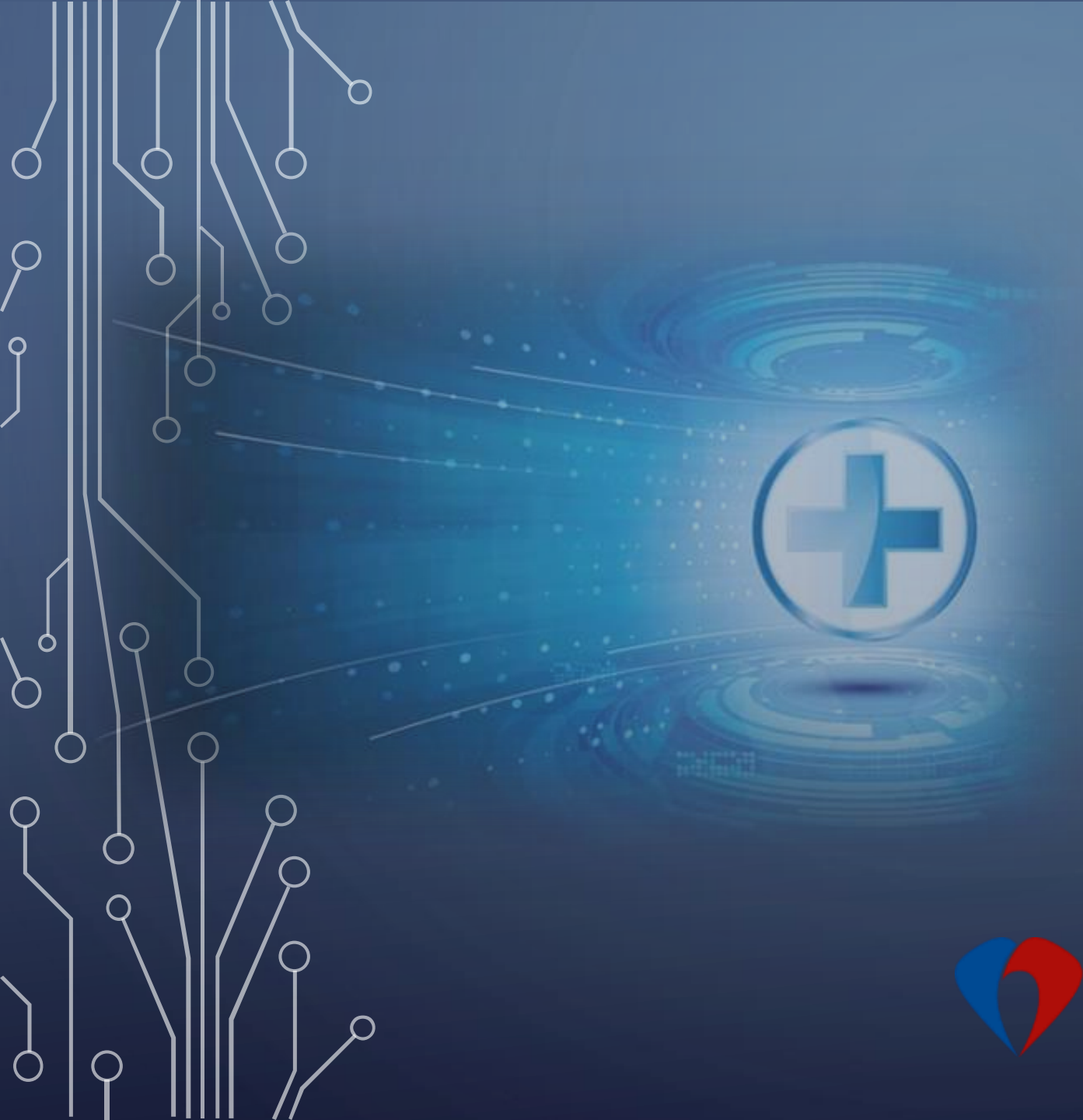


JAK SLADIT VELKOU NEMOCNICI SE ZÁKONEM O KYBERNETICKÉ BEZPEČNOSTI

ING. ANTONÍN HLAVINKA

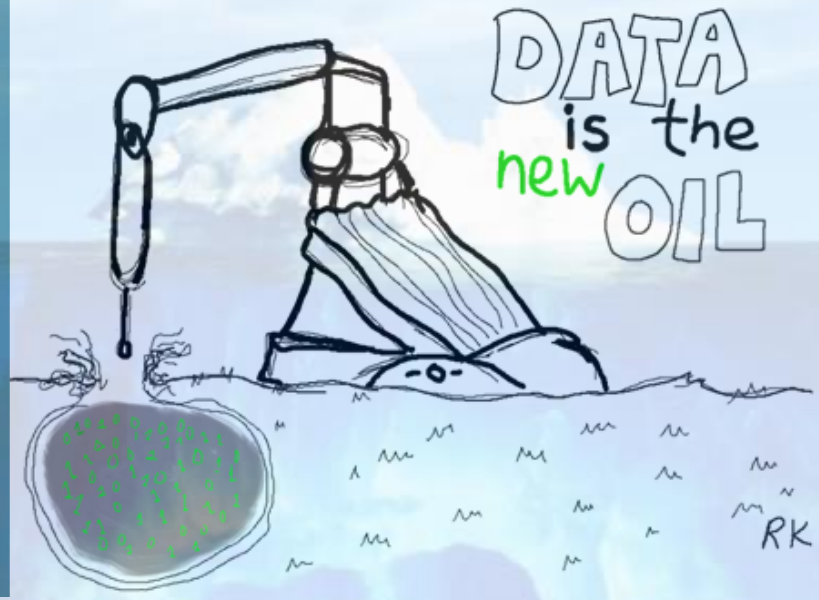
FNOL, NTMC

AHCM - 4. ÚNOR 2021

FAKULTNÍ NEMOCNICE® OLOMOUC

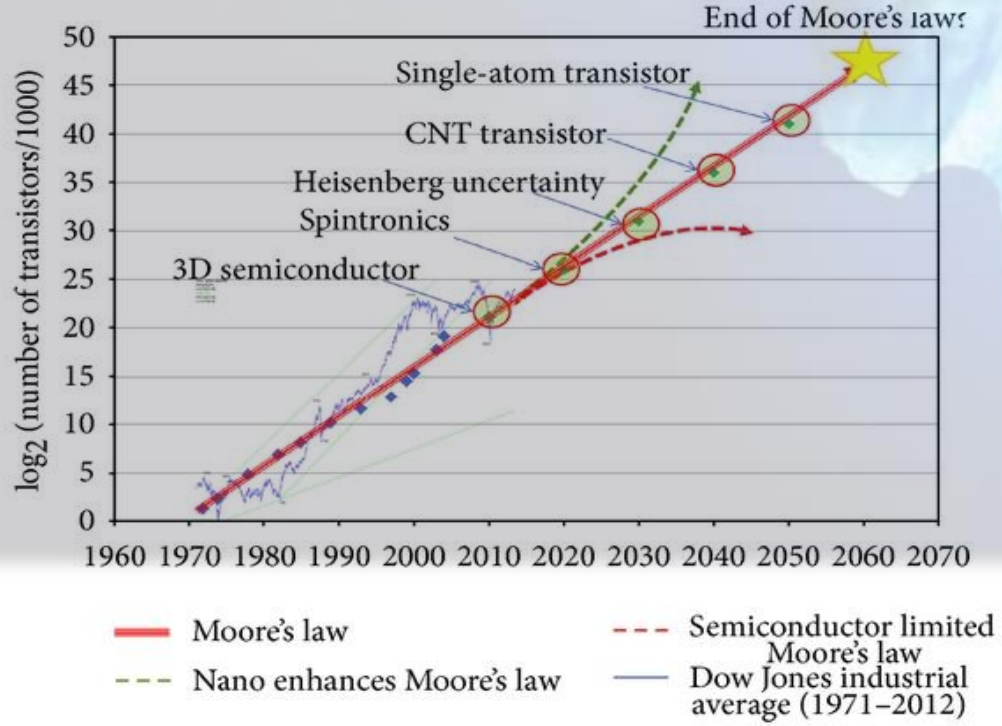
NÁRODNÍ TELEMEDICÍNSKÉ CENTRUM

DOBA DATOVÁ



"I ask that you think of Data as the next natural resource"

Ginni Rometty, IBM CEO



Data jsou komodita 21.století, bez dat nelze prakticky přežít

- **90%** všech na světě dostupných dat vzniklo v posledních **2 letech**
- Každou vteřinu vznikne tolik dat, že by naplnily **150 miliónů** knih

FAKULTNÍ NEMOCNICE OLOMOUC

PROČ JE BEZPEČNOST DŮLEŽITÁ?

- 2015 - Třetině pacientů v USA byla v loni odcizena osobní data, 80 mil. uživatelů jednorázově (celkem 120 mil. za rok 2015!), pokuta 16 mil. USD https://www.root.cz/clanky/tretine-pacientu-v-usa-byla-v-loni-odcizena-osobni-data/
  - Průměrně je hlášeno 250 incidentů úniků dat v USA
  - Dle studie společností IBM Security a Ponemon Institute postihuje únik dat až 90 % poskytovatelů zdravotních služeb v USA! https://www.ponemon.org/research/ponemon-library/security/nearly-90-percent-of-healthcare-organizations-suffer-data-breaches-new-ponemon-study-shows.html
- 2018 - Portugalská nemocnice Centro Hospitalar Barreiro Montijo dostala 400 tis. EUR pokutu za GDPR, únik dat https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/
- 2018 - Média informovala o možném úniku zdravotních dat téměř 2,9 milionů obyvatel Norska skrze napadení systémů Helse Sør-Øst, organizace, která spravuje nemocnice v jihovýchodním regionu Norska vč. Osla https://www.helse-sorost.no/nyheter/innbrudd-i-datasystemene-til-sykehuspartner-i-helse-sor-ost
