KYBERNETICKÁ BEZPEČNOST VE ZDRAVOTNICTVÍ Z POHLEDU NÚKIB

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

8. září 2021
TLP: WHITE

Adam Kučínský
ředitel
Odbor regulace

Ohlédnutí za útoky na zdravotnictví z pohledu NÚKIB…

- **11.12. 2019 – Incident v nemocnici v Benešově**
- **12. 3. 2020 – Incident ve FN Brno**
- 17. 3. 2020 – Vydáno reaktivní opatření (RO) pro nemocnice
- 18. 3. 2020 – Vydána metodika k RO
- 18. 3. 2020 – Vydáno a rozesláno doporučení pro poskytovatele zdravotních služeb vč. metodiky
- **27. 3. 2020 - Incident v psychiatrické léčebně Kosmonosy**
- 27. 3. 2020 - Nabídka služeb nemocnicím – e-learning, sken zranitelností, Turris Mox (ve spolupráci s CZ.NIC)
- 16. 4. 2020 – Varování
- 17. 4. 2020 – Doporučení k varování
- **Duben 2020 - Fakultní nemocnice Olomouc a Ostrava**

Průběžně:

- **Řešení větších či menších incidentů a událostí – konzultace, výměna informací, pomoc s vyšetřováním**

Co útoky na zdravotnictví přinesly…

- Škody řádově stovky milionů Kč.
- Všeobecný zájem o téma.
- Zjištění, že zdravotnictví JE závislé na ICT.
- Zjištění, že skoro vše je závislé na ICT.

- Změnu vyhlášky o PZS.
- Zařazení dalších nemocnic do PZS.
- Audity některých nemocnic.

Nemocnice jsou pro hackery stále snadným cílem. Útoků přitom přibývá

20. února 2021 18:51

Odložení operací, rychlý převoz akutních pacientů do vedlejšího špitálu. Tak to vypadalo v nemocnicích, které v poslední době ochromil velký kybernetický útok. Podobný scénář přitom hrozí celé řadě zdravotnických zařízení. Neblahou zkušenost s ním má nemocnice v Benešově, kterou hackeři předloni zcela ochromili, škody způsobili i v Brně. Problémem jsou peníze, ministerstvo teprve nyní chystá nápravu.

