Spisová značka: XXXXXXXXXX

Registrační číslo projektu: **CZ.06.3.05/0.0/0.0/15\_011/0003134**

Příloha č. 1 Zadávací dokumentace

Specifikace předmětu plnění

**„KYBERNETICKÁ BEZPEČNOST KVOP“**

Příloha č. 1 zadávací dokumentace obsahuje citlivé informace a vzhledem k tomu a z důvodů uvedených § 211 odst. 3 písm. d) zákona, bude tato příloha pouze k osobnímu vyzvednutí v sídle zadavatele. Předpokladem k jejímu vyzvednutí je podpis prohlášení o zachování mlčenlivosti, jehož vzor je uveřejněn na profilu zadavatele.

Obsah:

[1. Stávající stav 4](#_Toc503465290)

[1.1. Technická opatření – popis současného stavu 4](#_Toc503465291)

[1.1.1. §16 Fyzická bezpečnost 4](#_Toc503465292)

[1.1.2. §17 Nástroj pro ochranu integrity komunikačních sítí 5](#_Toc503465293)

[1.1.3. §18 Nástroj pro ověřování identity uživatelů 6](#_Toc503465294)

[1.1.4. §19 Nástroj pro řízení přístupových oprávnění 7](#_Toc503465295)

[1.1.5. §20 Nástroj pro ochranu před škodlivým kódem 7](#_Toc503465296)

[1.1.6. §21 Nástroj pro zaznamenávání činností 8](#_Toc503465297)

[1.1.7. §22 Nástroj pro detekci kybernetických bezpečnostních událostí 8](#_Toc503465298)

[1.1.8. §23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí 8](#_Toc503465299)

[1.1.9. §24 Aplikační bezpečnost 8](#_Toc503465300)

[1.1.10. §25 Kryptografické prostředky 9](#_Toc503465301)

[1.1.11. §26 Nástroje pro zajištění vysoké úrovně dostupnosti 9](#_Toc503465302)

[2. Specifikace předmětu veřejné zakázky 11](#_Toc503465303)

[2.1. Seznam dodávek 11](#_Toc503465304)

[2.2. Popis předmětu plnění veřejné zakázky 11](#_Toc503465305)

[2.2.1. Perimetr datových sítí s architekturou vysoké dostupností – modernizace firewallu 11](#_Toc503465306)

[2.2.2. Detekce anomálií datového provozu - analýza datových toků systémem zpracování NetFlow 13](#_Toc503465307)

[2.2.3. Implementace a zajištění centralizovaného sběru s vysokou dostupností a zpracování logovacích informací ze systémů – log management 13](#_Toc503465308)

[2.2.4. Implementace systému pro management bezpečnostních informací a událostí - SIEM 14](#_Toc503465309)

[2.2.5. Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech 15](#_Toc503465310)

[2.2.6. Implementace Provozně – technického monitorovacího systému (pro zajištění Performance a Capacity Management) a vybudování druhého záložního místa datového centra – Business Continuity 15](#_Toc503465311)

[2.2.7. Implementace systému testování zranitelností – Vulnerability Management 17](#_Toc503465312)

[2.2.8. Zvýšení fyzické bezpečnosti serveroven 20](#_Toc503465313)

[3. Specifikace minimálních požadavků řešení 25](#_Toc503465314)

[3.1. Perimetr datových sítí s architekturou vysoké dostupností – modernizace firewallu 25](#_Toc503465315)

[3.2. Detekce anomálií datového provozu - analýza datových toků systémem zpracování NetFlow 28](#_Toc503465316)

[3.3. Implementace a zajištění centralizovaného sběru s vysokou dostupností a zpracování logovacích informací ze systémů – log management 28](#_Toc503465317)

[3.4. Implementace systému pro management bezpečnostních informací a událostí - SIEM 31](#_Toc503465318)

[3.5. Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech 35](#_Toc503465319)

[3.6. Implementace Provozně – technického monitorovacího systému (pro zajištění Performance a Capacity Management) a vybudování druhého záložního místa datového centra – Business Continuity 38](#_Toc503465320)

[3.7. Implementace systému testování zranitelností – Vulnerability Management 41](#_Toc503465321)

[4. Implementace 42](#_Toc503465322)

[5. Požadavky na technickou podporu provozu 43](#_Toc503465323)

[6. Podmínky předání a převzetí – akceptace 44](#_Toc503465324)

[7. Záruky a servis – podpora provozu 45](#_Toc503465325)

[7.1. Záruka 45](#_Toc503465326)

[7.2. Servisní podpora provozu 45](#_Toc503465327)

[8. Harmonogram plnění 47](#_Toc503465328)

[9. Seznam zkratek 49](#_Toc503465329)

Seznam tabulek:

[Tabulka 1: Nástroj pro ověřování identity uživatelů ve VIS 7](#_Toc503465330)

[Tabulka 2: 2.2.8.3.13. Soupiska materiálu 23](#_Toc503465331)

[Tabulka 3: HW appliance firewallu kompatibilní se stávajícím zařízení Kernun UTM model 200 a zapojený do v Active/Passive Clusteru 25](#_Toc503465332)

[Tabulka 4: Rozšiřující moduly Kernun Clear Web, Antivirus, IDS/IPS pro Kernun UTM cluster 26](#_Toc503465333)

[Tabulka 5: Rozšiřující modul Adaptive Traffic Routing 27](#_Toc503465334)

[Tabulka 6: Rozšíření o Kernun Business Intelligence 27](#_Toc503465335)

[Tabulka 7: Detekce anomálií datového provozu - analýza datových toků systémem zpracování NetFlow 28](#_Toc503465336)

[Tabulka 8: Implementace a zajištění centralizovaného sběru a zpracování logovacích informací ze systémů 28](#_Toc503465337)

[Tabulka 9: Kapacitní požadavky – log management 30](#_Toc503465338)

[Tabulka 10: Omezení a limity – log management 31](#_Toc503465339)

[Tabulka 11: Implementace systému pro management bezpečnostních informací a událostí - SIEM 31](#_Toc503465340)

[Tabulka 12: Kapacitní požadavky – SIEM 33](#_Toc503465341)

[Tabulka 13: Požadavky na vstupy a zpracování dat – SIEM 33](#_Toc503465342)

[Tabulka 14: Mimofunkční požadavky – SIEM 35](#_Toc503465343)

[Tabulka 15: Limity a omezení – SIEM 35](#_Toc503465344)

[Tabulka 16: Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech 35](#_Toc503465345)

[Tabulka 17: Kapacitní požadavky – PIM/PAM 37](#_Toc503465346)

[Tabulka 18: Limity a omezení – PIM/PAM 37](#_Toc503465347)

[Tabulka 19: Virtualizační server pro záložní lokalitu – 1 ks 38](#_Toc503465348)

[Tabulka 20: Doplnění blade chassis HP C7000 – 2 ks switchů 39](#_Toc503465349)

[Tabulka 21: Aktivní prvky pro primární a záložní serverovnou – 4 ks 39](#_Toc503465350)

[Tabulka 22: Virtuální diskové pole – 2 ks 40](#_Toc503465351)

[Tabulka 23: Optické propojení 40](#_Toc503465352)

[Tabulka 24: Všechny varianty testů - požadované výstupy 41](#_Toc503465353)

[Tabulka 25: Požadavky – Implementace nabízeného řešení 42](#_Toc503465354)

[Tabulka 26: Požadavky na technickou podporu provozu 43](#_Toc503465355)

[Tabulka 27: Reakční doby pro řešení požadavků 46](#_Toc503465356)

**Seznam obrázků:**

[Obrázek 1: Schéma zapojení firewallu 12](#_Toc503465357)

[Obrázek 2: Harmonogram plnění 48](#_Toc503465358)

# Stávající stav

Kancelář veřejného ochránce práv se nachází v postavení povinné osoby z hlediska příslušných ustanovení §2, odst. d) e), zákona 181/2014 Sb. - Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (ZoKB), a to s ohledem na tam provedené vymezení povinné osoby ve smyslu §3, odst. e). To znamená, že z pohledu uvedeného zákona je organizace **správcem významného informačního systému**.

Odůvodnění:

Organizace Kancelář veřejného ochránce práv provedla oznámení kontaktních údajů v souladu s § 31 zákona 181/2014 Sb., kdy na základě vyhlášky 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, když identifikovala 3 významné informační systémy.

1. Informační systém spisové služby a ekonomických informací GINIS SSL a EKO
2. Personální informační systém VEMA (PAM, PER, KZP, RNP, ELD a STM)
3. Systém elektronické pošty MS Exchange

## Technická opatření – popis současného stavu

Lze konstatovat s ohledem na aplikovaná technická opatření, že organizace má zavedenu alespoň dílčím způsobem řadu opatření předpokládaných zákonem 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, tak, jak je tento zákon předepisuje.

Z pohledu požadavků na běžnou úroveň zabezpečení Kybernetické bezpečnosti v organizaci má Kancelář veřejného ochránce práv nasazené běžné, obvykle používané technické i organizační bezpečnostní opatření. V každodenní praxi převážná část klíčových opatření v organizaci funguje.

Organizace Kancelář veřejného ochránce práv však byla identifikována podle zákona jako „správce významného informačního systému “ dle § 3 písmene e). Na takový subjekt zákon a prováděcí vyhláška č.316/2014 Sb. klade zvýšené požadavky na zajištění Bezpečnostních opatření, uvedených v § 4 ZoKB, přesněji specifikované prováděcí vyhláškou č.316/2014 Sb.

Dopad požadavků těchto opatření na organizaci je významný a v přechodném období bude nezbytné implementovat řadu technických opatření nad současný rámec exitujících opatření vyplývajících z postavení organizace jako „správce významného informačního systému“.

### §16 Fyzická bezpečnost

Organizace sídlí v jednom objektu, ve kterém se nachází všechny prostory, kterých se týkají opatření kybernetické bezpečnosti.

Jedná se o tyto prostory:

* Hlavní místnost serverů - Serverovna
* Sklad informatiky / archiv, kde jsou umístěny zálohovací technologie
* Místnosti umístění rozvaděčů strukturované kabeláže (3x)

Přístup do Serverovny je přes neveřejné prostory oddělení IT a je řízen prostřednictvím klasického zámku s dozickým klíčem, klika zvenčí bez koule, interiérové dveře. V serverovně je čidlo EZS a EPS. Venkovní Okno v serverovně není chráněno mříží nebo jiným fyzickým zabezpečením a nachází se ve zvýšeném prvním patře. Okna jsou také směrem do chodbičky IT prostor pod stropem. Přístupy osob do serverovny nejsou nijak evidované, ani není monitoring prostor kamerovým systémem. Přístup do prostor IT přes interiérové dveře s koulí na vnější straně (prostory pro veřejnost). V serverovně je nainstalovaná klimatizace s dvěma jednotkami.

Přístup do skladu informatiky, kde je umístěna zálohovací technologie, je řízen prostřednictvím klasického zámku s dozickým klíčem interiérové dveře s klikou. Sklad se nachází na úrovni přízemí, v prostorách archivu a spisovny, jako samostatná oddělená místnost. V místnosti je čidlo EPS. Místnost je bez oken. Přístupy osob do skladu nejsou nijak evidované, ani není monitoring prostor kamerovým systémem. Do skladu mají přístup i další osoby, ale jedná se o omezenou skupinu osob. Přístup je možný univerzálním klíčem vydávaným proti podpisu.

Přístup do místností umístění rozvaděčů strukturované kabeláže je řízen prostřednictvím klasického zámku s dozickým klíčem, interiérové dveře. Místnost je bez oken, instalované čidlo EPS. Přístupy osob do místností nejsou nijak evidované ani není monitoring prostor kamerovým systémem.

Servery a další související podpůrná technická aktiva mají instalovaná zařízení pro zajištění ochrany před krátkodobým selháním dodávky elektrického napájení – UPS. Výjimkou jsou aktivní prvky ve 3ch místnostech rozvaděčů, kde nejsou instalovány UPS.

V objektu je instalovaný kamerový systém CCTV s 11 kamerami, které zabírají především okolí, plášť a vstupy do objektu a je vyveden u strážní služby.

V objektu je instalovaný přístupový systém ACS, který zabezpečuje přístupy do 2 zón

* Zóna neveřejných prostor všech pracovníků organizace
* Zóna prostor nejvyššího vedení

Přístupový systém pro identifikaci osoby používá bezkontaktní chipy.

**Doporučení:**

Přestože organizace používá prostředky a nástroje k zajištění fyzické bezpečnosti, avšak jejich aplikace není systémově zavedena a nevychází z iniciačního celkového hodnocení v rámci analýzy rizik nebo není dostatečně dokumentována v podobě nezbytné pro ZoKB. Nicméně vlastní technické opatření vyhovuje požadavkům ZoKB a VyKB kladeným na správce významného informačního systému. Přesto doporučujeme rozšíření současného přístupového systému ACS o další zónu pro ICT aktiva a instalaci řízení přístupu do výše uvedených prostor. A / nebo rozšířit kamerový systém CCTV o další kamery pro monitoring skladu informatiky a serverovny.

### §17 Nástroj pro ochranu integrity komunikačních sítí

1. a) Organizace používá firewall pro řízení přístupu mezi vnější a vnitřní sítí,

1. b) segmentace sítě existuje alespoň na 2 segmenty LAN a DMZ,

1. c) kryptografické prostředky se používají pro vzdálený přístup do vnitřní sítě jednak prostřednictvím prostředků technologie VPN pro dodavatele a na druhé straně pro uživatele organizace technologiemi vzdáleného terminálového přístupu

1. d) Organizace používá pouze částečně prostředky pro odstranění nebo blokování přenášených dat, spíše až na koncových bodech, ale ve směru z vnitřní sítě ven se prostředky nepoužívají. Opatření pro odstranění nebo blokování přenášených dat neodpovídají požadavkům na ochranu integrity komunikační sítě.

2. Organizace nevyužívá nástroj pro ochranu integrity komunikační sítě včetně její segmentace, ale tento nástroj není pro správce významného informačního systému mandatorně požadován.

Organizace má zkonfigurované v současnosti pouze 2 segmenty sítí a to vnitřní LAN síť a síť DMZ, přičemž segment DMZ je zatím nevyužívaný bez zařízení.

LAN síť je na páteři propojena optickými kabely na 1Gb centrální switch se 3 patrovými switchi v místnostech rozvaděčů.

Internetové připojení NREN síť (nekomerční sít) od Masarykovy university, 200Mbit optickým kabelem. Ukončené na rozhraní Cisco PIX ASA5505, hraniční firewall organizace (pouze Firewall a NAT pravidla), kde se ukončují VPN IPSec pro dodavatele. Cisco PIX logování se neposílá nikam externě např. na Syslog server. Z PIXe vede jedno datové rozhraní na další bezpečnostní zařízení Kernum UTM. Administraci VPN uživatelů provádí externí dodavatel a to firma Autocont nebo IT pracovník KVOP a je zajištěna přímo v Cisco PIXu, není provedena integrace na centrální direktory services organizace MS Active Directory.

Pro ochranu interní LAN sítě používá Firweall Kernum 200 UTM – Aplikační firewall. Pracuje ve funkci proxy serveru s kontrolou základních Internetových protokolů http/https/ftp, kontrola základní Smtp (bez Antispamu, antiviru). Současná konfigurace zařízení Kernum neobsahuje žádné funkcionality Antivirové ochrany, případně Antispamové ochrany email provozu, ani služby kontroly síťového provozu typu IPS/IDS. Logy se uchovávají interně a to 30dnů, existuje možnost ukládání na externí Log management server. Administrace systému Kernum je zajištěná jako služba prostřednictvím externího dodavatele.

Pro vzdálený přístup pracovníci organizace používají tyto technologie:

* MS OWA k emailovým schránkám uživatelů a synchronizaci Smartphone v počtu cca 25 licencí – protokol RPC over HTTPS
* Virtuální desktopy přes Citrix XEN desktop pro max. 10 uživatelských desktopů
* Pro IT Administraci se používá admin Terminálový služba
* LogMeIn – 6 licencí pro administraci systémů a pro přístup k uživatelským počítačům pracovníků KVOP (samostatné uživatelské přihlášení)

Pro všechny přístupy Autentizace jménem a heslem. V organizaci není provedena implementace technologie RADIUS server pro ověřování.

WiFi přístup do vnitřní LAN sítě organizace není implementovaný. Poskytuje se pouze přístup do veřejné sítě Internetu pro veřejnost prostřednictvím externího poskytovatele připojení a mimo síťovou infrastrukturu organizace

**Doporučení:**

Organizace používá nástroje pro ochranu integrity komunikačních sítí, jejich aktuální implementace není dostatečně dokumentována v podobě nezbytné pro ZoKB. Systémově chybí zavedení dílčích technických opatření. Nicméně vlastní technické opatření nevyhovuje požadavkům ZoKB a VyKB kladeným na správce významného informačního systému.

Organizace se chrání na svém perimetru z veřejného internetu dovnitř komunikační infrastruktury, ale nemá dostatečně vyřešený problém, pokud by útok probíhal z některé části vnitřní komunikační infrastruktury nebo pokud by se nějakým způsobem útočníkovi podařilo překonat zabezpečení hraničního perimetru. Stejně tak nejsou implementované žádné technologie detekce. Proto doporučujeme implementovat technologie vnitřní ochrany interní komunikační infrastruktury typu Intrusion detection system (IDS) / Intrusion Prevention Systems (IPS), případně další jako jsou NetFlow/IPFIX nebo/a Network behavior analysis (NBA).