- 2019/2020 - Kyberútoky na české zdravotnictví – Benešov (60 mil. Kč), Kosmonosy, FN Brno (až stovky mil. Kč), Ostrava… https://benesovsky.denik.cz/zlociny-a-soudy/utok-na-nemocnici-benesov-zpusobil-skodu-59-milionu-korun-20200818.html
- 2020 – Finsko, zcizeno přes 40 tis. zdravotních záznamů z 25 psychoterapeutických center (Vestaamo), vydírání jak center, tak i pacientů pod výhružkou zveřejnění (€ 500)! https://www.vice.com/en/article/n7vw9d/hackers-are-holding-psychotherapy-data-ransom
- 2021 – ČR, nemocnice Horažďovice, vyřazen NIS, škoda cca 150 tis. Kč,
  - Za poslední dva měsíce loňského roku počet kybernetických útoků ve zdravotnictví ve střední Evropě vzrostl o **145 procent**. Aktivity hackerů jsou přímo spojené s nouzovým stavem kvůli epidemii koronaviru.

CO JE TŘEBA ZABEZPEČIT?

- Autentizace pacientů a jejich přihlašování
  - Ověřování identity, NIA, IDRR, řízení souhlasů
- Integrace aplikací do NIS, sdílení dat, výsledků…
  - Originály zdr. dokumentace, platnost dokumentů
- Přenos dat mezi aplikací a certifikovanými zařízeními (BT - glukometry, váhy, tlakoměry…)
- Zabezpečený vzdálený přístup do aplikace/zařízení pacientů
  - Servisní služby (geek team)

NUTNÁ SYSTÉMOVÁ OPATŘENÍ

- Financování
  - Náklady na kyberbezpečnost z úhrady za zdravotní péči pojišťoven? Prof. Válek…
  - Motivace pro odborníky do státního sektoru
- Rezortní CERT
  - Spolupráce NUKIB, NAKIT, CESNET, MZd, UZIS, iniciativa již vznikla „hSOC“
  - **Priority v eHealth, jak chcete provozovat eHealth bez KB??? (EU React a další dotační tituly)**
- Rozšíření ZoKB na širší okruh poskytovatelů ZP (letos 19 nových)
  - Připojení do celonárodní eHealth sítě
  - Zákon o eHealth

hSOC – Hospital Security Operation Centre

Více na https://hsoc.cesnet.cz

Vznikl jako dobrovolná iniciativa „ajťáků“ nemocnic a krajů po kyber útocích – služby PZP jsou poskytovány ZDARMA

