Praktické řízení kybernetické bezpečnosti v nemocnici

Mgr. Jakub Machka, MBA

Manažer kybernetické bezpečnosti Fakultní nemocnice Plzeň a Nemocnice Na Homolce

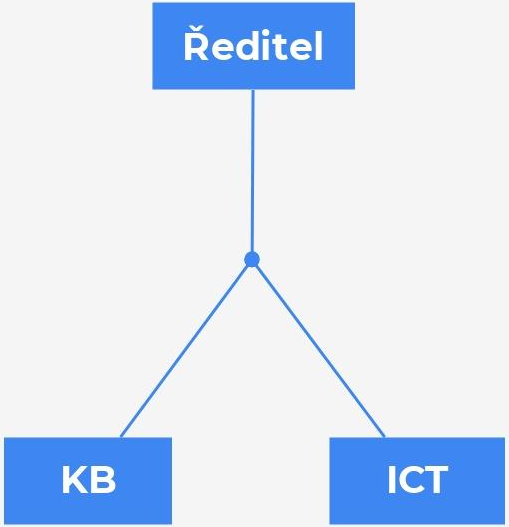
Nemocnice spadá pod zákon o kybernetické bezpečnosti a co teď?

Zkušenosti a dobrá praxe....

Agenda

1. Předpoklady fungování kybernetické bezpečnosti
2. Prvky kybernetické bezpečnosti
3. Procesy
4. Technologie
5. Lidé
6. Shrnutí a základní principy

Předpoklady fungování kybernetické bezpečnosti



Nemocnice ví o rizicích a chce je řešit

- Nemocnice si je **vědoma rizik** kybernetické bezpečnosti
- Vedení je ochotné a připravené **zajistit dostatečné zdroje** pro budování Systému řízení bezpečnosti informací
- Součástí **VŘKB** jsou členové vrcholového vedení

Organizační začlenění

- MKB **není** součástí organizační struktury ICT (rozdílné potřeby)
- MKB organizačně spadá **přímo pod statutárního zástupce** (přímá komunikace)
- **Blízkost** k vrcholovému vedení

Podpora vrcholového vedení

- **Aktivní** podpora, **řešení** problémů a **rozhodování**
- **Ochota a vůle** měnit zaběhlé procesy, postupy a chod nemocnice