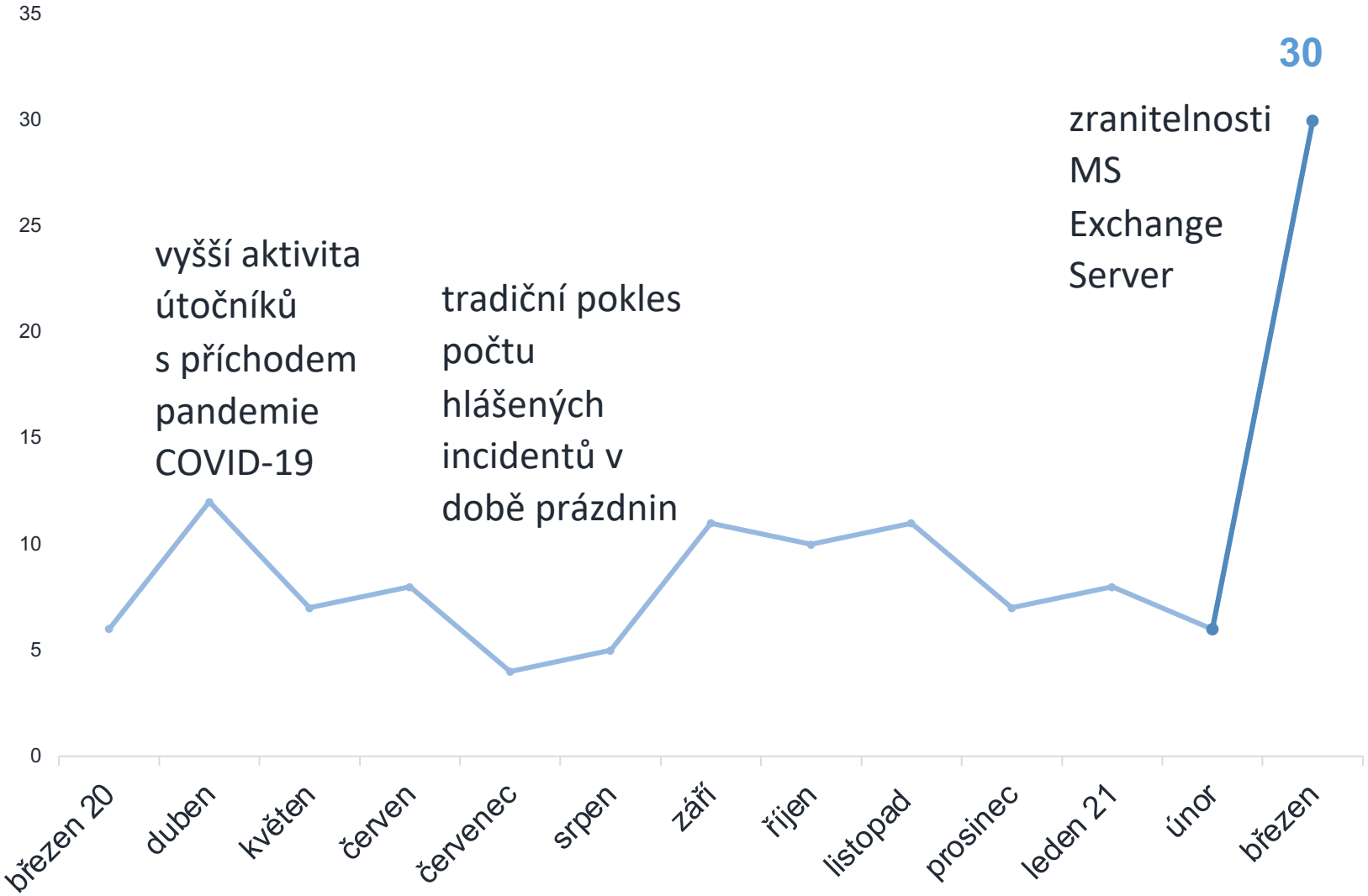
Proč se útoky staly

- Protože se to stává a stávat se to bude.
- Protože kyber zabezpečení nemocnic se neřešilo (čest výjimkám).
- Protože chybí koncepce a standard – jak v rámci architektury, tak v rámci zabezpečení.
- Nastavit koncepci je složité – různí poskytovatelé, různí zřizovatelé, různé zájmy.
- ICT a kybernetická bezpečnost je v nemocnicích poddimenzovaná.
- Uživatelé…

- Nejsou lidi.
- Nejsou peníze.

Incidenty řešené Vládním CERT

- Počet kybernetických útoků roste a útočníci se zlepšují.
- Dochází ke komoditizaci útoků.
- Dopady útoků se zvyšují s rostoucí závislostí na ICT.



Incidenty řešené Vládním CERT

99

Počet řešených incidentů

Počet hlášených incidentů

468

15

Zpracovaných situačních analýz ke KBI a kampaním

Počet vydaných přehledů KBI

17

48

Upozornění na zranitelnosti na webu

Upozornění na zvýšené riziko kybernetických útoků

2

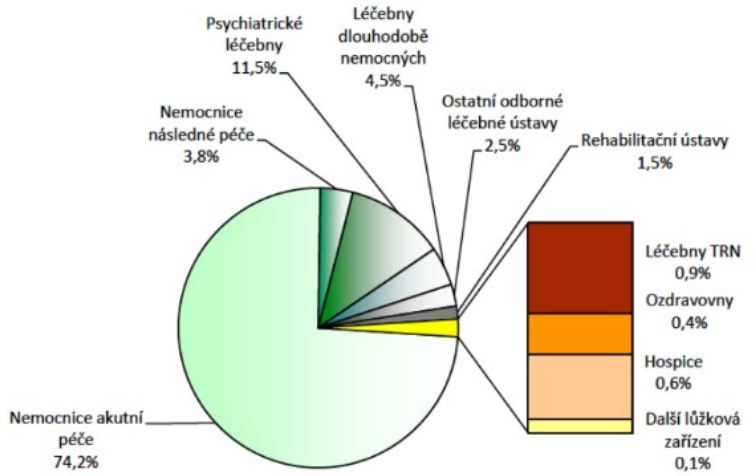
Zabezpečení zdravotnických zařízení není systematicky řešeno