ČVUT ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ČESKÝ INSTITUT INFORMATIKY ROBOTIKY A KYBERNETIKY

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY

cesnet

NÚKIB

NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

Mezi možné činnosti navrhovaného subjektu (SOC) by mělo patřit například:

- Bezpečnostní aspekty provozu a monitoringu bezpečné síťové infrastruktury.
- Koordinace systému včasné výstrahy před hrozbami.
- Bezpečnostní aspekty provozu vybraných sdílených informačních systémů resortu zdravotnictví (např. Národní kontaktní místo elektronického zdravotnictví).
- Příprava vzdělávacích programů zaměstnanců (včetně manažerů) poskytovatelů zdravotních služeb v oblasti kybernetické bezpečnosti. Možnost centrálního vzdělávání (e-learning) + místní odlišnosti (školení). Minimálně povinná položka plánu vzdělávání.
- Poskytování služeb laboratoře pro bezpečnostní testování a certifikaci.
- Vznik sdíleného akreditovaného CSIRT/response týmu.

Vize – Cílový stav

Poskytovatelé zdravotních služeb provozující bezpečné informační technologie s dostatečným technickým a personálním zázemím s podporou centralizované ochrany typu SOC.

JAK JSME POSTUPOVALI PŘI ZAVÁDĚNÍ ZKB?

1. PŘESVĚDČIT VEDENÍ FNOL, NEJDŮLEŽITĚJŠÍ KROK K POSÍLENÍ IT ODDĚLENÍ

ZKB vs. eHealth v ČR - rizika

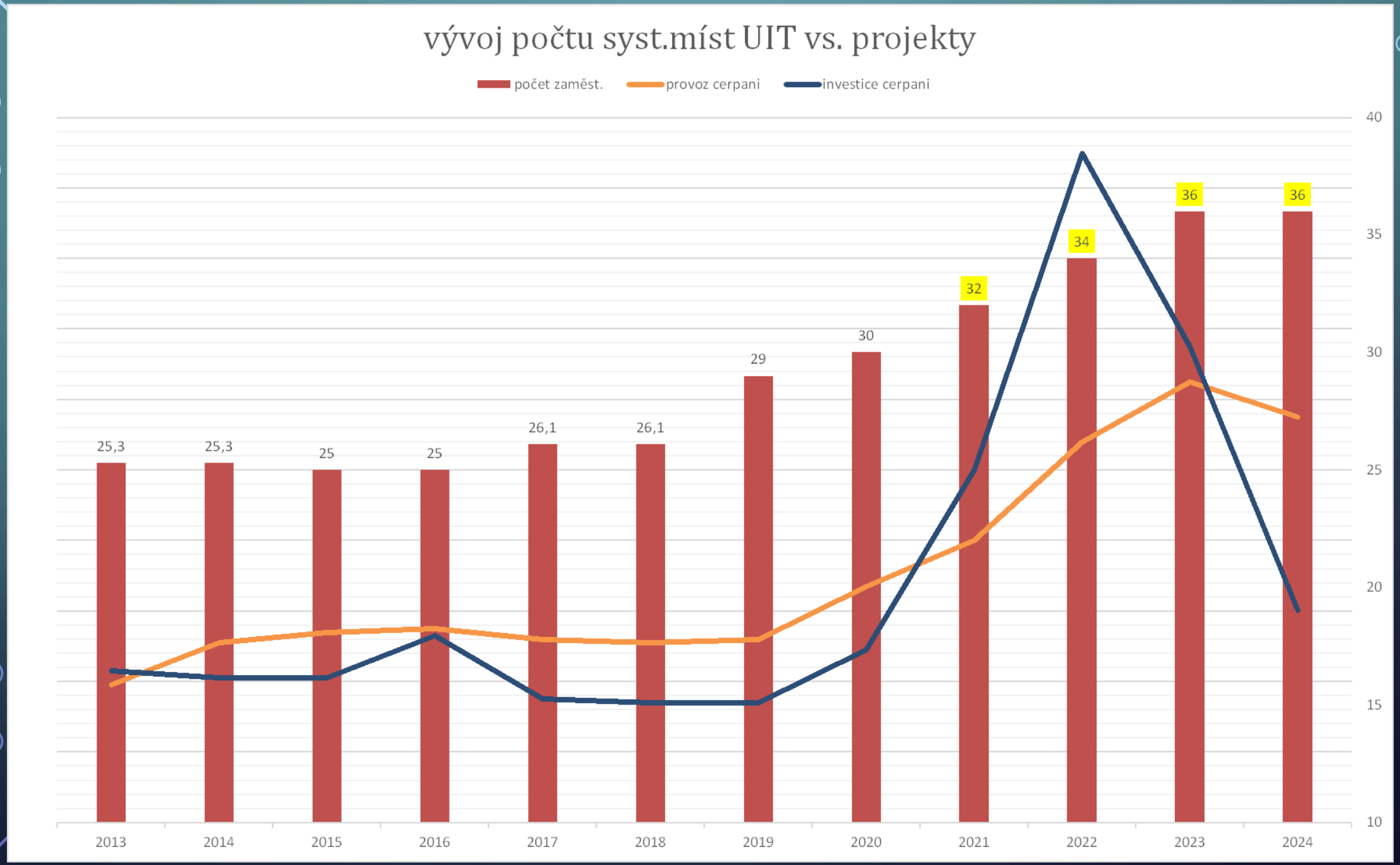
- **Není legislativní prostředí** pro zavedení digitálního zdravotnictví
- **Velmi omezená penetrace ZKB u poskytovatelů ZP**
- Neexistuje centrální bod pro sjednocení a připojení poskytovatelů ZP
- Datová nejednotnost a omezená strukturovanost zdravotnických dat a dokumentace (využití mezinárodních standardů a formátů)
- **Velké rezervy ve vzdělávání v ICT** nejen na lékařských fakultách
- Špatná spolupráce pojišťoven, větší angažovanost a potřeba dat (vlastní analytické pracoviště a spolupráce s poskytovateli e-Health dat)
- Zastaralost standardních dodavatelů NIS, nutná modularita, otevřenost a podpora standardů
- Celková rigidita a omezená pružnost celého zdravotnictví při nasazování Digital Health obecně
- **Málo IT profesionálů – málo důrazné a naléhavé IT oddělení, atraktivita zaměstnavatele pro IT profesionály** (finance)