Prvky kybernetické bezpečnosti

Princip založený na riziku

Lidé

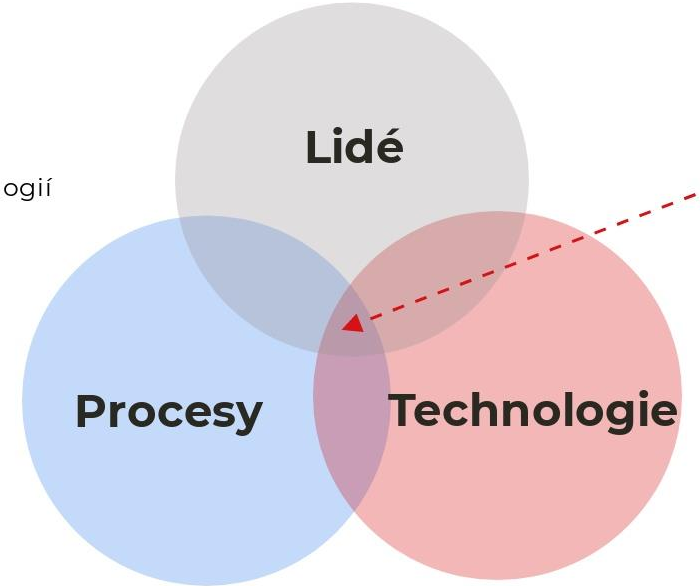
Role a odpovědnosti

Kapacitní plánování

Dodržování procesů a ovládání technologií

Schopnosti a kompetence

Kontinuální vzdělávání



Cílem je zajištění rovnováhy

Procesy

Systematické činnosti a formalizované procesy

Dokumentovaná pravidla, procesy a bezpečnostní opatření

Dodržování, kontrola a vymáhání plnění

Technologie

Správa, údržba a rozvoj ICT technologií

Bezpečnostní a provozní technologie

Zdravotnické prostředky

Procesy

Akceptace a porozumění prostředí nemocnice

Akceptace prostředí

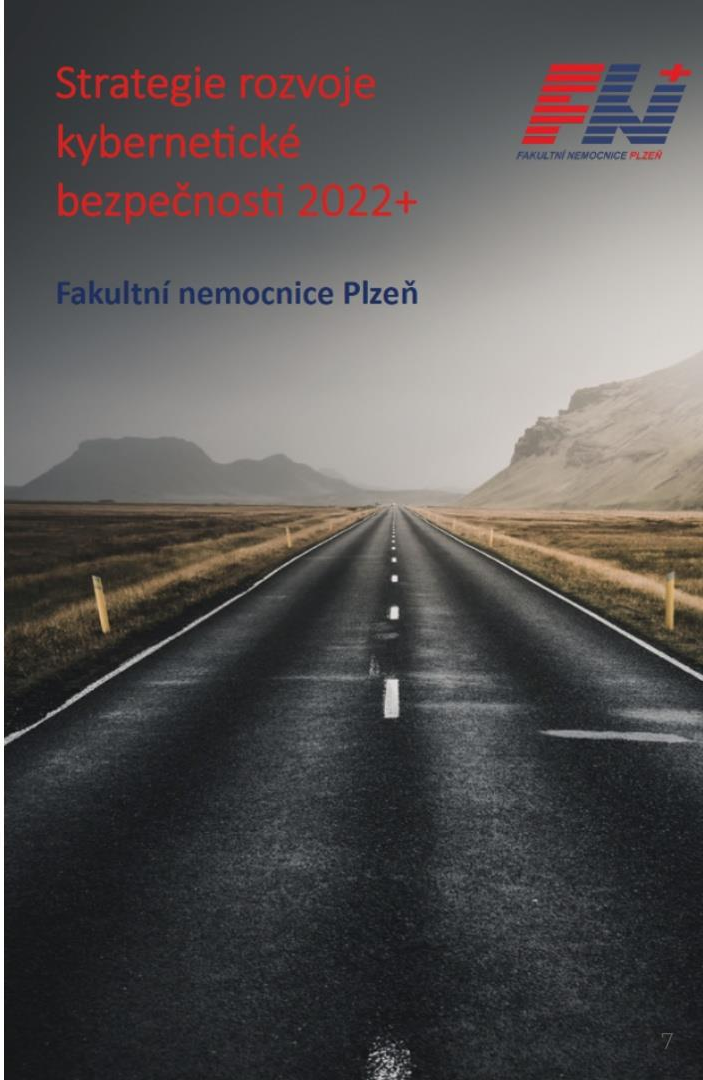
- Kybernetická bezpečnost je **podpůrnou službou** pro naplnění primárního cíle nemocnice

Porozumění prostředí nemocnice

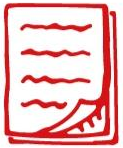
- Porozumění potřebám, zvyklostem, stavu a prioritám nemocnice
- Definování **rozsahu** Systému řízení bezpečnosti informací

Strategie a akční plán rozvoje kybernetické bezpečnosti

- Principy budování kybernetické bezpečnosti
- Strategické cíle
- Harmonogram činností (akční plán)



Poznání vnitřního prostředí nemocnice



Poznání procesů a dokumentů

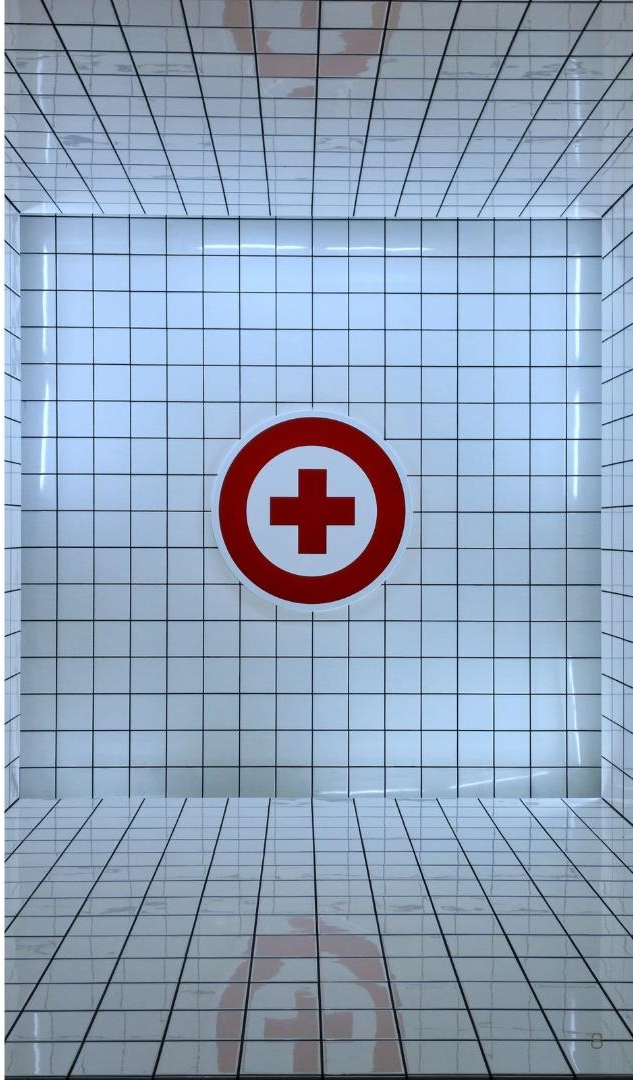
- Poznání závazných dokumentů řízené dokumentace
- Poznání zaběhlých a nezdokumentovaných procesů, pravidel a zvyklostí