- Specifické standardy pro architekturu a zabezpečení zdravotnických zařízení nejsou (a nejde jen o nemocnice)
- Problém neexistence standardů není řešen ani např. Národní strategií elektronického zdravotnictví na období 2016 – 2020 („NSEZ“)
  - NSEZ sama identifikuje bezpečnostní riziko u nemocničních informačních systémů z důvodu jejich podfinancování a zastaralosti. Uvědomuje si také dlouhodobou absenci koordinace elektronizace zdravotnictví v ČR na této úrovni (str. 126 NSEZ).
- Zdravotnická zařízení mohou vycházet z best practice, ale nemají na to znalosti, personál, finance a ani motivaci (povinnost)
- Žádná z nemocnic není určena jako kritická infrastruktura
- Do 31. 12. 2021 pod ZKB spadalo 16 nemocnic, nyní 44

Nastavit koncepci je složité – různí poskytovatelé, různí zřizovatelé, různé zájmy

- V ČR je cca 270 nemocnic
- Nemocnice jsou různé velikosti, různé specializace
- Zřizovatelé nemocnic jsou různí – kraje, stát, města, soukromé osoby
- Nejsou tady jen nemocnice – ambulance, polikliniky a další zařízení

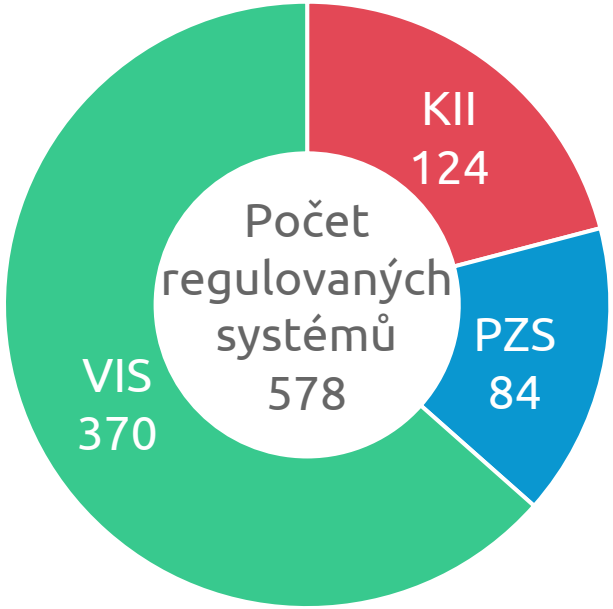
- Nelze stanovit detailní požadavky univerzálně použitelné po všechny



Role NÚKIB

- NÚKIB je regulátor
- Nastavuje standardy v oblasti kybernetické bezpečnosti (vyhlášky a zákon)
- Analyzuje a vyhodnocuje kybernetickou bezpečností situaci

- Dohlíží na kybernetickou bezpečnost povinných osob ze ZKB
  - VIS 370
  - KII 124
  - PZS 84
  - Ve zdravotnictví je to aktuálně 44 nemocnic
- A dělá řadu dalších činností…



- **NÚKIB není IT dodavatel a nesupluje úlohu správce systému!**
- **Za dopad incidentu i za jeho vyřešení je vždy odpovědný správce systému!**

