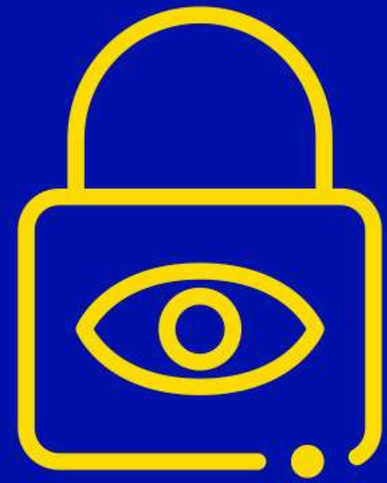
NIS2

Seminář o nové evropské směrnici



Úvod do problematiky NIS2

Radek Šichtanc, O2

Co NIS2 přináší a co znamená pro firmy

NIS2 je nový zákon Evropské unie, která si klade za cíl zvýšit odolnost institucí a firem proti kybernetickým rizikům.

1

Stanovuje minimální pravidla týkající se regulačního rámce a mechanismy účinné spolupráce mezi příslušnými orgány v každém členském státě.

2

Rozšiřuje oblast působnosti – více společností ve více odvětvích.

3

Zpřísňuje a zefektivňuje požadavky na kybernetickou bezpečnost.

4

Zlepšuje sdílení informací a spolupráci mezi orgány členských států.

5

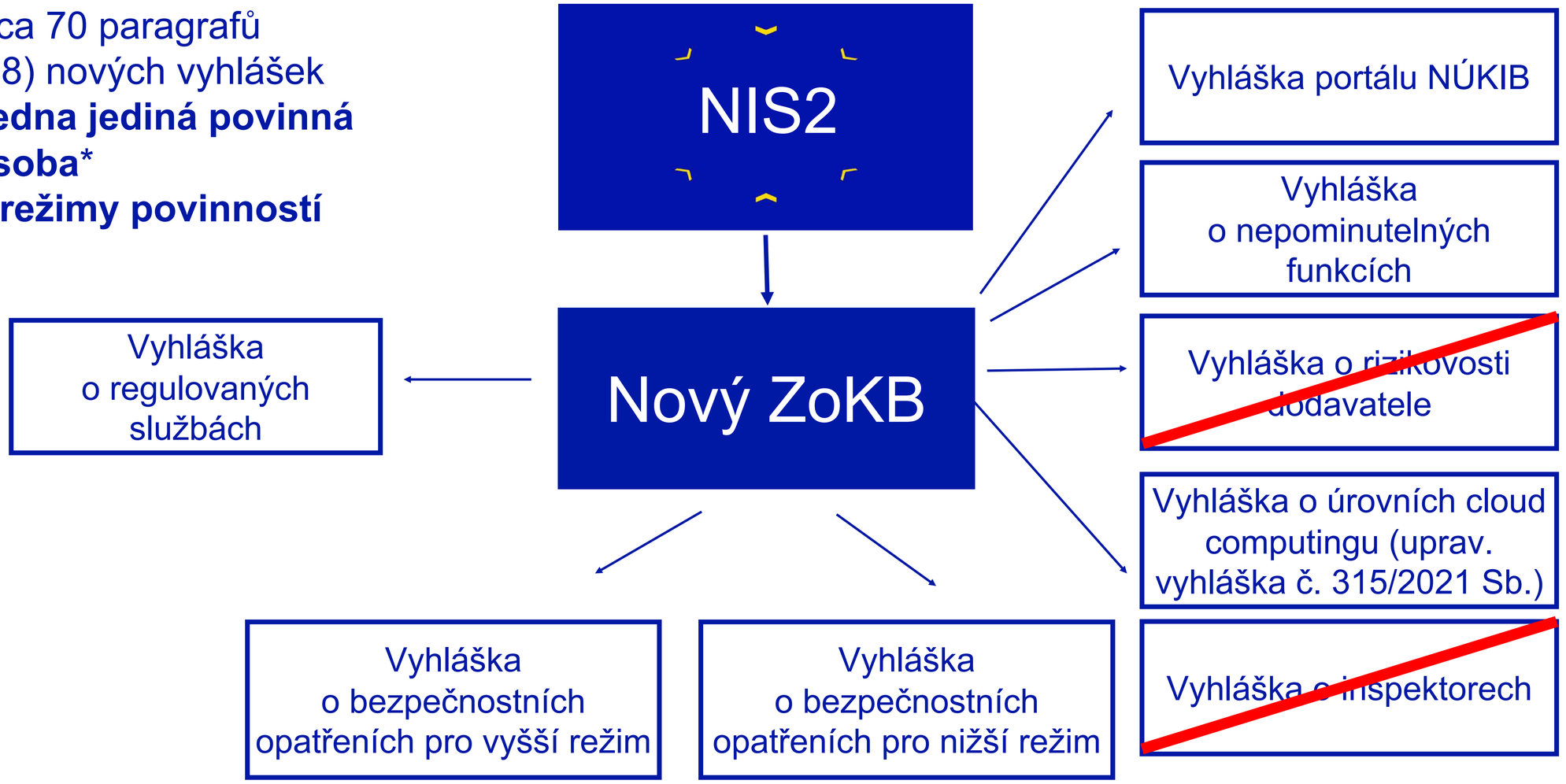
Posiluje řízení bezpečnosti a odpovědnosti vedoucích pracovníků podniku.

6

Zvyšuje sankce za nedodržení povinností.

Zákon o kybernetické bezpečnosti

- Cca 70 paragrafů
- 6(8) nových vyhlášek
- **Jedna jediná povinná osoba***
- **2 režimy povinností**



** Pro primární sadu povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů apod.*

Zákon o kybernetické bezpečnosti

Dříve

- Provozovatelé základní služby
- Kritická (nejen informační) infrastruktura
- Významné informační systémy
- Všechny subjekty z NIS2

Nyní

Poskytovatel regulované služby

Regulovaná služba

Naplňující alespoň jedno kritérium pro identifikaci regulované služby podle vyhlášky o regulovaných službách (objektivní naplnění kritérií).

nebo

Určená rozhodnutím NÚKIB na základě kritéria pro určení regulované služby.

Sebeidentifikace – kritéria

Odvětví / Činnost

+

Velikost subjektu

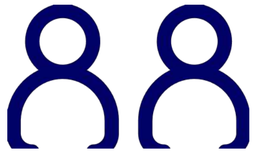
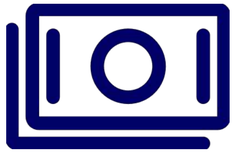
=

Vyšší režim

nebo

Nižší režim

Sebeidentifikace – velikost

Počet zaměstnanců		Obrat v mil. EUR		
	nebo		=	**Velký podnik**
250+		50+		
	nebo		=	**Střední podnik**
50+		10+		

Sebeidentifikace – odvětví

Služby uvedené v příloze 1 - Essential

- Energetika
- Zdravotnictví
- Veřejná správa
- Doprava
- Pitná voda
- Digitální infrastruktura
- Bankovnictví
- Odpadní voda
- Vesmír
- Infrastruktura fin. trhů
- Poskytovatelé řízených ICT služeb

Služby uvedené v příloze 2 - Important

- Poštovní služby
- Potravinářství
- Odpadní hospodářství
- Výroba
- Chemický průmysl
- Poskytovatelé digi služeb
- Výzkum

Subjekty, kterým plynou povinnosti z NIS2, ale nespadají do režimu essentail, ani important

- Subjekty, shromažďující a udržující přesnou a úplnou registraci názvu domén.