Identifikace primárních aktiv

- Procesy (služby) a informace nemocnice
- Identifikace garantů aktiv a seznámení s jejich rolí a odpovědnostmi

Identifikace podpůrných aktiv

- Vše, co je potřeba pro zajištění procesů (služeb) a informací
- Identifikace garantů aktiv a seznámení s jejich rolí a odpovědnostmi



	Název kategorie primárního aktiva	Popis	Rozsah ISMS	Dův.	Int.	Dost.	Norm Dův.	Norm Int.	Norm Dost.	Garant primárního aktiva	Organizační složka	Odůvodnění ohodnocení
PRI1	Řízení, vize, strategie a změny	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI3	Administrace a logistika pacientů	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI4	Ambulantní péče	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI5	Diagnostická péče	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI6	Hospitalizace – lůžková péče	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI7	Služby operačních sálů (COS)	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI8	Ošetřovatelská péče	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI10	Zdravotně sociální péče	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI11	Lékárna	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI12	Laboratoře	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI16	Správa a údržba zdravotnických prostředků	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI17	Věda a výzkum	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI19	Nákup a veřejné zakázky	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI20	Provoz a výstavba	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI21	Správa informačních systémů a technologií	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI22	Personalistika, vzdělávání a mzdy	.....	Ano/ne	1	1	1	1	1	1	.....	.....	.....
PRI23	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....

Budování ISMS

Plán vzniku bezpečnostní dokumentace		
Úroveň	**Dokument**	**Nový nebo doplnění**
Úroveň 1	Příručka kvality a bezpečnosti	Doplnění
	Organizační řád	Doplnění
	Politika systému řízení bezpečnosti informací	Nový
	Politika systému řízení bezpečnosti informací - deklarace	Nový
Úroveň 2	**Provozní bezpečnost ICT**	Nový
	Bezpečnostní příručka pro uživatele	Nový
	Ochrana osobních údajů	Doplnění
	Řízení dokumentů a záznamů	Doplnění
	Informační systém, pravidla jeho používání, bezpečnost dat	Doplnění
	Uzavírání smluv	Doplnění
	Postup při vzdělávání zaměstnanců	Doplnění
	Adaptační proces zaměstnanců	Doplnění
	Vzdělávání v oblasti bezpečnosti	Nový
	Vnitřní havarijní plán	Doplnění
	Plán krizové připravenosti	Doplnění
	Závazný postup realizace zakázek malého rozsahu	Doplnění
	Použití zdravotnických prostředků	Doplnění
	Nežádoucí události	Doplnění
	Interní audit kvality	Doplnění
	Organizace zadávání veřejných zakázek	Doplnění
	Zabezpečení BOZP	Doplnění
	.... a další	Doplnění
Úroveň 3	**Metodika identifikace a hodnocení aktiv a rizik**	Nový
	Metodia analýzy dopadů na provoz	Nový
	Záznamy a evidence	Nový