Rozhodně doporučujeme implementovat vícefaktorovou autentizaci integrovanou s centrální directory services organizace – MS Active Directory pro vzdálené přístupy do vnitřní infrastruktury organizace jak pro interní pracovníky, tak pro externí subjekty. Pro VPN vzdálené přístupy do vnitřní komunikační infrastruktury zapnout podrobné logování.

Stejně tak doporučujeme implementovat vícefaktorovou autentizaci pro vzdálený přístup pomocí Citrix virtuálních desktopů nebo MS terminálového přístupu.

### §18 Nástroj pro ověřování identity uživatelů

1. Organizace používá centralizovaný nástroj pro ověření identity typu Directory services a to založené na technologii Microsoft Active Directory v současnosti ve verzi 2003. Jednotlivé VISy používají různé mechanizmy autentizace, viz vysvětlení níže.

2. Nástroje na ověření identity zajišťují ověření identity uživatelů a to jak centralizovaně přes MS AD, tak i interními službami autentizace jednotlivých VISů pouze v rozsahu lokálního přihlášení.

Vzhledem k verzi MS AD nelze používat samostatné politiky hesel pro uživatele a samostatné pro administrátory.

3. Politika hesel stanovena ve Směrnici č. 9/2013 Zabezpečení přístupů a ochrana dat personálních počítačů v Kanceláři veřejného ochránce práv

4. Není mandatorní pro správce VISu.

Organizace v současnosti pokud už používá centralizovaný nástroj pro ověřování identity uživatelů directory services, tj. Microsoft Active Directory verze 2003, tato verze je zastaralá a v roce 2015 ji skončila podpora od výrobce tj. Microsoftu. Stejně tak tato verze nepodporuje některé vyžadované funkcionality jako je např. více politik pro hesla pro různé typy rolí.

V MS Active Directory existují celkem 3 Domain Controllery: 2x MS Windows 2008R2 Std., 1x MS Windows 2003 Std.

Systém Gordic používá integraci s MS Active Directory. Ekonomický modul používá výhradně autentizaci přes MS AD. Modul Spisové služby používá kombinovanou autentizaci jednak MS AD a také přes interní databázi uživatelů (spravuje IT, pár uživatelů z historických důvodů)

Systém VEMA používá pouze autentizaci přes interní systém VEMY bez integrace s MS AD, ale integrace s MS AD je potenciálně technicky možná.

Tabulka 1: Nástroj pro ověřování identity uživatelů ve VIS

|  |  |  |
| --- | --- | --- |
| **Typ VISu** | **Nástroj pro ověřování identity uživatelů** | **Poznámka** |
| Informační systém ekonomických informací GINIS EKO | MS Active Directory | Provedena integrace na MS AD, ale lze autentizovat i interní službou |
| Informační systém spisové služby GINIS SSL | Kombinovaná autentizaci jednak MS AD a také přes interní databázi uživatelů | viz modul EKO |
| Personální informační systém VEMA | Interní služba systému | Lze integrovat s MS AD |
| Systém elektronické pošty MS Exchange | MS Active Directory | Pouze integrace s MS AD |

**Doporučení:**

Doporučujeme provést přípravu projektu migrace MS AD na podporovanou verzi alespoň 2008 se zrušením nebo provedením upgrade serveru KVOPTSM z verze 2003 také na verzi 2008 nebo na vyšší. Následně doporučujeme provést plnou integraci s MS AD u obou VISů, z důvodu zajištění centralizace všech autentizačních informací včetně automatizaci správy politik hesel. Protože bez provázání VISů na jeden centrální MS AD nelze na jednom místě řídit bezpečnostní politiku a sbírat informace o aktivitách uživatelů, případně o prováděných změnách v konfiguraci od administrátorů.

### §19 Nástroj pro řízení přístupových oprávnění

1. Organizace používá nástroje pro řízení přístupových oprávnění, který zajistí řízení oprávnění dle bodu a), b).

2. Není mandatorní pro správce VISu. Organizace sice používá nástroje, které zaznamenávají použití přístupových oprávnění, ale centralizace těchto informací neexistuje, takže nelze jednoduše vyhodnocovat a porovnávat s bezpečnostní politikou.

Gordic má vlastní podrobné logování jednak Administračních změn, ale i operací nad daty, včetně toho kdo prohlížel (četl).

**Doporučení:**

Organizace z nástrojů nasazených v současnosti není schopná automatizovaně sbírat záznamy o použití přístupových oprávněních, centralizovaně zpracovávat a kontrolovat zda je použití přístupových oprávnění v souladu s bezpečnostními potřebami a politikou. Doporučujeme proto alespoň v prvním kroku provést plnou integraci VISů s MS AD a následně implementovat nástroj, který bude sbírat a centralizovat záznamy o využití přístupových oprávněních, který také bude schopen alespoň zpětně vyhodnotit soulad nebo nesoulad s platnou bezpečnostní politikou. Stejně tak je nezbytné provést integraci personálního systému VEMA obsahujícího informace o uživatelích s centralizovaným systémem řízení přístupových oprávnění MS AD, jak to specifikuje také §9 a zajistit tak i zpětné kontrolní mechanizmy.

### §20 Nástroj pro ochranu před škodlivým kódem

Organizace používá částečně nástroj pro ochranu před škodlivým kódem

a) pro komunikaci mezi vnitřní a vnější sítí, používá pouze Firewall,

b) u serverů a sdílených datových úložišť používá Antivirus na Windows serverech,

c) u pracovních stanic používá Antivirus,

a aktualizace nástroje pro ochranu před škodlivým kódem se provádí.

Organizace používá mezi vnitřní a vnější sítí dvě zařízení typu Firewall viz podrobný popis v také §17. Nicméně ani jedno zařízení na síťové úrovně neobsahuje funkcionality antivirové ochrany nebo technologie IPS/IDS.

Organizace používá pouze servery s operačním systém Windows server ve verzi Standard a na nich provozuje antivir Symantec Endpoint protection ver. 12. Speciálně na Email serveru s MS Exchange 2008 je nasazena verze antiviru Symantec Mail security, kde je také duplicitní funkcionalita s externí službou Virusfree. Pro kontrolu příchozího směru elektronické pošty Emailů se využívá externí služba Virusfree, která provádí filtrování příchozí pošty na Antispam a Antivir.

PC stanicích je nasazen hromadně antivir Symantec Endpoint protection ver 12. s funkcionalitou pouze Antivirus a centrální správou. Celkem je v organizaci 140 licencí Symantec Endpoint protection.

**Doporučení:**

Naopak organizace nepoužívá řešení ochranu komunikace před škodlivým kódem mezi vnitřní a vnější sítí například typu IPS/IDS systém, a také je především potřeba chránit celou komunikační infrastrukturu a ve všech směrech před škodlivými kódy. Takže doporučujeme implementovat nástroj pro ochranu veškerých komunikací dovnitř komunikační infrastruktury, jak bylo v opatření § 17 Nástroj pro ochranu integrity komunikačních sítí

### §21 Nástroj pro zaznamenávání činností

1. Organizace nepoužívá jeden centrální nástroj pro zaznamenávání činností a neprovádí body a), b).

2. Organizace na jednom místě neprovádí záznamy dle bodu a) – h).

3. Není mandatorní pro správce VISu.

4. Synchronizace systémového času jednotným způsobem je prováděna.

Windows server s funkcí MS AD Domain Controller (KVOPTSM 192.168.25.250) se synchronizuje s časovým normálem z internetu pomocí protokolu NTP. Z tohoto serveru jsou pak synchronizované všechny servery a počítače v MS AD a také virtualizační servery VMWare.

**Doporučení:**

Naopak organizace nepoužívá žádné řešení pro zaznamenávání činností, proto ke splnění požadavků technického opatření z §21 na nástroj pro zaznamenávání činností musí implementovat takový nástroj. Tímto nástrojem je chápán centralizovaný Log management systém - Nástroj pro zaznamenávání činnosti, který bude centralizovat ukládání logů / záznamů ze všech určených prvků infrastruktury a systémů včetně archivace po určené doby. Systém je nezbytný také jako jednotný zdroj logů pro případnou implementaci systému SIEM nebo napojení organizace na externí službu Security Operation Centrer – SOC.

Log Management je komplexní a přitom jednoduchý systém pro práci s logy v originálním formátu/tvaru. Log Management by měl zajišťovat příjem logů v jejich originální formě („RAW“), jejich bezpečné ukládání (šifrovaně, komprimovaně, s použitím TSA certifikačního razítka), rychlé vyhledávání a archivaci.

### §22 Nástroj pro detekci kybernetických bezpečnostních událostí

1. Organizace nepoužívá jednotný nástroj pro detekci kybernetických bezpečnostních událostí.

2. Není mandatorní pro správce VISu a organizace takový nástroj pro detekci kybernetických bezpečnostních událostí podle bodu a), b) nepoužívá.

**Doporučení:**

Organizace v současnosti nepoužívá žádný z nástrojů pro detekci kybernetických bezpečnostních událostí, přestože vnitřní komunikační infrastruktura organizace je jednou z nejklíčovějších částí celého ICT, protože po této infrastruktuře nezávisle funguje několik nejen identifikovaných KIS, ale i obchodně kritických aplikací a jiných bezpečnostních systémů.

### §23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Celkové hodnocení: - Mandatorně není vyžadován

Organizace v současnosti nepoužívá žádný z nástrojů pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

### §24 Aplikační bezpečnost

1. Organizace neprovádí pravidelně bezpečnostní testy zranitelnosti aplikací.

2. Není mandatorní pro správce VISu. Organizace zajistila aplikační bezpečnost tohoto bodu tak, že aplikace VIS nejsou přístupné z vnější sítě s výjimkou části aplikace MS Exchange funkcionality OWA. A dále aplikace VIS systém Ginis a Vema mají implementované ochrany transakcí, jak je popisuje písmeno b).

Testy zranitelnosti prováděla firma Anect v roce 2014 pomocí nástroje, tzn. Automatizované testy

**Doporučení:**

Organizace v minulosti provedla jednorázový test zranitelnosti externím dodavatelem. Pro splnění požadavků technického opatření je nezbytné provádět testy zranitelnosti, opakovaně v pravidelných cyklech. Tyto testy zranitelnosti musí být provedeny včetně odborného vyhodnocení a návrhu opatření k ošetření zjištěných zranitelností a problémů, které v tomto případě je nezbytné a není možné ho provést interními kapacitami. Nejdříve je nezbytné provést iniciační testy zranitelnosti, ke zjištění základní úrovně. Následně pak opakované, pravidelné testy zranitelnosti v intervalech stanovených interními pravidly.

### §25 Kryptografické prostředky

1. a) Organizace nestanovila úroveň kryptografické ochrany.

1. b) Organizace nestanovila pravidla kryptografické ochrany informací.

2. Není mandatorní pro správce VISu.

Nepoužívá se šifrování dat na souborových systémech u serverů ani na PC stanicích. Organizace používá cca 25 notebooků, ale ani tam není použito šifrování dat (např. Bitlocker).

Nepoužívají se technologie pro šifrování Emailů.

Nepoužívají se technologie pro šifrování dat předávaných mimo organizaci.

Nepoužívají se technologie šifrování dat v databázích.

Organizace neprovozuje vlastní PKI infrastrukturu, pro potřeby vydávání elektronických podpisů využívá služeb společnosti I.CA.

**Doporučení:**

Musí být vytvořeny pravidla pro kryptografické mechanizmy jednotlivých technologií, které jsou v souladu s VyKB.

### §26 Nástroje pro zajištění vysoké úrovně dostupnosti

1. Organizace používá nástroje pro zajištění úrovně dostupnosti informací splňující požadavky bodu a), b).

2. Není mandatorní pro správce VISu. Přesto organizace plní požadavky kladené v bodu 2., kdy zálohuje důležitá technická aktiva a také používá redundantní řešení v technických návrzích

Organizace používá virtualizační technologie VMWare na dvou Hewlett Packard serverech typu Blade s celkem 8 ks „žiletkových“ serverů v rozdělení 6 ks staré fyzické servery a 2ks nové fyzické servery.

Vlastní rozdělení je:

* 4x VMWare 4.x Enterprise servery (zapnuté DRS, HA vypnuté) asi 22 virtuálních serverů, aktivních 13
* 2x VMWare 5.5 Enterprise servery, vCenter 5 standard 7 virtuálních serverů

Bohužel celou virtualizační platformu založenou na technologii VMWare verze 4 není možné upgradovat na verzi 5.5 z důvodu nekompatibility hardware virtualizačních serverů. Proto byla také pořízena celá nová virtualizační platforma servery a VMWare ve verzi 5.5. Obě platformy jsou provozovány odděleně a předpoklad je přesunutí klíčových aplikací na novou virtuální platformu s následným postupným vypnutím staré platformy.

Pro zálohování používá organizace zase dvě zálohovací technologie a to:

* IBM Tivoli Storage Manager (IBM TSM)
* VMWare Data recovery

Jako zálohovací médium se používá

* Pásková mechanika Dell PowerVault TL2000 – 2x drive
* Datové úložiště

Zálohovací systém IBM TSM používá speciálního agenta pro zálohování souborů, zálohování databáze a zálohování Email serveru (MS Exchange)

Zálohovací systém IBM TSM server je pracuje na fyzickém serveru s operačním systémem Windows 2003R2, který je současně nositelem rolí MS AD jako Domain Controller.

VMWare se zálohuje přes virtuální appliance VMWare Data recovery, která ukládá data přes iSCSI diskové pole (1,4TB a 1,89TB)

Naopak organizace nepoužívá žádný z centralizovaných nástrojů pro Provozně – technický monitoring a dohled infrastruktury a aplikací.

**Doporučení:**

Organizace používá nástroje pro zajištění vysoké úrovně dostupnosti a to založené na virtualizačních technologiích firmy VMWare včetně odpovídajícího zálohování.

Virtualizační technologie firmy VMWare se používají ve dvou verzích a to ve staré verzi 4.x a v nové verzi 5.5. Vzhledem k předpokládanému vypnutí starší virtualizační technologie verze 4.x doporučujeme naplánovat doplnění virtualizační platformy VMWare 5.5 o další fyzický virtualizační server do některé oddělené místnosti v jiné části budovy.

Pro naplnění technického opatření je také nutné provést částečné a úplné testy obnovy prvků informačního systému kritické informační infrastruktury.

Pro naplnění technického opatření zajišťování úrovně dostupnosti informací je v organizaci provést implementaci některého z centralizovaných systémů Provozně – technického monitoringu, který zajistí dohled nad celým kybernetickým prostorem organizace a zprostředkuje informace o provozu nebo i výpadcích provozně – technické obsluze.

# Specifikace předmětu veřejné zakázky

V následujících kapitolách je uveden seznam dodávek, popis předmětu plnění veřejné zakázky a specifikace minimálních parametrů řešení nutných pro realizaci této veřejné zakázky.

## Seznam dodávek

Předmětem plnění je realizace technických opatření popsaných níže. Všechna opatření, která jsou předmětem plnění, budou sdílena všemi primárními aktivy (ve smyslu vyhlášky č. 316/2014 Sb.). Žádné navržené technické opatření nebude specifické jen pro jeden informační systém zadavatele.

Seznam dodávek – technická opatření jsou následující:

1. Perimetr datových sítí s architekturou vysoké dostupností – modernizace firewallu.
2. Detekce anomálií datového provozu – analýza datových toků systémem zpracování NetFlow.
3. Implementace a zajištění centralizovaného sběru s vysokou dostupností a zpracování logovacích informací ze systémů – log management.
4. Implementace systému pro management bezpečnostních informací a událostí - SIEM.
5. Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech.
6. Implementace Provozně – technického monitorovacího systému (pro zajištění Performance a Capacity Management) a vybudování druhého záložního místa datového centra – Business Continuity.
7. Implementace systému testování zranitelností – Vulnerability Management.
8. Zvýšení fyzické bezpečnosti serveroven.
9. Součástí realizace je projektové řízení.

Včetně zajištění podpory provozu předmětu veřejné zakázky po dobu udržitelnosti projektu tj. 5 let.

## Popis předmětu plnění veřejné zakázky

### Perimetr datových sítí s architekturou vysoké dostupností – modernizace firewallu

Posílení síťové bezpečnosti a komunikační bezpečnosti je požadováno na více úrovních, více dílčími technickými opatřeními, které korespondují s příslušnými ustanoveními vyhlášky č. 316/2014 Sb., konkrétně:

* dle § 17 – Nástroj pro ochranu integrity komunikačních sítí
* dle § 20 – Nástroj pro ochranu před škodlivým kódem.

Na síťovém perimetru zadavatele jsou zapojeny v sérii 2 firewally různých výrobců s různou funkcionalitou, která nepokrývá ani provozní potřeby zadavatele, ani požadavky vyhlášky č. 316/2014 Sb.

**Realizace tohoto technického opatření spočívá v:**

* Odpojení firewallu Cisco ASA PIX
* Zachování stávajícího firewallu Kernun UTM a jeho přesun přímo na síťový perimetr
* Doplnění firewallu Kernun UTM o další HW zařízení, tak aby se vytvořil HA cluster, např. v modu Active / Passive
* Doplnění další bezpečnostních funkcionalit do firewallu Kernun UTM, především IPS/IDS, ochrana před DDoS útokem, atd.