Hlavní povinnosti subjektů

1. **Hlásit** kontaktní a další údaje
2. **Stanovit rozsah** řízení kybernetické bezpečnosti (definuje rozsah regulace v organizaci)
3. **Zavádět bezpečnostní opatření** podle režimu, v kterém je služba určena (vyšší/nižší)
4. **Hlásit kybernetické bezpečnostní incidenty** podle režimu, v kterém je služba určena (vyšší/nižší)
5. **Informovat zákazníky** o incidentech a hrozbách
6. **Provádět protiopatření**
7. **Plnit povinnosti z tzv. mechanismu bezpečnosti dodavatelského řetězce** u vybraných (strategicky významných) služeb
8. **Zajistit dostupnost z České republiky** u vybraných (strategicky významných) služeb

Hlášení kybernetických bezpečnostních incidentů

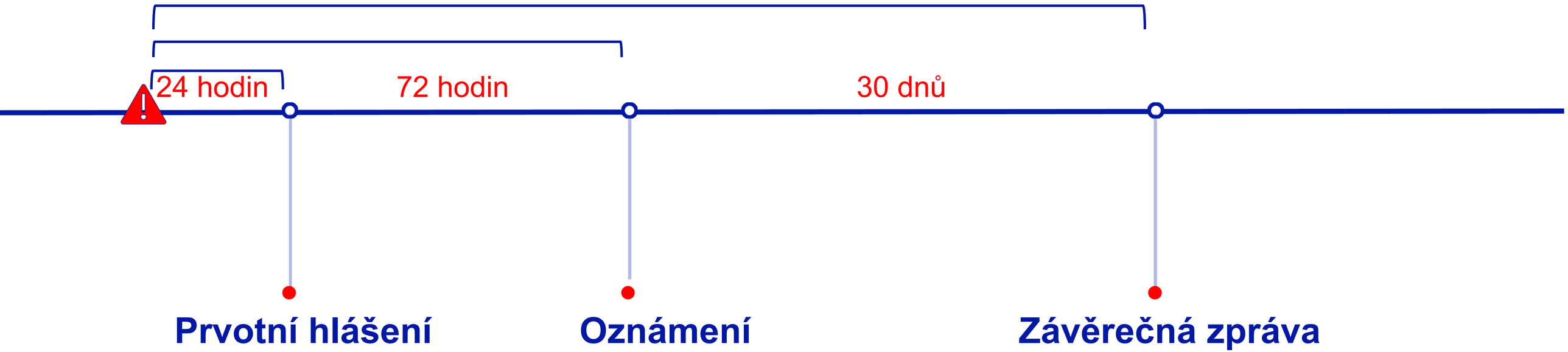
Kybernetickým bezpečnostním incidentem se rozumí narušení bezpečnosti informací v rámci aktiv (související s regulovanou službou).

Pro hlášení je potřeba posoudit dvě situace:

1. **významný dopad na poskytování regulované služby**
2. **úmyslné zavinění kybernetického bezpečnostního incidentu**

Vyšší režim	**Hlásí vše**	**NÚKIBu** Pozn.: Portál NÚKIB
Nižší režim	**Hlásí vše, co je úmyslné,** nebo to, **co je významné**	**Národnímu CERTu**

Hlášení kybernetických bezpečnostních incidentů



Sankce – výše pokuty

Subjekt v režimu vyšších povinností

250 mil. CZK

nebo

2 % obratu

Subjekt v režimu nižších povinností

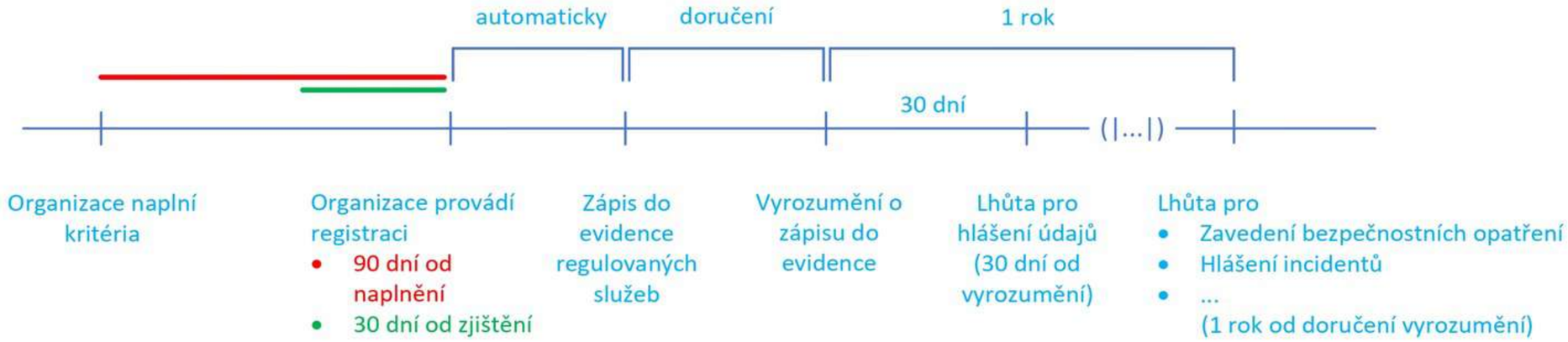
175 mil. CZK

nebo

1,4 % obratu

Lhůty

- Registrovat regulovanou službu – **do 30 dní**, resp. 90
- Hlásit kontaktní a další údaje – **do 30 dní** (15 dní změny)
- Stanovit rozsah řízení kybernetické bezpečnosti – **kdykoliv**
- Zavádět bezpečnosti opatření – **do 1 roku** (od evidence)
- Hlášení kybernetických bezpečnostních incidentů – **do 1 roku** (od evidence)
- Protiopatření (výstraha, varování, reaktivní opatření) – **ihned**
- Povinnost informovat poskytovatele regulované služby – **ihned**



Řízení dodavatelů

Nová oblast – nevyplývá ze směrnice NIS2, ale z **národního rozhodnutí.**

- Platí **pouze pro vybrané organizace v režimu vyšších povinností**
- Organizace v rámci této povinnosti **musí nahlásit dodavatele**
- Budou prověřováni **dodavatelé do kritické části systému**, kteří dodávají bezpečnostně významnou dodávku
- Stát prověří, zda dodavatel není hrozbou pro bezpečnost ČR, zájmy ČR, vnitřní a veřejnou bezpečnost
- NÚKIB může vydat **zákaz dodavatele** použít nebo **upozornění na riziko** (opatření)
  - Lze udělit výjimku (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu atp.)
  - K vyřazení již dodaných technologií nemusí dojít hned, počítá se s přechodnými lhůtami
- Hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby

Účinné **do 1 roku** od vyrozumění od označení služby jako **strategické.**

Časová osa nové regulace

reálně začátek 2025

Říjen 2024

Očekávaná účinnost zákona

Říjen 2025

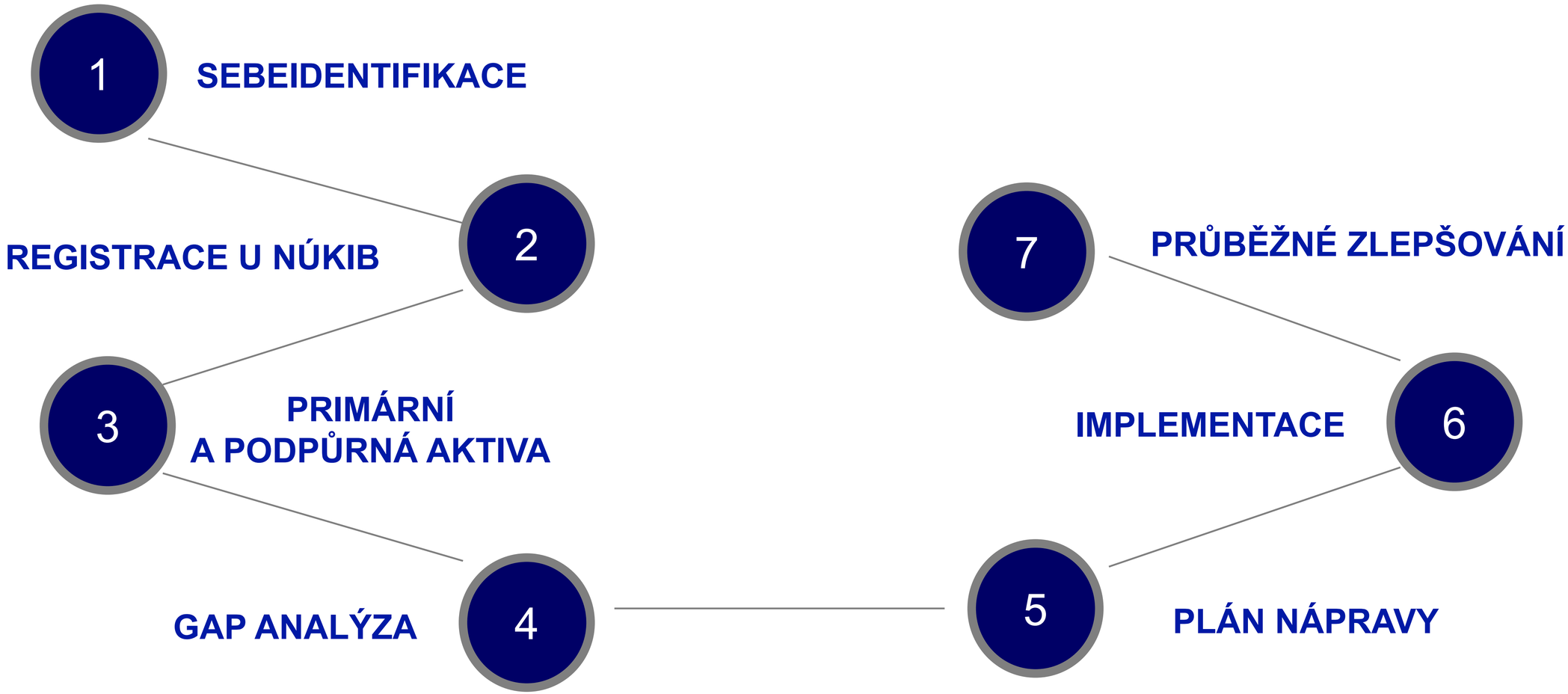
Zavedení bezpečnostních opatření

Dnes

Leden 2025

Registrace u NÚKIB

Shrnutí


1
SEBEIDENTIFIKACE
2
REGISTRACE U NÚKIB
3
PRIMÁRNÍ
A PODPŮRNÁ AKTIVA
4
GAP ANALÝZA
5
PLÁN NÁPRAVY
6
IMPLEMENTACE
7
PRŮBĚŽNÉ ZLEPŠOVÁNÍ

Jak se připravit na NIS2

Tomáš Svoboda, O_2 ITS

Organizační opatření

Role a odpovědnosti vrcholného vedení

Prokazatelná účast na školení

Zajištění dostupnosti zdrojů – interně nebo formou outsourcingu

Určení výboru pro řízení IKB a účast na jednáních

Min. 1x ročně schvalování:

- výsledků hodnocení rizik
- auditních zpráv
- analýzy dopadů – BIA

Schvalování bezpečnostních politik

Jmenování bezpečnostních rolí

Bezpečnostní politiky a jejich role v zajištění bezpečnosti

Politika zajišťování minimální úrovně kybernetické bezpečnosti

Rozsah, SLA

Bezpečnost lidských zdrojů

Školení, sankce za porušení povinností

Řízení aktiv a rizik

Identifikace aktiv, odpovědné osoby, přípustné použití aktiv

Řízení dodavatelů

Pravidla identifikace významného dodavatele, bezpečnostní požadavky do smluv s dodavateli

Bezpečnostní role

Nižší režim

Osoba odpovědná za kybernetickou bezpečnost

Vyšší režim

Manažer kybernetické bezpečnosti

Architekt kybernetické bezpečnosti

Garant aktiva – primární i podpůrná aktiva

Auditor kybernetické bezpečnosti

Zastupitelnost bezpečnostních rolí
Bezpečnostní role nesmí odpovídat za provoz

Řízení aktiv

Je nezbytné vědět, jaká aktiva jsou pro společnost klíčová

Primární

- informace nebo klíčová služba, která je poskytována

Podpůrná

- HW, SW, lidské zdroje, dodavatelé, lokality

Jak identifikovat aktiva?

Jak identifikovat garanty aktiv?

Klíčový vstup do řízení rizik

Aktiva nejsou pouze CMDB položky IT infrastruktury!

K čemu je to dobré? ☺

Řízení rizik

Je nezbytné vědět, jaká rizika mají vliv na zajištění regulované služby

Hrozby, zranitelnosti

Proces řízení rizik – minimálně 1x ročně

Odpovědnost v procesu řízení rizik

- bezpečnostní role, vedení

Analýza rizik aneb hrozby, zranitelnosti a kde je najít? ☺

Vyhodnocení rizik – prioritizace a kritéria pro řešení

Zvládání rizik

- akceptace, přenesení, sdílení, vyhnutí se riziku a jejich význam pro organizaci

Řízení dodavatelů

Nižší režim

Propsání požadavků do smluv s dodavateli

- CIA, audit, řetězení, řízení změn, NDA, exit strategie, BCM, sankce

Vyšší režim

Identifikace, informování a evidence dodavatelů

Pravidelný audit – interní i třetí stranou

Hodnocení rizik před uzavřením smlouvy

Požadavky KB ve smlouvách s dodavateli, pravidla chování dodavatele

- Bezpečnostní politiky, incidenty, aktiva, rizika, likvidace dat, odstoupení od smlouvy, předání dat do jiného státu

Školení

Plán rozvoje bezpečnostního povědomí = periodický plán školení

Nižší režim

Školení vrcholného vedení

Školení zaměstnanců

Školení dodavatelů

Vyšší režim

Školení bezpečnostních rolí

Co školit – doporučená školení v příloze č. 8

- Sociální inženýrství, VPN, elektronická komunikace, cloudová úložiště, aktuální hrozby, detekce zranitelností, používání zařízení pro soukromé účely

Řízení kontinuity

Kontinuita činností není pouze zálohování a disaster recovery.
Kontinuita činností = procesy a činnosti organizace, nejen IT systémů.

Nižší režim

Vazba na primární aktiva – pořadí obnovy primárních aktiv

Odpovědnosti, pravomoci

Zálohování

Vyšší režim

Metodika pro stanovení analýzy dopadů

Vstup do hodnocení rizik

Stanovení minimální úrovně poskytovaných služeb

BC plán per služba

Testování plánů kontinuity činností

Příklad: pandemie covidu-19 a vliv na lidské zdroje

Řízení incidentů

Nižší režim

Jak posuzovat incidenty?
Metodický postup – vazba na řízení kontinuity činností

Hlášení incidentů s významným dopadem

Závěrečná zpráva o kybernetickém incidentu

Vyšší režim

Odpovědnosti při detekci a řešení incidentů – IT, vedení, bezpečnostní role

Hlášení **všech** kybernetických incidentů dle zákona

Zajištění důkazních materiálů

Aktualizace analýzy rizik, BCP

Prvotní hlášení do 24 hodin

Řízení změn

Nižší režim

Řízení změn u dodavatelů

Vyšší režim

Změny mající vliv na kybernetickou bezpečnost

Politika řízení změn

Co jsou významné změny:

- dokumentace, role, odpovědnosti
- hodnocení rizik, analýza rizik, penetrační testování
- testování
- navrácení do původního stavu

Technická opatření

Řízení přístupu identit

Nižší režim

Každý uživatel jedinečný identifikátor

Nezapomenout na technické účty!