ZDRAVOTNICKÉ ZAŘÍZENÍ	Celkový počet zaměstnanců (SM)	Počet zaměstnanců (SM)IT pracovišť	% z celkem
Fakultní nemocnice [redacted]	5 433	73,6	1,35%
Fakultní nemocnice [redacted]	4 500	32	0,71%
Fakultní nemocnice [redacted]	3 000	31	1,03%
Fakultní nemocnice Olomouc	3 902	31	0,79%
Fakultní nemocnice [redacted]	4 668	27	0,58%
Fakultní nemocnice [redacted]	3 396	32	0,94%
Fakultní nemocnice [redacted]	3 100	42	1,35%
Fakultní nemocnice [redacted]	5667	98	1,73%
[redacted]	2409	28	1,16%
[redacted]	4 000	43	1,08%
		Průměr	1,07%
		Do průměru chybí 8 syst.míst UIT	

Během digitalizace bank byla penetrace IT pracovníků přes 9%!

SROVNÁNÍ IT PRACOVNÍKŮ K CELKOVÉMU POČTU SYSTEMIZOVANÝCH MÍST, PŘÍMOŘÍZENÉ NEMOCNICE

vývoj počtu syst.míst UIT vs. projekty



Pracovníci ZKB – z Analýzy rizik a BIA

Role /Činnost	Interní / externí zajištění	a. Reakce na kybernetické bezpečnostní incidenty	b. Řízení kyber. zranitelností a bezpečnostních testů	c. Zajištění bezpečnosti provozu ICT	d. Řízení bezpečnosti projektů a dodavatelů	e. Řízení bezpečnostní dokumentace	f. Bezpečnostní povědomí a příprava školení	g. Audity a kontroly	h. Zajištění systému kybernetické bezpečnosti	SUMA FTE
Manažer KB	FNOL	0,1	x	x	0,2	0,3	0,05	x	0,5	1,25
Technik oddělení KB	FNOL	0,1	0,15	0,1	0,7	0,2	0,25	0,1	0,3	1,575
Technik ICT	FNOL	~~0,3~~	0,6	0,6	x	0,2	x	x	x	1,4
Tiskový mluvčí	FNOL	0,05	x	x	x	x	x	x	x	0,05
Architekt KB	Externí	0,05	x	0,1	0,1	x	x	x	x	0,25
Právník	FNOL	x	x	x	0,1	x	x	x	x	0,1
Referent oddělení kvality	FNOL	x	x	x	x	0,05	x	x	x	0,05
Pracovník personálního úseku	FNOL	x	x	x	x	x	0,05	x	x	0,05
Interní auditor (odd. kvality)	FNOL	x	x	x	x	x	x	0,1	x	0,1

Závěr: Pro zajištění systému kybernetické bezpečnosti navrženo **1,6 FTE pro technika oddělení kybernetické bezpečnosti** a **1,4 FTE pro oddělení ICT**. Ostatní činnosti je možné částečně zajistit externí službou a v rámci stávajících pracovních úvazků zaměstnanců.

Celkem tedy minimální požadavek 1+1 člověk na KB (1 další bude externí dodávkou v rámci ZKB služeb).

JAK JSME POSTUPOVALI PŘI ZAVÁDĚNÍ ZKB?

2. ROZSAH ISMS, ANALÝZA RIZIK A BUSINESS IMPACT ANALÝZA (AR A BIA)

PLÁN PROJEKTU, ANEB OPRAVDU TO JDE ZVLÁDNOU ZA MĚSÍC ČI DVA? ANI NÁHODOU.

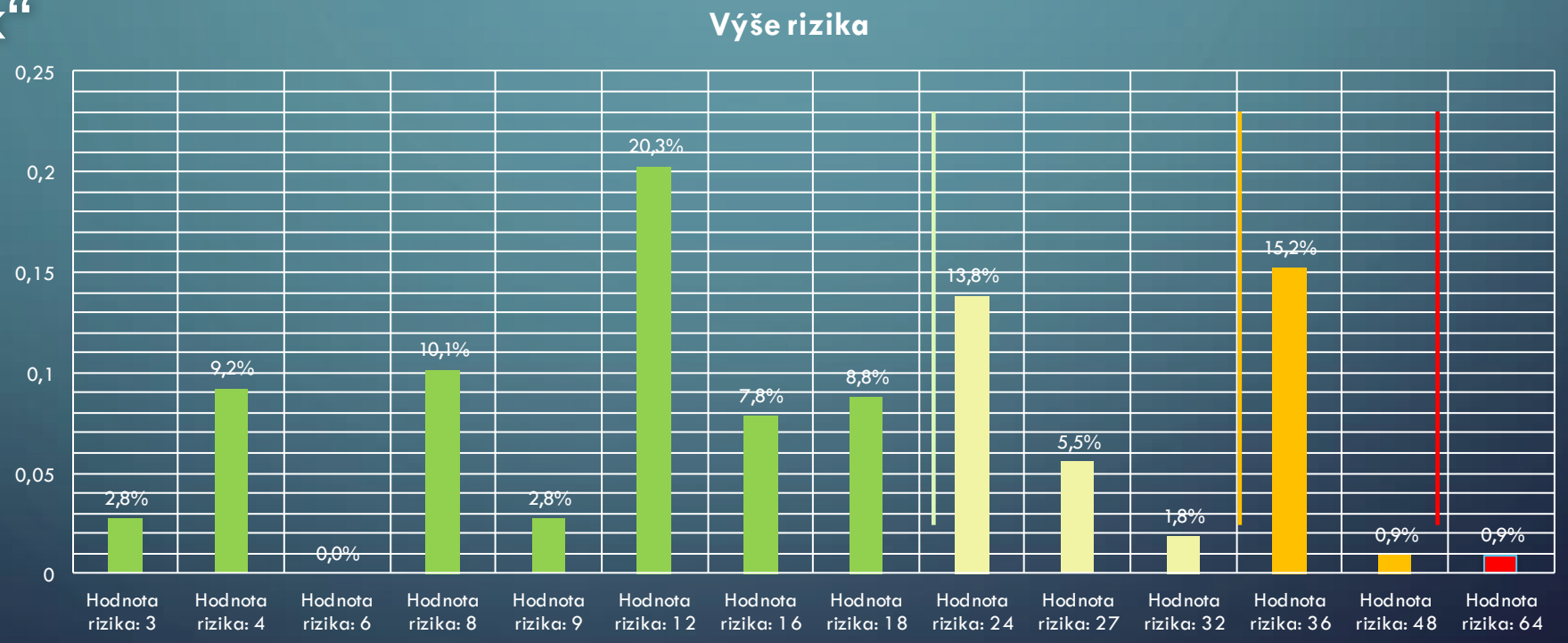
Etapa	Popis činnosti	Požadovaný termín
1. Fáze	Kick off	T
	Rozsah a hranice systému řízení informační bezpečnosti	T + 15
	Organizační role, odpovědnost a pravomoci v rámci ZoKB a ISMS	T + 30
	Metodika hodnocení rizik	T + 45
	Analýza rizik bezpečnosti informací (zahrnuje Identifikace a hodnocení aktiv)	T + 90
	Návrh plánu ošetření rizik /zvládání rizik a Prohlášení o aplikovatelnosti	T + 150
	Akceptace 1. fáze	T + 150
2. Fáze	Bezpečnostní politika a Bezpečnostní a provozní dokumentace, návrh ISMS - organizace, role, odpovědnost	T + 360
	Plán bezpečnostního vědomí zaměstnanců (školení, informovanost, odborná způsobilost)	T + 390
	Interní audity a Přezkoumání ISMS	T + 420
	Proces kontinuálního zlepšování	T + 450
	Harmonizace a podpora přípravy organizace v dalších činnostech	T + 465
	Akceptace 2. fáze	T + 465