- **Začlenění** ISMS do způsobu fungování nemocnice

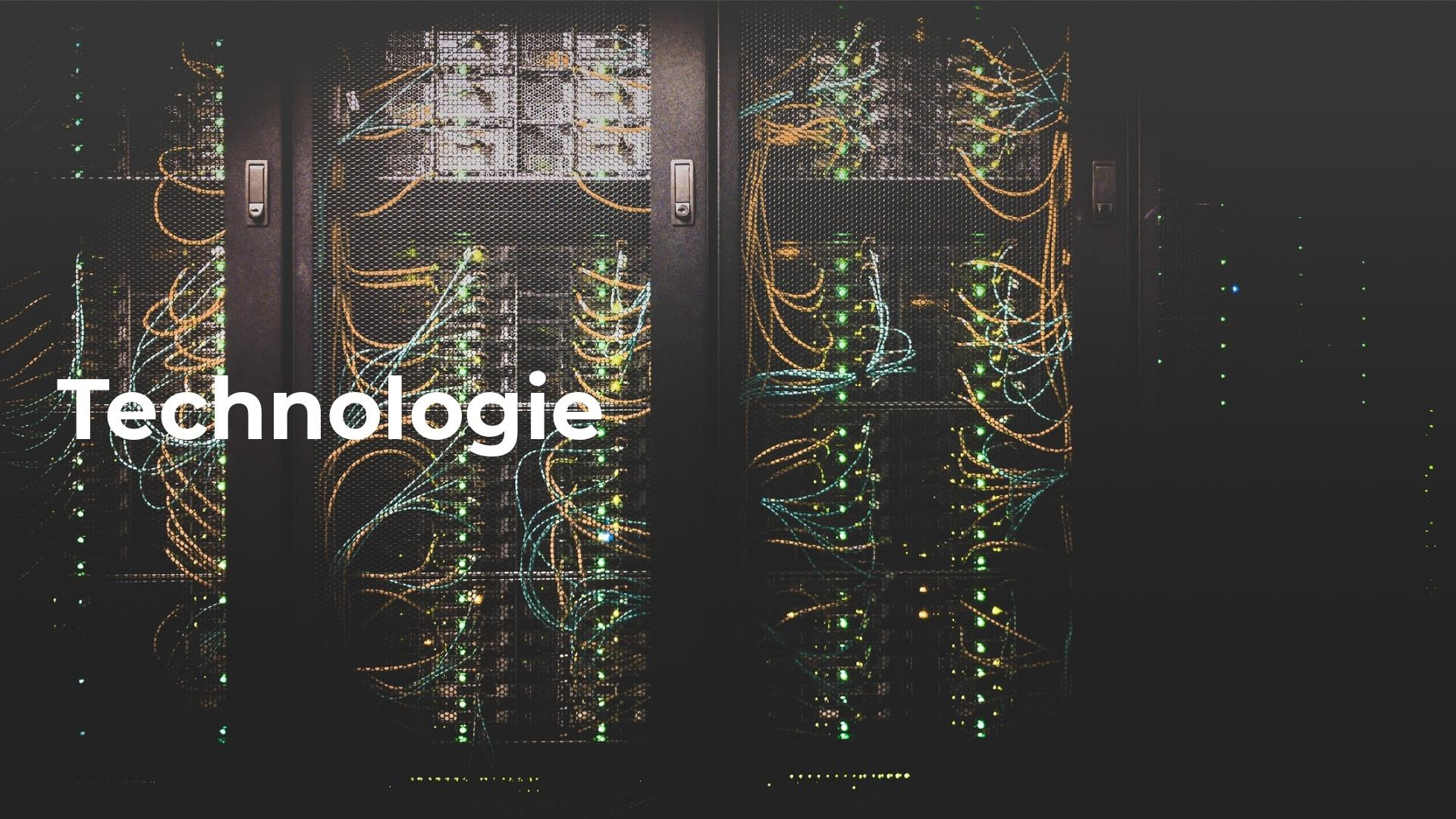
  Procesní uchopení budování Systému řízení bezpečnosti informací