Důvodem pro návrh zachování zařízení Kernun UTM oproti Cisco ASA PIX je skutečnost, že zařízení Kernun UTM je modernější zařízení a z pohledu síťové bezpečnosti nabízí daleko širší portfolio funkcionalit, které se dají jednoduše škálovat jen pomocí licencí.

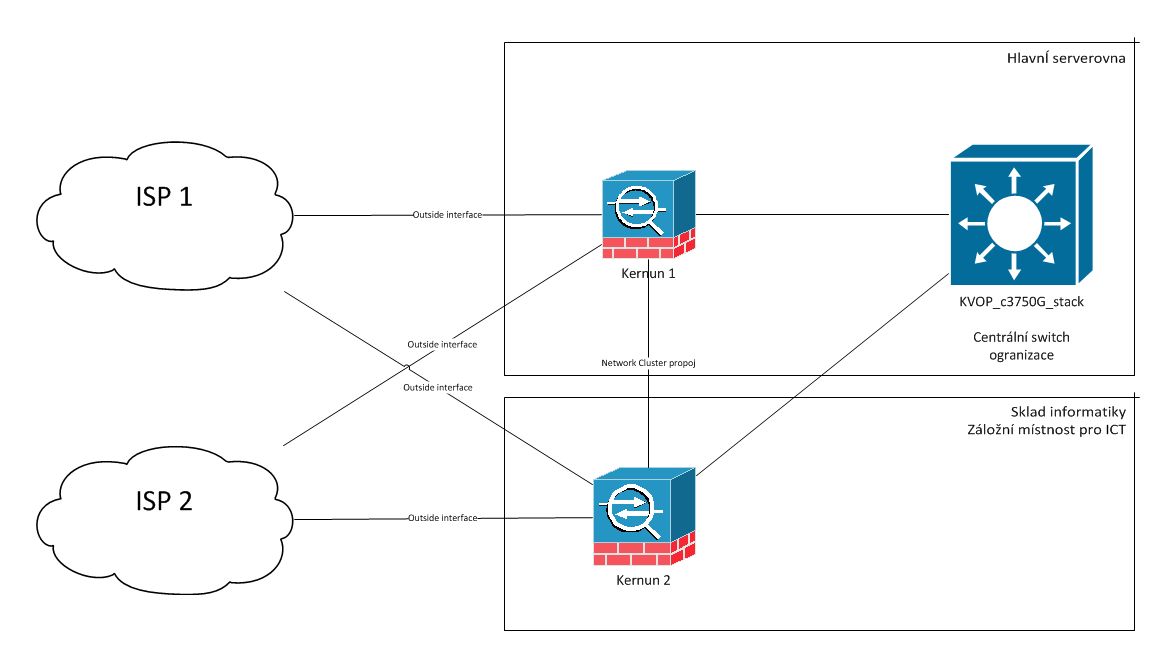
Technologii Kernun zadavatel již provozuje (a její pořízení v minulosti uhradil). Nyní zadávaný předmět plnění má využít dřívější investice, technologii zachovat a rozšířit její využitelnost. Zadavatel považuje Kernun za moderní, funkčně zcela vyhovující řešení. Kromě toho zadavatel již dříve vysoutěžil (zadal ve veřejné zakázce) softwarovou i hardwarovou podporu (smlouva do 30.6.2019), jakož i provozní podporu.

Technické podmínky v této veřejné zakázce jsou stanoveny prostřednictvím odkazu na konkrétní výrobek proto, že to je odůvodněno předmětem veřejné zakázky. V souladu s ustanovením § 89 odst. 6 zákona zadavatel umožňuje nabídnout rovnocenné řešení založené i na jiné technologii, pokud řešení beze zbytku naplní věcné požadavky uvedené v zadávací dokumentaci; současně by musela být vyřešena softwarová, hardwarová a provozní podpora.

**Požadované funkcionality, které zařízení bude nově plnit, jsou následující:**

* Hraniční firewall organizace na síťovém perimetru, kde budou ukončena síťová rozhraní dvou poskytovatelů služeb. Nově se bude kontrolovat veškerý příchozí a odchozí provoz včetně provádění bezpečnostních kontrol (oproti dosavadnímu stavu kontroly jen příchozího směru).
* Využití funkcionality monitorování kvality síťových rozhraní poskytovatelů s reakcí na výpadek dostupnosti tak, aby se směroval provoz přes funkční konektivitu. (V případě technologie Kernun by šlo o využití funkcionality Adaptive Traffic Routing - ATR.)
* Zajištění vzdálených přístupů do interní síťové infrastruktury přes VPN přístupy s autentizací uživatelů vůči MS Active Directory Společně s omezením přístupů přes technologie Logme-In, Teamviewer.
* Kernun UTM bude rozšířen o modul pro filtraci webového provozu Kernun Clear Web; podobně v případě jiné technologie než je Kernun; uchazeč v nabídce uvede popis funkcionality.
* Kernun UTM bude rozšířen o modul pro antivirovou kontrolu provozu minimálně pro http, https, ftp, smtp, pop3 a imap4 provoz; podobně v případě jiné technologie než je Kernun; uchazeč v nabídce uvede popis funkcionaliy.
* Kernun UTM bude rozšířen o systém narušení IDS/IPS; podobně v případě jiné technologie než je Kernun; uchazeč v nabídce uvede popis funkcionality.
* Kernun UTM bude rozšířen o Kernun Business Intelligence; samostatný nástroj pro detailní pohled do sítového provozu organizace a analýzu provozních záznamů řešení.

Obrázek 1: Schéma zapojení firewallu



Zadavatel požaduje, aby mu dodavatel na vyzvání (nikoli automaticky) předal zdrojový kód firewallu; takto předaný kód zadavatel použije výhradně za účelem certifikace ze strany NBÚ nebo jiného státního orgánu.

**Pořizované položky řešení:**

* HW appliance firewallu kompatibilní se stávajícím zařízení Kernun UTM model 200 a zapojený do v Active/Passive Clusteru. Konfigurace z jednoho grafického rozhraní.
* Rozšiřující moduly Kernun Clear Web, Antivirus, IDS/IPS pro Kernun UTM cluster
* Rozšiřující modul Adaptive Traffic Routing
* Rozšíření o Kernun Business Intelligence
* Instalace a implementace.

### Detekce anomálií datového provozu - analýza datových toků systémem zpracování NetFlow

Posílení síťové bezpečnosti a komunikační bezpečnosti je požadováno na více úrovních, dvěma dílčími technickými opatřeními, které korespondují s příslušnými ustanoveními vyhlášky č. 316/2014 Sb., konkrétně dle § 22 Nástroj pro detekci kybernetických bezpečnostních událostí.

Jako další technické bezpečnostní opatření pro ochranu interní datové infrastruktury se požaduje využití řešení pro analýzu a detekci anomálií pomocí monitorování sítí na bázi datových toků (NetFlow/IPFIX); takové řešení musí být schopné provádět diagnostiku výkonnostních problémů datové infrastruktury, provádět detekci pokročilých kybernetických hrozeb a následně provést eventuálně např. i zastavení DDoS útoků.

Tyto NetFlow systémy se sondami analyzují každý procházející paket a na základě těchto dat generují NetFlow statistiky. Tyto statistiky jsou exportovány, uloženy a připraveny pro vizualizaci a analýzu uživatelem. Při doplnění o s behaviorální analýzou datových toků (NBA) vzniká tak systém detekce anomálií a nežádoucího chování v datové síti, založený na permanentním vyhodnocování statistik o provozu na síti, který automatizovaně dokáže odhalovat bezpečnostní a provozní problémy, a zvýšit vnější i vnitřní bezpečnosti datové sítě. A také propojit tento systém do SIEM systému.

**Požadavky na nasazení:**

Implementace do interního prostředí organizace, které využívá centrální Cisco switch stack, je požadováno pomocí autonomní hardwarové sondy. Tato hardwarová netflow sonda bude připojena k centrálnímu Cisco switchi pomocí metalických vedení s kapacitou 4 × 1Gb Ethernet.

Další komponentou nebo funkcionalitou musí pak být systém, který bude provádět vlastní detekce anomálií a analýzy chování sítě (NBAD) síťovou infrastrukturou, klíčová je schopnost detekce cílených útoků nebo identifikace neznámého malware na síťové úrovni schopnost reakce na takové specifické hrozby reagovat. Funkcionalita na rozdíl od provozně – technického monitoringu např. na úrovni SNMP musí sledovat celkové chování zařízení v síti a identifikovat hrozby pro které neexistuje signatura stejně jako Heuristické analýzy antivirových systémů. Takto se doplní základní bezpečnostní opatření na bázi firewallů, IDS/IPS systémů a antivirových systémů.

Další požadovanou funkcionalitou je aplikace, která by monitorovala a analyzovala skutečný provoz mezi uživateli a aplikační infrastrukturou. Na základě pokročilé analýzy aplikačních protokolů a komunikace mezi aplikací a databázovými servery musí poskytovat přesné informace o skutečné výkonnosti aplikací v reálném čase.

**Požadované / pořizované položky řešení:**

* Nástroj na analýzu síťových toků (NetFlow HW)
* Systém detekce anomálií
* Systém monitorování aplikací
* Instalace
* Implementace
* Hardware appliance
* Integrace se SIEM.

### Implementace a zajištění centralizovaného sběru s vysokou dostupností a zpracování logovacích informací ze systémů – log management

Technické opatření § 21 vyhlášky č. 316/2014 Sb. – Nástroj pro zaznamenávání činností

Pro zajištění tohoto technického bezpečnostního opatření se požaduje implementovat centralizovaný Log management systém – Nástroj pro zaznamenávání činnosti, který bude centralizovat ukládání logů / záznamů ze všech určených prvků infrastruktury a systémů včetně archivace po určené doby. Systém je architekturně nezbytný pro bezvýpadkové nasazení systémů typu Security Information & Event Management.

Požaduje se Log Management jakožto komplexní systém pro práci s logy v originálním formátu/tvaru. Log Management musí zajišťovat příjem logů v jejich originální formě („RAW“), jejich bezpečné ukládání (šifrovaně, komprimovaně, s použitím TSA certifikačního razítka), rychlé vyhledávání a archivaci. Log Management není Event Management, jak je někdy prezentováno. Požadovaný Log Management musí být nezávislý technicky a procesně na SIEM řešení, tedy při nedostupnosti SIEMu se neztrácí logy (jak u většiny SIEM řešení, kde je Log Management jenom maličká část SIEMu, která zajišťuje archivaci přijatých logů), jeho výkon a parametry je možné škálovat bez ohledu na požadavky SIEMu (reálné výkonnostní požadavky na Log Management jsou 2x až 10× větší než na SIEM).

**Požadavky na nasazení:**

Požadavky na implementaci Log management systému do interního prostředí organizace vychází z oddělení Log management systému od případného SIEM systému. Pro vlastní Log management systém se požaduje využití samostatného / dedikovaného fyzického zařízení pro zpracování všech Logových informací. Celkové řešení Log Managementu je realizováno v zapojení pro High Availability. Požadavek na HA funkcionalitu vychází z požadavku zajistit v každém případě uložení a evidenci všech logů i případě kybernetického útoku nebo jiného selhání. Zajistí se tak možnost zpracování a analýza informací i následně např. i 3 stranou.

**Log Management System musí umožňovat napojení na tyto konkrétní typy zdrojů:**

* Modernizované firewall řešení Kernun
* Systém pro NetFlow – analýza interních síťových datových toků
* Microsoft Active Directory domain controlery všechny v infrastruktuře – min. 2x
* Napojení na Virtualizační infrastrukturu VMWare - v současném stavu 2× vCenter
* MS Exchange – email systém jako VIS
* Gordic IS systém jako VIS
* VEMA HR systém jako VIS
* Microsoft SQL server
* Plánovaný Provozně – technický monitoring
* Celkem včetně VISů a podpůrné infrastruktury 6× Windows server

### Implementace systému pro management bezpečnostních informací a událostí - SIEM

Jde o technické opatření podle Vyhlášky č. 316/2014 Sb. § 23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí je známý pod zaužívanou zkratkou SIEM systém (Security Information and Event Management) a provádí management bezpečnostních informací a událostí; je to analytický nástroj vytvářející závěry o bezpečnostní situaci v reálném čase, který musí velmi rychle analyzovat získaná log data o následcích s informacemi o možných příčinách. Aby SIEM plnil svoji úlohu, je nutné zajistit základní kontrolu a monitoring bezpečnosti dané infrastruktury, vhodné zdroje Log informací (popsaných viz výše). Samotný SIEM jenom identifikuje bezpečnostní události a incidenty na základě poskytnutých informací z bezpečnostní infrastruktury. Např. pokud bezpečnostní infrastruktura neobsahuje skener zranitelností, tak SIEM nedokáže rozlišit, jestli nálezy IDS/IPS jsou věrohodné nebo false positive. A proto řešení SIEM musí umožňovat formou volitelných komponent doplnit bezpečnostní infrastrukturu tak, aby při maximální efektivitě byl zajištěn sběr všech potřebných informací pro detekci bezpečnostní incidentů.

**Požadavky na nasazení:**

Přestože pro zadavatele, který je správcem významného informačního systému, není povinností nasadit technické opatření podle § 23 vyhlášky č. 316/2014 Sb. „Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“, požaduje se implementovat systém SIEM, protože je povinností zadavatele nějakým způsobem detekovat kybernetické bezpečnostní události a následně kybernetické bezpečnostní incidenty reportovat na vládní CERT.

Návrh implementace SIEM systému do interního prostředí organizace vychází z provedené implementace Log management systému, který bude zdrojovým systémem pro SIEM systém. Na rozdíl od Log management systému zde není požadavek na implementaci v High Availability módu. V případě odděleného Log Managementu a SIEM nástroje je možné zpětně vyhodnocovat logy, a proto není nutné budovat SIEM v HA módu.

### Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech

1. **PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech**

PIM/PAM je systém řízení privilegovaných účtů. Pojmem privilegovaný účet označuje pro tento účel účet v informačním systému, který má vysoké oprávnění, tj. účty typu root v Linux/UNIX systémech, účty typu Administrator ve Windows systémech, systémové účty používané aplikacemi nebo sdílené účty, které nejsou vázané na fyzickou osobu. S těmito účty pracují privilegovaní uživatelé. Pojem privilegovaný uživatel označuje fyzickou osobu, která používá privilegované účty. Jedná se o pracovníky provozu, dodavatele, nebo vývojáře. Cílový systém označuje systém, na který se privilegovaný uživatel připojuje prostřednictvím privilegovaných účtů.

PIM/PAM zaznamenává činnost systémového administrátora, který přistupuje k citlivým datům anebo provádí konfigurační činnost. Systém vytváří auditní stopu. Auditní záznamy mohou být přehrávány jako video, takže je možné sledovat události přesně tak, jak se ve skutečnosti odehrály.

**Požadavky na nasazení:**

Systém musí zajistit:

* centrální autentizace a řízení přístupu,
* detailní a exaktní monitorování zaměstnanců a partnerů,
* rychlejší a kvalitnější auditováni,
* vyšší odpovědnost IT personálu a jednoznačná odpovědnost,
* nižší náklady na detekci problémů a forenzní analýzy,
* zlepšení dodržování předpisů a regulatorních požadavků,
* zvýšená bezpečnost proti rizikům, vyplývajícím z lidského faktoru.

### Implementace Provozně – technického monitorovacího systému (pro zajištění Performance a Capacity Management) a vybudování druhého záložního místa datového centra – Business Continuity

Technické opatření § 26 vyhlášky č. 316/2014 Sb. – Nástroje pro zajištění vysoké úrovně dostupnosti.

Provozně – technický monitorovací systému nebo také dohledový systém musí provádět aktivní automatizovaný monitoring a dohled nad celou ICT infrastrukturou organizace včetně síťové infrastruktury, provozních parametrů serverové infrastruktury, ale také vlastních aplikací a příslušných služeb v aplikacích.

Dohledový systém na základě definovaných pravidel musí identifikovat vzniklý technický problém a okamžitě zahájit eskalační proces řešení problému, např. odeslat upozornění na předdefinované kontakty pomocí stanoveného kanálu (email, SMS apod.). Dohledový systém má fungovat tak, že monitorovací služba periodicky kontroluje specifikované koncové uzly, běžící aplikace a služby. K tomu využívá tzv. agenty, pomocí kterých je výsledek kontroly odesílán do dohledového systému, nicméně existují také monitorovací služby, které nevyužívají vlastní agenty a používají k monitorování standardizované nástroje a protokoly, jako je např. protokol SNMP. Dohledový systém povede Aktuální stav historie záznamů jednotlivých kontrolovaných systémů a na základě historických a aktuálních záznamů z monitoringu bude zobrazovat trendy, se kterými je možné také pracovat v eskalačních procesech. Záložní místo datového centra (tj. záložní serverovnu) požaduje zadavatel vybudovat v přízemí v místnosti č. 003.1, viz příloha A schéma 1. Rozvody slaboproudu PZTS, EKV – přízemí v „SLB\_KVOP\_PRIZEMI.pdf“.