URČENÍ PRIMÁRNÍCH + PODPŮRNÝCH AKTIV, A JEJICH VAZBY

Podpůrná aktiva			Primární aktiva																							
Typ	**Kategorie**	**Podpůrná aktiva**	ta AQURE	ta Astraia	**ta BTL Cardiopoint**	ta CareLink Personal	**ta CATO**	ta Centrální registr	ta COBASIT	ta Coffalyser	ta Cryus	**ta EnvisKUK**	ta Evidenční kniha	ta FERDA	ta FONS - Akord	**ta IMPAX**	**ta Lims**	ta Lucia	**ta Marie PACS**	ta MASC	**ta MEDEA**	ta MEDIX	ta MOSAIQ	**ta Nefris**	ta NEUROL - EMG	**ta OpenLims**	ta Operační kniha
HW	HW - servery služeb infrastuktury	backup	x	x	x		x	x	x		x	x	x	x	x	x	x	x		x	x	x		x		x	
HW	HW - bezpečnost	externí FW																	x								
HW	HW - bezpečnost	interní fw																	x								
HW	HW - bezpečnost	IPS																	x								
HW	HW - provozní podmínky	chlazení serveroven	x	x	x		x	x	x		x	x	x	x	x	x	x	x	x	x	x	x		x		x	
HW	HW - provozní podmínky	napájení serveroven	x	x	x		x	x	x		x	x	x	x	x	x	x	x	x	x	x	x		x		x	
HW	HW - provozní podmínky	pájení distribučních bodů	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
HW	HW - provozní podmínky	napájení koncových prvků	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
HW	HW - zdravotnická technika	IVD															x									x	
HW	HW - zdravotnická technika	diagnostické přístroje - životní funkce			x																						
HW	HW - zdravotnická technika	diagnostické přístroje - ostatní																	x								
HW	HW - zdravotnická technika	terapeutické přístroje s databází																									
HW	HW - zdravotnická technika	terapeutické přístroje bez databáze																									
HW	HW - zdravotnická technika	Implantabilní přístroje																									
Objekt	Prostory	klíčové prostory	x	x	x		x	x	x		x	x	x	x	x	x	x	x	x	x	x	x		x		x	
Objekt	Prostory	ostatní prostory		x	x					x		x					x		x				x		x	x	x
SW	LIS	AQURE	x																								

ANALÝZA RIZIK A JEJÍ VÝSLEDKY

- V rámci analýzy rizik bylo identifikováno a ohodnoceno **217 rizik.** Jejich popis a interpretace je uvedena ve „Zprávě o hodnocení aktiv a rizik“



ANALÝZA RIZIK A JEJÍ VÝSLEDKY

- Nejrizikovější aktiva/skupiny aktiv – TOP5

Skupina aktiv	Součet hodnoty rizika
Endpoint	588
Zdravotnická technika diagnostická - ostatní	452
Zdravotnická technika diagnostická - životní funkce	448
Síťová a bezpečnostní infrastruktura	428
Skupina aktiv informačního systému KIS	404

- Hrozby s nejvyšším rizikem – TOP4 *(hodnoty 64 a 48)*

Skupina aktiv	Hrozba	Výše rizika
Skupina aktiv - Endpoint	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživ. a admin.	64
Skupina aktiv - Endpoint	Zneužití identity	64
Skupina aktiv informačního systému KIS	Porušení bezp. politiky, provedení neoprávněných činností	48
Skupina aktiv informačního systému KIS	Zneužití identity	48

VÝSTUPY BIA

Dopady nedostupnost	15M	1H	4H	12H	1D	1W	1M	MTPD	MIPD
Medea	0	1	1	2	2	3	4	1W	12H
Zdravotnická technika - hospitalizace	0	3	3	3	3	3	3	1H	1H
Openlims	1	2	3	3	3	3	4	4H	1H
PACS	0	3	4	4	4	4	4	1H	1H
LIMS	0	0	0	1	2	3	4	1W	1D
Analyzátory	1	2	3	3	3	3	3	4H	1H
Modality	1	2	4	4	4	4	4	4H	1H

Závěr

a) Při porovnání časů MTPD a MIPD se jeví kritičnost jednotlivých analyzovaných systémů FNOL následovně:

1. PACS + modality
2. Zdravotnická technika – sloužící k monitoringu vitálních funkcí
3. Openlims + analyzátory
4. Medea
5. Lims