Pravidelné přezkoumání

Vícefaktorová autentizace jako cíl

Klíče, certifikáty, hesla

Jak řídit obálkové účty?

Vyšší režim

Centralizovaný nástroj pro řízení oprávnění

Evidence aktiv, kde není nasazena vícefaktorová autentizace

Výchozí hesla náhodně generovaná

Jak uchopit procesy?

Fyzická bezpečnost

Nižší režim

Zamezení neoprávněnému přístupu

Vyšší režim

Dokumentace perimetrů

Rozdělení na úrovně

Evidence vstupů, detekce narušení

Best practice (kamery, EZS, EPS, VSS /CCTV/, čidla v RACku)

- Vstupy do bezpečnostního monitoringu, analýzy rizik, implementace opatření

Bezpečnost komunikačních sítí

Nižší režim

Zejména oddělení provozního a zálohovacího prostředí

Evidence povolených komunikací

Bezpečné síťové protokoly – NÚKIB

Vyšší režim

Oddělení provozního, zálohovacího, vývojového, testovacího a jiného specifického prostředí

Vzdálené přístupy a vzdálená správa aktiv

Kryptografie

Evidence povolených komunikací

Firewally, NGFW, aplikační firewally

Aplikační bezpečnost

Nižší režim

Patch management

Evidence nepodporovaných systémů, omezení jejich komunikace, náhradní bezpečnostní opatření – best practice?

Skenování zranitelností relevantních aktiv – vychází z řízení aktiv analýzy rizik

Vyšší režim

Pravidelné skenování zranitelností 1x ročně a penetrační testy 1x za 2 roky (interní a externí síť)

Výsledky jako vstup do řízení rizik

Penetrační testy před uvedením do provozu a významných změnách

Retesty

Penetrační testy jako celku max. do 5 let

Logování a vyhodnocování událostí

Nižší režim

Ochrana před škodlivým kódem – antiviry, EDR včetně jejich aktualizace – vazba na aplikační bezpečnost

Kontrola dat na perimetru – FW, NGFW

Včasné varování osob o incidentu

Vyšší režim

Centrální nástroj pro detekci – best practice – log management, SIEM, SOAR

Časová synchronizace

Překlad adres – NAT!

Uchování logů nejméně 18 měsíců. Forenzní úložiště?

Vyhodnocování událostí jako vstup do analýzy rizik a plánu zvládání rizik

Kryptografie

Nižší režim

Odolné algoritmy a kde je najít

Použití tam, kde je to vhodné

Hodnocení aktiv a rizik

Vyšší režim

Kryptografické klíče a certifikáty

Systém správy klíčů – certifikační autority

Best practice – procesy generování, změny a zneplatnění klíčů – kompletní dokumentace PKI procesů a infrastruktury

Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Nižší režim

Stanovit únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, který představuje úhrn nejvyšší škody a nemajetkové újmy vzniklý v souvislosti s kybernetickým bezpečnostním incidentem, v jehož důsledku ještě nejsou ohroženy život či zdraví osob nebo schopnost poskytovatele regulované služby dostát svým závazkům

Hodnocení dopadů – využít metodiku NÚKIB

Metodika k vodítkům pro hodnocení dopadů

BCM

Vyšší režim

Hlásí se všechny incidenty s původem v kyberprostoru

Dostupnost regulované služby

Nižší režim

Není specifikováno

Vyšší režim

Zajištění dostupnosti služby podle cílů v BCM

Redundance aktiv

Zálohování

- Testy integrity dostupnosti a obnovitelnosti záloh a dokumentace těchto testů – téměř nikdo dnes neprovádí
- Šifrování záloh
- Table-top cvičení jsou nedostatečná

Průmyslová, řídící a jiná specifická aktiva

Nižší režim

Není specifikováno

Vyšší režim

Standardní opatření

- Segmentace sítě
- Řízení přístupu
- Omezení vzdálených přístupů
- Ochrana před zranitelnostmi
- Fyzická bezpečnost