**Požadavky na nasazení:**

Požadavky na implementaci Provozně – technického monitorovacího systému do interního prostředí organizace vycházejí z aktuálního stavu ICT infrastruktury. Stávající stav infrastruktury je popsán v kap. 1.

Z technického pohledu je nezbytné instalovat Provozně – technický monitorovací systém do virtuálního prostředí VMWare, které bude zaručovat vlastními prostředky nezbytnou dostupnost. Eskalační procesy budou nastaveny, aby interní IT pracovníci byli vždy informování a mohli okamžitě problém začít řešit. Jedná se o přibližný celkový počet 60 monitorovaných hostů (serverů a dalších zařízení) a na nich běžících služeb, které mají být monitorovány.

#### Virtualizační server

Požaduje se server pro montáž do datového rozvaděče s velikostí maximálně 2RU, jehož součástí budou výsuvné ližiny, sklopné rameno pro uchycení kabeláže a přední bezpečnostní uzamykatelný kryt. Server musí být osazen dvěma procesory, každý s minimálně 8 jádry s podporou HyperThreadingu a pamětí L3 cache velikosti 20MB. Výkon pro obě CPU dle PassMark – CPU Mark musí být minimálně 16500 bodů. Server musí dále disponovat minimálně 24 DIMM sloty pro paměti DDR4 2400MHz a musí být osazen pamětí velikosti minimálně 128GB typu DDR4 2400při využití modulů o minimální kapacitě 32GB.

Šasi serveru musí obsahovat minimálně 3 PCIe 3.0 sloty z čehož minimálně 2 sloty budou volné, a musí být vybaveno minimálně 3 porty USB 3.0, přičemž minimálně jeden musí být přístupný z přední strany serveru.

Do serveru musí být z přední strany umožněno osazení minimálně 12 pevných disků, server musí být dodán minimálně se 4 disky velikosti 4 TB s rychlostí 7200 otáček připojenými rozhraním SAS 12Gb k samostatnému dvouportovému řadiči RAID. Tento RAID řadič se zálohovanou pamětí Cache velikosti minimálně 2GB nesmí zabírat volný PCIe slot a musí umožňovat hardwarový RAID v režimech 0, 1, 0+1, 5, 6, 5+0, 6+0.

Start systému virtualizačního hypervisoru musí být umožněn prostřednictvím integrovaných a redundantních flash pamětí velikosti minimálně 8GB.

Server musí být dále vybaven dvěma redundantními hotswap napájecími zdroji výkonu minimálně 750W a redundantními, za provozu vyměnitelnými ventilátory.

Pro konektivitu do sítě LAN musí být k dispozici minimálně 8 portů 1 Gbps ethernetu s rozhraním RJ45.

Pro management serveru musí být k dispozici dedikovaný LAN RJ-45 port, umožňující zabezpečený přístup přes síť – webovým prohlížečem i přes SSH. Management bude zpracovávat nezávislý procesor, který musí pracovat i při nenabootovaném operačním systému serveru. Tento integrovaný nezávislý procesor pro vzdálenou správu umožní vzdálené vypínání a zapínání serveru, plně integrovanou grafickou konzoli s možností sdílení více uživateli současně, připojení virtuálních médií (FDD, DVD, ISO i jejich image), podporu standartu SNMP/ SSL/ SSH/ IPMI. Management serveru musí umět odesílat hlášení o stavu HW na definovaný email bez nutnosti instalace agentů do OS.

Součástí serveru musí být z důvodu kompatibility se stávajícím prostředím dodána licence hypervisoru VMware vSphere Enterprise Plus pro 2 CPU.

LAN síť bude na páteři propojena redundantními optickými kabely na 1Gb centrální switch se 3 patrovými switchi v místnostech rozvaděčů.

Stávající prostředí v hlavní serverovně je tvořeno dvěma blade servery HP ProLiant BL460c Gen8 a HP ProLiant BL460c Gen9 v blade šasi HP C7000. Toto chassis je připojeno do datové sítě prostřednictvím switchů HP 6125G Blade switch, prostřednictvím SAN switchů Brocade jsou připojeny FC disková pole 3PAR Storeserv 7200c a HP MSA 2040. Nad těmito servery je provozována virtualizace VMware, nad níž běží provozní virtuální servery.

Do záložní serverovny požadujeme dodávku jednoho fyzického serveru pro virtualizační platformu. Nový server musí být schopen plnit funkci dalšího ESX serveru ve virtuálním prostředí VMware vSphere 5.5 jako součást clusteru, tvořeného chassis HP C7000 se stávajícími dvěma blade servery (HP ProLiant BL460c Gen8 a HP ProLiant BL460c Gen9) + disková pole. Disky v novém ESX serveru musí být ve VMware clusteru viditelné/použitelné libovolným z ESX serverů tak, aby se libovolný virtuální server mohl za provozu migrovat na libovolný ze zbývajících dvou esx serverů. Zároveň požadujeme řešení redundance uložených dat mezi hlavní serverovnou a záložní serverovnou prostřednictvím virtuálního diskového pole tak, aby se libovolný virtuální server mohl za provozu migrovat na libovolný ze zbývajících dvou esx serverů.

Pro realizaci požadujeme změnu připojení blade šasi do datové sítě na rychlost 10 Gbps, součástí dodávky musí být i příslušné redundantní switche v obou lokalitách, které budou tvořit jeden virtuální přepínač. Do těchto switchů bude v obou lokalitách, hlavní serverovně a záložní serverovně, připojena konektivita z patrových rozvaděčů s přístupovými aktivními prvky. Součástí dodávky bude realizace redundantních optických tras mezi patrovými rozvaděči a záložní serverovnou, stejně jako posílení optického propoje mezi hlavní serverovnou a záložní serverovnou.

**Požadované / pořizované položky řešení:**

* SW monitorovací systém
* instalace
* implementace
* HW server
* SW server
* rozvody, optický kabel.

### Implementace systému testování zranitelností – Vulnerability Management

Technické opatření dle § 24 vyhlášky č. 316/2014 Sb. – Aplikační bezpečnost

Pro naplnění tohoto technického bezpečnostního opatření bude dodavatelem vytvořena interní metodika pro pravidelné testování zranitelností aplikací a infrastruktury. Metodika musí popisovat postup pro pravidelné testování zranitelností aplikací a infrastruktury a musí také stanovit rámec pro jeho vyhodnocování a pro návazný proces zlepšování úrovně zabezpečení.

Dále budou provedeny testy zranitelnosti a penetrační testy, včetně odborného vyhodnocení a návrhu opatření k ošetření zjištěných zranitelností a problémů, které v tomto případě je nezbytné a není možné ho provést interními kapacitami.

Nejdříve je nezbytné provést iniciační testy zranitelnosti, ke zjištění základní úrovně. Tímto krokem, tj. provedením iniciačních testů zranitelností, se vytvoří i základní informační báze pro pozdější testování a srovnání.

Dále bude dodán nástroj pro pravidelné testování zranitelností (tzv. vulnerability scanner), který bude provozován u zadavatele. S využitím tohoto nástroje budou realizovány pravidelné testy zranitelností s cílem zajistit dlouhodobou odolnost vůči vnějším i vnitřním hrozbám.

Toto technické opatření bude provedeno následně po provedení modernizace firewallu na síťovém perimetru, aby byla provedena nezávislá kontrola implementace řešení firewallu s případnými odhaleními bezpečnostních problémů

**Pořizované položky řešení:**

* Penetrační testy a testy zranitelnosti
* Metodika pro realizaci testů zranitelností
* Nástroj pro testování zranitelností.

Předmětem plnění je komplexní dodávka služby Testování souboru opatření – penetračních testů infrastruktury a aplikací zadavatele.

**Cíle nového řešení:**

Testování souboru opatření – penetrační testy infrastruktury a aplikací organizace nesleduje jen splnění požadavků na ni kladených ze zákona, ale také současně kontrolu vybraných opatření v dynamicky se vyvíjející problematice Kybernetické bezpečnosti, která zasahuje všechny oblasti, kde zadavatel pohybuje.

**Představy cílového řešení:**

Testování aplikací a systému, jež je zadavateli uloženo platnou legislativou, představuje nezbytnou složku měření účinnosti aplikovaných opatření, které dále rozvíjí o oblast KB přiměřeně aktuálním potřebám organizace a způsobu zajištění prvků kritické infrastruktury, jež reprezentuje. Zadavatel počítá v první řadě s penetračním testováním uvedených infrastruktur a aplikací na úrovni externích penetračních testů a testů perimetru organizace, jehož rozsah je dále příslušně specifikován.

#### Rámcové požadavky

**Obecné požadavky na způsob provedení:**

Poskytovatel provede službu dle této zakázky jako projekt s příslušnou částí projektového řízení a kontroly kvality, řízení rizik projektu a dalších obvyklých náležitostí projektového postupu dle mezinárodně platných a standardů projektového řízení. V intencích tohoto ustanovení ustaví společně s delegovanými pracovníky Objednatele – vizte dále oddíl Součinnost – příslušné struktury projektového řízení a organizace, v jejichž gesci projekt příslušným způsobem provede.

**Obecné požadavky na testování:**

Všechny testy musí obsahovat testy přístupové a provozní infrastruktury, která je potřebná, očekávaná nebo obvyklá pro provozování daného typu aplikace.

Pro testování infrastruktury uchazeč užije přiměřeně postupy uvozené v metodických rámcích OWASP, OSSTMM.

**Externí penetrační testy perimetru:**

Musí být otestováno celkem asi 30 IP adres a to formou běžného anonymního uživatele (black box

test).

Testy musí být nedestruktivního charakteru. V průběhu testování musí být využity automatizované a manuální testovací postupy. Úkolem je ověřit nejenom možnosti exploatace známých zranitelností, ale i odolnost vůči průniku simulací činností útočníka, který se například bude snažit ověřit administrátorské chyby v konfiguracích – designu apod., které se mohou vyskytovat na systémech/službách využívaných zadavatelem, kterými jsou zejména (ne však výlučně):

* operační systémy
* webové servery
* aplikační servery
* databázové servery
* mail servery
* firewally
* routery
* systémová rozhraní
* další publikované síťové služby.

**Penetrační testy webových aplikací:**

Tyto testy budou probíhat na testovacích aplikacích, pokud by hrozilo jejich omezení provozu nebo výpadek. Testy budou opět z pohledu anonymního útočníka, tak i z pohledu legitimního uživatele v případě testování částí aplikací, které vyžadují autentizaci uživatele. V průběhu testování musí být využity automatizované a manuální testovací postupy. Testy musí být v souladu s metodikou OWASP, tedy musí prověřit odolnost vůči následujícím (ne však výlučně) technikám útoků:

* Injections (SQL, XML, HTML atd.)
* Broken Authentication and Session Managementů
* Cross-site scripting
* Cross-Site Request Forgery
* Insecure Direct Object References
* Security Misconfiguration
* Sensitive Data Exposure
* Missing Function Level Access Control
* Using Components with Known Vulnerabilities
* Unvalidated Redirects and Forwards

Jedná se o cca 3 webové aplikace.

**Penetrační testy základního interního perimetru:**

Anonymní uživatel provede pokus o průnik do interní sítě nebo z vybrané ethernetové zásuvky pro ni určené a ověří zranitelnosti firemní wifi, popř. se pokusí o průnik do interních serverů

Tento test bude proveden v sídle zadavatele.

#### Všechny varianty testů - požadované výstupy

Výstupem penetračního testu prostředků a služeb objednatele bude výsledná zpráva, která bude popisovat postup prověrky a nalezené zranitelnosti, včetně jejich kategorizace a podrobného popisu s doporučenými opatřeními pro jejich odstranění nebo zmírnění následků zneužití, zachycující:

* veškeré vstupní informace testu
* testovací žurnál
* identifikaci testovacích nástrojů a jejich konfiguraci při testu
* úplný výpis výsledků
* postup a závěr hodnocení
* manažerské shrnutí testu.

**Zpráva o provedeném testu:**

Zhotovitel o provedeném testu vypracuje zprávu v souladu se shora uvedenými metodickými rámci, zachycující nejméně:

* manažerské shrnutí – název aplikace, přehled hlavních zjištění a doporučení
* shrnutí známých informací o testované aplikaci a prostředí, s jasným oddělením toho, které informace byly předány zadavatelem před zahájením testu a které informace byly získány z testování a jsou tedy dostupné potenciálnímu útočníkovi
* přehledný seznam identifikovaných zranitelností, seřazený sestupně podle jejich závažnosti a jejich popis
* výčet všech pokusů dodavatele o průnik a výsledek takového průniku. U dobře známých a jednoduše prokazatelných zranitelností bude uveden i postup zneužití dané zranitelnosti (např. odkazem na www stránky s postupem)
* doporučený postup předcházení uvedeným zranitelnostem, pokud takový existuje, případně popis vhodných alternativních protiopatření.

**Přílohy k výstupní zprávě o provedeném testu:**

* Seznam použitých nástrojů vč. verze nástroje a příp. verze databáze testovacích vzorků
* Termíny skenů (od, do) + použitý nástroj a orientační konfigurace nastavení těchto nástrojů,
* Protokoly o testech z jednotlivých nástrojů
* Veškerá projektová dokumentace k provedeným testům
* Výstup testu bude samostatně prezentovatelným celkem s úplnou informační strukturou zachycující stav testovaného cíle v okamžiku provedení testu a popis podmínek pro opakování testu metodou úplné rekonstrukce.

**Výstupy budou provedeny ve formě:**

* Shora uvedené dokumentace ve formě samostatného dokumentu nebo do této formy upraveného výstupu projektového systému zhotovitele nebo objednatele.
* Samostatného dokumentu zprávy o provedeném testu a jeho výsledcích
* Workshopu s pracovníky objednatele k provedenému testu v rozsah min. 1×2hod k prezentaci a projednání závěrů zprávy

#### Součinnost zadavatele

Zadavatel předpokládá určení kontaktní osoby, která bude průběžně informována o zahájení, průběhu a ukončení jednotlivých částí testů, event. o některých specifických okolnostech průběhu testů, jež je na místě referovat bezodkladně a dále delegování pracovníků k účasti na workshopech k výsledkům testů.

Kromě toho zadavatel poskytne:

* Pro testy aplikací předá:
  + URL nebo IP adresu aplikace,
  + přístupové údaje pro minimálně dva platné účty v testované aplikaci, případně další náležitosti nutné k autentizaci vůči testované aplikaci (např. certifikáty),
  + informace o způsobu autentizace vůči testované aplikaci.
* Pro externí testy infrastruktury:
  + předá IP adresní rozsah, který má být testován,
  + v případě zablokování IP adres, ze kterých je testováno provede jejich odblokaci a sdělí testerovi, z jakého důvodu byly IP adresy zablokovány
* Pro interní testy infrastruktury předá, poskytne:
  + základní informace o vnitřní síti,
  + přístup do prostor zadavatele a možnost připojit zařízení testera do sítě,
  + údaje pro autentizaci vůči AD (pokud je to pro daný test nutné),
* Pro všechny typy testů předá:
  + informace o čase, kdy je možné testovat,
* V odůvodněných případech poskytne také:
  + možnost zřízení emailového účtu.

Doba trvání shora uvedené součinnosti se předpokládá po celou dobu plnění zakázky.

### Zvýšení fyzické bezpečnosti serveroven

Technické opatření dle § 16 vyhlášky č. 316/2014 Sb. – Fyzická bezpečnost

Zadavatel již vlastní a provozuje poměrně rozsáhlý (ve srovnání s předmětem plnění) systém PZTS, EKV a CCTV. Předmětem plnění je jeho rozšíření, ovšemže tak, aby nová část byla zcela slučitelná s částí již provozovanou a aby nevzniklo nové dozorové pracoviště, které by vyžadovalo další personál obsluhy. Naopak, dodáno musí být zařízení, které není samostatným systémem, nýbrž kterým se rozšíří systémy stávající; nejvhodnější bude zařízení stejných typů, jaké zadavatel již má.

Kromě toho má zadavatel ke stávajícímu zařízení uzavřenou smlouvu na servis do 30.6.2018.

Specifickým charakterem této části předmětu veřejné zakázky je odůvodněno použití odkazu na určité dodavatele nebo výrobky, jak připouští ustanovení § 89 odst. 5 písm. a) zákona. Zadavatel z tohoto důvodu poskytuje jako součást zadávacích podmínek výkaz výměr z projektové dokumentace zadávaného rozšíření a předpokládá, že dodavatelé budou soutěžit o dodávku a instalaci zařízení podle výkazu výměr. Zadavatel nicméně v souladu s ustanovením § 89 odst. 6 zákona umožňuje nabídnout rovnocenné řešení založené i na jiné technologii, pokud řešení beze zbytku naplní věcné požadavky uvedené v zadávací dokumentaci a bude na stávající systém navazovat mechanicky (rozměrově), elektricky (signálově) i funkčně (včetně jednotné obsluhy).

#### Popis a řešení PZTS, EKV

Poplachový zabezpečovací a tísňový systém (PZTS) je soubor technických prostředků - ústředny, čidla, signalizační a doplňkové prostředky vytvářející systém, který slouží k včasné signalizaci místa narušení chráněného objektu. Tento systém umožňuje předání poplachové informace na zvolená místa, čímž usnadní činnost zásahové služby. Navazuje na klasickou a režimovou ochranu objektu, doplňuje ji a zkvalitňuje celkové zabezpečení.