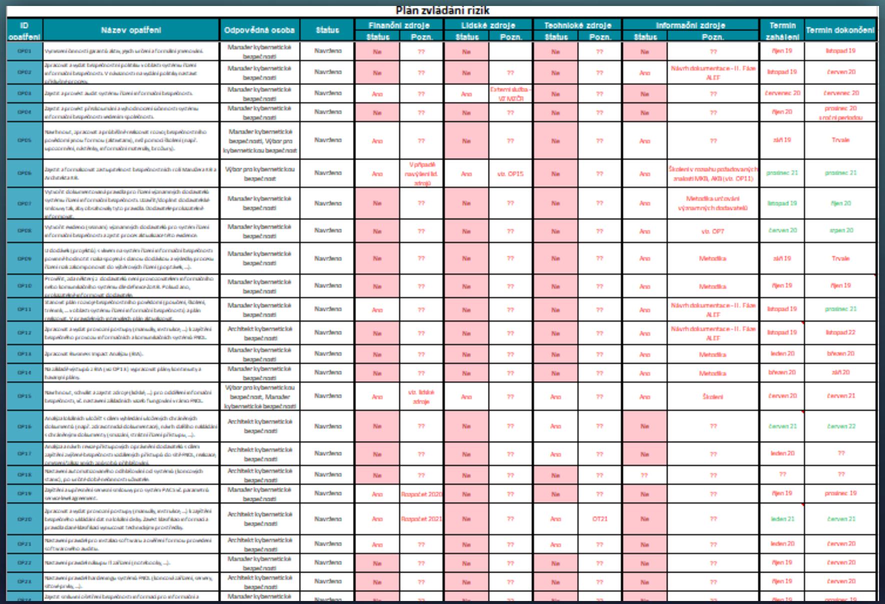
JAK JSME POSTUPOVALI PŘI ZAVÁDĚNÍ ZKB?

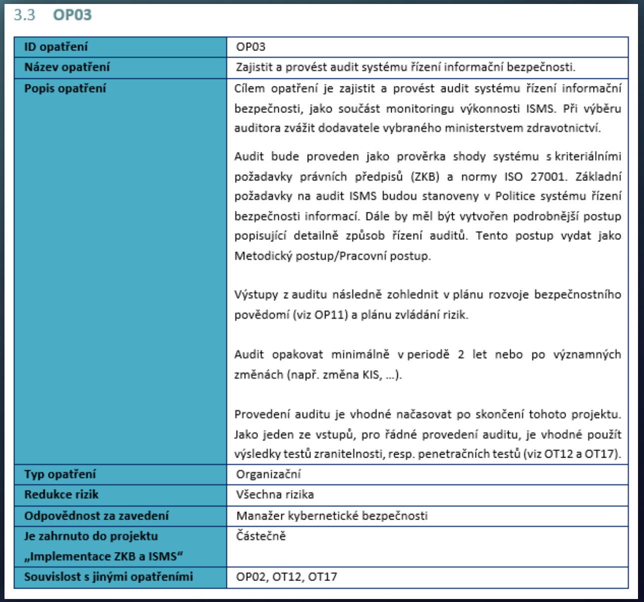
3. PLÁN ZVLÁDÁNÍ RIZIK

OPATŘENÍ KE ZVLÁDÁNÍ RIZIK

- V návaznosti na analýzu rizik a požadavky zákona 181/2014 Sb. o kybernetické bezpečnosti bylo identifikováno **51 opatření**, z toho **29 organizačních a 22 technických**
- Přehled opatření je uveden dokumentu „Plán zvládání rizik“, jejich detailní popis v dokumentu „Popis opatření plánu zvládání rizik“.

Až v tento okamžik mohu plánovat pořízení HW a SW pro KB, často se to děje adhoc, riziko!





3.3 OP03

ID opatření	OP03
Název opatření	Zajistit a provést audit systému řízení informační bezpečnosti.
Popis opatření	Cílem opatření je zajistit a provést audit systému řízení informační bezpečnosti, jako součást monitoringu výkonnosti ISMS. Při výběru auditora zvážit dodavatele vybraného ministerstvem zdravotnictví. Audit bude proveden jako prověrka shody systému s kriteriálními požadavky právních předpisů (ZKB) a normy ISO 27001. Základní požadavky na audit ISMS budou stanoveny v Politice systému řízení bezpečnosti informací. Dále by měl být vytvořen podrobnější postup popisující detailně způsob řízení auditů. Tento postup vydat jako Metodický postup/Pracovní postup. Výstupy z auditu následně zohlednit v plánu rozvoje bezpečnostního povědomí (viz OP11) a plánu zvládání rizik. Audit opakovat minimálně v periodě 2 let nebo po významných změnách (např. změna KIS, …). Provedení auditu je vhodné načasovat po skončení tohoto projektu. Jako jeden ze vstupů, pro řádné provedení auditu, je vhodné použít výsledky testů zranitelnosti, resp. penetračních testů (viz OT12 a OT17).
Typ opatření	Organizační
Redukce rizik	Všechna rizika
Odpovědnost za zavedení	Manažer kybernetické bezpečnosti
Je zahrnuto do projektu „Implementace ZKB a ISMS“	Částečně
Souvislost s jinými opatřeními	OP02, OT12, OT17