Častý problém – nepodporovaná nebo proprietární zařízení

- Evidence zařízení, analýza rizik, ekonomicko-bezpečnostní posouzení

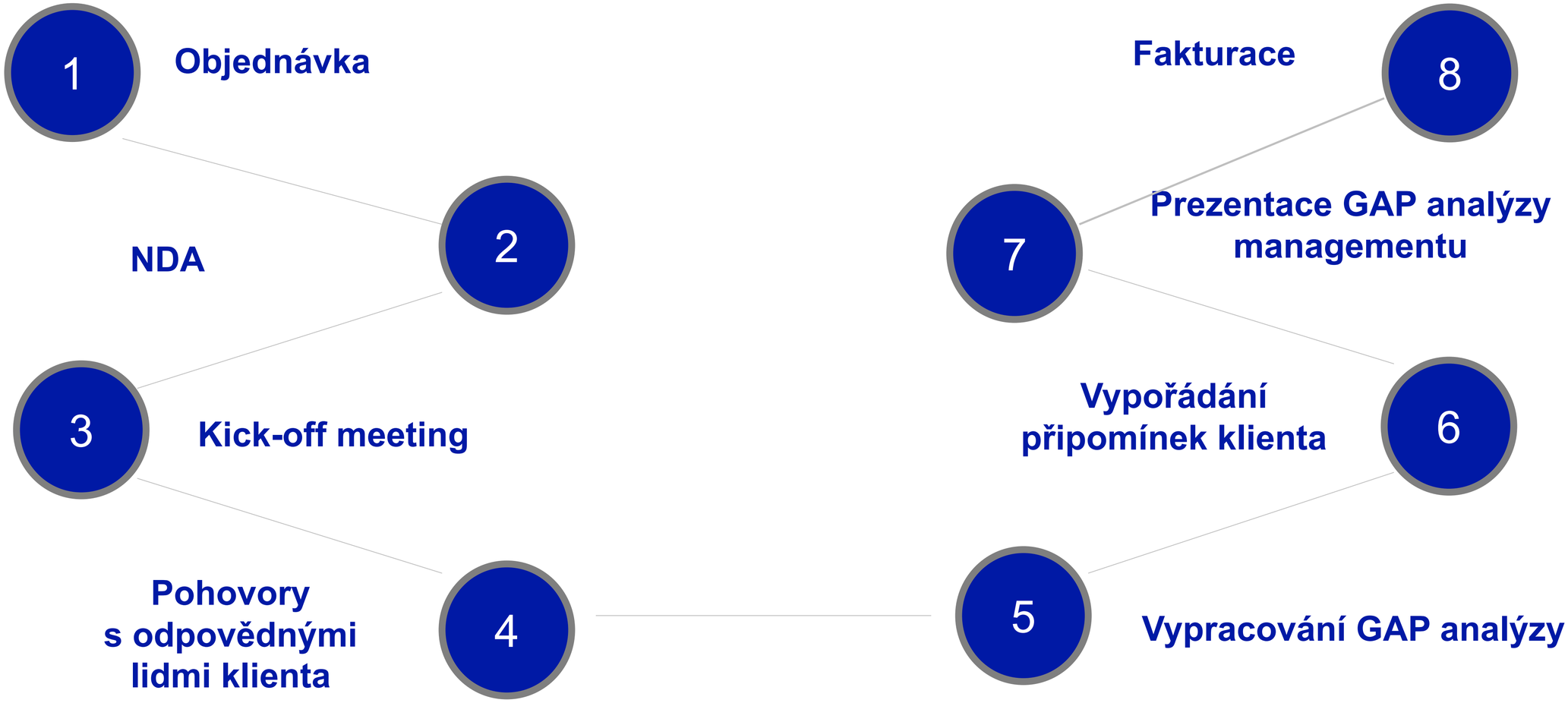
GAP analýza z pohledu O_2

Nejčastější zjištění v rámci GAP analýzy

1. Není stanoven rozsah řízení kybernetické bezpečnosti
2. Neexistuje identifikace a řízení aktiv
3. Neexistuje identifikace a řízení rizik
4. Chybí DR a BCP plány, strategie a politiky
5. Vrcholné vedení není začleněno v procesu řízení bezpečnosti
6. Bezpečnost je kompletně řízena IT oddělením
7. Nejsou definovány procesy řízení incidentů a změn (nebo v nich není začleněna bezpečnost)

Klíčové kroky

Porovnání aktuálního stavu implementace organizačních a technických opatření s NIS2



Ukázka výstupu

Zhodnocení stávajícího stavu dle jednotlivých paragrafů Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Ukázka

Oblast Vyhlášky	Paragraf	Status	Sta	ds	Cílový stav
Systém řízení bezpečnosti informací	4	Nonexistent		ptimized	5
Povinnosti vrcholového vedení	5	Nonexistent	0	Optimized	5
Bezpečnostní role	6	Nonexistent	0	Optimized	5
Řízení bezpečnostní politiky a bezpečnostní dokumentace	7	Limited	2	Optimized	5
Řízení aktiv	8	Ad-hoc	1	Optimized	5
Řízení rizik	9	Nonexistent	0	Optimized	5
Řízení dodavatelů	10	Ad-hoc	1	Optimized	5
Bezpečnost lidských zdrojů	11	Ad-hoc	1	Optimized	5
Řízení změn	12	Nonexistent	0	Optimized	5
Akvizice, vývoj a údržba	13	Ad-hoc	1	Optimized	5
Řízení přístupu	14	Limited	2	Optimized	5
Zvládání kybernetických bezpečnostních událostí a incidentů	15	Nonexistent	0	Optimized	5

Souhrn zjištění a nápravných opatření

Ukázka

§8 Řízení aktiv	Ad-hoc	1		
Popis současného stavu	**Návrh opatření**		**Pracnost**	**Priorita**
Není stanovena metodika pro identifikaci a hodnocení aktiv včetně úrovně aktiv.	Vytvoření metodiky pro identifikaci a hodnocení aktiv a pro provedení analýzy dopadů viz. §7 Řízení bezpečnostní politiky a bezpečnostní dokumentace.		**Interně:** 10 MD Manažer KB **Outsourcing:** 5 MD	1

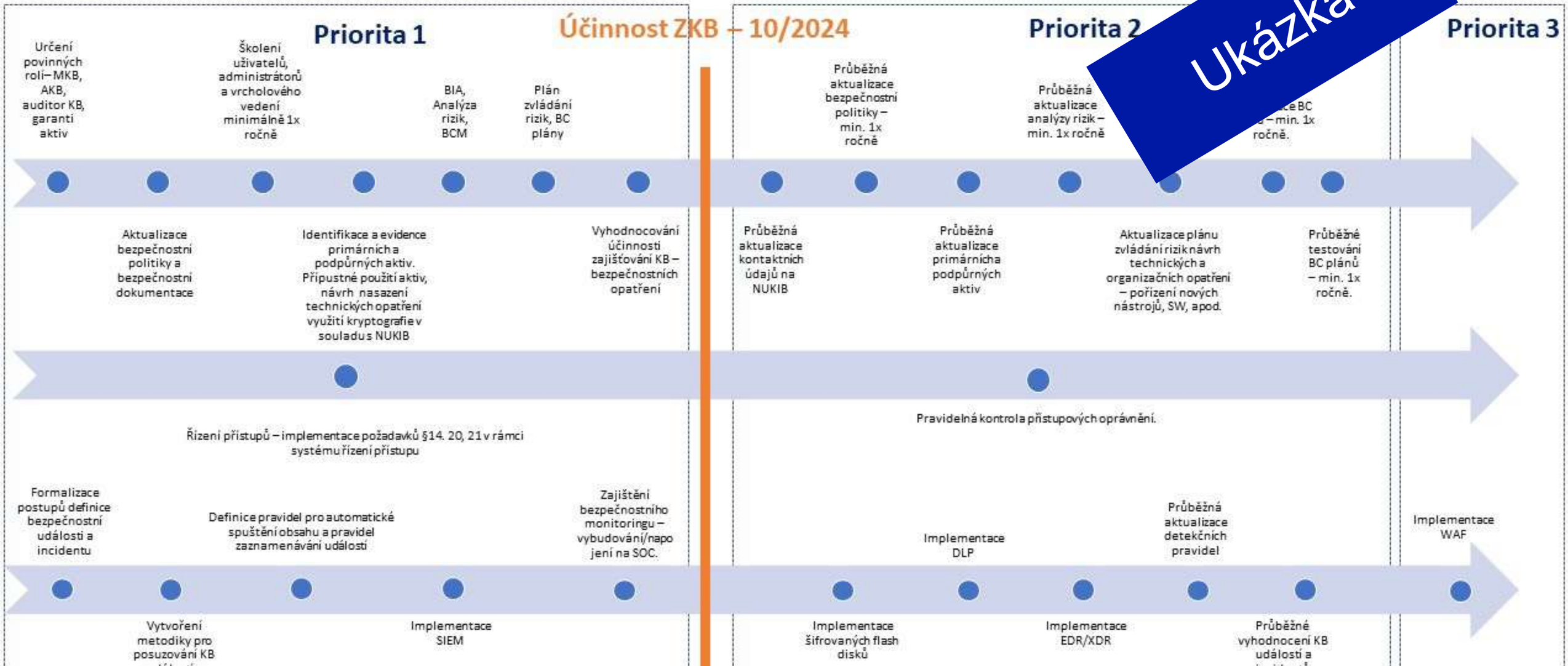
§20 Správa a ověřování identit	Limited	2		
Popis současného stavu	**Návrh opatření**		**Pracnost**	**Priorita**
V rámci implementovaného nástroje pro správu a ověřování identity administrátorů, uživatelů a technických aktiv nedochází k opětovnému ověření identity po stanovené době nečinnosti.	Úprava GPO politik v rámci Active Directory, které budou zajišťovat vynucování opětovné ověření identity po stanovené době nečinnosti.		**Interně:** 0,5 MD IT	1

Přehled časové náročnosti (v MD)

Ukázka

Paragraf	MD – interní	MD – outsourcing	Cena outsourcing bez DPH v Kč
§4 Systém řízení bezpečnosti informací	80–110	40-60	XXX XXX,-
§5 Povinnosti vrcholného vedení	39–53	21-33	XXX XXX,-
§6 Bezpečnostní role	6–11	1	XXX XXX,-
§7 Řízení bezpečnostní politiky a			XXX XXX,-

Časová osa implementace opatření podle priorit



Ukázky a příklady implementace NIS2

Ivo Kubíček, O_2

Jsme partnerem pro kybernetickou bezpečnost a pomáháme s NIS2, kterou sami řešíme

Vstupní konzultace

Provedeme úvodní konzultaci pro zhodnocení vašich bezpečnostních potřeb v souladu s NIS2.