Plněním veřejné zakázky je zvýšení bezpečnosti serveroven instalací systému kontroly vstupu prostřednictvím bezkontaktních čteček karet a elektromechanických zámků. Stávající systém PZTS bude rozšířen o řídící jednotky pro přístupový systém, který bude zapojen na stávající sběrnici. K řídícím jednotkám budou připojeny čtečky bezkontaktních karet a elektromechanické zámky. Řídící modul k přístupovému systému bude použit MAXM2000. Pro snímání teploty racků budou využity digitální detektory překročení teploty připojené ke stávajícím nebo nově instalovaným expanderům PZTS.

Pro zvýšení bezpečnosti m.č. 003.1 bude k nově instalovanému expanderu přidán PIR detektor. Čelní sádrokartonová zeď v této místnosti bude vyztužena 1-1.5mm plechem ukotveným na stávající SDK zeď (viz. výkres č. SLB/001).

V prvním patře místnosti č.148 budou na stoly instalovány dvě tlačítka pro ovládání zámků vstupních dveří v m.č.146 (Z5.1). Tato tlačítka budou připojena na vstupy řídící jednotky ŘJ4. Na vstup ŘJ4 bude taktéž připojeno stávající tlačítko z recepce, kterým lze vzdáleně ovládat zámek dveří do m.č.158 (Z5.2). Vedle čtečky ČT5.2 bude nově instalován bezdrátový zvonek-vysílač, který bude zvonit na recepci-přijímač.

V objektu bude provedena instalace prvků s platným certifikátem odpovídající stupni zabezpečení objektu.

Pro nově instalované prvky bude do místnosti č.154 instalován nový zdroj, který bude pomocí sběrnice připojen do stávajícího systému PZTS. U tohoto zdroje budou monitorovány stavy porucha a porucha akumulátoru.

Z nově instalovaného zdroje 12V/5A s akumulátorem 37 Ah budou napájeny zvlášť řídící jednotky a elektromechanické zámky.

#### Popis a řešení CCTV

V objektu je instalován stávající systém CCTV. Na stávající NVR je připojeno 13 stávajících kamer přes PoE switch. Na tomto switchi jsou volné pozice, na které budou připojeny dvě nové IP box kamery. NVR společně s PoE switchem jsou umístěny ve stávajícím Racku v místnosti č.154.

Nové kamery budou současně s nově instalovaným přístupovým systémem sloužit ke zvýšení zabezpečení vchodů do serveroven.

#### Podrobný popis požadovaného řešení PZTS, EKV a CCTV

Zadavatel požaduje rozšíření stávajícího zabezpečovacího systému o detekci teploty racků a instalaci přístupového systému do místností serveroven. Současně se bude rozšiřovat stávající kamerový systém o nové kamery.

##### Předpisy a normy

Dílo bude zpracováno dle platných norem ČSN EN 50131-1, ČSN EN 50 131.1-Z1, ČSN 34 2300, ČSN 33 2000 - 4 – 41, ČSN EN 50132-1, ČSN EN 50133-1 a souvisejících předpisů.

##### Základní technické údaje

**Napěťové soustavy:**

ústředna PZTS a posilový zdroj: TN-S 230 V, 50 Hz, L+PE+N

rozvody PZTS: bezpečným napětím 12 Vdc

rozvody CCTV: bezpečné napětí PoE

**Ochrana před nebezpečným dotykem:**

Ochrana před nebezpečným dotykovým napětím bude u neživých částí provedena v souladu s normou ČSN 33 2000 – 4 – 41 ed.2 čl. 413.1 a s normami k této normě příslušejícími.

Ochrana před nebezpečným dotykem živých částí bude provedena krytím vyhovujícím ČSN 33 2000 – 4 – 41 ed.2, čl. 412.2.2 (Ochrana kryty).

Ochranná svorka musí mít odpor vodivého spojení se všemi kovovými částmi přístupnými dotyku maximálně 0,1 ohmů.

**Prostředí dle ČSN:**

Prostředí dle ČSN 33 2000-5-51 ed. 3 v jednotlivých prostorách objektu.

##### Popis a řešení PZTS, EKV

Poplachový zabezpečovací a tísňový systém je soubor technických prostředků - ústředny, čidla, signalizační a doplňkové prostředky vytvářející systém, který slouží k včasné signalizaci místa narušení chráněného objektu. Tento systém umožňuje předání poplachové informace na zvolená místa, čímž usnadní činnost zásahové služby. Navazuje na klasickou a režimovou ochranu objektu, doplňuje ji a zkvalitňuje celkové zabezpečení.

Požadavkem investora je zvýšení bezpečnosti serveroven instalací systému kontroly vstupu prostřednictvím bezkontaktních čteček karet a elektromechanických zámků. Stávající systém PZTS bude rozšířen o řídící jednotky pro přístupový systém, který bude zapojen na stávající sběrnici. K řídícím jednotkám budou připojeny čtečky bezkontaktních karet a elektromechanické zámky. Řídící modul k přístupovému systému bude použit MAXM2000. Pro snímání teploty racků budou využity digitální detektory překročení teploty připojené ke stávajícím nebo nově instalovaným expanderům PZTS.

Pro zvýšení bezpečnosti m.č. 003.1 bude k nově instalovanému expanderu přidán PIR detektor. Čelní sádrokartonová zeď v této mísnosti bude vyztužena 1-1.5mm plechem ukotveným na stávající SDK zeď (viz. výkres č. SLB/001).

V prvním patře místnosti č.148 budou na stoly instalovány dvě tlačítka pro ovládání zámků vstupních dveří v m.č.146 (Z5.1). Tato tlačítka budou připojena na vstupy řídící jednotky ŘJ4. Na vstup ŘJ4 bude taktéž připojeno stávající tlačítko z recepce, kterým lze vzdáleně ovládat zámek dveří do m.č.158 (Z5.2). Vedle čtečky ČT5.2 bude nově instalován bezdrátový zvonek-vysílač, který bude zvonit na recepci-přijímač.

V objektu bude provedena instalace prvků s platným certifikátem odpovídající stupni zabezpečení objektu.

Pro nově instalované prvky bude do místnosti č.154 instalován nový zdroj, který bude pomocí sběrnice připojen do stávajícího systému PZTS. U tohoto zdroje budou monitorovány stavy porucha a porucha akumulátoru.

Z nově instalovaného zdroje 12V/5A s akumulátorem 37Ah budou napájeny zvlášť řídící jednotky a elektromechanické zámky. Přesné zapojení je součástí blokového schématu (viz. výkres SLB/005).

##### Popis a řešení CCTV

V objektu je instalován stávající systém CCTV. Na stávající NVR je připojeno 13 stávajících kamer přes PoE switch. Na tomto switchi jsou volné pozice, na které budou připojeny dvě nové IP box kamery. NVR společně s PoE switchem jsou umístěny ve stávajícím Racku v místnosti č.154.

Nové kamery budou současně s nově instalovaným přístupovým systémem sloužit ke zvýšení zabezpečení vchodů do serveroven.

##### Signalizace poplachu

Signalizace poplachu zůstavá stávající a beze změn.

##### Napájení a zálohování systému

Ústředna PZTS a posilové zdroje jsou napájeny ze sítě 230V/50Hz z rozvaděče 2RS1 typ RE G72P, výr. č. 19/01. Rozvaděč 2RS1 typ RE G72P, výr. č. 19/01 je umístěný v místnosti velínu (technické místnosti) č. 154 v 1. patře hlavní budovy.

Přívodní vedení k ústředně PZTS a posilovým zdrojům, CYKY 3Cx1,5 mm², vedené v PVC žlabech je jištěno jističem LSN B 6A, pozice 13,

Ústředna a posilové zdroje jsou umístěny v místnosti velínu (technické místnosti) č. 228 v 1. patře budovy. Jsou instalovány v kovových skříních a spojené s ochranným vodičem.

Nově instalovaný posilový zdroj bude napájen ze sítě 230V/50Hz, kabelem CYKY 3Cx1,5 mm² se samostatnými ochrannými vodiči, viz požadavek profese silnoproud.

##### Kabelové rozvody

Vedení bude provedeno dle odpovídajících ČSN a předpisů. Propojovací vedení bude měděné. Budou dodrženy zásady o úpravě rozvodných skříní, označování svorkovnic, křižování a souběhu se silovým vedením dle ČSN 34 27 10.

**PZTS** - Veškeré prvky systému PZTS budou ke koncentrátorům připojeny kabely SYKFY 3x2x0,5. Na sběrnici bude použit kabel UTP 4x2x0,5mm.

**EKV** - Čtečky karet budou připojeny k řídící jednotce pomocí kabelu SYKFY 5x2x0,5. Napájení řídících jednotek a elektromechanických zámků bude provedeno kabely J-Y(st)Y 2x2x0,8 (řídící jednotky) + CYSY 2x2,5 (elektromechanické zámky).

**CCTV** - Pro rozvody CCTV bude použit kabel taktéž kabel UTP 4x2x0,5.

Rozvody PZTS, CCTV budou uloženy s převážné většiny případů v podhledech v pevných trubkách a po stěnách v elektroinstalačních žlabech 17x17 či 40x20.

##### Montáž

Umístění jednotlivých prvků PZTS, CCTV bude koordinováno s umístěním silnoproudých a ostatních zařízení. Instalace celého zařízení bude provedeno dle norem ČSN EN 50131-1 ed.2, ČSN 33 2000-4-41, ČSN 34 23 00.

##### Upozornění

Během montáže musí být dodržovány bezpečnostní předpisy pro práci v objektu, zvláště bezpečnostní předpisy pro práci na elektrickém zařízení a při práci na žebřících.

##### Požární bezpečnost

Z hlediska požární bezpečnosti musí být veškeré prostupy (sloužící pro vedení kabeláže) mezi různými požárními úseky zabezpečeny dokonalým požárním utěsněním. Zadavatel požaduje protipožární odolnosti přepážek (ucpávek) a na možnost jejich dodatečné rozebíratelnosti.

##### Uvedení do provozu a provoz zařízení PZTS

Bude provedena výchozí revize a zkušební provoz před uvedením zařízení PZTS do trvalého provozu.

Při předávání díla do provozu požadujeme zpracovat pokyny pro osoby opouštějící objekt poslední (příp. jeho samostatně ovládané části), kontrolu uzavření oken, dveří. Rovněž požadujeme zpracovat směrnici o činnosti v případě vyhlášení poplachu, zvláště způsob součinnosti zaměstnanců se zásahovou jednotkou.

V rámci místních předpisů budovy bude určena:

- osoba zodpovědná za provoz systému

- osoby pověřené obsluhou a prokazatelně proškolené

Osoby pověřené obsluhou zařízení PZTS

- požadujeme proškolení dodavatelem

##### Požadavky na profese

Pro nový napájecí zdroj PZTS zadavatel zajistí samostatný přívod 230V, jištění 6A do m.č.154

##### Schémata rozvodů slaboproudu

Schémata rozvodů slaboproudu jsou uvedeny v příloze A.

##### Soupiska materiálu

Tabulka 2: 2.2.8.3.13. Soupiska materiálu

|  |  |  |
| --- | --- | --- |
| **Dodávka PZTS - Zařízení** |  |  |
| **Popis položky** | **Počet** | **MJ** |
| Koncentrátor v kovovém krytu pro 8 zón a 4 PGM výstupy | 2 | ks |
| Duální prostorový detektor | 1 | ks |
| Digitální detektor překročení teploty 0 - 60°C se dvěma výstupy | 5 | ks |
| Bezdrátový zvonek, 6 tónů, dosah 150m | 1 | ks |
| Plastové odchodové tlačítko s NO kontaktem | 2 | ks |
| Řídící modul v kovovém krytu pro připojení dvou bezkontaktních čteček | 5 | ks |
| Čtečka EM / HID Prox karet, úzké provedení | 6 | ks |
| Elektromechanický samozamykací panikový zámek,vč bezp.kování,protiplech,průchodka,propojovací kabel | 6 | ks |
| Spínaný zdroj v kovovém krytu 13,8 Vss / 5A s výstupy a odpojovačem | 1 | ks |
| AKU 12V/38Ah se šroubovými svorkami M6 a životností až 10 let, VdS | 1 | ks |
|  |  |  |
| **Dodávka PZTS - Instalační materiál** |  |  |
| Kabel SYKFY 3x2x0.5mm | 90 | m |
| Kabel SYKFY 5x2x0.5mm | 45 | m |
| Kabel UTP cat.5e, lanko, PVC | 85 | m |
| Kabel J-Y(St)Y 2x2x0,8 | 155 | m |
| Kabel H05VV-F 2x2.5mm2 | 125 | m |
| Trubka pevná pr.20/17,4mm, šedá | 90 | m |
| Příchytky - klipy, světle šedé 20mm | 105 | ks |
| Trubka pevná pr.25/22,1mm, šedá | 85 | m |
| Příchytky - klipy, světle šedé 25mm | 85 | ks |
| Ochranná hadice FX 20 šedá, PVC | 25 | m |
| Lišta 17x17mm, bílá | 75 | m |
| Lišta 40x20mm, bílá | 30 | m |
| Plastová nízká propojovací krabice, 24+1 šroubovací svorka | 6 | ks |
|  |  |  |
| **Dodávka CCTV - Zařízení** |  |  |
| IP box kamera, TD/N, HD 1080p, 2MP, WDR 140dB, Light fighter | 2 | ks |
| Objektiv AI pro full HD 1080p kamery (až 3MP), 1/3", f=2.8÷8mm, IR | 2 | ks |
| Krátká konzole pro upevnění kamery na zeď | 2 | ks |
|  |  |  |
| **Dodávka CCTV - Instalační materiál** |  |  |
| Kabel UTP cat.5e, lanko, PVC | 80 | m |
| Trubka pevná pr.20/17,4mm, šedá | 80 | m |
| Ochranná hadice FX 20 šedá, PVC | 25 | m |
| Příchytky - klipy, světle šedé 20mm | 105 | ks |
| Lišta 17x17mm, bílá | 10 | m |
| Konektor RJ45 8pinů, nestíněný - drát | 4 | ks |
| Patch kabel 2m UTP, CAT5E, | 2 | ks |
| Drobný instalační materiál | 1 | ks |

# Specifikace minimálních požadavků řešení

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované minimální požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění minimálních požadavků ve sloupci **„Účastníkem nabízená hodnota“**, tak že tam nakopíruje text ze sloupce „Specifikace minimálních požadavků“, případně doplní nebo upraví popis nabízené hodnoty, ze kterých bude patrné, že splňuje minimální požadavky.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

## Perimetr datových sítí s architekturou vysoké dostupností – modernizace firewallu

Tabulka 3: HW appliance firewallu kompatibilní se stávajícím zařízení Kernun UTM model 200 a zapojený do v Active/Passive Clusteru

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | HW appliance – ucelená jednotka v RACK provedení |  |  |
|  | All-in-one HW+OS+SW |  |  |
|  | Rozhraní minimálně 8 x 1 Gbps Ethertnet, 1 x remote console, podpora agregace a redundance interface |  |  |
|  | Propustnost IP inspekce min. 1Gbps per port |  |  |
|  | Propustnost proxy inspekce min. 500 Mbps per port |  |  |
|  | Propustnost šifrování min. 250 Mbps per port |  |  |
|  | FW řešení podporující technologii stavového paketového filteru i aplikačních proxy bran firewallu tj. spojení je terminováno na FW |  |  |
|  | Podpora NAT / PAT |  |  |
|  | Možnost řízení komunikace volitelně na sítových vrstvách L3 až L7 |  |  |
|  | Možnost řízení komunikace na úrovni jednotlivých aplikačních příkazů (aplikační proxy) a to pro protokoly: HTTP, SMTP, POP3, IMAP4, DNS, FTP, SIP, h.323, SQLNet |  |  |
|  | Integrovaná VPN brána - podpora VPN (IPsec, OpenVPN) |  |  |
|  | Podpora VLAN |  |  |
|  | Podpora IPv6 |  |  |
|  | Podpora ICAP rozhraní |  |  |
|  | Podpora SNMP |  |  |
|  | Synchronizace času pomocí NTP |  |  |
|  | QoS – řízení šířky pásma podle uživatele, portu i typu souboru |  |  |
|  | Podpora autentizace (Kerberos, NTLM, LDAP, RADIUS) |  |  |
|  | Podpora Integrace s Microsoft Active Directory včetně řízení dle skupin uživatelů a podpory SSO tj. transparentní autentizace bez nutnosti ověřování mezi klientem a firewallem. |  |  |
|  | Výjimky z autentizace dle zdrojové nebo cílové IP adresy, nebo user agenta |  |  |
|  | Podpora automatické detekce proxy WPAD |  |  |
|  | Možnost ukončení TLS / SSL komunikace na FW s prováděním všech kontrol v šifrovaném provozu a to jak v provozu na server i klienta včetně rozšifrování a zašifrování spojení – https inspekce |  |  |
|  | Výjimky z HTTPS inspekce na vybrané IP adresy, servery nebo kategorie |  |  |
|  | Rozpoznávání a kontrola skutečných typů souborů v rámci HTTP komunikace (MIME Type) – nikoliv na základě deklarace klienta či serveru |  |  |
|  | Filtrace HTML stránek a možnost odstranění spustitelného kódu z těchto stránek (zejména Java, JavaScript, ActiveX). |  |  |
|  | Možnost definice časové platnosti ACL pravidla, od-do |  |  |
|  | Podpora Syslog, možnost exportu logu, možnost vzdáleného logování |  |  |
|  | Podpora paralelní instalace více verzí firmware s možností okamžitého návratu k poslední verzi a libovolné přepínání |  |  |
|  | Logování s podporou více úrovní a možností úplného záznamu komunikace na úroveň dump IP komunikace. |  |  |
|  | HW appliance – ucelená jednotka v RACK provedení |  |  |