Plán zvládání rizik

ID opatření	Název opatření	Odpovědná osoba	Status	Finanční zdroje		Lidské zdroje		Technické zdroje		Informační zdroje		Termín zahájení	Termín dokončení
				Status	Pozn.	Status	Pozn.	Status	Pozn.	Status	Pozn.		
OP22	Nastavení pravidel nákupu IT zařízení (notebooky, ...).	Manažer kybernetické bezpečnosti	Navrženo	Ne	??	Ne	??	Ne	??	Ne	??	říjen 19	červen 20
OP23	Nastavení pravidel hardeningu systémů FNOL (koncová zařízení, servery, síťové prvky, ...).	Architekt kybernetické bezpečnosti	Navrženo	Ne	viz. Dotační program 5000000	Ne	??	Ne	??	Ne	??	říjen 19	prosinec 20
OP24	Zajistit smluvní ošetření bezpečnosti informací pro informační a komunikační systémy umístěné v lokalitě UPOL.	Manažer kybernetické bezpečnosti	Navrženo	Ne	??	Ne	??	Ne	??	Ne	??	říjen 19	červen 20
OP25	Rozšíření počtu zaměstnanců IT oddělení, zastupitelnost a vzdělávání.	VKB, Manažer kybernetické bezpečnosti	Navrženo	Ne	finanční zdroje jsou obsaženy v lidských zdrojích	Ano	viz. Analýza	Ne	??	Ano	školení správců	leden 21	prosinec 21
OP26	Zpracovat a vydat politiku pro řízení informační bezpečnosti zdravotnických prostředků.	Vedoucí Oddělení biomedicínského inženýrství	Navrženo	Ne	finanční zdroje jsou obsaženy v lidských zdrojích	Ano	široká škála zdrav. přístrojů	Ano	úprava evidence sw. např. FIS EFA	Ano	školení personálu	září 20	prosinec 21
OP27	Zpracovat a vydat provozní postupy (manuály, instrukce, ...) pro řízení informační bezpečnosti zdravotnických prostředků (nákup, provoz, údržba a servis, ...).	Vedoucí Oddělení biomedicínského inženýrství	Navrženo	Ano	realizace navrhnutých postupů, nákupy licencí jsou skryty v technických zdrojích	Ano	široká škála zdrav. přístrojů	Ano	nákupy licencí, případná obnova nebo upgrade nevyhovující zdravotnické techniky	Ano	školení personálu	září 20	prosinec 21
OP28	Zpracování a vydání pravidel (standardu) pro minimální fyzické zabezpečení prostředků zdravotnické techniky. Následná úprava fyzických perimetrů dle standardu.	Vedoucí Oddělení biomedicínského inženýrství	Navrženo	Ano	realizace navrhnutých postupů, nákupy licencí jsou skryty v technických zdrojích	Ano	široká škála zdrav. přístrojů	Ano	nákupy tech. prostředků na fyzické zabezpečení prostor se zdrav. technikou	Ano	školení personálu	září 20	prosinec 21
OP29	Nastavení a dokumentace pravidel procesu zvládání bezpečnostních událostí a incidentů.	Architekt kybernetické bezpečnosti	Navrženo	ANO	EFA, SIEM	Ne	??	Ano	EFA, SIEM	??	Aplikační školení	??	červenec 20
OT01	Přísnější vynucování pravidel provozu mezi segmenty vnitřní sítě	Vedoucí IT	Navrženo	Ne	??	Ano	??	Ne	??	Ano	??	březen 20	duben 21
OT02	Řízení přístupu k vnitřní síti local area network a wireless local area network (WLAN)	Vedoucí IT	Navrženo	Ano	výměna starých AP	Ano	??	Ano	??	Ne	??	květen 20	červen 23
OT03	Zjednodušení systému vzdáleného přístupu	Vedoucí IT	Navrženo	Ne	2-faktor auth.	Ne	??	Ne	??	Ne	??	leden 20	prosinec 20
OT04	Zvýšení úrovně zabezpečení přístupu k Internetu	Vedoucí IT	Realizováno	Ano	výměna FW	Ano	??	Ano	??	Ano	Aplikační školení	prosinec 19	říjen 20
OT05	Obnovení / aktualizace IPSec VPN bran	Vedoucí IT	Navrženo	Ano	ASA	Ano	??	Ano	??	Ne	??	duben 20	prosinec 20
OT06	Zavedení systému silné autentizace uživatelů	Vedoucí IT	Navrženo	Ano	2-faktor auth., zatím síla hesla	Ne	??	Ano	??	Ano	Rozšíření znalostí, povědomí uživatelů	červen 20	březen 23
OT07	Zvýšení granularity řízení přístupu pro administraci síťových a bezpečnostních prvků	Vedoucí IT	Navrženo	Ne	??	Ne	??	Ne	??	Ne	??	listopad 19	leden 20
OT08	Zvýšení integrace systémů s centrální správou identit a přístupů	Vedoucí IT	Navrženo	Ano	ISE KIS	Ano	??	Ne	??	Ne	??	březen 20	červen 23

OPATŘENÍ – ORGANIZAČNÍ (TOP 4)

- Zdroje na zajištění a podporu informační bezpečnosti
  - OP15 - Zdroje (lidské, …) pro oddělení infomační bezpečnosti
  - OP25 - Rozšíření počtu zaměstnanců IT oddělení
  - OP06 - Zastupitelnost rolí Manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti

OPATŘENÍ – ORGANIZAČNÍ (TOP 4)

- Vzdělávání a edukace zaměstnanců
  - OP11 - Stanovit a realizovat plán rozvoje bezpečnostního povědomí (poučení, školení, trénink, … v oblasti systému řízení informační bezpečnosti) a plán realizovat
  - Navrhnout, zpracovat a průběžně realizovat rozvoj bezpečnostního povědomí jinou formou (aktivitami), než pomocí školení/vzdělávání

OPATŘENÍ – TECHNICKÁ (TOP 4)

- Autentizace uživatelů a řízení přístupu
  - OT06 - Zavedení systému silné autentizace uživatelů
  - OT07 - Zvýšení granularity řízení přístupu pro administraci síťových a bezpečnostních prvků
  - OT08 - Zvýšení integrace systémů s centrální správou identit a přístupů
  - OT19 - Revize pravidel pro autentizaci heslem

JAK JSME POSTUPOVALI PŘI ZAVÁDĚNÍ ZKB?