- **Postupné** zavádění změn a neustálé vysvětlování

- **Minimalizace** nových dokumentů

  Např. tvorba 5 nových celonemocničních dokumentů

- **Obohacení** v současné době existujících dokumentů



Technologie

Bezpečnostní technologie a řízení dodavatelů

Výběr a nákup technologie

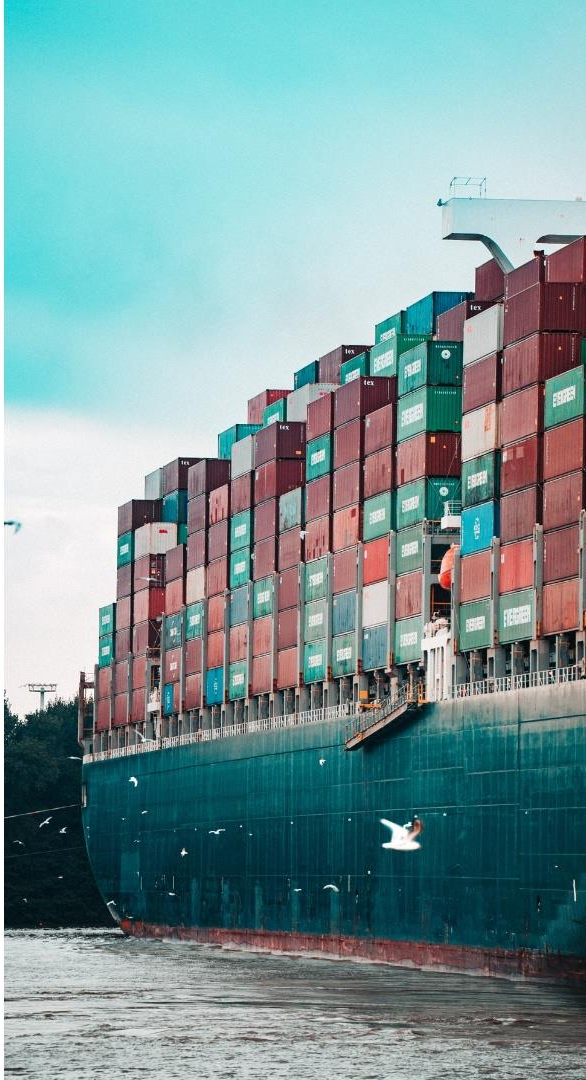
- Financování (IROP, NPO...)
- Důsledná příprava návrhu a prostředí
- Řízení kapacit a udržitelnost

Správa a rozvoj technologie

- Implementací vše nekončí, ale začíná - neustálá optimalizace
- Dodavatel vše nevyřeší, často prostředí nezná a nerozumí provozu nemocnice

Řízení dodavatelů

- Koordinace dodavatele s interním týmem nemocnice
- Důsledná kontrola plnění dodávek a služeb
- Kontrola plnění SLA a smluvnách ujednání



… na co se soustředit a co dál?

Řízení technických zranitelností

- Technická zranitelnost = otevřené dveře pro útočníka
- Mít nástroj pro automatizované skenování zranitelností (DMZ, servery, uživatelská síť…)
- Mít proces a pravidelné vyhodnocování a odstraňování zranitelností

DLP a ochrana důvěrnosti informací

- Mít nástroj, proces …
- Podpora vedení a aktivní kroky při řešení incidentů
- Zpětná vazba pro zaměstnance

Nástroj pro řízení aktiv a jejich bezpečnosti

- Automatizovaný real-time přehled o ZP a dalších technických aktivech v síti
- Řízení zranitelností a nebezpečných komunikací
- Řízení změn


Lidé

Klíčový prvek kybernetické bezpečnosti

Kategorie lidských zdrojů

- Vrcholové vedení
- Garanti aktiv
- Běžní uživatelé

Odlišná komunikace

- Ke každé kategorii je potřeba přistupovat jiným způsobem
- Sdělovat stejné informace jiným jazykem

Vzdělávání a naslouchání

- Je potřeba mít stále otevřené dveře a naslouchat požadavkům (KB je něco nového)
- Základem je neustálé vzdělávání

Vzdělávání uživatelů

- **Jeden dokument**, jedno místo, kde se dozví vše o bezpečnosti
- **Každoroční školení**
  Test, který nelze "opsat"
- **Navštěvovat** porady a **propagovat** oblast KB
  Porada vrchních sester
  Porada primářů a přednostů
  a další .....
- **Seriál kybernetické bezpečnosti**
  Vysvětlovat základní pravidla jednoduchou cestou
  Vydání příručky v tištěné podobě