Tabulka 4: Rozšiřující moduly Kernun Clear Web, Antivirus, IDS/IPS pro Kernun UTM cluster

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Antivirová kontrola provozu pro HTTP, HTTPs, SMTP, POP3, IMAP4, FTP |  |  |
|  | IPS (Intrusion Prevention System) ochrana stanic a uživatelů, možnost definice vlastních IPS signatur |  |  |
|  | Podpora webfilteru a definice politik přístupu na web v režimu monitorování, povolení, zakázání či omezení provozu |  |  |
|  | Řízení a filtrování webového přístupu dle kategorizace obsahu webových stránek (realizovaný formou web proxy) |  |  |
|  | Webfiltr musí podporovat alespoň 60 kategorií www stránek a umožňovat řízení přístupu na webové stránky v režimech: |  |  |
|  | Stránka obsažena ve všech vyjmenovaných kategoriích |  |  |
|  | Stránka obsažena v alespoň jedné z vyjmenovaných kategorií |  |  |
|  | Možnost definovat ve webfiltru výjimky formou white / black listů a to i pro jednotlivé uživatele či skupiny samostatně |  |  |
|  | Možnost definovat ve webfiltru politiku přístupu dle času, kategorií, cílové URL, cílové IP adresy |  |  |
|  | Aktualizace databáze webfiltru o nezařazené domény z webového provozu organizace do druhého pracovního dne |  |  |
|  | Rozpoznání webového provozu řešením je vyžadována minimálně na úrovni 90 % pro typickou organizaci státní správy a samosprávy v ČR |  |  |
|  | Filtrace HTML, JavaScript/Java/ActiveX obsahu |  |  |
|  | Je požadováno, aby databáze pro kategorizaci byla přímo na dodaném zařízení a nebyla závislá na dostupnosti on-line služby |  |  |
|  | Možnost definovat samostatnou kategorii pro interní domény |  |  |

Tabulka 5: Rozšiřující modul Adaptive Traffic Routing

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Propustnost 40.000 DNS požadavků za sekundu |  |  |
|  | Podpora Global Server Load Balancingu s využitím DNS serveru (odpovědí s krátkým TTL |  |  |
|  | Podpora Load Balancer algoritmů Round Robin a Maximum Throughput |  |  |
|  | Podpora detekce nedostupnosti některého z cílových serverů a jeho automatické vyřazení z poolu cílových serverů |  |  |
|  | Podpora IPv4, IPv6, IPv4/IPv6, VLAN, SNMP, NTP |  |  |
|  | Podpora Syslog, možnost exportu logů, možnost vzdáleného logování- napojení na SIEM řešení |  |  |
|  | Podpora diagnostiky spojení s možností úplného záznamu IP komunikace |  |  |

Tabulka 6: Rozšíření o Kernun Business Intelligence

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Centrální sběr provozních záznamů z jednotlivých zařízení, zejména KERNUN UTM |  |  |
|  | Algoritmy strojového učení a umělé inteligence |  |  |
|  | Detekce anomálií a hlášení incidentů |  |  |
|  | Agregace dat pro rychlou odezvu |  |  |
|  | Efektivní filtrování dat a vyhodnocení dotazů |  |  |
|  | Analýza zobrazená v logických souvislostech |  |  |
|  | Dedikované úložiště zálohy záznamů |  |  |
|  | Z pozice potřeb administrátora musí řešení zabezpečovat:   * Centrální sběr a úložiště záznamů ze sledovaných zařízení * Detailní přehled o sítové komunikaci a stavu systému * Detekování bezpečnostních incidentů a anomálií v provozu * Bezpečný vzdálený přístup ke konfiguračním změnám a nastavením * Periodická tvorba reportů a zasílání zpráv odpovědným manažerům * Podpora integrace s ostatními zdroji sítových dat a záznamů řešení Kernun pro:   - Sítový provoz (TCP/ UDP)  - Webový provoz (HTTP / HTTPS)  - E-mail (SMTP)  - Virtuální privátní síť (VPN)  - Překlad doménových jmen (DNS)  - Telefonní hovory (SIP)  - Antivirová kontrola  - IDS / IPS. |  |  |

## Detekce anomálií datového provozu - analýza datových toků systémem zpracování NetFlow

Tabulka 7: Detekce anomálií datového provozu - analýza datových toků systémem zpracování NetFlow

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Systém pro analýzu datových toků bude schopen přijímat tato data a provádět nad nimi analýzu a detekci anomálií. |  |  |
|  | Systém musí být schopen pojmout NetFlow nebo IPFIX. |  |  |
|  | Detailní monitoring síťového provozu v reálném čase a umožnit získat přehled o síťové aktivitě v rámci specifikovaného časového období v minulosti. |  |  |
|  | Získat přesné informace o veškeré síťové aktivitě – např. kdo komunikoval s kým, kdy, kolik se přeneslo dat, pomocí které služby atd. |  |  |
|  | NetFlow statistiky exportovány, uloženy a připraveny pro vizualizaci a analýzu uživatelem |  |  |
|  | Zvýšit bezpečnost síťového provozu odhalením vnějších i vnitřních útoků. |  |  |
|  | Detekce anomálií a analýzy chování sítě (NBAD) síťovou infrastrukturou. |  |  |
|  | Schopnost detekce cílených útoků nebo identifikace neznámého malware na síťové úrovni schopnost reakce na takové specifické hrozby reagovat. |  |  |
|  | Identifikace hrozeb, pro které neexistuje signatura stejně jako Heuristické analýzy antivirových systémů. |  |  |
|  | Monitoring a analýza skutečného provozu mezi uživateli a aplikační infrastrukturou. |  |  |
|  | Integrace se SIEM |  |  |

## Implementace a zajištění centralizovaného sběru s vysokou dostupností a zpracování logovacích informací ze systémů – log management

Tabulka 8: Implementace a zajištění centralizovaného sběru a zpracování logovacích informací ze systémů

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Podpora vstupních protokolů (sources ~ zdrojů log záznamů) a **přenosu dat:**   * SNMP * **syslog**:   + UDP (dle RFC 3164)   + TCP   + IETF (RFC 5424) + TLS * **Aktivní sběr logů z databází (přes ODBC).** * Agent/Client pro sběr log záznamů jak pro prostředí Windows, tak i pro prostředí Linux/Unix (HP-UX, Solaris, …)/AIX:   + sběr Windows EVT záznamů i z kontejnerů Windows Server   + sběr AIX/Solaris/HP-UX/IRIX auditních OS záznamů   + **sběr textových logů ze souborů**   + přenos log dat (tj. forward přes syslog) šifrovaným kanálem * Podpora RELAY funkce (tj. přeposílací servery, např. pro infrastrukturu v DMZ) |  |  |
|  | **Podpora BUFFER/CACHE na výstupu** jak u Agenta, tak pro RELAY, a také pro Server/Appliance. |  |  |
|  | Podpora výstupních protokolů (destinations ~ umístění log záznamů):   * syslog (UDP, TCP, IETF) * **zápis logových dat napřímo do databází (ODBC)** * zápis logových dat do JSON formátu * SNMP Trap |  |  |
|  | **Možnost konfigurace pokročilého filtrování logových záznamů** (jakýkoli vstup logových dat prochází libovolnou sadou filtrů na libovolný výstup) |  |  |
|  | **Ukládání log dat:**   * **Textové úložiště v originálním (RAW) formátu** * **Šifrované úložiště (sklad logů) s podporou šifrování privátním klíčem/certifikátem a TSA podpisem, pro zajištění právních potřeb forenzního šetření** * **Podpora indexace logových dat pro rychlé vyhledávání údajů i v nestrukturovaných v datech (položka message u syslog protokolu)** * **Podpora komprimace jako součást daného úložiště** |  |  |
|  | **Řešení zajistí uživatelskou dostupnost na úrovni implementovaných prvku.** **Prezentace dat** musí být provedena i v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple MacOS, Apple iOS. |  |  |
|  | **Řízení přístupů** (AAA):   * řízení přístupu na úrovni jednotlivých úložišť (sklad logů) * podpora GROUP managementu * podpora autentizace přes RADIUS * Podpora lokální /externí databáze uživatelů – LDAP |  |  |
|  | **Zálohování, Archivace, Export, Sdílení log dat:**   * nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (sklady logů) * nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat * podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru |  |  |
|  | **Alerting:**   * RATE alerting (detekce změn „nestandardního chování zdrojů logových záznamů“ pro nastavené limitní hladiny datových přenosů v čase) * Výskyt definovaného slova/znaku v logu (Např. „error“, „fail“ nebo „alert“) * Artificial Ignorance – funkcionalita, která identifikuje, co je informačně nezajímavé a potlačuje eskalaci. Nebo identifikuje, co informačně systém Log managementu ještě nikdy neviděl a eskaluje anomálii. |  |  |
|  | **Řešení musí podporovat zapojení pro High Availability**, tj. vysoká dostupnost. |  |  |
|  | **Nezávislost na SIEM**   * **Řešení je koncipováno jako čistý Log Management, nejedná se tedy o Event Management – pro plnou funkci není potřeba tvorby parserů** * Řešení není provázáno na SIEM a je plně nezávislé jak fyzicky, tak logicky na SIEM řešeních. Nejedná se tedy o ALL-IN-ONE řešení, s konfigurací pro Log Management |  |  |
|  | **Vyhledávání a Reporting:**   * **Rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů), tedy velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích.** * **Umožnění vytváření vlastních analytických pohledů.** * Dashboardy/Statistiky Log management infrastruktury * Uživatelsky konfigurovatelný reporting strukturovaných dat (timestamp, facility, priority, tag, program, hostname, atd.) * Definice vlastních vyhledávacích filtrů a „pohledů“   + Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů) |  |  |
|  | **Peering**   * Možnost přepojit více Log Management serverů a vyhledávání nad nimi přes jedno rozhraní. * Definice vyhledávacích filtrů a „pohledů“ nad „peeringoovými“ servery   + Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů) |  |  |

Tabulka 9: Kapacitní požadavky – log management

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Řešení musí výkonově pokrýt špičkový krátkodobý vstup a bezztrátové zpracování alespoň 40 000 EPS. |  |  |
|  | Licence řešení pokryje sběr událostí z minimálně 250 zařízení, v odhadované kapacitě 40GB/den, a zajistí dlouhodobě schopnost sběru 10 000 EPS (událostí za vteřinu - průměr za 24 hod.). |  |  |
|  | Licenční krytí řešení nesmí mít jakékoli omezení na maxima krátkodobých špiček objemu zpracovaných událostí (EPS). |  |  |
|  | Řešení musí být škálovatelné tak, aby rychlost i kapacita všech částí mohla být bez ztráty dat navýšena nejméně na 1 000 zdrojů a 20 000 EPS. |  |  |
|  | Disková kapacita řešení musí zajistit uložení všech logů v RAW podobě minimálně po dobu 100 dní. |  |  |

Tabulka 10: Omezení a limity – log management

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Řešení bude implementováno bez přerušení nebo narušení provozu IT Zadavatele. |  |  |
|  | Řešení umožní znovupoužití a využití již pořízených prostředku a služeb na straně zadavatele, a to jak z hlediska již provozované infrastruktury, tak i z hlediska platformy, na níž bude samo vystaveno. |  |  |
|  | Řešení umožní iterativní nasazení, tedy nasazení po jednotlivých částech. |  |  |
|  | Řešení nesmí zavádět proprietární protokoly nebo formáty tam, kde jsou k dispozici kvalitativně srovnatelné průmyslové standardy, akceptované dalšími výrobci. |  |  |
|  | Řešení LM obsahujícího sklady logů bude ve formě HW appliance, s minimálně těmito parametry:   * + 8GB RAM+   + 4TB HDD v RAID1 nebo RAID10   + Podpora šifrování na úrovni HW   + 4x LAN   + ILO/remote MGMT. |  |  |

## Implementace systému pro management bezpečnostních informací a událostí - SIEM

Tabulka 11: Implementace systému pro management bezpečnostních informací a událostí - SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Navrhované řešení musí být odolné proti výpadkům a poruchám. Všechny komponenty systému musí být schopny dlouhodobého bezobslužného provozu bez změny chování a úbytku výkonu. |  |  |
|  | Řešení musí být vybaveno redundantními napájecími zdroji s tím, že každý zdroj samostatně musí být schopen pokrýt plně požadavky na napájení. Zdroje musí být vyměnitelné za chodu. |  |  |
|  | Řešení zajistí uživatelskou dostupnost na úrovni implementovaných prvků. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple MacOS, Apple iOS. |  |  |
|  | Řešení musí splňovat základní požadavky na informační bezpečnosti, zejména pak:   * Důvěrnost * Citlivost * Dostupnost * Autentizaci * Autorizaci * Nepopiratelnost |  |  |
|  | Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup). |  |  |
|  | Řešení musí podporovat autentizaci uživatelů z externích zdrojů autentizačních dat, nejméně protokoly Radius, LDAP a integrovatelné užití externí autentizace. |  |  |
|  | Řešení musí umožnit automatizovanou obnovu komponenty po jejím výpadku zpět do požadovaného stavu, implementován musí být princip zálohování nutných konfigurací. |  |  |
|  | Součástí řešení bude rovněž nástroj pro odhalování zranitelností, provázaný s korelační vrstvou řešení tak, aby umožňoval automatické stanovení relevance jednotlivých událostí. Licence musí umožnit rovněž scanování všech v řešení evidovaných aktiv na dostupné zranitelnosti. |  |  |
|  | Řešení musí být rozšiřitelné o další komponenty jak z hlediska výkonu, tak redundance nebo distribuce topologie. Rozšíření musí být možné bez ztráty dat. |  |  |
|  | Řešení musí být rozšiřitelné způsobem, který umožní jeho rozdělení nebo vydělení v samostatné části, funkčně shodné s originálem. |  |  |
|  | Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat. |  |  |
|  | Řešení musí umožnit vytváření incidentů a reportů v souladu s normami řady ISO / IEC 27000 |  |  |
|  | Součástí dodávky a implementace řešení musí být i licence (prostředí) pro tvorbu vlastních parserů. |  |  |
|  | Řešení musí zaznamenávat vlastní auditní žurnál po nastavitelnou dobu a tento musí být chráněn proti modifikaci.  Řešení musí obsahovat plně integrovaný nástroj pro řízení celého životního cyklu incidentu. |  |  |
|  | Řešení využije jako zdroj dat externí log management systém a vrstva sběru logů bude funkčně i technicky oddělena. |  |  |
|  | Řešení bude podporovat zpracování NetFlow dat. |  |  |
|  | Řešení bude podporovat kompresi dat mezi zdrojem a vstupem řešení. |  |  |
|  | Řešení umožní ochranu vstupních dat šifrováním. |  |  |
|  | Řešení umožní filtraci vstupních dat tak, aby jejich tok mohl být směrován k jinému zpracování, ale aby se odfiltrovaná data nezapočítávala k žádnému licenčnímu ukazateli řešení. |  |  |

Tabulka 12: Kapacitní požadavky – SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Řešení musí být licencováno na minimálně 1 000 EPS (událostí za vteřinu - průměr za 24 hod.). |  |  |
|  | Řešení musí být výkonově schopné dlouhodobě zpracovat 5 000 EPS (událostí za vteřinu - průměr za 24 hod.) a ve špičkovém zatížení krátkodobě odbavit 10 000 EPS. |  |  |
|  | Licenční krytí řešení nesmí mít omezení na maxima krátkodobých špiček objemu zpracovaných událostí (EPS). |  |  |
|  | Řešení musí umět zpracovat data bez (licenčního) omezení počtu zdrojů. |  |  |
|  | Řešení musí umět zpracovat data bez (licenčního) omezení počtu evidovaných aktiv. |  |  |
|  | Řešení nesmí být licenčně omezené na počet uživatelů nebo konzolí. |  |  |
|  | Řešení musí být škálovatelné tak, aby rychlost i kapacita všech částí mohla být bez ztráty dat navýšena nejméně o 100 %. |  |  |
|  | Sběr logů z Log Managementu bude realizován v HA zapojení. Vyhodnocování není požadováno v HA, ale je požadováno, aby při výpadku „vyhodnocovací” komponenty nedošlo k ztrátě logů a přijímané logy byli ukládány do cache. Po obnovení spojení musí SIEM zpracovat tyto uložené „historické logy” se správnými časovými značkami. |  |  |
|  | Řešení bude podporovat možnost nasazení/rozšíření na plné High Availability (dále a výše jen „HA“) bez rekonfigurace/ztráty dat pomocí přidání dalšího serveru/appliance. |  |  |