4. INTERNÍ POLITIKY A DOKUMENTACE

PLÁN VYDÁVÁNÍ KB POLITIK

Etapa	Dokument	Odevzdáno	Revize 1	Revize 2	Schválený obsah MKB
1	Plán rozvoje bezpečnostního povědomí	26.11.2019	12.12.2019		27.02.2020
	Politika bezpečnosti lidských zdrojů	25.11.2019	12.12.2019	26.03.2020	27.02.2020
	Politika systému řízení bezpečnosti informací	15.01.2020	07.02.2020		27.02.2020
	Politika řízení aktiv	24.02.2020	05.03.2020		26.03.2020
	Politika organizační bezpečnosti	06.03.2020	26.03.2020		18.06.2020
	Politika bezpečného chování uživatelů	15.01.2020	05.02.2020		13.02.2020
	Politika řízení dodavatelů	06.03.2020	26.03.2020		08.05.2020
	Politika ochrany osobních údajů	06.03.2020	27.05.2020		15.07.2020
	Politika fyzické bezpečnosti	15.01.2020	27.05.2020		30.06.2020
	Politika řízení kontinuity činností	17.04.2020			28.04.2020
	Politika řízení změn	17.04.2020	08.05.2020		14.05.2020
	Politika zvládání kybernetických bezpečnostních incidentů	11.03.2020	26.03.2020		23.04.2020
2	Politika řízení provozu a komunikací	18.06.2020			30.06.2020
	Politika bezpečnosti komunikační sítě	18.06.2020			30.06.2020
	Politika řízení přístupu	27.04.2020	08.05.2020		14.05.2020
	Politika bezpečného předávání a výměny informací	18.06.2020			30.06.2020
	Politika ochrany před škodlivým kódem	27.05.2020	05.06.2020		18.06.2020
	Politika řízení technických zranitelností	18.06.2020			15.07.2020
	Politika bezpečného používání mobilních zařízení	27.04.2020	08.05.2020	27.05.2020	18.06.2020
3	Politika akvizice, vývoje a údržby	15.07.2020			30.07.2020
	Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí	30.07.2020			30.07.2020
	Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí	30.07.2020			30.07.2020
	Politika zálohování a obnovy a dlouhodobého uchovávání	30.07.2020			30.07.2020
	Politika bezpečného používání kryptografické ochrany	15.07.2020			30.07.2020

JAK JSME POSTUPOVALI PŘI ZAVÁDĚNÍ ZKB?

5. IMPLEMENTACE A PŘEZKOUMÁNÍ ISMS, ZÁVĚR

ZPRÁVA O UKONČENÍ 2. FÁZE PROJEKTU

Celkový stav projektu

FNOL – Implementace ISMS

Aktuální stav projektu

- Odevzdány všechny požadované dokumenty
  - Prohlášení k bezpečnostní politice
  - Bezpečnostní politika - obsahuje 23 politik, bude vydáváno postupně
  - Plán rozvoje bezpečnostního povědomí
    - Matice bezpečnostního vzdělávání a povědomí
  - Zpráva z přezkoumání ISMS
  - Interní audity
    - Metodika řízení auditů ISMS
    - Plán_auditu_ISMS_XX_2020
    - Program_auditu_ISMS_r_2020
    - Zpráva_z_auditu_ISMS_XX_2020
  - Neustálé zlepšování systému řízení bezpečnosti informací

K řešení FNOL

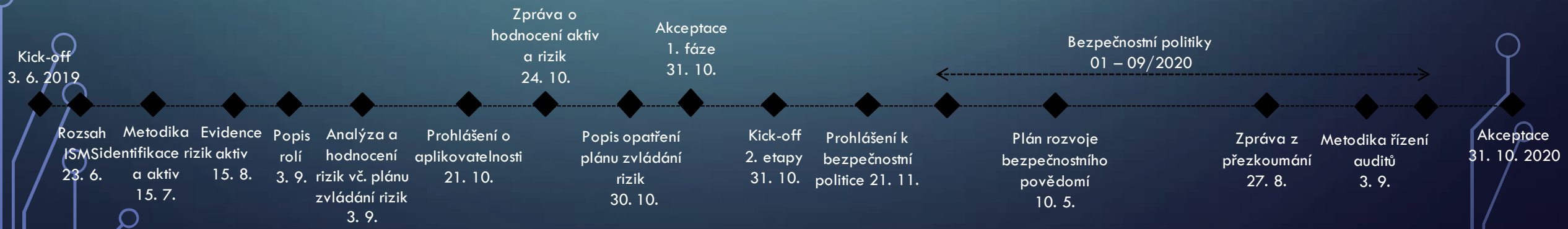
- Prezentovat výsledky 1. a 2. etapy vedení nemocnice
- Vydat dokumenty z 1. a 2. etapy etapy odborem kvality
- Řešit prioritizaci – Plán zvládání rizik – prezentace M. Zedníček – 2.10.
- Vypracovat havarijní plány a plány kontinuity a obnovy
- Vytvořit vzdělávací plán na 3 roky

Vícepráce

- 1. etapa - Návrh koncepce skupiny kybernetické bezpečnosti ve FNOL
- 2 etapa - Business Impact analýza

1. fáze projektu

2. fáze projektu



Vše podle plánu

Problémy bez většího dopadu na projekt

Problémy s velkým dopadem na klíčové ukazatele projektu (čas, rozsah, rozpočet)

VÝSTUPY AUDITU NÚKIB (30.11.2020-21.1.2021)

FNOL se nachází ve fázi zavádění systému řízení bezpečnosti informací (dále jen „ISMS“), čemuž odpovídá i množství a charakter nálezů.

Dosavadní odvedenou práci, včetně plánů do budoucna, auditní skupina **hodnotí jako kvalitní**, jen je nutné upozornit na skutečnost, že **fázi zavádění ISMS je nutné co nejdříve ukončit a nově nastavované procesy začlenit mezi ostatní činnosti organizace.**

Velmi pozitivně hodnotí auditní skupina fakt, že zaměstnanci FNOL si uvědomují důležitost zdravotnické techniky z hlediska vlivu na zajišťování kybernetické bezpečnosti. **Tento přístup je příkladný pro ostatní obdobné subjekty.**

Z technického pohledu je možno vyzdvihnout úsilí FNOL v oblasti stavby interní sítě a její rozdělení na dílčí funkční a logické celky, což může významně pomoci zabránit šíření případného škodlivého kódu.

VÝSTUPY AUDITU NÚKIB (30.11.2020-21.1.2021)

Zároveň je potřeba upozornit na nedostatky a možná rizika. Jedním z nich je nedostatečné sledování stavu sítě a uchovávání historických záznamů, které umožňuje provedení analýzy v případě bezpečnostního incidentu.

U informačních systémů (dále jen „IS“) podporujících poskytování zdravotních služeb je potřeba odstranit řadu nedostatků, aby byl jejich provoz bezpečný. Nápravu lze provést např. pořízením nástroje pro kontrolu účtů s vyššími přístupovými právy a oprávněními, kontrolu aktivit dodavatelů provádějících zásahy do těchto IS, šifrování nebo zaznamenávání činností administrátorů.

Dalším bodem, na který je potřeba upozornit je chybějící testování zabezpečení jednotlivých IS. K těmto preventivním činnostem slouží penetrační testování a pravidelné skenování zranitelností.

DĚKUJI ZA POZORNOST

Ing. Antonín Hlavinka

FNOL, NTMC