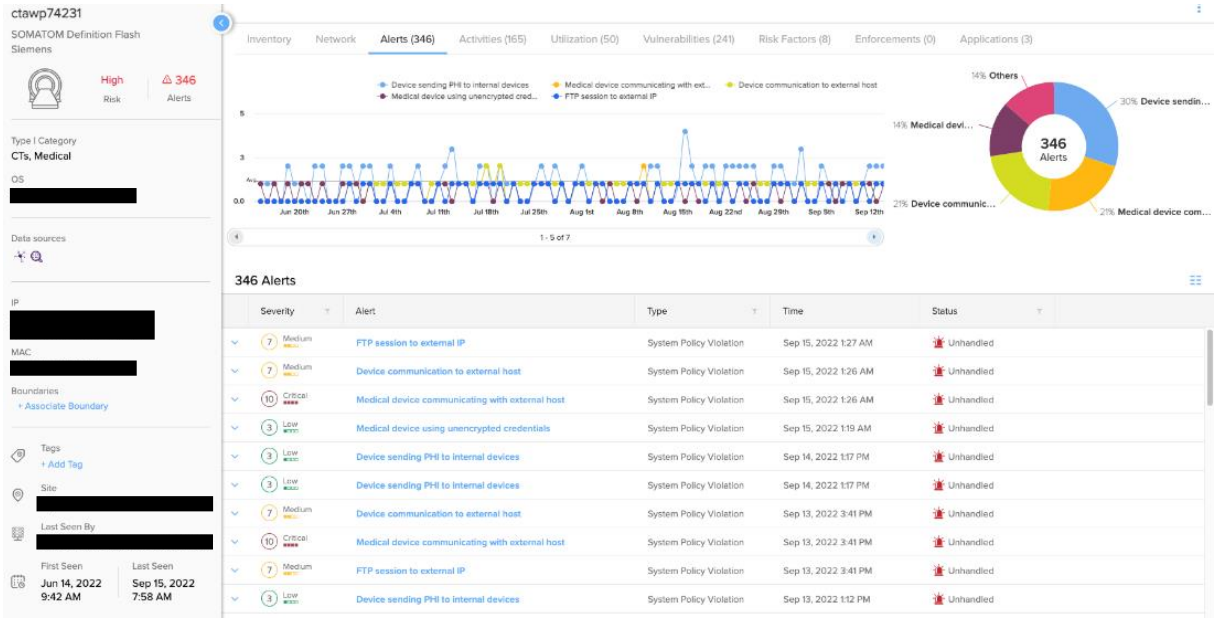
Obrázek č.2 – SW Armis, detail identifikovaného zařízení



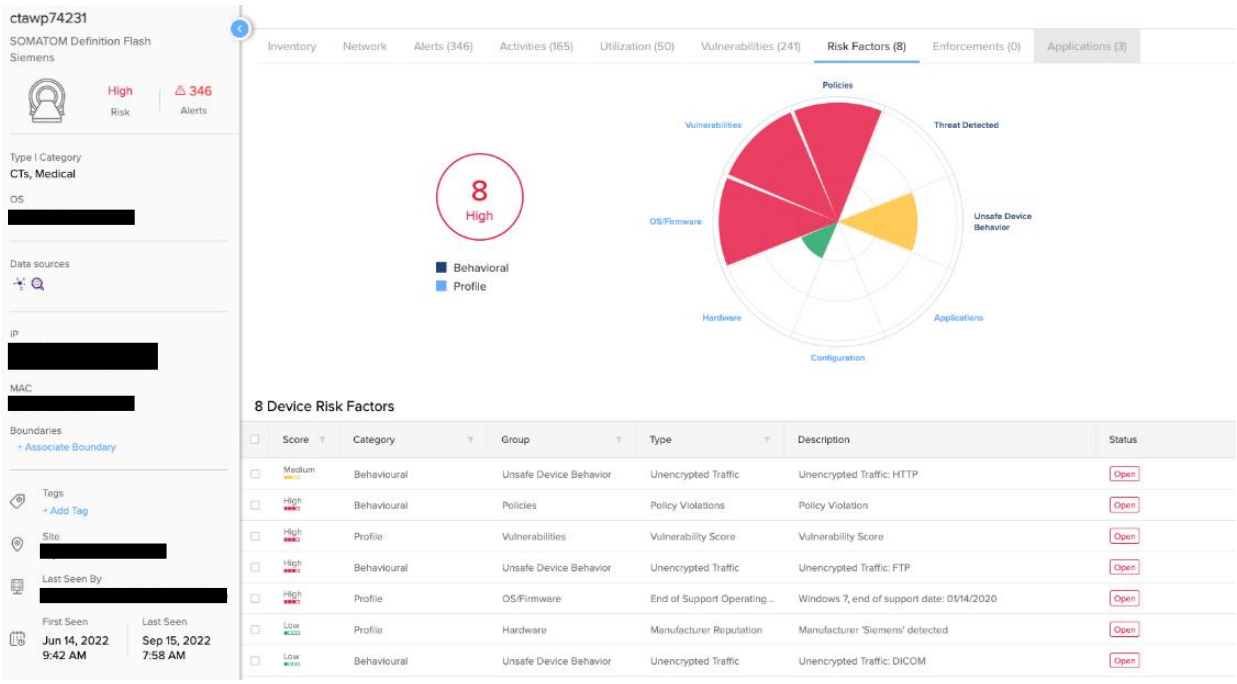
Obrázek č. 3 – SW Armis, zobrazení komunikace zařízení



Obrázek č. 4 – SW Armis, zobrazené aletry zařízení v čase



Obrázek č. 5 – SW Armis, zobrazené aletry zařízení



Výstup/přínosy PoC

Výstupy z provedeného PoC slouží jako přínos a ponaučení pro další aktivity MZČR, či jeho přímo řízené organizace. Již nyní se výstupy projevují v následujících oblastech činností:

- Připravujeme metodiku pro práci se zdravotnickými prostředky
- Pro přípravu metodiky čekáme na výsledky druhého PoC jiného nástroje
- Posuzuje se možnost informování o správné konfiguraci a funkci jednotlivých prostředků prostřednictvím webu NCEZ v rámci sdílení znalostí

Výstupy projektu lze hodnotit značně pozitivně. SW byl schopen identifikovat infrastrukturní prvky a jejich zranitelnosti. Následující kroky v rámci popsání jednotlivých zdravotnických prostředků jsou spojeny s mravenčí prací v objemech stovek člověkodní, kdy budou ve spolupráci s výrobcem prověřeny zjištěné aletry a popsáno korektní chování každého zdravotnického prostředku. Po rozdělení zdravotnických prostředků podle potenciálních rizik plynoucích z využitých HW a SW infrastrukturních prvků těchto prostředků je možné zahájit tvorbu bezpečnostních opatření. Bezpečnostní opatření předpokládáme v rozdělení zdravotnických prostředků do více VLAN podle „nebezpečnosti“ a řízení jejich komunikace.

Seznamte se

Představujeme aktualizovaný seznam organizací podílejících se na zavádění kybernetické bezpečnosti v rámci resortu Ministerstva zdravotnictví ČR, a osoby, které se na realizaci podílí.

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 ČR	ÚZIS ČR je správcem Národního zdravotnického informačního systému.
NCeZ	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.

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
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
NCKB	Národní centrum kybernetické bezpečnosti je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)
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