Analýza bezpečnosti

Vypracujeme podrobnou analýzu stávajících bezpečnostních organizačních opatření a identifikujeme slabá místa.

Návrh řešení

Navrhneme ucelené bezpečnostní řešení vyžadující minimální čas na nasazení, správu a provoz.

Implementace a outsourcing

Poskytujeme kompletní implementaci navrženého řešení a možnost outsourcingu bezpečnostních služeb.

Splňujeme nejvyšší požadavky na bezpečnost a jsme subjektem, na který se NIS vztahuje už nyní

- Systém informační bezpečnosti dle **ISO 27001**
- Bezpečnost cloudových služeb **ISO 27017**
- Bezpečnost osobních údajů v cloudovém prostředí **ISO 27018**
- Certifikace **SOC 2 Typ 2** pro O_2 Cloud a navázaná řešení v oblasti kybernetické bezpečnosti
- Bezpečnostní tým **O2.cz CERT Accredited** (Trusted Introducer)

Příklad z praxe I
Stuxnet v českých garážích neuspěje

Situace:

- Dopravní společnost parkuje v garážích i autobusy na plyn.
- Garáže jsou monitorované mj. i čidly na únik plynu.
- Levná čidla byla napojena na veřejně dostupnou wifi.
- Alarmy řešené systémem na PC s Windows XP.

Problém:

- Spouštění alarmů bez indikace úniku plynu přes wifi nebo zranitelné PC.

Řešení:

- Samostatná VLAN pro monitorovací systémy.
- Server se sirénou měl mnoho kritických zranitelností, a proto je obestavěný zdí ZTNA pravidel.

Příklady z praxe II
Peníze ušetřené za AI jsme investovali do lidí

Situace:
- Obchodní společnost zvažuje navýšení bezpečnosti o službu EDR.
- Důvodem byl zvýšený objem malwaru u zaměstnanců, který nebyl detekován tradičním antivirem.

Problém:
- V rámci výběru znervózněli z referencí o možnosti výskytu problémů při instalaci a správy funkčního systému.

Řešení:
- Nalezeno optimální řešení provozu, které problém řešilo částečně funkcionalitami AD/O365 a nasazením ZTNA modelu.
- Ušetřené finance investovány na školení běžných uživatelů IT pro zvýšení odolnosti jak s firemními, tak soukromými kyberidentitami.

Příklad z praxe III
Kontex udělal z DDoSu průmyslovou špionáž

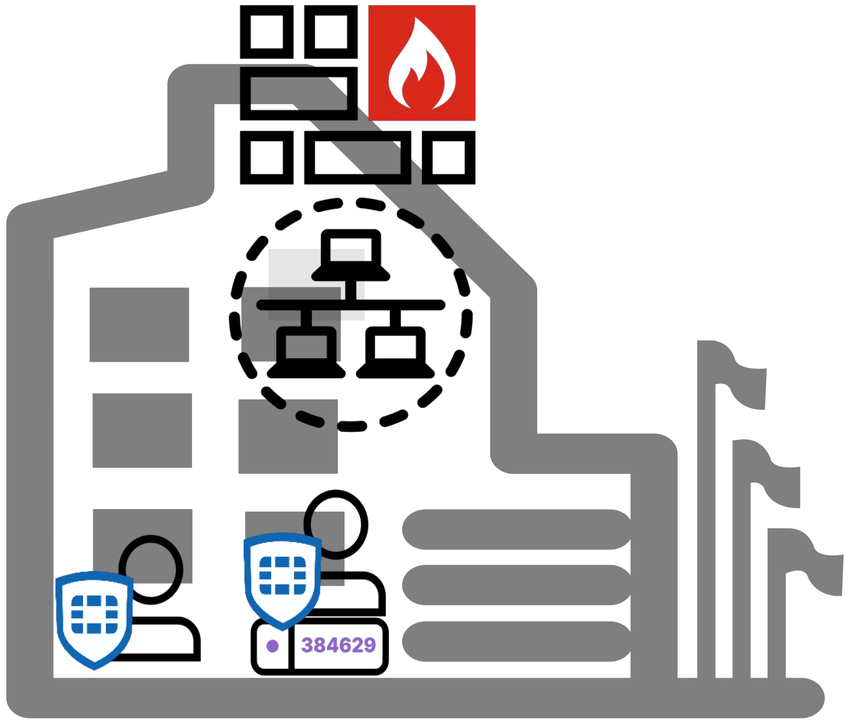
Situace:
- Poskytovatel služeb prezentoval na svém webu, jaké všechny služby umí jak a kde poskytovat.

Problém:
- Jednou se na web přiřítila nečekaná vlna provozu/dotazů, kterou stroje detekovaly jako DDoS.

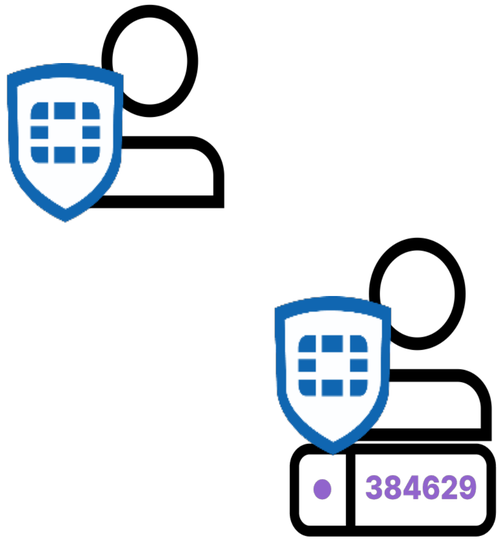
Řešení:
- Díky součinnosti O_2 bezpečnostního dohledu a provozních složek zákazníka bylo identifikováno strojové vyčítání databáze o schopnostech poskytovaní služeb.
- Včasné a přesné zjištění důvěryhodnosti a integrity dat zákazníka umožnilo upravit rozhodování při nákupu a dalších investicích.