Činnost NÚKIB v případě incidentu

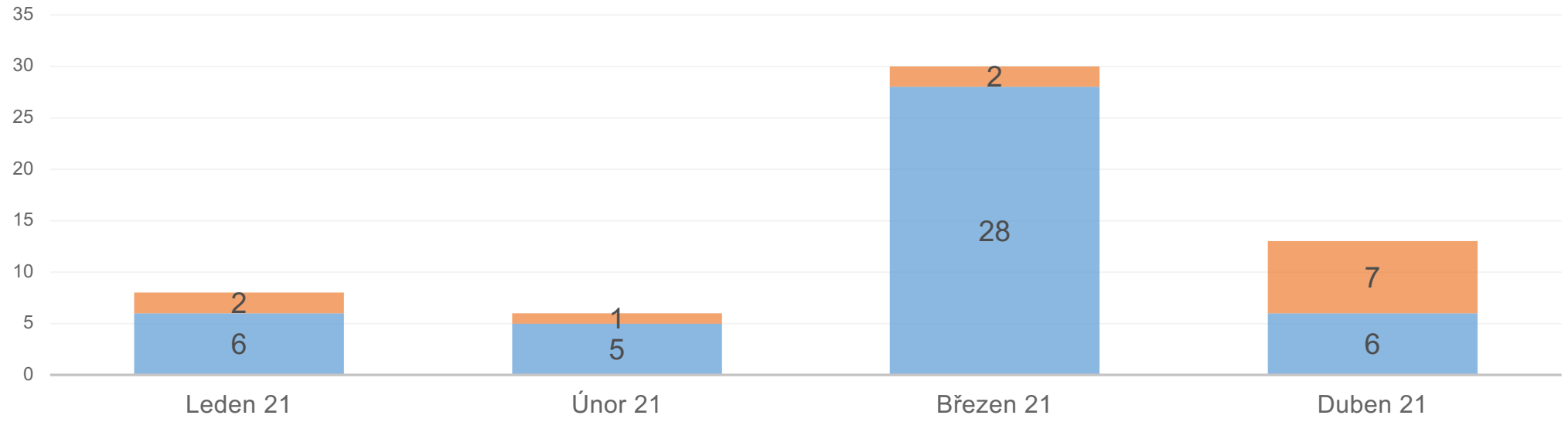
- Hlášení incidentu/Zpráva v médiích
- Snaha kontaktovat napadenou organizaci
- Zjištění základního přehledu o situaci
- Rozhodnutí o pomoci a vyslání response týmu
- Vyslán response tým
  - Analyzuje
  - Doporučuje
  - Navrhuje opatření
- Zajištění stop, indikátorů kompromitace a jejich vyhodnocení
- Rozhodnutí o případném dalším postupu – sdílení informací o incidentu, vydání opatření, upozornění ostatních apod.

Činnost NÚKIB v případě incidentu

- Analýza stavu
- Určení časového i věcného rozsahu kompromitace systémů
- Návrh **možných** postupů při procesu obnovy dat
- Výpomoc při odstraňování a analýze škodlivého kódu
- Doporučení pro zabezpečení systémů a sítě

Nárůst ransomwarových útoků

- V dubnu 2021 se více než polovina incidentů (7 z 13) řešených GovCERT týkala ransomwarového útoku



Vektory útoku

- Phishingový e-mail
- Nezabezpečené veřejně dostupné služby z internetu
  - Remote desktop protocol (RDP)
  - Secure Shell (SSH)
  - Webový e-mailový klient
  - Informační systémy
- Zneužití odcizených přihlašovacích údajů
- Neautorizovaný přístup k vnitřní síti
  - Špatně zabezpečené Wifi
  - Ethernet přípojky
- Kompromitace skrze poskytovatele služeb
- Osobní zařízení, notebooky

Typické chyby v zabezpečení

- Technické nedostatky
  - Nedostatečná segmentace sítě
  - Nejsou řešeny a vyhodnocovány zranitelnosti, nedochází k aktualizacím systémů
  - Nedostatečně řešené zálohování
  - Vystavování služeb do internetu bez řádného důvodu
  - Ignorace „best practices“
- Manažerské nedostatky
  - Pravidlo minimálního nutného přístupu
  - Provoz šéfuje bezpečnosti
  - Management nejde příkladem
  - Ignorace „best practices“
- Školení uživatelů
  - Uživatelé bez proškolení jsou bezpečnostní hrozbou
- Monitoring
  - Nedochází k analýze provozu – nedostatečný síťový monitoring