Tabulka 13: Požadavky na vstupy a zpracování dat – SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | **Technologie sběru dat** - řešení musí být schopno užít externí log management systém jako základní zdroj dat a komunikovat s ním průmyslově standardními protokoly (minimálně TCP syslog). Log Management řešení zajištuje sběr, přenos a uložení RAW logů z více než 100 zařízení v 25 lokalitách v HA zapojení. |  |  |
|  | **Logující zařízení** - Windows, CISCO IOS, MSSQL, VMWARE, sonda FlowMon a proprietární aplikace. |  |  |
|  | **Base line analýza** - Řešení musí umět porovnat neobvyklý počet určitých událostí oproti jinému období z minulosti |  |  |
|  | **Agregace** - reportovací nástroj musí podporovat trendový reporting nad velkými objemy dat ve velkém časovém období (1 rok) a tvorbu vlastních agregačních (sumarizačních) tabulek s možností nastavit různé sumarizační časové rámce (minimálně hodiny, dny). |  |  |
|  | **Členění aktiv** - Aktiva musí být možno rozdělit dle jejich důležitosti. Aktiva musí mít uživatelsky definovatelné kategorie a parametry |  |  |
|  | **Relevance zranitelnosti** - U aktiv musí být ověřena relevantnost incidentů pro dané aktivum vulnerability scanerem |  |  |
|  | **Kategorizace aktiv/zdrojů** - Řešení musí umět evidovat a vyhodnotit kategorie aktiv dle povahy zdrojových dat a dle těchto kategorií utvářet další pravidla nebo reporty |  |  |
|  | **Manuální parsovací pravidla** - Řešení musí mít plnou podporu ručního vytváření parsovacích definic (parserů/konektorů/normalizátorů). |  |  |
|  | **Historická korelace** - Řešení umožní ověření nového korelačního pravidla proti historickým datům.  **Reporty** - Řešení umožní provádět on-demand spouštění některých pravidel a z výstupu vytvářet reporty, s možností načasování |  |  |
|  | **Režim Maintenance** - Řešení musí být schopno běhu v režimu údržby, kdy se nebudou z jednotlivých zdrojů/aktiv vyhlašovat alerty |  |  |
|  | **Automatické rozpoznání** - Řešení musí automaticky rozpoznat typ zařízení dle povahy vstupních dat a provádět parsování bez zásahu administrátora |  |  |
|  | **Session logy** - Řešení musí být schopno provázat několik přístupových záznamů tak, aby byl schopen rozpoznat "admin hopping" = přihlášení z bodu A do D přes prostředníky B a C, za předpokladu, že přímý prostup není dovolen |  |  |
|  | **Sdílené účty** - Řešení musí být schopno provázat několik přístupových záznamů tak, aby bylo možno provázat privilegované přístupy pro konkrétního uživatele |  |  |
|  | **NAT** - Korelátor řešení musí být schopno spárovat nebo sdružit různé IP adresy k sobě, pokud je jedna z adres přeložena pomocí NAT, a to na základě automatizovaně definovatelných překladových tabulek, a to i v případě užití IPv6 |  |  |
|  | **Ukládání dat** – řešení zajistí ukládání „aktivních/online” logů, eventů a alertů interně, externí úložiště bude využito jen pro zálohy a archivaci. |  |  |

Tabulka 14: Mimofunkční požadavky – SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Řešení musí být umožňovat více jazykových mutací, minimálně však češtinu, angličtinu, alespoň v částech řešení, které jsou přístupné pro koncové uživatele |  |  |
|  | Řešení musí být umožňovat úpravy vzhledu rozhraní pro koncové uživatele do korporátního designu |  |  |
|  | Zadavatel předpokládá řešení ve formě HW a SW / appliances a výslovně uvádí, že pro zajištění požadovaných vlastností řešení neposkytne s výjimkou prostor pro umístění, napájení, kapacity pro zálohy dat a komunikační infrastruktury a nutné součinnosti dle smluvních ujednání žádný další technický nebo netechnický příspěvek na své straně, zejména, avšak nikoliv výhradně kapacitu vizualizační infrastruktury, HW, SW, licence, nebo jiné prostředky. |  |  |

Tabulka 15: Limity a omezení – SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Zadavatel pro účely zálohování vyhradí kapacitu max. 5TB dat vlastními zálohovacími prostředky. Zadavatel pro vyloučení všech pochybností uvádí, že samu schopnost zálohy a obnovy po výpadku nebude hodnotit jako dostatečnou aplikaci opatření zajišťujících HA funkce řešení. |  |  |
|  | Řešení bude implementováno bez přerušení nebo narušení provozu zadavatele |  |  |
|  | Řešení umožní iterativní nasazení, tedy nasazení po jednotlivých částech. |  |  |
|  | Řešení nesmí zavádět proprietární protokoly nebo formáty tam, kde jsou k dispozici kvalitativně srovnatelné průmyslové standardy, akceptované dalšími výrobci. |  |  |
|  | Řešení SIEM bude ve formě HW appliance, s minimálně těmito parametry:   * + 128GB RAM+   + 2TB HDD v RAID1 nebo RAID5/6   + Podpora šifrování na úrovni HW   + 4x LAN   + ILO/remote MGMT |  |  |

## Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech

Tabulka 16: Implementace PIM/PAM nad privilegovanými uživateli – kontrola vykonaných činností privilegovaných uživatelů v klasifikovaných informačních systémech

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | **Řešení zajistí uživatelskou dostupnost na úrovni implementovaných prvku. Prezentace dat** musí být provedena i v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple MacOS, Apple iOS. |  |  |
|  | Řešenípodporuje externí autentizaci Microsoft AD, LDAP nebo RADIUS |  |  |
|  | **Řízení přístupů** (AAA):   * + řízení přístupu na úroveň jednotlivých politik prístupu   + podpora GROUP managementu   + podpora autentizace přes RADIUS   + Podpora lokální /externí databáze uživatelů – LDAP |  |  |
|  | **Řešení musí podporovat zapojení pro High Availability**, tj. vysoká dostupnost. |  |  |
|  | Řešeníumožnuje vygenerovat report o činnosti systému |  |  |
|  | Řešeníumožňuje automatický reporting (plánované reporty anebo reporty které vznikají na základě události) |  |  |
|  | **API rozhraní** |  |  |
|  | **Vytváření auditních záznamů**:   * + Řešenízaznamenává aktivitu uživatele na cílovém systému   + Řešení umožňuje přehrávat všechny uživatelské aktivity   + Řešení přehrává zaznamenané aktivity přesně jako video. Všechny akce uživatelů jsou viditelné tak, jak byly zobrazovány na jejich monitoru.   + Přehrávání podporuje rychlé "převíjení" během přehrávání, vyhledávání událostí (např. Napsané příkazy nebo stisknutí "Enter") a textů, prohlížených uživatelům. |  |  |
|  | **Práce s auditními záznamy**:   * + Řešení zaznamenaná data lze uložit a zajistit jejich integritu: šifrování, podpis a časová značka   + Řešení zaznamenaná data lze vyhodnocovat on-line nebo off-line   + Obsah auditních záznamů je indexován (OCR metadata)   + Řešení umožňuje vyhledávání událostí s využitím indexů   + Řešení umožňuje konfigurovat a využívat nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivé politiky přístupu   + Řešení umožňuje konfigurovat a využívat nezávislé archivační (data retention) politiky pro jednotlivé politiky přístupu   + Řešeníumožňuje export dat v originálním formátu |  |  |
|  | Řešenímusí, byť schopný fungovat v plně transparentním módu, zcela nezávislém od klientů a serverů (bez agentní přístup). |  |  |
|  | Řešeníumožňuje dohledovat protokoly:   * + SSH   + RDP   + HTTP(s)   + Citrix ICA   + Telnet, TN3270/TN5250   + VNC   + X11 |  |  |
|  | Řešení zaznamenává přenosy dat SCP, SFTP and HTTP(s) |  |  |
|  | Řešení dokáže vygenerovat syslog správu, do externího syslog serveru, obsahující informace kdo a kam se snaží připojit |  |  |
|  | Řešení umožnuje aplikovat princip autorizace čtyř očí. (Privilegovány uživatelé mohou přistupovat k serveru až po vydání povolení schvalující osoby. Schvalující má také možnost monitorovat, případně ukončit, práci administrátora v reálném čase, tak jako by sledovali současně stejnou obrazovku |  |  |
|  | Řešení dokáže monitorovat síťový provoz v reálném čase a provádět různé akce v případě, že se na obrazovce objeví určitá kombinace (např. podezřelý příkaz, název okna nebo text). V případě, že zaregistruje podezřelou akci, může poslat e-mailová a syslog notifikaci, nebo okamžitě ukončit spojení. Systém tedy dokáže zablokovat spojení ještě předtím, než destruktivní příkaz administrátora (např. Delete) zaúčinkuje. |  |  |
|  | Řešeníse musí dát využít i jako centrální autentizační gateway, který vynucuje silnou autentizaci před přístupem uživatelů k citlivým IT aktivům. |  |  |
|  | Řešení musí být schopné dodatečně autentizovat uživatele přihlašujícího se na sdílený účet (typicky root/Administrator) pomoci dodateční autentizaci v které se využije metoda jednoznačně přiřazující identitu k účtu |  |  |
|  | Přihlašovací údaje pro přístup k serveru jsou využívány transparentně ať už z lokálního úložiště v samotným řešení nebo z jiného password management systému, respektive RADIUS serveru. (uživatelé nemusí vlastnit / vědět reálně přihlašovací údaje k cílovému serveru.) |  |  |

Tabulka 17: Kapacitní požadavky – PIM/PAM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Systém musí umožnit uchováni meta dát o vykonaných transakcích minimálně po dobu 1 roku |  |  |
|  | Systém musí umožnit uchování kompletních auditních záznamů po dobu minimálně tří měsíců |  |  |

Tabulka 18: Limity a omezení – PIM/PAM

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Systém umožnuje v základní licenci současně dohledovat následující počty:   * počet dohledovaných systémů, resp. cílových IPv4 nebo IPv6 adres je minimálně 25 * počet privilegovaných uživatelů je minimálně 250 * počet identit v systémech je minimálně 1000 * počet současné přihlášených uživatelů je minimálně 10 |  |  |
|  | Systém umožnuje měnit licenci, parametr na základě, kterého je licencován bez nutnosti nové implementace.   * Řešení SIEM bude ve formě HW appliance, s minimálně těmito parametry:   + 8GB RAM+   + 4TB+ HDD v RAID1 nebo RAID10   + Podpora šifrování na úrovni HW   + 4x LAN   + ILO/remote MGMT. |  |  |

## Implementace Provozně – technického monitorovacího systému (pro zajištění Performance a Capacity Management) a vybudování druhého záložního místa datového centra – Business Continuity

Tabulka 19: Virtualizační server pro záložní lokalitu – 1 ks

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Maximální velikost 2RU, osazení do datového rozvaděče 19 palců |  |  |
|  | Možnost osazení minimálně 16 disky SFF 2,5“ |  |  |
|  | Včetně výsuvných lyžin do datového rozvaděče a organizéru kabelů |  |  |
|  | 2× CPU minimálně 8 jader, výkon pro obě CPU dle PassMark – CPU Mark minimálně 16500 bodů |  |  |
|  | Podpora minimálně 24 modulů RAM DDR4, celková paměť minimálně 128 GB v maximálně 4 modulech, minimální rychlost pamětí 2400 MT/s |  |  |
|  | RAID řadič SAS 3.0 s podporou připojení 16 disků, podporou RAID 0, 1, 10, 5, 50, 6 a 60, paměť Cache minimálně 2 GB, možnost využít SSD disků pro zrychlení čtení |  |  |
|  | Hrubá disková kapacita minimálně 12TB, při čtení 90% a zápisu 10% při použití RAID6 minimálně 800 IOPS |  |  |
|  | SD nebo USB paměť pro nasazení virtualizačního hypervisoru s redundancí a kapacitou minimálně 8 GB |  |  |
|  | Redundantní, hot-plug napájecí zdroje, min. 750W, napájení jednofázové 220-240V |  |  |
|  | Redundantní, za provozu vyměnitelné ventilátory |  |  |
|  | Konektivita min. 4× 1000Base-T a 2× 10Gbit/s SFP+ porty s podporou NIC, iSCSI a FCoE. |  |  |
|  | Včetně 2 kusů originálních (ne OEM) SFP+ DAC kabelů kompatibilních s touto síťovou kartou |  |  |
|  | Dedikovaný RJ-45 port, umožňující zabezpečený přístup přes síť – webovým prohlížečem i přes SSH. |  |  |
|  | Integrovaný nezávislý procesor pro vzdálenou správu umožňující vzdálené vypínání a zapínání serveru, plně integrovanou grafickou konzoli s možností sdílení více uživateli současně, připojení virtuálních médií (FDD, DVD, ISO i jejich image) a podporu standartu SNMP/ SSL/ SSH/ IPM |  |  |
|  | Management serveru musí umět odesílat hlášení o stavu HW na definovaný email bez nutnosti instalace agentů do OS. |  |  |
|  | 5-letá servisní podpora výrobcem v režimu 9×5 s reakční dobou nejpozději následující pracovní den v místě instalace. |  |  |

Tabulka 20: Doplnění blade chassis HP C7000 – 2 ks switchů

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | L3 přepínač s podporou OSPF |  |  |
|  | Fyzické konektory – minimálně 8× SFP+, minimálně 2 porty pro stohování switchů |  |  |
|  | Konektivita k serverům v chassis – 16× 10 Gbps |  |  |
|  | Propustnost do LAN i k serverům minimálně 160 Gbps |  |  |
|  | Podpora IPv4, IPv6 |  |  |
|  | Podpora FCoE N\_Port Virtualization a FIP Snooping mode |  |  |
|  | Možnost virtuálního stohování switchů do jednoho virtuálního přepínače |  |  |
|  | Podpora HW based ACL, LLDP, Dynamic ARP protection, STP Root Guard, DHCP Protection |  |  |
|  | Možnost nastavit limity pro broadcast a multicast na síti |  |  |
|  | Podpora QoS s 8 frontami a klasifikací provozu na L2-L4, podpora SP, WRR, WFQ a WRED |  |  |
|  | Možnost nastavení zrcadlení provozu na vybraný port switche pro jeho další analýzu |  |  |
|  | Včetně 4 kusů originálních (ne OEM) SFP+ DAC kabelů kompatibilních s těmito switchi. |  |  |

Tabulka 21: Aktivní prvky pro primární a záložní serverovnou – 4 ks

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | L3 přepínač s podporou OSPF |  |  |
|  | Velikost maximálně 1RU, montáž do datového rozvaděče 19 palců |  |  |
|  | Minimálně 16 SFP portů |  |  |
|  | Minimálně 8 metalických portů nebo sdílených portů metalický/SFP |  |  |
|  | Minimálně 4 SFP+ porty 10 Gbps |  |  |
|  | Možnost rozšíření minimálně na 12 portů 10 Gbps formou modulů |  |  |
|  | Propustnost minimálně 280 Gbps |  |  |
|  | Podpora IPv4, IPv6 |  |  |
|  | Možnost virtuálního stohování switchů do jednoho virtuálního přepínače |  |  |
|  | Podpora ACL, LLDP, Dynamic ARP protection, STP Root Guard, DHCP Protection |  |  |
|  | Možnost nastavit limity pro broadcast a multicast na síti |  |  |
|  | Podpora QoS s 8 frontami a klasifikací provozu na L2-L4, podpora SP, WRR, WFQ a WRED |  |  |
|  | Možnost nastavení zrcadlení provozu na vybraný port switche pro jeho další analýzu |  |  |
|  | Redundantní zdroje |  |  |
|  | Kompatibilní s 10Gb DAC kabely dodanými pro záložní server a blade switch. |  |  |
|  | Každý prvek včetně originálního (ne OEM) SFP+ DAC kabelu 1m a 10G SFP+ MM modulu kompatibilního s tímto prvkem. |  |  |
|  | 5-letá záruka na HW. |  |  |

Tabulka 22: Virtuální diskové pole – 2 ks

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Podpora režimu active/active a automatického rozkladu zátěže |  |  |
|  | Plně redundantní systém, který zajistí nepřetržitý přístup k datům a automatický failover a failback – bez zásahu administrátora |  |  |
|  | Jednoduchá rozšiřitelnost bez nutnosti odstávky a jednotný grafický management celého clusteru, možnost rozložení provozu do více geografických lokalit |  |  |
|  | podpora funkcí thin provisioning, synchronní replikace, asynchronní replikace, podpora automatického tieringu |  |  |
|  | podpora Network RAID 10,5,6 |  |  |
|  | možnost bezvýpadkového rozšíření diskového úložiště až na 12 storage nodů, podpora aktualizace firmware pole bez přerušení provozu, podpora on-line upgradů |  |  |
|  | Licence umožňující osazení kapacity až 10TB s možností navýšení licence na 50TB |  |  |
|  | Certifikace pro VMware Metro Storage Cluster a VMware SRM |  |  |
|  | Kompatibilita se stávajícími diskovými poli SAN |  |  |
|  | 5-leté předplatné licencí a technická podpora. |  |  |

Tabulka 23: Optické propojení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Realizace optického propojení ze záložní serverovny do jednotlivých patrových rozvaděčů. Mezi záložní serverovnou a každým z rozvaděčů bude zajištěna konektivita minimálně 12× MM 50/125 OM3 s ukončeními SC v nové optické vaně na obou stranách. |  |  |
|  | Realizace optického propojení ze záložní serverovny do hlavní serverovny. Mezi záložní serverovnou a hlavní serverovnou bude zajištěna konektivita minimálně 24× MM 50/125 OM3 s ukončeními SC v samostatné nové optické vaně na obou stranách. |  |  |
|  | Pro optickou kabeláž včetně jejího ukončení doložení certifikátu o splnění norem ČSN EN 50266-2-2 (IEC 60332-3A), ČSN EN 50267-1:99, ČSN EN 50267-2-2:99, ČSN EN 61034-1:06, ČSN EN 61034-2:06, ČSN IEC 60331-11:01, ČSN IEC 60331-25:01, ČSN EN 60332-3-10:10, ČSN EN 60332-3-22:10 |  |  |
|  | 25 letá systémová garance (záruka) výrobcem optických komponent |  |  |
|  | Montáž komponent certifikovanou společností na dodávanou technologii. |  |  |

## Implementace systému testování zranitelností – Vulnerability Management

Tabulka 24: Všechny varianty testů - požadované výstupy

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Výstupem penetračního testu prostředků a služeb objednatele bude výsledná zpráva, která bude popisovat postup prověrky a nalezené zranitelnosti, včetně jejich kategorizace a podrobného popisu s doporučenými opatřeními pro jejich odstranění nebo zmírnění následků zneužití, zachycující:   * veškeré vstupní informace testu * testovací žurnál * identifikaci testovacích nástrojů a jejich konfiguraci při testu * úplný výpis výsledků * postup a závěr hodnocení * manažerské shrnutí testu. |  |  |
|  | Metodika pro realizaci testů zranitelností |  |  |
|  | Nástroj pro testování zranitelností |  |  |

# Implementace

K implementaci bude sestaven realizační tým za účasti dodavatele i objednatele, budou probíhat schůzky vedení projektu s cílem koordinovat záměry objednatele, záměry projektu a požadovaným stavem funkčnosti předmětu veřejné zakázky.