Univerzální CPE je vhodným základem pro zvýšení kybernetické bezpečnosti

Řídí přístupy
uvnitř LAN a na perimetru



Řídí přístupy
mimo chráněné sítě



Řídí přístupy
včetně přístupů k různým
cloudovým službám

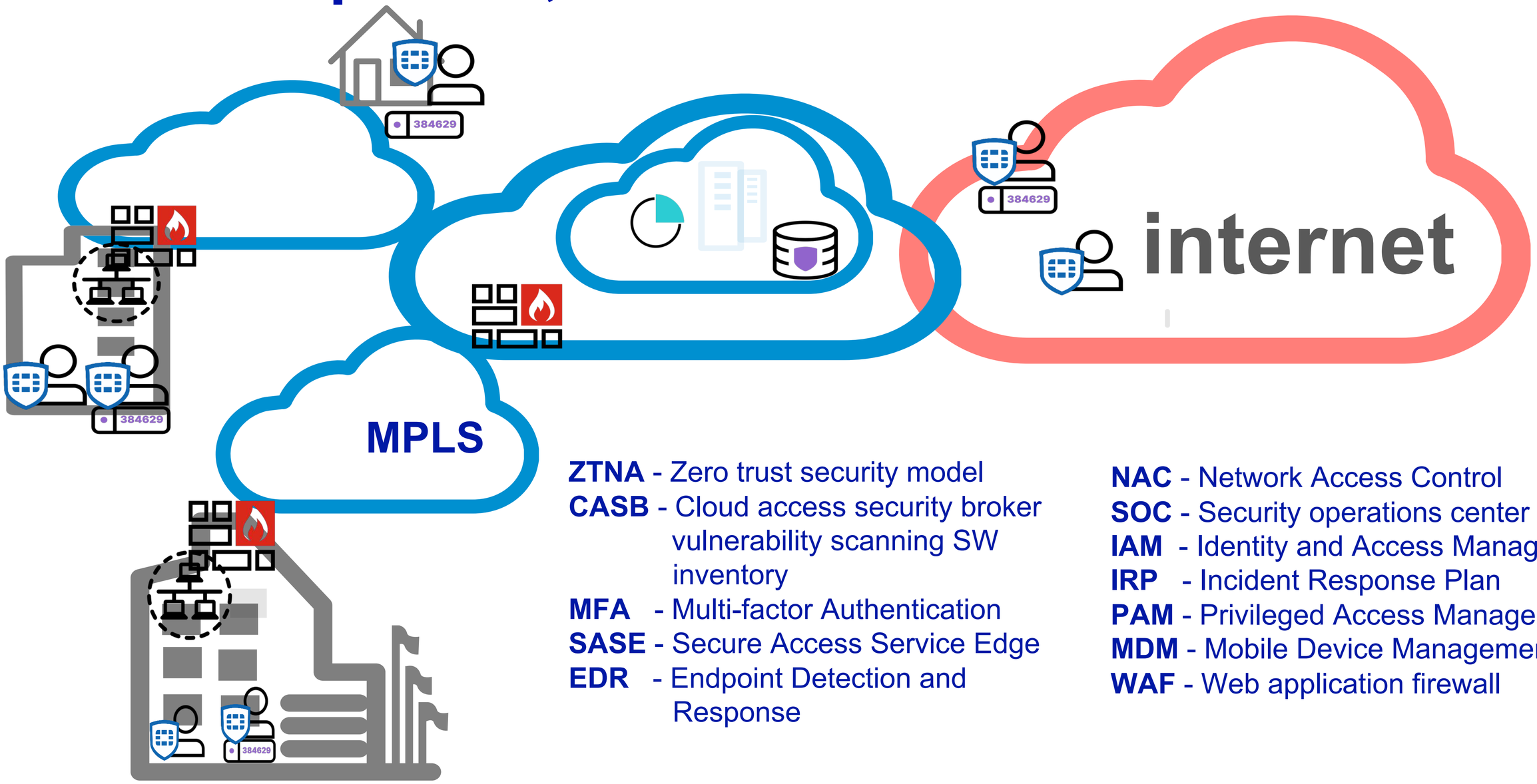
iCloud

Office 365

Google Cloud

Logy z UniCPE a ZTNA umožní analytiku i automatizaci.

Jednoduché řešení přinese mnoho funkcí se snadnou správou, které můžeme rozšiřovat

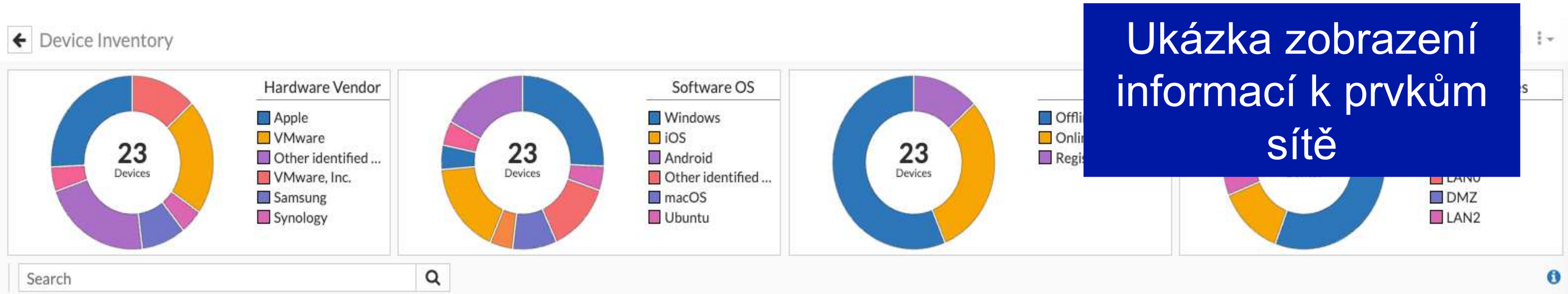


ZTNA - Zero trust security model
CASB - Cloud access security broker vulnerability scanning SW inventory
MFA - Multi-factor Authentication
SASE - Secure Access Service Edge
EDR - Endpoint Detection and Response

NAC - Network Access Control
SOC - Security operations center
IAM - Identity and Access Management
IRP - Incident Response Plan
PAM - Privileged Access Management
MDM - Mobile Device Management
WAF - Web application firewall