Doporučení v rámci **prevence**

- **Zálohy**
  - Pravidlo 3 – 2 – 1 - Nejméně 3 kopie na 2 různých zařízeních, z toho 1 mimo organizaci.
  - Neaktivní záloha - jedna nebo více záloh musí být neaktivní.
  - Obnovitelnost – plán obnovy, testování záloh.

- **Segmentace sítě**
  - Správně nakonfigurovaná segmentace dokáže zkomplikovat rozšíření malware.
  - Rozdělení sítě do více segmentů a řízení přístupu do jednotlivých segmentů.
- **Aktualizace**
  - Aktualizace, testování, konfigurace

Doporučení v rámci **prevence**

- **Zálohy**
  - Pravidlo 3 – 2 – 1 - Nejméně 3 kopie na 2 různých zařízeních, z toho 1 mimo organizaci.
  - Neaktivní záloha - jedna nebo více záloh musí být neaktivní.
  - Obnovitelnost – plán obnovy, testování záloh.

- **Segmentace sítě**
  - Správně nakonfigurovaná segmentace dokáže zkomplikovat rozšíření malware.
  - Rozdělení sítě do více segmentů a řízení přístupu do jednotlivých segmentů.
- **Aktualizace**
  - Aktualizace, testování, konfigurace

Doporučení v rámci **prevence**

- **Otevřené služby – ponechat jen ty nezbytné**
  - kontrola otevřených portů na stanicích a blokace služeb otevřených do veřejné sítě včetně služeb pro vzdálený přístup.
  - Často zneužívanými službami jsou protokoly RDP, SMB, telnet a SSH s heslem
  - Ověřit, jak je spravovaná síť a její služby reálně viditelné z internetu (provést skenování sítě, možnost nahlédnout do výstupů internetových skenovacích nástrojů jako např. Shodan apod.).
  - **Vládní CERT nabízí možnost oskenování otevřených služeb v rámci programu průběžného skenování zranitelností.**
- **Uživatelé a hesla**
  - používat pro různé služby různá hesla
  - Složitost hesel, ideálně MFA

Doporučení v rámci **prevence**

- **Uživatelské účty**
  - Omezení admin oprávnění - pro běžnou práci pouze běžná práva.
- **E-maily a přílohy**
  - Pokud nepoužíváte makra zakažte je.
  - Pokud makra využíváte zaveďte ve vaší organizaci podepisování maker a technicky vynuťte spuštění pouze podepsaných maker.
  - Poučení uživatelů.
  - Počet podvržených, a tedy potenciálně nebezpečných e-mailů je možné snížit pomocí kontroly záznamu SPF, DKIM a DMARC u přijatých e-mailů na straně e-mailového serveru.
  - Nastavení restrikce spouštění souborů na klientských stanicích, případně nasadisezení technických prostředků sloužící k prověření škodlivosti příloh před doručením uživateli (např. sandboxing).

Doporučení v rámci **prevence**

- **Logy**
  - Logování a bezpečné ukládání logů (ideálně mimo doménu).
- **Proaktivní monitoring infrastruktury**
  - Prostředky pro detekci anomálií.
- **Krizový plán**
  - Postup reakce na úspěšný ransomwarový útok a obnovu systémů (Disaster Recovery Plan).
  - Minimalizace dopadů útoku na chod organizace (Business Continuity Plan).
  - Plán komunikace.