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované minimální požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění minimálních požadavků ve sloupci **„Účastníkem nabízená hodnota“**, tak že tam nakopíruje text ze sloupce „Specifikace minimálních požadavků“, případně doplní nebo upraví popis nabízené hodnoty, ze kterých bude patrné, že splňuje minimální požadavky.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

Tabulka 25: Požadavky – Implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | projektové řízení |  |  |
|  | návrh řešení před zahájením implementace |  |  |
|  | rozdělení implementace na dílčí na sebe navazujících části (etapy) |  |  |
|  | provedení instalace a konfigurace dodaných HW a SW |  |  |
|  | provedení potřebné integrace v rámci stávajícího ICT prostředí |  |  |
|  | nastavení HW a SW dle požadavků zákazníka (customizace řešení) |  |  |
|  | testování implementovaného HW a SW |  |  |
|  | zahájení ostrého provozu (převedení HW a SW do produkčního prostředí). |  |  |
|  | vypracování a předání dokumentace popisující průběh implementace a konečný skutečný stav předmětu veřejné zakázky |  |  |
|  | zaškolení správců systému v rozsahu správy dodaného HW a SW, tak aby byli schopni spravovat předmět veřejné zakázky. |  |  |

# Požadavky na technickou podporu provozu

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované minimální požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění minimálních požadavků ve sloupci **„Účastníkem nabízená hodnota“**, tak že tam nakopíruje text ze sloupce „Specifikace minimálních požadavků“, případně doplní nebo upraví popis nabízené hodnoty, ze kterých bude patrné, že splňuje minimální požadavky.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

Tabulka 26: Požadavky na technickou podporu provozu

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Dodavatel zajistí kvalitní a včasnou technickou podporu, a to jak pomocí internetového rozhraní tzv. Help-desk, tak telefonické konzultace v pracovní dny od 7.00 do 17.00 hod. |  |  |
|  | Dodavatel se zavazuje poskytovat i osobní konzultace a školení na vyžádání Objednatele v době rutinního využívání IS. |  |  |
|  | Součástí technické podpory jsou také schůzky vedení projektu, po dobu udržitelnosti projektu, s cílem zajistit stabilní provoz informačního systému, a to v rozsahu minimálně jedenkrát za půl roku. |  |  |

# Podmínky předání a převzetí – akceptace

Předání a převzetí bude provedeno na základě akceptačního protokolu, ve kterém budou zaznamenány výsledky splnění předmětu smlouvy o dílo:

1. Dodávka HW a SW dle smlouvy o dílo;
2. Dodávka technické dokumentace skutečného provedení díla;
3. Úspěšné provedení akceptačních testů v rozsahu dle požadavků zadavatele.

# Záruky a servis – podpora provozu

## Záruka

**Záruka je požadována v minimální délce 24 měsíců.**

Záruka za jakost díla bude realizována dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.

Záruka se nevztahuje pouze na:

* vady způsobené nesprávnou manipulací se zařízením, neodborným zacházením nebo nedodržením návodu k obsluze;
* vady způsobené přepětím v elektrické napájecí síti;
* vady vzniklé živelnou pohromou;
* vady způsobené mechanickým poškozením;
* vady způsobené krádeží nebo jinou trestnou činností;
* vady způsobené nesprávnými podklady nebo informacemi objednatele;
* vady způsobené objednatelem změnou zhotovitelem určených parametrů chodu informačního systému bez souhlasu zhotovitele;
* vady způsobené v důsledku nesprávnosti dat vkládaných do informačního systému objednatele přímo objednatelem**.**

## Servisní podpora provozu

Jedná se o servisní podporu provozu předmětu veřejné zakázky během doby udržitelnosti projektu.

Předmětem projektu je dodávka servisní podpory provozu předmětu veřejné zakázky, aby byl zajištěn nepřetržitý funkční chod předmětu veřejné zakázky. V rámci servisní podpory je Účastník povinen dodat v požadovaných parametrech nové zařízení (resp. díl) na požadované místo určení (místo instalace zařízení). Zadavatel vyžaduje takový typ servisní podpory výrobce, při kterém bude schopen řešit servisní požadavky přes libovolnou servisní organizaci výrobce, stejně jako u výrobce přímo. V rámci služby podpory provozu Zadavatel požaduje poskytnutí software update.

Linka zákaznické podpory pro předmět veřejné zakázky bude dosažitelná prostřednictvím internetového portálu, emailu či telefonu. Požadavek podporu bude realizován pracovníky úřadu, kteří v případě výskytu problému kontaktují linku zákaznické podpory a následně pracují dle instrukcí.

Servisní podpora je vyžadována v následujícím rozsahu:

* Získat nárok na výměnu vadného zařízení, dodání náhradního dílu do místa instalace do 3 pracovních dní po nahlášení závady.
* Přímý přístup na technicko - asistenční centrum výrobce za účelem čerpání technické podpory při odstraňování problémů předmětu veřejné zakázky.
* Získat nárok na přímý přístup ke stažení aktuálního SW pro předmět veřejné zakázky.

Dodavatel zajistí služby zajišťující rutinní provoz systému:

* Provoz služby zákaznické podpory pro zadávání požadavků a provozních závad předmětu veřejné zakázky s garantovanou dostupností služby v pracovní dny od 7:00 do 17:00 hod.
* Legislativní soulad dodaného předmětu veřejné zakázky.
* Garantovanou reakční dobu řešení požadavků na závadu předmětu veřejné zakázky.

Závadou předmětu veřejné zakázky řešení se rozumí jakýkoliv stav předmětu veřejné zakázky znemožňující provoz dle dokumentace k předmětu veřejné zakázky. Pro rozlišení urgentnosti závad bude využívána stupnice:

1. Kritická závada systému, jedná se o stav předmětu veřejné zakázky, kdy je znemožněna práce s předmětem veřejné zakázky, nelze použít alternativní zásah. Součástí této závady je také nesoulad předmětu veřejné zakázky s platnou legislativou.
2. Méně závažná závada systému, jedná se o stav předmětu veřejné zakázky, který lze dočasně překlenou jiným postupem koncového uživatele.
3. Závada neohrožující funkčnost, námět na změnu, jedná se o stav předmětu veřejné zakázky, který je charakterizovaný požadavkem uživatele na změnu funkčnosti předmětu veřejné zakázky.

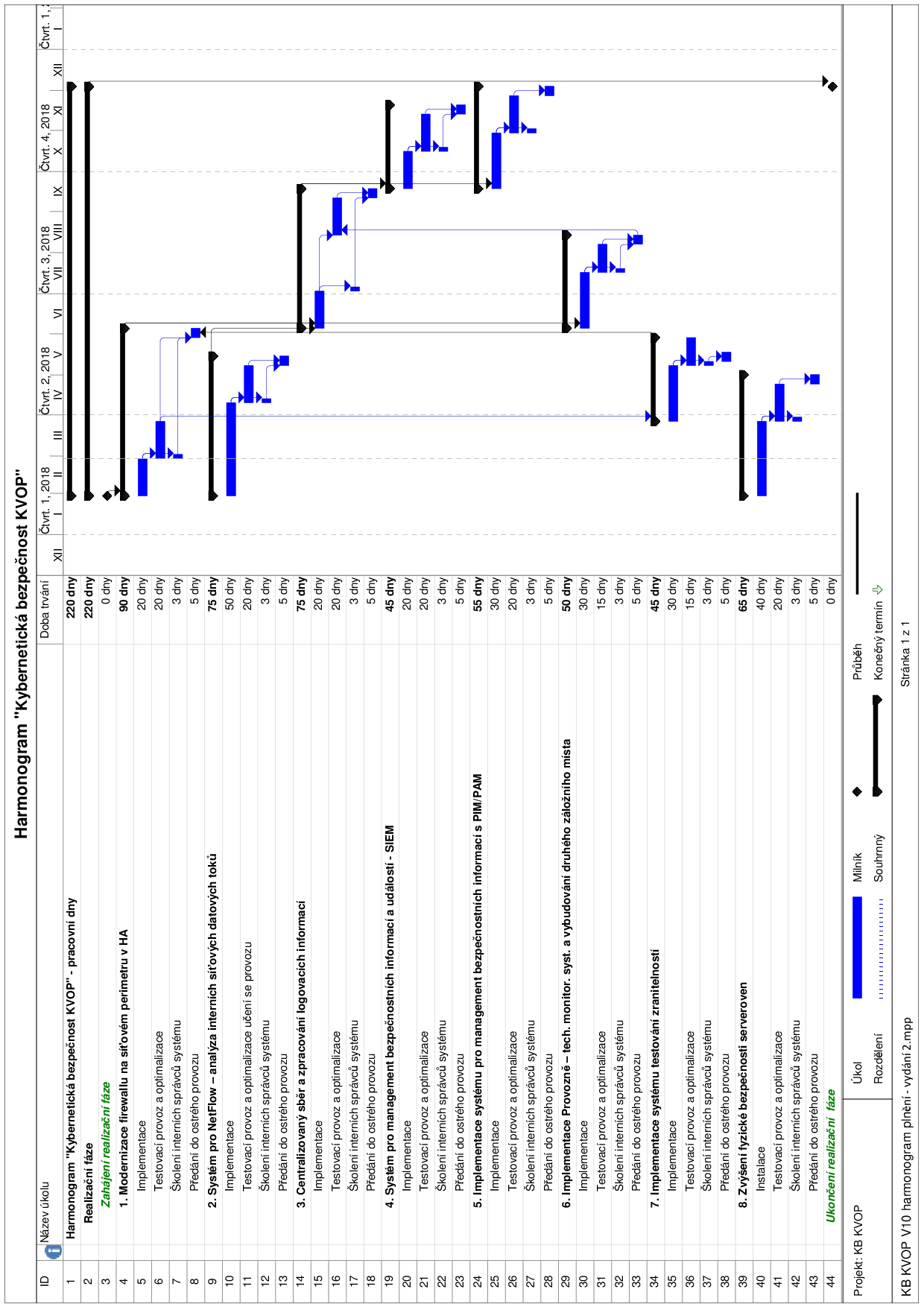
Tabulka 27: Reakční doby pro řešení požadavků

|  |  |  |  |
| --- | --- | --- | --- |
|  | **A: Kritická závada** | **B: Méně závažná vada** | **C: Návrh na změnu** |
| Zahájení řešení požadavku | Do 3 pracovních hodin, v pracovní dny od nahlášení požadavku. | Do 8 pracovních hodin, v pracovní dny od nahlášení požadavku. | Do 5 pracovních dnů, v pracovní dny od nahlášení požadavku. |
| Zprovoznění systému, nebo informace o postupu řešení | Do 8 pracovních hodin, v pracovní dny od nahlášení požadavku. | Do 5 pracovních dnů, v pracovní dny od nahlášení požadavku. | Do 10 pracovních dnů, v pracovní dny od zapsání nahlášení požadavku. |
| Úplné vyřešení požadavku | Do 3 pracovních dnů, v pracovní dny od nahlášení požadavku. | Do 10 pracovních dnů, v pracovní dny od nahlášení požadavku. | Do 30 pracovních dnů, v pracovní dny od nahlášení požadavku. |

# Harmonogram plnění

Harmonogram plnění – časový plán je zobrazen na následujícím obrázku. Skutečný termín zahájení realizace může být posunut na základě data uzavření smlouvy.

Obrázek 2: Harmonogram plnění



# Seznam zkratek

ADS systém detekce anomálií (Anomaly Detection Systém)

API rozhraní pro programování aplikací (Application Programming Interface)

APM monitoring výkonu aplikací (Application Performance Monitoring)

ATR adaptivní směrování provozu (Adaptive traffic rating)

CA certifikační autorita

CCTV uzavřený televizní okruh (Closed Circuit Television)

ČSN Česká státní norma

DB databáze

DDoS distribuovaný DoS (Distributed Denial of Service)

DDHM drobný dlouhodobý hmotný majetek

DDNM drobný dlouhodobý nehmotný majetek

DHM dlouhodobý hmotný majetek

DNM dlouhodobý nehmotný majetek

DPH daň z přidané hodnoty

DRP Plán obnovy po havárii (Disaster Recovery Plan)

DMZ demilitarizovaná zóna (Demilitarized zone)

DoS odepření služby (Denial of service)

EKV elektronická kontrola vstupu

ESO Evidence stanovisek ombudsmana

FTP protokol pro přenos souborů mezi počítači pomocí počítačové sítě (File Transfer Protocol)

GINIS SSL Informační systém spisové služby

GINIS EKO Informační systém ekonomických informací

HA vysoká dostupnost (High availability)

HTTP internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML (Hypertext Transfer Protocol)

HTTPS nadstavba síťového protokolu HTTP (Hypertext Transfer Protocol Secure)

HW hardware

ICT Informační a komunikační technologie

IDS systém pro detekci průniku

IISSP Integrovaný informační systém Státní pokladny

IKT Informační a komunikační technologie

IPS systém prevence průniku

IROP Integrovaný regionální operační program

IS Informační systém

ISDS Informační systém datových schránek

ISMS Systém řízení bezpečnosti informací

ISVS Informační systémy veřejné správy

ISZR Informační systém základních registrů

KVOP Kancelář veřejného ochránce práv

LAN lokální síť (Local Area Network)

MS OWA Microsoft Outlook Web Access

MS AD implementace adresářových služeb LDAP firmou Microsoft (Active Directory)

NBA behaviorální analýza datových toků (Network Behavior Analysis)

NBAD detekce anomálií a analýzy chování sítě (Network Behavior Anomaly Detection)

NCKB Národní centrum kybernetické bezpečnosti ČR

OS Operační systém

OSS Organizační složka státu

PDCA cyklus plánuj, udělej, zkontroluj, jednej (Plan-Do-Check-Act)

PIM správa privilegovaných účtů (Privileged Identity Management)

PZTS Poplachový zabezpečovací a tísňový systém

RPC vzdálené volání procedur (Remote procedure call)

ŘO řídící orgán

SIEM management bezpečnostních informací a událostí (Security Information and Event Management)

SLA dohoda o poskytovaných službách (Service Level Agreement)

SŘBI Systém řízení bezpečnosti informací

SSL vrstva bezpečných socketů (Secure Sockets Layer)

SW software

TLS kryptografický protokol (Transport Layer Security)

UPS zdroj nepřerušovaného napájení (Uninterruptible Power Supply/Source)

VEMA ELD Evidenční listy důchodového pojištění

VEMA KZP Komunikace se zdravotními pojišťovnami

VEMA PAM Mzdy

VEMA PER Personalistika

VEMA RNP Registr nemocenského pojištění

VEMA STM Systemizace

VIS Významný informační systém

VPN virtuální privátní síť (Virtual Private Network)

VS Veřejná správa

VyKB Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti

WiFi bezdrátová komunikace v počítačových sítích

ZoKB Zákon o kybernetické bezpečnosti č. 181/2014

**Přílohy:**

**Příloha A: Schémata rozvodů slaboproudu**

1. Rozvody slaboproudu PZTS, EKV – přízemí
2. Rozvody slaboproudu PZTS, EKV – 1. patro
3. Rozvody slaboproudu PZTS, EKV – 2. patro
4. Rozvody slaboproudu PZTS, EKV – 3. patro
5. Blokové schéma PZTS, EKV