Zmapováním prostředí plníme povinnosti paragrafu Řízení aktiv

Ukázka zobrazení informací k prvkům sítě

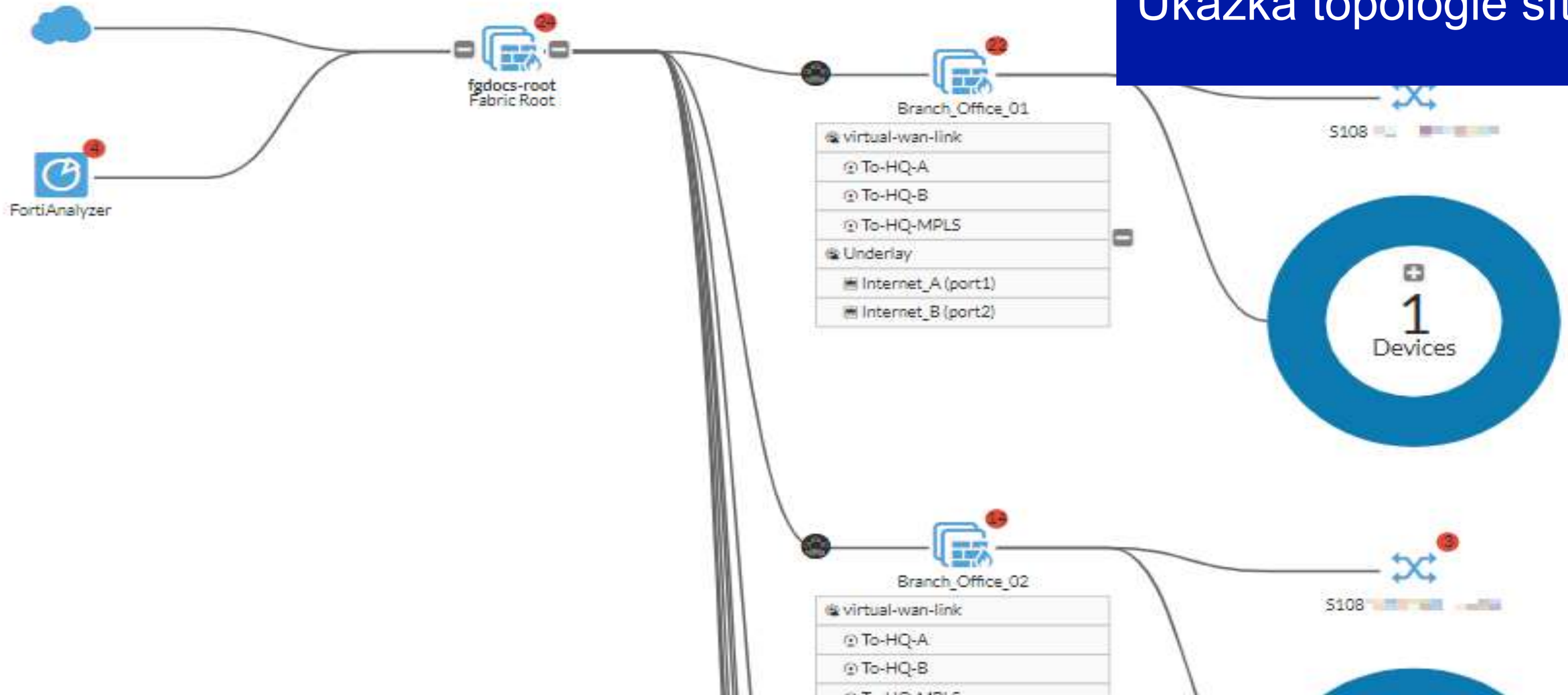


Search

Device	User	Address	Software OS	Device Family	Hardware Version	Endpoint Tags
Apple 6						
0a:3c:5f:4f:00:87		192.168.50.103 0a:3c:5f:4f:00:87	iOS			
MBC02K65LNQ6LR		192.168.50.110 70:ae:d5:55:4b:95	macOS	Mac	MacBook Air	
iPhone-Honza		192.168.50.101 9a:c5:dd:37:27:25	iOS	iPhone	13 Pro Max	
c2:2a:00:6f:64:0c		192.168.50.100 c2:2a:00:6f:64:0c	iOS			
MBC02J42BAQ6LR		192.168.50.104 d0:88:0c:73:f3:57	macOS	Mac	MacBook Air	
e2:06:76:a7:93:1c		192.168.50.103 e2:06:76:a7:93:1c	iOS			

Zmapováním prostředí plníme povinnosti paragrafu Řízení aktiv

Ukázka topologie sítě



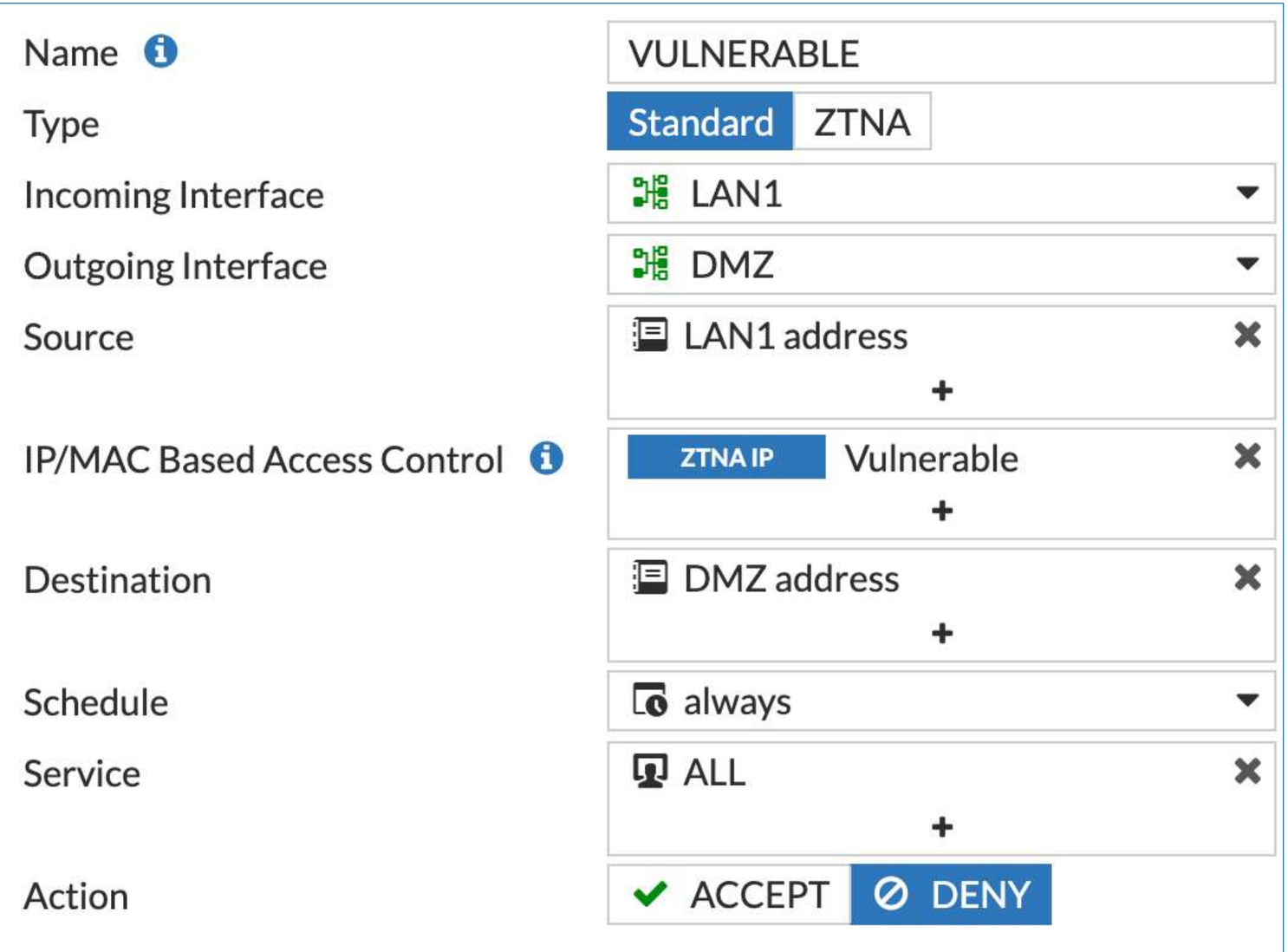
V zmapovaném prostředí plníme povinnosti paragrafu Řízení rizik

Ukázka zajištění informací

Total View 1086	108 Operating System	28 Browser	0 Microsoft Office
950 Third Party App	0 Service	0 User Config	0 Other

Ve zmapovaném a vyčištěném prostředí vyřešíme paragraf Řízení přístupů a identit

Ukázka přístupu



Ve zmapovaném a vyčištěném prostředí vyřešíme paragraf Řízení přístupů a identit

Ukázka centrálního systému

Status	Device	User	Software OS	Hostname	Address	MAC	Interfaces	Domain	Endpoint Tags
Registered - Online - On-Net	WIN1	user1	Windows	WIN1	192.168.101.101 00:0c:29:9b:c8:a6	00:0c:29:9b:c8:a6	LAN1	o2lab.cz	ZTNA IP Vulnerable ZTNA MAC Vulnerable ZTNA IP all_registered_clients ZTNA MAC all_registered_clients
Registered - Online - On-Net	WIN2	admin	Windows	WIN2	192.168.101.102 00:0c:29:52:78:b9	00:0c:29:52:78:b9	LAN1	o2lab.cz	ZTNA IP Vulnerable ZTNA MAC Vulnerable ZTNA IP all_registered_clients

Zajistíme, že vaše organizace bude v souladu se všemi paragrafy nového ZoKB.

Jsme partnerem pro kyberbezpečnost i pro řešení požadavků NIS2

Komplexní řešení bezpečnosti

Pomůžeme vám efektivně eliminovat konkrétní hrozby. Získáte vyšší odolnost vůči útokům zvenčí a ochranu klíčových firemních aktivit.

Úspora nákladů

Na základě analýzy bezpečnosti definujeme priority a navrhneme strategii, kam cílit investice.

Expertní know-how

Pomůžeme vám zajistit řádné plnění procesních, dokumentačních a technických povinností a zvýšit efektivitu fungování.

Konkurenční výhoda

Naplněním legislativních povinností splníte požadavky na nově určené povinné osoby tak, jak potřebují vaši zákazníci.

Děkujeme