Phishingová kampaň

Cílem je zvýšení bezpečnostního povědomí a obezřetnosti uživatelů

Celoroční komplexní kampaň

Působení na emoční prožitek uživatele

Specifika kampaně

Průběžně (2-3 měsíce) rozesílání e-mailů napříč odděleními a klinikami nemocnice

Rozdílná náročnost e-mailů

Propagace alespoň 2 měsíce dopředu

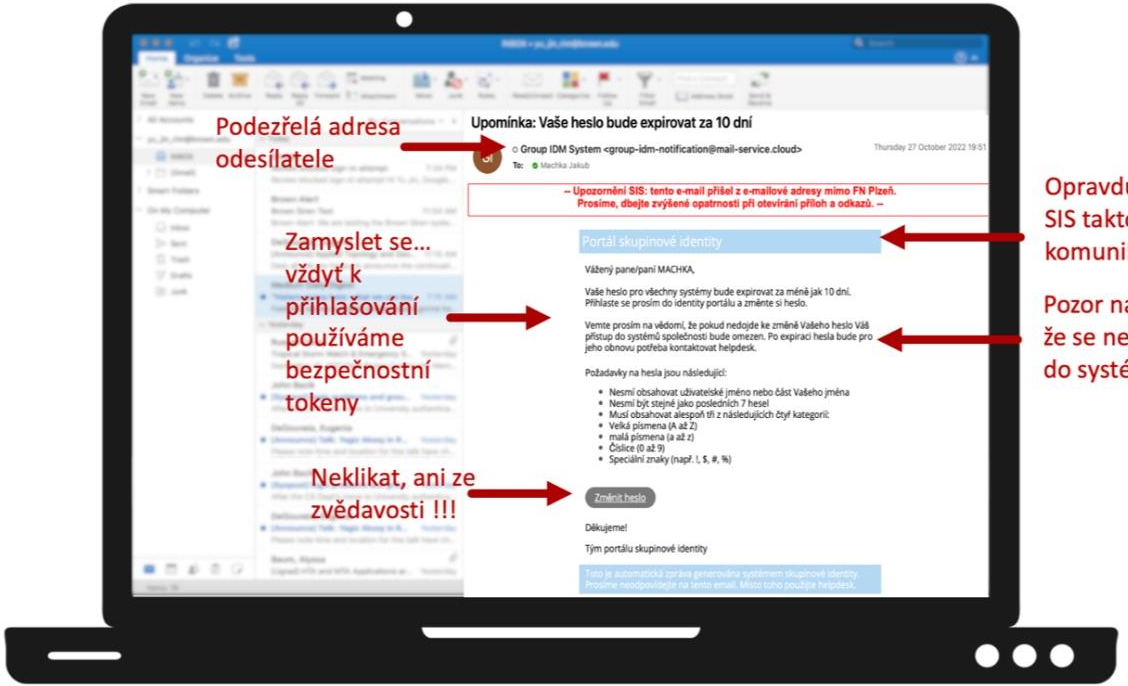
Informování uživatelů o cíli, způsobu vedení kampaně

Zpětná vazba

Získání zpětné vazby od uživatelů

Vyhodnocování přínosů a reálného posunu bezpečnostního povědomí

Důležitá je zpětná vazba a prezentace vhodné reakce…



Vzdělávání a komunikace vrcholového vedení

Přímý přístup

- Mít přístup k členům vrcholového vedení - ideálně být členem porady vedení
- Mít prostor pro diskuzi

Výbor pro řízení kybernetické bezpečnosti

- Mít zástupce vrcholového vedení ve Výboru pro řízení kybernetické bezpečnosti
- Prezentování stavu a rozvoje kybernetické bezpečnosti

Způsob komunikace

- Jednoduše vysvětlovat technické i netechnické oblasti
- ...pokud něčemu rozumím, tak o tom můžu rozhodnout

Principy budování kybernetické bezpečnosti

1

Respektování nemocničního prostředí a zavedených procesů

Přizpůsobení Systému řízení bezpečnosti informací

Začlenění nových dokumentů, pravidel a procesů do již existujících – obohacení již existujících

2

Důraz na **nenarušení kontinuity** běžného chodu

Kybernetická bezpečnost je podpůrnou službou pro zajišťování zdravotní péče

3

Neustále **zvyšování povědomí** a **propagace** oblasti kybernetické bezpečnosti

Zvyšování bezpečnostního povědomí uživatelů a vrcholového vedení

Diskuze nad rolemi a odpovědnostmi

4

Vzájemná spolupráce a **komunikace** napříč nemocnicí

Zajištění kybernetické bezpečnosti není jenom o IT

Je nezbytná součinnost všech zaměstnanců

Aktivní účast vrcholového vedení

Postupné informování a komunikace o novinkách a změnách

Děkuji za pozornost

Mgr. Jakub Machka, MBA

machkaj@fnplzen.cz

https://www.linkedin.com/in/jakub-machka/