V rámci **reakce** je třeba

- Mít seznam klíčových lidí z organizace a decision makerů (MKB, DPO, vedoucí/ředitel/náměstek IT, ředitel organizace) a stanovený komunikační plán v případě takového incidentu.
- Mít dostatečný rozpočet pro obnovu infrastruktury.
- Neplatit výkupné.
- Kontaktovat Policii ČR a NÚKIB.
- Definovat nejdůležitější služby, systémy a aktiva pro chod instituce
- Zjistit stav online a off-line záloh.
- Zajistit alternativní internetové připojení.
- Navrhnout novou architekturu sítě.
- Definovat segmentaci sítě.
- Vytvořit čistou VLAN, ve které se začne budovat nová infrastruktura

Co udělal NÚKIB v reakci na útoky ve zdravotnictví

- Znovelizoval vyhlášku č. 437/2014 Sb., o provozovatelích základních služeb.
- Určil dalších 28 nemocnic jako PZS (v prosinci 2020 bylo v odvětví zdravotnictví 16 PZS, nyní jich je 44).
- Provedl audit 16 nemocnic určených jako PZS.
- Provedl řadu penetračních testů.
- Spustil monitoring pro zdravotnická zařízení.
- Spustil online kurz uzpůsobený pro nemocnice (pro všechny).

- Vydal Minimální bezpečnostní standard a řadu dalších doporučení…

Novela vyhlášky č. 437/2014 Sb., o provozovatelích základních služeb

Odvětvová kritéria			Dopadová kritéria
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
5.1. Poskytování zdravotních služeb	Poskytovatel zdravotních služeb podle zákona o zdravotních službách	a) Celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 800, ~~nebo~~ b) statut centra vysoce specializované traumatologické **onkologické, cerebrovaskulární, kardiovaskulární a komplexní kardiovaskulární péče** podle zákona o zdravotních službách, **c) zajišťování urgentního příjmu podle zákona o zdravotnické záchranné službě v zařízení s celkovým počtem lůžek intenzivní péče v posledních třech kalendářních letech nejméně 40 nebo** **d) poskytovatel akutní lůžkové péče s průměrným počtem unikátních ošetřených pacientů v posledních třech kalendářních letech nejméně 100 000 za jeden kalendářní rok.**	Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit I. závažné omezení druhu služby postihující více než 50 000 osob, II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, III. nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření, V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému, nebo VI. kompromitaci citlivých osobních údajů o více než 200 000 osobách.

Minimální bezpečnostní standard

- **Cíl:** Stanovit minimální bezpečnostní požadavky na systémy mimo ZKB
- Dokument obsahuje zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti
- **Nosné části:**
  - Manažerská část – organizační opatření,
  - Technická část – technické opatření;
  - ➢ Bez analýz, seznam požadavků.
- **Vztah k ZKB:** Nelze bez dalšího aplikací standardu mít ZKB za splněný

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Minimální bezpečnostní standard

Další služby

- Ransomware - Doporučení pro mitigaci, prevenci a reakci
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/navody/
- Všechny vzdělávací materiály najdete na stránkách
  - https://nukib.cz/cs/vzdelavani/
  - https://osveta.nukib.cz/
- Informace o hrozbách
  - https://nukib.cz/cs/infoservis/hrozby/
- Scan zranitelností pro nemocnice
  - Žádost na e-mail: nckb@nukib.cz
  - Předmět „Žádost o **scan** zranitelností *nemocniceXY*“
  - V odpovědi na e-mail dostanete informace o dalším postupu
- Monitoring zranitelnosti
  - Žádost na e-mail: nckb@nukib.cz
  - Předmět „Žádost o **monitoring** zranitelností *nemocniceXY*“
  - V odpovědi na e-mail dostanete informace o dalším postupu
- E-learning
  - Žádost na e-mail: vzdelavani@nukib.cz.

Co dělat dál?

Na úrovni státu

- Stanovit standardy pro různé úrovně poskytovatelů zdravotních služeb.
- Stanovit povinnost tyto standardy dodržovat.
- Na tyto standardy navázat financování.
- Zajistit metodickou podporu plnění standardů.

Na úrovni poskytovatelů

- Nečekat, že to za ně někdo udělá
- Stanovit si plán, začít aspoň s něčím..
- Školení uživatelů (možno realizovat přes NÚKIB)

+ financování

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz