

Požadované minimální parametry musí nabízené řešení závazně splňovat v rámci nabídky. Splnění konkrétního parametru deklaruje dodavatel vyplněním hodnoty Ano/Ne ve sloupci Splněno.
Udržitelnost projektu je stanovena na 5 let.

1 Obecné požadavky zadavatele

1.1 Požadavky na implementaci

Číslo	Požadavek	Splněno Ano/Ne
1	Dodávka a implementace bude realizována v souladu s požadavky zadavatele uvedenými v zadávací dokumentaci a dle schváleného prováděcího projektu.	
2	Instalace a zprovoznění všech částí díla bude provedena v místě plnění do stávajícího ICT prostředí zadavatele ve spolupráci s odborným personálem zadavatele.	
3	Instalace a zprovoznění všech částí díla bude prováděna za plného provozu informačních systémů zadavatele, bez jejich omezení.	
	Instalační a migrační práce na přepínačích přístupové vrstvy sítě zahrnují přenesení konfigurace přístupových portů ze stávajících prvků se zachováním přístupových práv jednotlivých uživatelů dle současné bezpečnostní politiky sítě LAN zadavatele.	
	Nabízené řešení nesmí odesílat žádná data z místní sítě, pokud to není předmětem dodávky. Pokud je předmětem dodávky externí komunikace, bude v rámci prováděcího projektu přesně popsán datový tok, aby bylo možné nastavit bezpečnostní kontroly komunikace.	
	Implementovaná zařízení a sw zakomponuje dodavatel do stávajícího monitorovacího systému (HP Intelligent Management Center).	
4	V průběhu implementace bude prováděno funkční testování jednotlivých komponent.	
5	Zkušební provoz bude součástí realizační fáze (implementace).	
6	Dodavatel bude povinen zajistit, že veškeré vlastnosti díla, včetně jeho případného update, legislativního update, upgrade a legislativního upgrade budou po celou dobu účinnosti této smlouvy odpovídat vždy aktuálním obecně platným právním předpisům ČR.	
7	Součástí implementace jsou veškeré práce a služby nezbytné pro řádné a úplné zprovoznění díla včetně vytvoření dokumentace a implementačních postupů pro správce ke všem částem díla, které budou součástí realizace, a které budou obsahovat jednotlivé kroky implementace a konfigurace umožňující přesné opakování postupů. Dokumentace nebude chráněna dle autorského zákona, bude umožněno ji dále upravovat a předávat dalším subjektům, které se podílejí na chodu informačních systémů.	
8	Součástí budou rovněž práce a služby, které ve smlouvě nejsou uvedeny ale zhotovitel, jakožto odborník, o nich vědět měl nebo mohl vědět.	
9	Pro dodávané HW komponenty uchazeč v nabídce doloží osvědčení výrobce nebo oficiálního zastoupení pro ČR, ze kterého budou zřejmé tyto skutečnosti: ✓ dodávané komponenty jsou nové a originální (zadavatel nepřipouští ekvivalentní řešení) ✓ dodávané komponenty nebyly doposud používány ✓ dodávané komponenty pochází z oficiálního distribučního kanálu pro Český trh	
10	Dodávané komponenty budou licencované jménem zadavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.	

1.2 Požadavky na zpracování detailní analýzy a prováděcího projektu

Číslo	Požadavek	Splněno Ano/Ne
1	Detailní analýza a prováděcí projekt, které budou zpracovány do jednoho dokumentu	
2	Prováděcí projekt bude obsahovat podrobný návrh architektury a specifikace rozsahu realizace všech částí díla včetně odpovídající implementační a konfigurační dokumentace	
3	Návrh akceptačních kritérií a testů, včetně akceptačního protokolu a bezpečnostních testů, pro všechny dodávané části díla.	
4	Návrh monitoringu, zálohování a obnovy všech částí díla.	
5	Časový harmonogram realizace	
6	Dokument analýzy a prováděcího projektu bude vypracován v písemné i elektronické editovatelné podobě, ve formátu MS Word/Excel, MS Visio.	

1.3 Požadavky na technickou dokumentaci

Číslo	Požadavek	Splněno Ano/Ne
1	Uživatelské příručky k dodávaným částem díla zahrnující popis uživatelských postupů	
2	Administrátorské příručky k dodávaným částem díla	
3	Dokumentace konečného provedení	
4	Provozní a bezpečnostní dokumentace zahrnující doporučení pro údržbu a zálohování, postupy obnovy v případě havárie apod. (může být součástí administrátorské příručky)	
5	Školící dokumentace	
6	Součástí dokumentace je i dokumentace výrobce dodávaných produktů, která musí být minimálně dostupná na webových stránkách	
7	Veškerá dokumentace bude vypracována v písemné i elektronické editovatelné podobě, ve formátu MS Word/Excel, MS Visio.	

1.4 Požadavky na licence

Číslo	Požadavek	Splněno Ano/Ne
1	Zadavatel požaduje poskytnutí veškerých nezbytných licencí k řádnému plnění díla.	
2	Zhotovitel specifikuje název, počet a licenční podmínky ke všem nutným licencím v příloze smlouvy o dílo, a to včetně odůvodnění zvolené licenční nabídky, dále pak uvede licenční politiku, pravidla pro přidělení a případné změny v počtu licencí, typy a verze licencí.	
3	Veškeré dodávané licence budou majetkem zadavatele.	

1.5 Požadavky na školení

Číslo	Požadavek	Splněno Ano/Ne
1	V případě dodání a implementace řešení na technologiích v současné době využívaných v síti KÚ zajistí dodavatel školení administrátorů na obsluhu a správu systému v nezbytně nutném rozsahu, včetně poskytnutí potřebných školících materiálů.	
2	V případě dodání a implementace technologicky odlišného řešení od technologií v současné době využívaných v síti KÚ požaduje zadavatel zajištění školení administrace a správy v rozsahu: ✓ minimálně 5 x 8 hodin, ✓ počet účastníků školení bude 5 dle výběru zadavatele.	
3	Pro dodávané opatření ID 10 (Zaznamenávání a řízení bezpečnostních událostí a incidentů) požaduje zadavatel zajištění školení administrace a správy v rozsahu: ✓ minimálně 3 x 8 hodin, ✓ počet účastníků školení bude 8 dle výběru zadavatele, ✓ administrátoři musí být na základě školení schopni spravovat dodaný SIEM, včetně napojování nových zdrojů ve standardním formátu a vytváření nových korelačních pravidel.	
4	Struktura a rozsah školení bude součástí nabídky uchazeče.	
5	Veškerá školení se uskuteční v místě zadavatele.	
6	Za organizační zajištění školení zodpovídá dodavatel	

1.6 Akceptační a bezpečnostní testy

Číslo	Požadavek	Splněno Ano/Ne
1	Akceptační testy budou provedeny na konci zkušebního provozu před předáním díla do rutinního provozu.	
2	Testy provede zhotovitel ve spolupráci s pracovníky zadavatele za stejných podmínek, za jakých bude pracovat dílo v rutinním provozu.	
3	Tam, kde to dílo vyžaduje, budou akceptační testy zahrnovat i testy redundance a odolnosti proti plánovanému selhání jednonásobné chyby u redundantních komponent.	
4	Návrh akceptačních kritérií a testů, včetně akceptačního protokolu, pro všechny dodávané části díla bude součástí prováděcího projektu.	

1.7 Požadavky zadavatele na záruku a poskytování technické podpory a servisu:

Číslo	Požadavek	Splněno Ano/Ne
1	Záruční doba díla bude sjednána na 60 měsíců ode dne protokolárního ukončení zkušebního provozu a předání celého díla do rutinního provozu a bude se vztahovat rovněž na veškerý software, který je součástí dodávaného hardware, včetně práva zadavatele na poskytování nových verzí software.	
2	Technická podpora a servis budou poskytovány od počátku zkušebního provozu po celou dobu udržitelnosti projektu. Poskytování technické a servisní podpory bude odpovídat nejlepším praxím dle rámce ITIL/ITSM.	
3	Technická podpora a servis zařízení HW a SW budou realizovány zhotovitelem případně prostřednictvím odpovídajícího servisního kanálu výrobce.	
4	Technická podpora a servis budou realizovány v místě zadavatele.	
5	Veškeré požadavky budou evidovány v systému servisní podpory zhotovitele.	
6	Kontaktní místo umožní příjem požadavku na servisní zásah prostřednictvím služby Hot-line a služby HelpDesk.	
7	Hot-Line umožní příjem požadavku na servisní zásah v českém jazyce na telefonním čísle v pracovních dnech v době 7:00 -19:00, příjem požadavku bude zajištěn lidskou obsluhou.	
8	HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24x365.	
9	HelpDesk umožní zadavateli upřesnit nebo doplnit požadavek.	
10	Požadavek na servisní zásah se považuje za nahlášený okamžikem jeho zapsání na HelpDesk, nebo okamžikem jeho telefonického zadání.	
11	Systém servisní podpory musí zadavateli poskytovat přehled o aktuálně nahlášených požadavcích, jejich stavu a aktuálním způsobu jejich řešení. Systém bude zadavateli zasílat notifikace o změně stavu jeho požadavku (např. zadáný, v řešení, uzavřený, ...) a musí zadavateli umožnit schvalování uzavření nahlášeného požadavku.	
12	Systém servisní podpory musí poskytovat zadavateli přístup i k databázi uzavřených požadavků a způsobu jejich řešení, který bude poskytovat podrobné údaje o historii požadavků od jejich nahlášení, po jejich vyřešení.	
13	Systém servisní podpory musí umožňovat export dat, včetně obsahu požadavku a způsobu vyřešení. Tato funkcionality bude zhotovitelem poskytována bezúplatně minimálně na vyžádání zadavatele ve formátu minimálně *.xls a *.csv.	
14	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení.	
15	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware.	

1.8 Technická specifikace opatření ID1 Chlazení a klimatizace

Níže uvedené technické specifikace uvádějí parametry pro realizaci dodávky rozšíření stávajícího systému klimatizace a chlazení v hlavním datovém centru kraje (DC1), která zahrnuje dodávku nového systému chlazení a klimatizace datového centra včetně dodávky a implementace řídicího a monitorovacího systému umožňujícího centrální správu s podporou sítí LAN a WAN. Součástí dodávky musí být i demontáž starého zařízení, montáž vnitřní a venkovní jednotky a veškeré práce a dodávky materiálu související s instalací jako jsou např. zednické začistištění, dodávka potřebného potrubí, doplnění chladiva, úprava elektroinstalace a elektro revize, přezkoušení a projektová dokumentace. Je požadováno zaškolení obsluhy na místě.

Na kompletní realizaci bude poskytnuta záruka a podpora výrobce na min. 5 let ode dne předání celého díla do rutinního provozu, v režimu 8x5 a odstraněním vady následující pracovní den od okamžiku oznámení.

Kompletní dodávka zahrnuje:

2 kusy venkovní jednotka

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Chladicí výkon Qch	25 kW	
2	Rozměry Š x V x H (maximální)	950 x1650x500	
3	Hladina akustického hluku (min./max.)	59/61 dB	
4	Energetická účinnost SEER	3,30	
5	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	

6	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
7	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

2 kusy vnitřní jednotka

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Typ - zavěšená podstropní nebo kanálová	SPLNĚNO	
2	Chladicí výkon Qch	25 kW	
3	Rozměry Š x V x H (maximální)	1400 x500x920	
4	Hladina akustického hluku (min./max.)	37/47 dB	
5	Energetická účinnost SEER	3,30	
6	Kabelový ovladač	SPLNĚNO	
7	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
8	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
9	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

1 kus integrovaný řídicí systém chlazení a klimatizace

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Integrovaný řídicí systém pro centrální správu splňující následující požadavky: ✓ možnost připojení PC přes LAN i internet ✓ Úroveň přístupu je kontrolována heslem / ID uživatele ✓ Uložení dat na pevný disk nebo paměťovou kartu SD ✓ Funkce zálohování v případě výpadku proudu (po dobu 24 hodin)	1 kus	
5	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
6	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
7	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

Montáž a příslušenství

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Demontáž starého zařízení	SPLNĚNO	
2	Potrubí (Cu)	32 m	
3	Komunikační kabel	32 m	
4	Odvod kondenzátu (napojení na stávající rozvod HT DN 40)	16 m	
5	Kompletní instalace včetně případných úprav elektroinstalace, elektro revize, oživení a zkoušek	SPLNĚNO	
6	Projektová dokumentace	SPLNĚNO	

1.9 Technická specifikace opatření ID2 Přepínače přístupové vrstvy sítě

Níže uvedené technické specifikace uvádějí parametry přepínačů, které jsou zamýšleny jako generační obměna stávajících přepínačů přístupové vrstvy sítě.

Tyto budou instalovány do stávajícího síťového prostředí a očekává se plná funkcionalita se zařízeními jak na jejich přístupových portech (např. 618 stávajících Cisco IP telefonů typů CP7921, CP7925, CP8821 využívající protokoly CDP a autentizaci EAP-FAST), tak i při připojení ke stávající, páteřní vrstvě sítě představované dvojicí přepínačů Cisco 6800-XL v konfiguraci Virtual Switching System (VSS), přičemž každý přepínač je umístěn

v geograficky odděleném datovém centru a jako síťový celek vytváří jednu logickou entitu pracující v režimu vysoké dostupnosti (HA) a sdílení provozní zátěže (load balancing).

Je požadována kompatibilita a integrace na další plánované technické opatření ID9 Řízení přístupu k síťovým prostředkům (AAA řešení na bázi 802.1x).

Kompletní dodávka zahrnuje:

21 kusů PoE přepínačů

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Uplink porty	2 x 10G SFP+	
2	Access porty	48 x 1G	
3	Nutná podpora technologie Multi-chassis Etherchannel (LACP) pro připojení ke stávajícím páteřním přepínačům Cisco 6800-XL v konfiguraci Virtual Switching System (VSS)	SPLŇUJE	
4	Nutná podpora technologie síťové segmentace VLAN	SPLŇUJE	
5	Nutná podpora technologie Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), LLDP for Media Endpoint Devices (LLDP-MED) pro podporu koncových zařízení (např. stávající Cisco IP telefony)	SPLŇUJE	
6	Nutná podpora 802.1x (včetně RADIUS Change of Authorization) pro řízení přístupu na úrovni portů (integrace s AAA serverem plánovaného v rámci ID9 Řízení přístupu k síťovým prostředkům)	SPLŇUJE	
7	Nutná podpora SNMP v2/v3 pro integraci se stávajícím provozním dohledem (HP IMC)	SPLŇUJE	
8	Nutná podpora Syslog pro integraci se SIEM	SPLŇUJE	
9	Nutná podpora Netflow pro integraci se SIEM (případně jiný protokol umožňující obdobnou funkcionality monitoringu síťových toků)	SPLŇUJE	
10	Nutná podpora PoE 740 W (15,4 W na port)	SPLŇUJE	
11	Nutná podpora Dynamic ARP Inspection (DAI) a IP source guard (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
12	Nutná podpora pro IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) a Multiple Spanning Tree Protocol (MSTP)	SPLŇUJE	
13	Nutná podpora Bridge protocol data unit (BPDU) Guard (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
14	Nutná podpora Spanning Tree Root Guard (STRG) (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
15	Nutná podpora IGMP filtering (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
16	Nutná podpora stohování (počty stohovacích propojů: 21)	SPLŇUJE	
17	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
18	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
19	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

6 kusů přepínačů bez PoE

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Uplink porty	2 x 10G SFP+	
2	Access porty	48 x 1G	
3	Nutná podpora technologie Multi-chassis Etherchannel (LACP) pro připojení ke stávajícím páteřním přepínačům Cisco 6800-XL v konfiguraci Virtual Switching System (VSS)	SPLŇUJE	
4	Nutná podpora technologie síťové segmentace VLAN	SPLŇUJE	
5	Nutná podpora technologie Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP)	SPLŇUJE	
6	Nutná podpora 802.1x (včetně RADIUS Change of Authorization) pro řízení přístupu na úrovni portů (integrace s AAA serverem)	SPLŇUJE	

7	Nutná podpora SNMP v2/v3 pro integraci se stávajícím provozním dohledem	SPLŇUJE	
8	Nutná podpora Syslog pro integraci se SIEM	SPLŇUJE	
9	Nutná podpora Netflow pro integraci se SIEM (případně jiný protokol umožňující obdobnou funkcionalitu monitoringu síťových toků)	SPLŇUJE	
10	Nutná podpora Dynamic ARP Inspection (DAI) a IP source guard (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
11	Nutná podpora pro IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) a Multiple Spanning Tree Protocol (MSTP)	SPLŇUJE	
12	Nutná podpora Bridge protocol data unit (BPDU) Guard (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
13	Nutná podpora Spanning Tree Root Guard (STRG) (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
14	Nutná podpora IGMP filtering (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
15	Nutná podpora stohování (počty stohovacích propojů: 6)	SPLŇUJE	
16	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
17	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
18	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

Délky a počty stohovacích kabelů

Číslo	Druh a rozměr kabelu	Požadované množství	Splněno Ano/Ne
1	Stohovací kabel délky 50 cm	19 ks	
2	Stohovací kabel délky 1 m	7 ks	
3	Stohovací kabel délky 3 m	1 ks	

Specifikace a počty SFP modulů

Číslo	Požadovaná funkcionalita	Požadované množství	Splněno Ano/Ne
1	SFP pro rychlost 10 Gb/s v režimu multi-mode do 220m (a v režimu single-mode G.652 do vzdálenosti 300 m), záruka 5 let	30 ks	
2	SFP pro rychlost 10 Gb/s v režimu single-mode G.652 do vzdálenosti 10km, záruka 5 let	2 ks	

Specifikace a počty propojovacích optických kabelů

Číslo	Druh a rozměr kabelu	Požadované množství	Splněno Ano/Ne
1	Optický kabel MM 50/125 2m, LC/SC	13 ks	
2	Optický kabel MM 50/125 3m, LC/SC	13 ks	
3	Optický kabel SM 2m, LC/LC	1 ks	
4	Optický kabel SM 3m, LC/LC	1 ks	
5	Mode conditioning optický kabel 2m, LC/SC	2 ks	
6	Mode conditioning optický kabel 3m, LC/SC	2 ks	

1.10 Technická specifikace opatření ID3 Přístupové body bezdrátové části přístupové vrstvy sítě

Níže uvedené technické specifikace uvádějí parametry přístupových bodů bezdrátové části přístupové vrstvy sítě, které jsou zamýšleny jako generační obměna stávajících prvků.

Tyto budou instalovány do stávajícího síťového prostředí, kde nahradí současné přístupové body a očekává se tedy plná funkcionalita se stávajícími koncovými zařízeními (například bezdrátové Cisco IP telefony CP7921, CP7925, CP8821 využívající autentizaci pomocí protokolu EAP-FAST).

Přístupové body bezdrátové sítě jsou řízeny dvojicí stávajících bezdrátových kontrolérů Cisco Wireless Services Module 2 (WiSM2) umístěných v páteřních přepínačích Cisco Catalyst 6800-XL, kontroléry pracují v režimu vysoké dostupnosti (HA) v konfiguraci aktivní - záložní.

Je požadována kompatibilita a integrace na další plánovaná opatření:

- Integrace s plánovaným technickým opatřením ID6 Monitoring bezdrátové části přístupové vrstvy sítě (SW modul pro sledování bezdrátové části přístupové vrstvy sítě LAN HP IMC)
- Integrace s plánovaným technickým opatřením ID9 Řízení přístupu k síťovým prostředkům (AAA řešení na bázi 802.1x)

Kompletní dodávka zahrnuje:

192 kusů interních přístupových bodů

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Třída zařízení	Bezdrátový WiFi bod	
2	Použití uvnitř budovy - interní antény	SPLŇUJE	
3	Počet portů 10/100/1000 Base-T PoE	1	
4	Počet rádii	2	
5	Pásmo 2,4 GHz	SPLŇUJE	
6	Pásmo 5 GHz	SPLŇUJE	
7	Podpora technologie 802.11ac s 3x3:2 MIMO	SPLŇUJE	
8	Řízeno kontrolérem, plná kompatibilita se stávajícím kontrolérem bezdrátové sítě - Cisco Wireless Services Module 2 (WiSM2)*	SPLŇUJE	
9	Detekce rušení	SPLŇUJE	
10	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
11	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
12	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

*Je umožněno dodání přístupových bodů WiFi, které nevyužijí stávající kontroléry Cisco Wireless Services Module 2 za předpokladu, že dodavatel jako součást dodávky zajistí instalaci a konfiguraci odpovídajícího řídicího a kontrolního prvku bezdrátové sítě (jiné kontroléry či funkcionálně adekvátní řešení).

6 kusů externích přístupových bodů

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Třída zařízení	Bezdrátový WiFi bod	
2	Použití uvnitř budovy - externí antény	SPLŇUJE	
3	Externí panelová anténa 2.4-GHz/5-GHz MIMO, zisk 6 dBi	SPLŇUJE	
4	Počet portů 10/100/1000 Base-T PoE	1	
5	Počet rádii	2	
6	Pásmo 2,4 GHz	SPLŇUJE	
7	Pásmo 5 GHz	SPLŇUJE	
8	Podpora technologie 802.11ac s 3x4:3 MIMO	SPLŇUJE	
9	Řízeno kontrolérem, plná kompatibilita se stávajícím kontrolérem bezdrátové sítě - Cisco Wireless Services Module 2 (WiSM2)*	SPLŇUJE	
10	Spektrální analýza (např. CleanAir)	SPLŇUJE	
11	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
12	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
13	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

**Je umožněno dodání přístupových bodů WiFi, které nevyužijí stávající kontroléry Cisco Wireless Services Module 2 za předpokladu, že dodavatel jako součást dodávky zajistí instalaci a konfiguraci odpovídajícího řídicího a kontrolního prvku bezdrátové sítě (jiné kontroléry či funkcionálně adekvátní řešení).*

1.11 Technická specifikace opatření ID4 Rozšíření přepínačů v agregační vrstvě sítě

Níže uvedené technické specifikace uvádějí parametry přepínačů, které jsou zamýšleny jako doplnění stávajících přepínačů agregační vrstvy sítě.

Tyto přepínače budou instalovány do stávajícího síťového prostředí jako rozšíření stávajícího stohu 4 agregačních přepínačů HP 5800, zapojených tak, že každá dvojice je umístěna v geograficky odděleném datovém centru. Celek všech čtyř přepínačů představuje jednu logickou síťovou entitu (cluster) tvořenou technologií HP IRF (Intelligent Resilient Framework). Očekává se tedy plná kompatibilita na úrovni IRF (Intelligent Resilient Framework).

Kompletní dodávka zahrnuje:

2 kusy přepínačů 24x 10GE SFP+

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Access porty	48x 10G SFP+	
2	LAN porty	4x 10/100/1000 RJ-45	
3	Nutná plná kompatibilita stohování (IRF) se stávajícími prvky HP 5800-24G Switch (P/N: JC100A)	SPLŇUJE	
4	Nutná podpora redundantního napájecího zdroje (interní)	SPLŇUJE	
5	Počet zdrojů osazených (AC)	2	
6	Kapacita směrování / přepínání	488 Gbps	
7	Latence (64-byte pakety)	max. 5 µs	
8	Wirespeed na všech portech	SPLŇUJE	
9	Tabulka MAC adres pro 32000 záznamů	SPLŇUJE	
10	Počet podporovaných VLAN	4096	
11	Nutná podpora pro MAC-based VLAN	SPLŇUJE	
12	Nutná podpora pro IP subnet-based VLAN	SPLŇUJE	
13	Nutná podpora směrování RIP, OSPF a OSPFv3, IS-IS pro IPv4 i IPv6	SPLŇUJE	
14	Nutná podpora směrování BGP4 a BGP4+	SPLŇUJE	
15	Nutná podpora vytváření ACL a klasifikace toků na Layer2-Layer4 minimálně na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/v6 adresa, číslo zdrojového/cílového portu, protokol, číslo VLAN	SPLŇUJE	
16	Nutná podpora 802.1x (včetně RADIUS Change of Authorization) pro řízení přístupu na úrovni portů (integrace s AAA serverem)	SPLŇUJE	
17	Nutná podpora SNMP v2/v3 pro integraci se stávajícím provozním dohledem	SPLŇUJE	
18	Nutná podpora Syslog pro integraci se SIEM	SPLŇUJE	
19	Nutná podpora Netflow pro integraci se SIEM (případně jiný protokol umožňující obdobnou funkcionalitu monitoringu síťových toků)	SPLŇUJE	
20	Nutná podpora IP source guard (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
21	Nutná podpora pro IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) a Multiple Spanning Tree Protocol (MSTP)	SPLŇUJE	
22	Nutná podpora Bridge protocol data unit (BPDU) Guard (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
23	Nutná podpora Spanning Tree Root Guard (STRG) (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
24	Nutná podpora IGMP filtering (případně jiná technologie zajišťující identickou funkcionalitu)	SPLŇUJE	
25	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
26	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
27	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den	SPLNĚNO	

	od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware		
--	------------------------------------------------------------------------	--	--

1 kus přepínače 48x 10/100/1000

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Uplink porty	4x 10G SFP+	
2	Access porty	48x 10/100/1000 RJ-45	
3	Nutná plná kompatibilita stohování (IRF) se stávajícími prvky HP 5800-24G Switch (P/N: JC100A)	SPLŇUJE	
4	Kapacita směrování / přepínání	256 Gbps	
5	Latence (64-byte pakety)	max. 5 µs	
6	Wirespeed na všech portech	SPLŇUJE	
7	Tabulka MAC adres pro 32000 záznamů	SPLŇUJE	
8	Počet podporovaných VLAN	4096	
9	Nutná podpora pro MAC-based VLAN	SPLŇUJE	
10	Nutná podpora pro IP subnet-based VLAN	SPLŇUJE	
11	Nutná podpora směrování RIP, OSPF a OSPFv3, IS-IS pro IPv4 i IPv6	SPLŇUJE	
12	Nutná podpora směrování BGP4 a BGP4+	SPLŇUJE	
13	Nutná podpora vytváření ACL a klasifikace toků na Layer2-Layer4 minimálně na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/v6 adresa, číslo zdrojového/cílového portu, protokol, číslo VLAN	SPLŇUJE	
14	Nutná podpora 802.1x (včetně RADIUS Change of Authorization) pro řízení přístupu na úrovni portů (integrace s AAA serverem)	SPLŇUJE	
15	Nutná podpora SNMP v2/v3 pro integraci se stávajícím provozním dohledem	SPLŇUJE	
16	Nutná podpora Syslog pro integraci se SIEM	SPLŇUJE	
17	Nutná podpora Netflow pro integraci se SIEM (případně jiný protokol umožňující obdobnou funkcionality monitoringu síťových toků)	SPLŇUJE	
18	Nutná podpora IP source guard (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
19	Nutná podpora pro IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) a Multiple Spanning Tree Protocol (MSTP)	SPLŇUJE	
20	Nutná podpora Bridge protocol data unit (BPDU) Guard (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
21	Nutná podpora Spanning Tree Root Guard (STRG) (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
22	Nutná podpora IGMP filtering (případně jiná technologie zajišťující identickou funkcionality)	SPLŇUJE	
23	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
24	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
25	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

Délky a počty DAC kabelů

Číslo	Druh a rozměr kabelu	Požadované množství	Splněno Ano/Ne
1	DAC kabel, 3m	16 ks	

1.12 Technická specifikace opatření ID5 Rozšíření dostupnosti technologické vrstvy

Jedná se o pořízení síťových karet stávajících databázových a aplikačních serverů IBM.

Kompletní dodávka zahrnuje:

4 kusy síťových karet pro systém IBM x3690 X5

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	A148 Emulex 10GbE Integrated Virtual Fabric Adapter II for IBM System x Half x8 PCIe	PN: 49Y7940	
2	Záruka min. 5 let	SPLŇUJE	

4 kusy síťových karet pro systém IBM x3850 X5

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	A18Z Emulex 10GbE Virtual Fabric Adapter II for IBM System x	PN: 49Y7950	
2	Záruka min. 5 let	SPLŇUJE	

Délky a počty DAC kabelů

Číslo	Druh a rozměr kabelu	Požadované množství	Splněno Ano/Ne
1	Passive SFP+ DAC Cable včetně SFP+ modulů, 3m	16 ks	

1.13 Technická specifikace opatření ID6 Monitoring bezdrátové části přístupové vrstvy sítě

Níže uvedené technické specifikace uvádějí parametry SW modulu pro sledování bezdrátové části přístupové vrstvy sítě LAN, které jsou zamýšleny jako rozšíření stávajícího systému provozního dohledu.

Toto SW rozšíření bude plně integrováno do stávajícího nástroje (HP iMC Standard Edition Software Platform, P/N: JG747AAE, 100 nodes) pro provozní dohled síťové infrastruktury.

Je požadovaná kompatibilita s plánovaným opatřením ID3 Přístupové body bezdrátové části přístupové vrstvy sítě, tedy schopnost monitorovat dodávané přístupové body bezdrátové sítě a jejich řídicí prvky.

Kompletní dodávka zahrnuje:

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Zásuvný modul do management nástroje výrobce pro správu drátové sítě výrobce (integrována správa drátové a bezdrátové sítě z jediné aplikace)	SPLŇUJE	
2	Správa přístupových bodů a kontrolérů	SPLŇUJE	
3	Počet spravovaných bezdrátových přístupových bodů	200	
4	Grafické statistické přehledy o vytížení sítě - počet klientů, distribuce v pásmech, propustnost atd.	SPLŇUJE	
5	Možnost vytváření a aplikace nových SSID profilů na skupiny bezdrátových přístupových bodů	SPLŇUJE	
6	Topologie bezdrátové sítě a mapa pokrytí	SPLŇUJE	
7	Lokalizace koncových stanic a jejich statistiky (úroveň signálu, MAC adresa apod.)	SPLŇUJE	
8	Historie roamingu pro jednotlivé stanice	SPLŇUJE	
9	Podpora plánování pokrytí a vykreslení frekvenčního pásma	SPLŇUJE	
10	Podpora vizualizace výsledků spektrální analýzy WiFi pásma	SPLŇUJE	
11	Vizualizace spektrální analýzy musí umožňovat minimálně: přehled spektra v reálném čase, spektrogram se záznamem vývoje v časovém intervalu a pracovní cyklus rušení	SPLŇUJE	
12	Wireless intrusion detection včetně vyhledání neoprávněných bezdrátových přístupových bodů a zjištění portu, do kterého jsou připojeny	SPLŇUJE	
13	Reporting	SPLŇUJE	
14	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
15	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
16	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

1.14 Technická specifikace opatření ID7 Ochrana síťového perimetru

Níže uvedené technické specifikace uvádějí parametry řešení, které je zamýšleno jako ochrana síťového perimetru.

Dvojice HW NGFW (Next-Generation Firewall) bude instalována jako vysoce dostupné řešení dle níže uvedené specifikace. Vlastní zařízení budou umístěna v oddělených, datově propojených lokalitách, a budou propojena do funkčního, vysoce dostupného clusteru, umožňujícího výměnu konfiguračních a stavových informací pro režimy provozu aktivní - aktivní a aktivní - záložní.

Součástí řešení bude také centrální management, logovací a reportovací nástroj, instalovaný samostatně jako virtuální appliance pro VMware, který bude s řešením NGFW plně integrován.

Kompletní dodávka zahrnuje:

2 kusy HW NGFW

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	HW appliance NGFW/UTM firewall s montáží do racku	SPLŇUJE	
2	HW akcelerované sloty 10GE	2 x 10G SFP+	
3	HW akcelerované sloty 1GE	16x 1GE SFP	
4	HW akcelerované sloty porty 1GE	16x 10/100/1000 RJ45	
5	Management porty	2x GE RJ45	
6	Konzolový port pro management	SPLŇUJE	
7	HW akcelerované architektura (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, apod.)	SPLŇUJE	
8	Možnost doplnit druhý napájecí zdroj (interní nebo externí), nebo zařízení vybavené dvěma zdroji	SPLŇUJE	
9	Podpora režimu vysoké dostupnosti (režim L2 cluster, tedy využití virtuálních MAC adres. Celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-active (A/A) a active-passive (A/P).	SPLŇUJE	
10	Integrovaný disk (nerotační technologie) min. 250 GB pro lokální ukládání logů v případě výpadku centrálního log serveru	SPLŇUJE	
11	Celková propustnost firewall min. 30 Gbps (měřeno na UDP paketech 64B pro IPv4 a IPv6)	SPLŇUJE	
12	Vložená latence firewallu nepřesahuje 3 μs (měřeno na UDP paketech 64B)	SPLŇUJE	
13	Počet nově navázaných TCP spojení za sekundu	250.000	
14	Celkový počet současných TCP spojení firewallu	10.000.000	
15	Podpora SSL dekrypce/SSL inspekce s propustností (TLS 1.2/AES256-SHA, měřeno v kombinaci s IPS kontrolou)	3,5 Gbps	
16	Funkce IPSEC VPN ✓ podpora site-to-site VPN ✓ podpora klientských VPN ✓ dostupnost VPN klienta pro koncové stanice (Windows, MacOS) ✓ funkce klientských IPsec VPN bez omezení počtu uživatelů	SPLŇUJE	
17	Minimální počet IPSEC VPN tunelů typu lokalita-lokalita	2.000	
18	Minimální počet klientských IPSEC VPN tunelů	10.000	
19	Propustnost IPsec VPN (měřeno při AES 256)	20 Gbps	
20	Funkce SSL VPN - podpora klientského i bezklientského (portálového) režimu		
21	Minimální počet současně navázaných SSL VPN tunelů	5.000	
22	Minimální propustnost SSL VPN	3 Gbps	
23	Podpora RADIUS protokolu	SPLŇUJE	
24	Funkce kategorizace webových stránek ✓ založená na centrálně spravované databázi výrobce ✓ možnost definice vlastních kategorií ✓ možnost definice vlastních seznamů zakázaných URL ✓ kategorizace musí zahrnovat i české a slovenské internetové	SPLŇUJE	

	stránky		
25	Funkce detekce aplikací na L7 (Application Control) <ul style="list-style-type: none"> ✓ detekce známých aplikací na základě signatur ✓ signatury automaticky aktualizované výrobcem ✓ alespoň 2.000 podporovaných aplikací ✓ možnost tvorby vlastních signatur ✓ detekované aplikace je možné: povolit, monitorovat, blokovat ✓ na základě typu aplikace je možné omezit šířku pásma pro danou aplikaci ✓ funkce Application Control se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům 	SPLŇUJE	
26	Funkce detekce a potlačení narušení (IPS/IDS) <ul style="list-style-type: none"> ✓ signatury automaticky aktualizované výrobcem ✓ alespoň 5.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem ✓ možnost tvorby vlastních signatur ✓ funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům 	SPLŇUJE	
27	Propustnost NGFW = IPS + Application Control (Enterprise Traffic Mix)	5 Gbps	
28	Funkce antivirové kontroly <ul style="list-style-type: none"> ✓ ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem ✓ signatury automaticky aktualizované výrobcem ✓ AV kontrolu lze rozšířit o inspekci tzv. Sandbox technikou, poskytovanou formou služby dodávané výrobcem FW nebo formou lokální HW appliance stejného výrobce ✓ funkce AV kontroly se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům 	SPLŇUJE	
29	Propustnost IPS + Application Control + Anti-Malware, (Enterprise Traffic Mix)	3 Gbps	
30	Funkce ochrany před únikem citlivých informací (DLP) <ul style="list-style-type: none"> ✓ možnost analýzy běžných typů dokumentů a protokolů ✓ možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a kontroly typu file checksum 	SPLŇUJE	
31	Podpora routovacích protokolů RIP, OSPF, BGP	SPLŇUJE	
32	podpora funkce explicit proxy	SPLŇUJE	
33	Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatele na terminálovém serveru	SPLŇUJE	
34	Možnost definice FW pravidel v tzv. NGFW režimu (tj. možnost definice pravidel pomocí aplikační vrstvy, názvů jednotlivých aplikací či jejich funkcionalit bez nutnosti aplikace specifikovat pomocí informací L3/L4 vrstvy)	SPLŇUJE	
35	Nutná podpora VLAN	1000	
36	Nutná podpora LACP	SPLŇUJE	
37	Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.	SPLŇUJE	
38	Podpora řízení přístupu ke konfiguračnímu rozhraní dle rolí pro různé skupiny administrátorů (RBAC)	SPLŇUJE	
39	Počet virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)	10	
40	FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici	SPLŇUJE	
41	Jediné management rozhraní pro celý cluster (jakákoliv změna je mezi jednotlivými členy clusteru synchronizována automaticky)	SPLŇUJE	
42	Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě HP iMC	SPLŇUJE	
43	Podpora otevřeného API (možnost integrace vybraných funkcí do	SPLŇUJE	

	stávající management infrastruktury)		
44	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
45	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
46	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

1 kus dedikovaný management, logovací a reportovací nástroj

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	VM appliance pro platformu VMware vSphere	SPLŇUJE	
2	Nástroj pro správu od stejného výrobce jako NGFW	SPLŇUJE	
3	Nutná plná integrace s FW řešením, včetně obousměrné komunikace (tj. logy uložené na logserveru musí být možné prohlížet přímo z management rozhraní firewallu)	SPLŇUJE	
4	Možnost detailního prohledávání logů	SPLŇUJE	
5	Přehled o aktuálním stavu FW clusteru a událostí formou widgetů s podporou funkce DrillDown	SPLŇUJE	
6	Široká nabídka předpřipravených reportů (bezpečnostní incidenty, využití konektivity, navštěvované kategorie stránek, apod.)	SPLŇUJE	
7	Možnost tvorby vlastních detailních reportů	SPLŇUJE	
8	Podpora vyhodnocování událostí a upozornění na ně (email, snmp trap)	SPLŇUJE	
9	Podpora multi-tenantního prostředí (tj. oddělené rozhraní na management/log/reporting)	SPLŇUJE	
10	Podpora pro ukládání logů	100 GB	
11	Denní objem přijatých logů	1 GB / den	
12	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
13	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
14	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

1.15 Technická specifikace opatření ID8 Ochrana před DDoS útoky

Níže uvedené technické specifikace uvádějí parametry řešení, které je zamýšleno jako ochrana před DDoS útoky.

Dvojice HW DDoS zařízení dle níže uvedené specifikace bude nasazena na primární i sekundární Internetovou konektivitu.

Součástí řešení bude také služba výrobce tzv. IP reputační databáze, která bude pravidelně aktualizována po dobu min. 5 let.

Kompletní dodávka zahrnuje:

2 kusy HW DDoS

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	HW appliance s montáží do racku	SPLŇUJE	
2	Porty 1GE	8x 1G RJ45/SFP	
3	Integrovaný bypass na ethernetových portech jako ochrana před nedostupností sítě při výpadku DDoS sondy	SPLŇUJE	
4	Nezávislý management interface	2x 1GE RJ45	
5	Správa přes HTTPS a SSH	SPLŇUJE	
6	Datová propustnost mixovaného provozu	2,6 Gbps	
7	Paketová propustnost	3,6 Mpps	
8	Maximální doba mitigace útoku od jeho rozpoznání	3 s	
9	Maximální latence paketu	60 μs	
10	Pravidelně aktualizovaná IP reputační databáze	SPLŇUJE	

11	Schopnost naučení se provozu a vygenerování hraničních hodnot pro zabránění útoku	SPLŇUJE	
12	Heuristická analýza	SPLŇUJE	
13	Ochrana proti tzv. zero-day útokům	SPLŇUJE	
14	Možnost oddělení hraničních hodnot pro mitigaci na základě vstupního/výstupního páru rozhraní anebo cílového subnetu	SPLŇUJE	
15	Identifikace a mitigace útoků na 3, 4 a 7 vrstvách OSI	SPLŇUJE	
16	Ochrana před L3 flood útoky (source, destination) anti-spoofing a podpora geolokace	SPLŇUJE	
17	Ochrana před L4 útoky (TCP, UDP, ICMP)	SPLŇUJE	
18	Ochrana před SYN Attack, Slowloris, Connection floods	SPLŇUJE	
19	Ochrana před L7 útoky (HTTP)	SPLŇUJE	
20	Ochrana před útoky založenými na DNS (DNS Flood)	SPLŇUJE	
21	Podpora black/white listů	SPLŇUJE	
22	Podpora REST API	SPLŇUJE	
23	Podpora logování přes syslog, snmp	SPLŇUJE	
24	Statistiky provozu sondy v podobě grafů, logů a podrobných reportů týkajících se konkrétních vrstev a protokolů	SPLŇUJE	
25	Možnost rozdělení administrátorských rolí	SPLŇUJE	
26	Možnost použití k ověření administrátora vzdálený server – LDAP, RADIUS	SPLŇUJE	
27	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
28	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
29	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

1.16 Technická specifikace opatření ID9 Řízení přístupu k síťovým prostředkům

Níže uvedené technické specifikace uvádějí parametry řešení, které je zamýšleno pro řízení přístupu k síťovým prostředkům.

Dedikované HW zařízení se specializovaným programovým vybavením bude nasazeno jako náhrada stávajícího Cisco Secure ACS, který již není výrobcem podporován.

Systém pro řízení přístupu k síťovým prvkům je kritickým bodem celé infrastruktury a musí být zvolen s ohledem na dosažení maximální kompatibility se stávající infrastrukturou a nově plánovanými technickými opatřeními:

- Řízení přístupu stávajících Cisco IP telefonů v rámci drátové i bezdrátové přístupové sítě (618 IP telefonů typu CP7921, CP7925, CP8821 využívající autentizaci pomocí protokolu EAP-FAST)
- Integrace s plánovaným technickým opatřením ID2 Přepínače přístupové vrstvy sítě
- Integrace s plánovaným technickým opatřením ID3 Přístupové body bezdrátové části přístupové vrstvy sítě

Kompletní dodávka zahrnuje:

1 kus HW appliance

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Dedikovaná HW appliance s montáží do racku max. 2U	SPLŇUJE	
2	Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síťovým prvkům definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, lokalita apod.)	SPLŇUJE	
3	Minimální počet současných spojení (připojitelných a spravovaných koncových zařízení) daných HW omezením (kapacitní strop HW appliance)	7500	
4	Minimální počet požadovaných (licencovaných) koncových zařízení	500	
5	Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity	SPLŇUJE	

6	Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	SPLŇUJE	
7	Poskytuje AAA funkce	SPLŇUJE	
8	RADIUS pro autentizaci, autorizaci, zaznamenávání	SPLŇUJE	
9	Proxy funkce pro externí RADIUS	SPLŇUJE	
10	Podpora pro protokoly PAP, MS-CHAP, MS-CHAPv2	SPLŇUJE	
11	Podpora TACACS+ pro centrální řízení administrativního přístupu na zařízení	SPLŇUJE	
12	Podporované databáze uživatelů (s možností definovat pořadí průchodu) ✓ Interní ✓ více nezávislých Active Directory ✓ LDAP (RFC 2251) ✓ RADIUS Token identity source (RFC 2865) ✓ RSA RADIUS token server	SPLŇUJE	
13	- Ověření uživatelů heslem	SPLŇUJE	
14	Řízení přístupu k síťovým prvkům pomocí pravidel, založených na kombinacích následujících parametrů: ✓ uživatele (role, skupiny) v podporovaných databázích ✓ atributy uživatele v podporovaných databázích ✓ typ síťového zařízení (přepínač, směrovač, atd.)	SPLŇUJE	
15	Možnost definovat „per command“ autorizaci pro TACACS+ přístup	SPLŇUJE	
16	Zaznamenávání aktivity uživatelů připojených k síťovým prvkům	SPLŇUJE	
17	Dotazovací systém, korelace záznamů, centralizované výkazy	SPLŇUJE	
18	Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází)	SPLŇUJE	
19	Otevřené API pro podporu propojení se zařízeními třetích stran	SPLŇUJE	
20	Centralizovaná správa – definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	SPLŇUJE	
21	Grafické rozhraní pro definici pravidel přístupu k síťovým prvkům	SPLŇUJE	
22	Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	SPLŇUJE	
23	Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	SPLŇUJE	
24	Zaznamenávání událostí na externí syslog server	SPLŇUJE	
25	Podpora SNMPv3	SPLŇUJE	
26	NTP pro synchronizaci času	SPLŇUJE	
27	SMTP pro zasílání zpráv a výstrah přes e-mail	SPLŇUJE	
28	Možnost licenčního rozšíření na plnohodnotný Policy server (NAC, profiler, BYOD, guest přístup, šifrování L2, atd.) prostým dokoupením SW licence.	SPLŇUJE	
29	Záruka a podpora výrobce na min. 5 let	SPLNĚNO	
30	Garantovaná doba odezvy na nahlášené vady bude do 4 hodin od okamžiku oznámení vady nebo výzvy k výměně vadného zařízení	SPLNĚNO	
31	Odstranění nahlášené vady a obnovení funkce zařízení nebo výměna vadného zařízení bude provedena nejpozději následující pracovní den od okamžiku oznámení vady nebo učinění výzvy k výměně vadného hardware	SPLNĚNO	

1.17 Technická specifikace opatření ID10 Zaznamenávání a řízení bezpečnostních událostí a incidentů.

Níže uvedené požadavky a technické specifikace uvádějí parametry pro implementaci opatření na zaznamenávání a řízení bezpečnostních událostí a incidentů, které bude realizováno dodávkou technologického řešení „Security Information and Event Management“ (dále jen SIEM).

V rámci realizace opatření se jedná o pořízení jediného jednotného řešení, které kombinuje funkcionality tří nástrojů – SIEM, Log manager a nástroj na skenování zranitelností ICT prostředí (dále jen SIEM). Tato kombinace je mandatorní a zadavatel díky ní realizuje výraznou úsporu nákladů. Systém bude provozován samostatně a nezávisle na stávající infrastruktuře zadavatele a dodávka „core“ infrastruktury bude z důvodu dostatečného výkonu realizovaná formou HW řešení. Bude-li to nutné a vhodné, mohou doplňkové systémy navrhovaného řešení (např. vrstva sběru událostí) využít prostředků virtuálního prostředí datového centra KHK. Řešení bude dodáno jako ucelená platforma pro sběr a vyhodnocování bezpečnostních událostí a podporu

následného hlášení kybernetického bezpečnostního incidentu dle § 7 a § 8 zákona č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů.

1.17.1 Obecné požadavky na SIEM

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Řešení SIEM bude dodáno jako all-in-one appliance s možností snadného škálování (rozšiřitelnosti)	SPLŇUJE	
2	Řešení kombinuje minimálně funkcionalitu tří nástrojů – SIEM, Log manager a nástroj na skenování zranitelnosti ICT prostředí	SPLŇUJE	
3	Všechny komponenty systému SIEM jsou dostupné v českém nebo anglickém jazyce.	SPLŇUJE	
4	Systém musí umožňovat provoz v režimu vysoké dostupnosti tak, aby nedošlo ke ztrátě sbíraných Log záznamů v případě výpadku některé komponenty. Tato funkcionalita musí být zajištěna automaticky.	SPLŇUJE	
5	Systém umožňuje zasílání log záznamů do více lokalit najednou; zároveň musí poskytovat možnost automatického zasílání logů do sekundárního umístění, pokud je primární lokalita nedostupná.	SPLŇUJE	
6	Všechny komponenty a požadované funkce se spravují a využívají přes společnou řídicí konzoli (dále jen „Centrální správa“), která je přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím prohlížeče Internet Exploreru 10 a novějších a Chrome.	SPLŇUJE	
7	Centrální správa systému SIEM musí podporovat GUI a skriptovací nástroje.	SPLŇUJE	
8	Veškerá konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů atd. musí probíhat z grafického rozhraní systému SIEM.	SPLŇUJE	
9	Správa uživatelů systému SIEM musí být integrovatelná s aktuálním IDM zadavatele (Identity Management FAMA+ od spol. Tesco SW a.s) a Microsoft Active Directory. Rozsah integrace s IDM bude upřesněn v rámci zpracování detailní analýzy a prováděcího projektu.	SPLŇUJE	
10	Systém SIEM musí rovněž umožňovat přihlašování pomocí lokálních účtů.	SPLŇUJE	
11	Přístup uživatelů musí být založen na volně definovaných oddělených rolích s možností granularního přidělování práv v rámci role podle zdrojů logů, skupiny zařízení, jednotlivých serverů, typu logu apod.	SPLŇUJE	
12	Systém SIEM musí vyhledávat dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech v uložených lozích a v auditních lozích systému.	SPLŇUJE	
13	Systém SIEM musí zaznamenávat vlastní auditní logy po nastavitelnou dobu a musí být chráněny proti modifikaci.	SPLŇUJE	
14	Systém SIEM musí poskytovat informace při vlastním běhu a vyhodnocování logů.	SPLŇUJE	
15	Systém SIEM podporuje monitorování vlastní dostupnosti a jeho jednotlivých částí (zařízení) prostřednictvím SNMP v2/v3 nebo logováním na vzdálený syslog server.	SPLŇUJE	
16	Systém SIEM musí poskytovat funkcionalitu pro behaviorální analýzu uživatelů a musí být integrováno přímo s řešením SIEM.	SPLŇUJE	
17	Behaviorální analýza uživatelů musí využívat machine learning	SPLŇUJE	
18	Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel).	SPLŇUJE	
19	Systém musí obsahovat plně integrovaný nástroj pro řízení celého životního cyklu incidentu, který podporuje nezávislé fronty.	SPLŇUJE	
20	Systém umožňuje komunikaci se systémy třetích stran – standardizované API, SDK (software development kit), nadstavbové aplikace rozšiřující funkčnost, podpora skriptování.	SPLŇUJE	
21	V rámci předání dokumentace konečného provedení dodavatel předá zadavateli standardizované API	SPLŇUJE	
22	Nabízené řešení musí poskytovat automatické upozornění na dostupné aktualizace řešení, jejich stažení a implementaci bez pomoci	SPLŇUJE	

	profesionálních služeb dodavatele/výrobce.		
--	--------------------------------------------	--	--

1.17.2 Požadavky na výkonost, škálovatelnost

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Systém SIEM musí mít srozumitelně a prokazatelně deklarované vedení licenční politiky a to včetně uvedení funkcionalit, které nejsou součástí základní licence, u kterých bude uvedeno, zda a za jakých podmínek je možné je dokupovat. Orientační ceny v Kč bez DPH budou součástí nabídky.	SPLŇUJE	
2	Licence pro zpracování min 1 500 EPS (events per second) s možností rozšíření bez nutnosti HW upgrade až na 5 000 EPS.	SPLŇUJE	
3	Licence pro zpracování min 25 000 FPM (flow per minute) s možností rozšíření bez nutnosti HW upgrade až na 85 000 FPM.	SPLŇUJE	
4	Systém SIEM musí mít garantovanou licenci pro zpracování min. 5 000 EPS v denních špičkách.	SPLŇUJE	
5	Komponenta sbírající logy, musí být schopna trvale zpracovávat 5 000 EPS bez jakýchkoliv výkonostních nebo licenčních omezení.	SPLŇUJE	
6	Systém SIEM musí být schopný nárazově (minimálně po dobu 72 hodin) zpracovat 5 000 EPS, bez jakýchkoliv výkonostních nebo licenčních omezení, včetně zachování plné funkcionality u všech komponent.	SPLŇUJE	
7	Systém SIEM musí splňovat, aby nedocházelo k zahození událostí (events) při dočasném překročení licence.	SPLŇUJE	
8	Minimální kapacita interního úložného prostoru: ✓ Systém SIEM musí umožnit interně uložit log záznamy (RAW formát) po dobu min. 12 měsíců ✓ Systém SIEM musí umožnit interně uchovat normalizované log záznamy po dobu min. 12 měsíců	SPLŇUJE	
9	Systém SIEM musí umožňovat rozšiřování kapacity a výkonu formou distribuce zátěže na více samostatných systémů např. více Logserverů s jedním centrálním místem pro vyhodnocování (event management).	SPLŇUJE	
10	Systém SIEM musí podporovat současnou práci min. 10 uživatelů	SPLŇUJE	
11	Licence musí obsahovat možnost minimálně 500 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje, atd.)	SPLŇUJE	
12	Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů a vlastních custom logů	SPLŇUJE	

1.17.3 Požadavky na sběr dat

Vrstva sběru logů musí splňovat následující požadavky

Číslo	Požadovaná funkcionalita	Minimální požadavky	Splněno Ano/Ne
1	Musí být funkční samostatně bez centrálního prvku	SPLŇUJE	
2	Musí pokrýt čas výpadku SIEM pro dočasné uložení logů bez jejich ztráty	SPLŇUJE	
3	Nesmí nijak zasahovat do sbíraných systémů a sběr logů musí probíhat vzdáleně pro všechny zdroje (bezagentový sběr logů bez instalace agenta na cílový systém)	SPLŇUJE	
4	Musí podporovat (sbírat, zpracovat a interpretovat) minimálně následující typy logů a protokolů: Syslog, SNMP Trap v2/v3, jedno a víceřádkové textové logy (včetně "custom logs"), Windows Event Logs (včetně "custom Event logs"), agentless Windows, ODBC (logy v DB tabulkách), sdee, ftp, ssh, scp, http, sftp, nfs, cifs, file, xml, cef, netflow v5 a v9	SPLŇUJE	
5	Musí podporovat sběr událostí ze síťových zařízení a jejich parsování za účelem identifikace útoku na L3 a L2 vrstvu (minimálně Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard)	SPLŇUJE	

6	Musí podporovat načítání log souborů, kde tyto soubory budou mít stanovenou strukturu a význam dat	SPLŇUJE	
7	Musí podporovat načítání logů z databáze (zejména MS SQL, Postgres SQL, Oracle, atd), kde tyto logy budou mít stanovenou strukturu a význam dat	SPLŇUJE	
8	Musí umožňovat načtení a zpracování jakýchkoli typů logů, i z vlastních aplikací, tato možnost musí být k dispozici bez součinnosti výrobce nebo dodavatele řešení. Kvalita výstupu a možnosti využití musí být stejné jako v případě standardně podporovaného zdroje logů	SPLŇUJE	
9	Minimální administrace (výběr zařízení ze seznamu od výrobce) pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače Cisco a HP, FortiNet)	SPLŇUJE	
10	Automatické připojení zařízení výrobců Cisco a HP	SPLŇUJE	
11	Podpora sběru síťových toků (NetFlow, JFlow, Sflow) z infrastrukturních prvků (switche, routery, NetFlow sondy)	SPLŇUJE	
12	Komponenta sbírající logy je posílá dále zašifrované a komprimované a umožňuje regulovat šířku užívaného pásma.	SPLŇUJE	

1.17.4 Požadavky na archivaci a ukládání

Systém SIEM musí umožňovat:

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Interně uchovat data bez ztráty informací, tzv. RAW logy (bez filtrace, normalizace, redukce) po dobu minimálně 12 měsíců	SPLŇUJE	
2	Interně uchovat normalizované log záznamy po dobu minimálně 12 měsíců	SPLŇUJE	
3	Diskové pole musí být odolné vůči výpadku minimálně dvou mechanik pevných disků.	SPLŇUJE	
4	Ukládání dat v komprimované podobě pro úsporu diskové kapacity	SPLŇUJE	
5	Ukládání dat bez nutnosti RDBMS systémů a s možností vytváření „databázového schématu“ ad-hoc „live“ při tvorbě dotazu	SPLŇUJE	
6	Automaticky archivovat a zálohovat RAW logy podle nastavených požadavků	SPLŇUJE	
7	Systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu	SPLŇUJE	
8	Systém musí umožňovat rychlou obnovu uložených logů pro případ obnovy systému po eventuální havárii	SPLŇUJE	
9	Systém musí poskytovat mechanismus detekce neautorizovaných změn dat v souborech systému SIEM	SPLŇUJE	
10	Zajištění autenticity a integrity archivačních souborů (např. digitálním podpisem apod.)	SPLŇUJE	
11	Systém SIEM musí splňovat některou z mezinárodních certifikací, které garantují bezpečné a nezpochybnitelné ukládání logů	SPLŇUJE	
12	Možnost filtrování událostí před archivací	SPLŇUJE	
13	Podpora nezávislého a neomezeně velkého úložného prostoru pro data (lokální disky, externí pole, apod.)	SPLŇUJE	
14	Ukládání všech dat bez jakýchkoliv změn v původním tvaru po libovolně dlouhou dobu, bude-li dostupná disková kapacita. Archiv může být uložen na externím diskovém úložišti, ale k datům musí být vždy okamžitý přístup bez nutnosti zpětného importu	SPLŇUJE	
15	Systém musí podporovat pravidelné automatické přesuny dat z interního do externího úložiště resp. archivu podle definovaných pravidel	SPLŇUJE	

1.17.5 Požadavky na zpracování událostí

Systém SIEM musí umožňovat:

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
-------	--------------------------	---------------------	----------------

1	Používání regulárních výrazů na straně agentů (pokud budou využity) i serveru systému SIEM	SPLŇUJE	
2	Normalizaci bezpečnostních událostí v systému SIEM do jednotného formátu (centrální logy musí mít stejný formát ze všech zdrojů) a doplnění o další detailní informace (např. doplnění jména uživatele na základě uživatelského účtu apod.).	SPLŇUJE	
3	Kategorizaci logů, která poskytuje univerzální taxonomii nezávislou na výrobci zdroje události, aby bylo možné homogenně vyhledávat, reportovat nebo porovnávat události z různých zařízení bez nutnosti znalosti konkrétního logu	SPLŇUJE	
4	Vyhodnocovat i vlastní provozní logy	SPLŇUJE	
5	Zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem.	SPLŇUJE	
6	Export a import pravidel i log parserů.	SPLŇUJE	
7	Definování / přidávání vlastních korelačních pravidel a log parserů bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů	SPLŇUJE	
8	Real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému)	SPLŇUJE	
9	Korelaci událostí dávkově importovaných do systému SIEM tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů.	SPLŇUJE	
10	Automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací	SPLŇUJE	
11	Vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat)	SPLŇUJE	
12	Agregace událostí v systému SIEM do jedné události po definovaném čase	SPLŇUJE	
13	Ukládání logů v systému SIEM ve tvaru ve kterém je možné jejich prohledávání tj. minimálně musí poskytovat vyhledávání na základě regulárních nebo logických výrazů podle času a klíčových slov	SPLŇUJE	
14	Na jakoukoliv událost musí být možné navázat automatickou akci: ✓ notifikaci přes mail s možností definovat pravidla pro zaslání na různé adresy podle kritičnosti, zdroje apod. ✓ spuštění externího skriptu	SPLŇUJE	
15	Musí poskytovat zabudovanou "security knowledge" tj. předdefinovaná pravidla rozpoznávání a zpracování událostí a jejich pravidelné aktualizace od výrobce, minimálně 1x měsíčně. Musí obsahovat minimálně: ✓ generické politiky ✓ generické korelační pravidla ✓ generické předdefinované reporty, pokud budou k dispozici ✓ předdefinované analytické nástroje a akce pro identifikaci hrozeb a obranu vůči nim	SPLŇUJE	
16	Musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí: ✓ útoky robotů, červů a virů (chyby antivirů) ✓ útoky typu DoS, DDoS ✓ monitorování databází (chyby a varování, přístupy do DB, konfigurace) ✓ neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace) ✓ chyby a změny v sítích (chyby a stavy síťových zařízení) ✓ monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma)	SPLŇUJE	

	<ul style="list-style-type: none"> ✓ VPN útoky (chyby při ověřování, změny konfigurace, aktivita připojování) ✓ uchvácení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla, změny konfigurace) 		
Detekce změn nastavení			
17	<p>SIEM automaticky vygeneruje varování (alert) při detekci zásadních událostí, mezi které bude patřit minimálně (nejen):</p> <ul style="list-style-type: none"> ✓ Změna politiky (konfigurace) na bezpečnostním síťovém zařízení typu firewall, IDS, IPS, apod. ✓ Změna politiky (konfigurace) na síťovém zařízení typu switch, router, AP, apod. ✓ Změna group politiky (GPO) v doménové struktuře Active Directory ✓ Uživatel je zablokován účet v doméně vlivem nesprávného zadání hesla ✓ Uživatel s administrátorským oprávněním je odblokován účet v doméně po jeho předchozím zablokování vlivem nesprávného zadání hesla ✓ Uživatel zadá špatně heslo N-krát během časového intervalu M (detekce pokusu o brute-force útok) ✓ Uživatel zadá špatně heslo N-krát během časového intervalu M a následuje úspěšné přihlášení uživatele (detekce úspěšného brute-force útoku – prolomení hesla) ✓ Z jedné stanice je zaznamenána sekvence pokusů o přihlášení se na N systémů během časového intervalu M (podezření na infekci malwarem) ✓ Vznik Domain Security Group nebo Local Security Group ✓ Zánik Domain Security Group nebo Local Security Group ✓ Vznik členství uživatele v Domain Security Group nebo Local Security Group ✓ Zánik členství uživatele v Domain Security Group nebo Local Security Group ✓ Změna oprávnění existujícího uživatelského účtu ✓ Změna oprávnění existující skupiny uživatelských účtů ✓ Změny nastavení auditingu (rozsahu auditingu) ✓ Přístup administrátora do systému pod univerzálním generickým účtem (administrator, admin, root). <p>Konkrétní rozsah událostí a detaily alertů budou upřesněny v detailní analýze a prováděcím projektu.</p>	SPLŇUJE	
Detekce šíření malware			
18	SIEM bude schopen detekovat existenci a šíření malware	SPLŇUJE	
19	Detekce malware musí pracovat s historií chování a reagovat na nové podněty v reálném čase	SPLŇUJE	
20	<p>SIEM automaticky vygeneruje varování (alert) při detekci zásadních událostí, mezi které bude patřit minimálně (nejen):</p> <ul style="list-style-type: none"> ✓ Nezvyklý nárůst událostí informujících o přístupu přes perimetr na porty a hosty, na které není definovaná politika a oproti minulosti se jedná o významnou změnu v běžném profilu síťového provozu. ✓ Nezvykle vysoký počet událostí související se síťovým objektem (zdroj nebo cíl), který má: <ul style="list-style-type: none"> ○ v dostupných reputačních databázích na Internetu skóre „high risk“ nebo ○ je veden interně jako aktivum s významným skóre „High priority“ nebo ○ má vazbu na internetové destinaci, která je vedena na blacklistech jako „malicious site“ <p>Konkrétní rozsah událostí a detaily alertů budou upřesněny v detailní analýze a prováděcím projektu.</p>	SPLŇUJE	
Monitoring virtualizačního prostředí			
21	SIEM bude monitorovat a detekovat anomální aktivity virtualizační platformy. Jako datový vstup poslouží logy ze stávajících systémů VMware.	SPLŇUJE	

22	SIEM automaticky vygeneruje varování (alert) při detekci zásadních událostí, mezi které bude patřit minimálně (nejen): ✓ Manipulace s virtuální instancí stroje – kopírování, mazání, přesun, ✓ Pokus o přihlášení uživatele na ESX server v lock-down režimu, ačkoliv oficiální cesta je přes VMware vCenter ✓ Shutdown nebo reboot důležité komponenty virtuální platformy Konkrétní rozsah událostí a detaily alertů budou upřesněny v detailní analýze a prováděcím projektu.	SPLŇUJE	
Monitoring vzdáleného VPN přístupu			
23	SIEM automaticky vygeneruje varování (alert) při detekci zásadních událostí, mezi které bude patřit minimálně (nejen): ✓ Neoprávněný přístup uživatele přes VPN, který není na seznamu oprávněných uživatelů (řízení vzdáleného VPN přístupu). ✓ Pokus o neoprávněný přístup uživatele na zařízení v interní síti, které není na seznamu zařízení, na které má daný uživatel mít přístup. Konkrétní rozsah událostí a detaily alertů budou upřesněny v detailní analýze a prováděcím projektu.	SPLŇUJE	

1.17.6 Požadavky na reporting a interpretaci dat

Číslo	Požadovaná funkcionality	Minimální požadavky	Splněno Ano/Ne
1	Předdefinované reporty a informační panely (dashboards) systému SIEM a musí být modifikovatelné uživatelem v GUI.	SPLŇUJE	
2	Uživatel může vytvářet vlastní dashboards a reporty	SPLŇUJE	
3	Systém SIEM musí poskytovat reporty i ve formě grafů a tabulek.	SPLŇUJE	
4	Systém SIEM vytváří reporty ve formátech PDF, HTML, XLS a CSV, popř. dalších.	SPLŇUJE	
5	Systém SIEM musí umožňovat export dat minimálně ve formátu XML, PDF nebo CSV.	SPLŇUJE	
6	Systém SIEM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.	SPLŇUJE	
7	Systém SIEM musí umožňovat vyhledávání zadáním ad-hoc dotazu do vyhledávacího pole pomocí vyhledávacího jazyka. Dotaz může být tvořen manuálně přímo ve vyhledávacím poli nebo s využitím „průvodce“ (wizzardu)		
8	Systém musí poskytovat report o aktivitách vybraných uživatelů resp. skupiny uživatelů.	SPLŇUJE	
9	Systém SIEM musí mít optimalizovanou databázi logů pro rychlé prohledávání a reportování (indexace).	SPLŇUJE	
10	Systém SIEM musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzv. raw-message.	SPLŇUJE	
11	Systém SIEM musí poskytovat pro každého uživatele vlastní personalizovaný dashboard.	SPLŇUJE	
12	Systém SIEM musí umožňovat přiřazení incidentů různým řešitelům.	SPLŇUJE	
13	Drill-down analýza v GUI tj. od obecnějších informací vedou linky na konkrétnější informace (např. z reportu o počtu bezpečnostních událostí podle jednotlivých typů OS je možné na jeden klik dostat report o počtu bezpečnostních událostí na jednotlivých hostech s daným operačním systémem a dále pokračovat na report o počtu bezpečnostních událostí v jednotlivých aplikacích / lozích / zdrojů na daném hostu apod.).	SPLŇUJE	
14	Systém musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	SPLŇUJE	
15	Systém SIEM musí podporovat grafickou interpretaci vzorků standardního a nestandardního chování (včetně real-time režimu).	SPLŇUJE	
16	Systém SIEM zajistí podporu pro ohlašovací povinnost bezpečnostních incidentů NÚKIB podle zákona č. 181/2014 Sb., o kybernetické	SPLŇUJE	

	bezpečnosti a vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, příloha č. 5 až č. 7.		
--	-------------------------------------------------------------------------------------------	--	--

1.17.7 Požadavky na implementaci

A. Rozsah implementace

Implementace SIEM do prostředí zadavatele bude zahájena na základě akceptovaného a předaného prováděcího projektu.

Při implementaci budou v rámci realizace do SIEM napojena „Primární aktiva“, kterými jsou významné informační systémy Krajského úřadu Královéhradeckého kraje (VIS). Dále budou napojena „Podpůrná aktiva“, kterými jsou prvky IT infrastruktury, která pro VIS zajišťuje jak jejich provozní dostupnost, tak přístup uživatelů včetně důvěrnosti a integrity informací.

Primární aktiva

Dle Vyhlášky č. 317/2014 Sb. (Vyhláška o významných informačních systémech a jejich určujících kritériích) se jedná o následující významné informační systémy:

- 1) Spisová služba EZOP
- 2) Ekonomický informační systém

Podpůrná aktiva

- 1) Aktivní síťové prvky:
 - a) Aktivní síťové prvky dodávané v rámci jednotlivých technických opatření realizované veřejné zakázky „Bezpečnostní infrastruktura a rozvoj TCK – dodavatel technických opatření včetně servisní podpory“, zejména
 - ✓ ID2 Přepínače přístupové vrstvy sítě
 - ✓ ID3 Přístupové body bezdrátové části přístupové vrstvy sítě
 - ✓ ID4 Rozšířená přepínačů v agregační vrstvě sítě
 - ✓ ID7 Ochrana síťového perimetru
 - ✓ ID8 Ochrana před DDoS útoky
 - ✓ ID9 Řízení přístupu k síťovým prostředkům
 - b) Aktivní síťové prvky stávající síťové infrastruktury, které nebudou nahrazeny v rámci realizace veřejné zakázky. Bližší informace viz Popis stávající infrastruktury v kap. 2 Požadavky na kompatibilitu dodávaných technologií.
- 2) Ostatní prvky.
 - a) Autentizace a autorizace uživatelů (MS Active Directory, Identity Management FAMA+)
 - b) Databázové systémy (MS SQL)
 - c) Monitoring HP IMC
 - d) Operační systémy Windows
 - e) Virtualizační vrstva VMware

Podrobný rozsah napojených podpůrných aktiv (aktivních síťových prvků a ostatních prvků) bude specifikován a odsouhlasen v rámci zpracování detailní analýzy a prováděcího projektu.

B. Předpokládaný další rozvoj

V rámci rozvoje se předpokládá rozšíření počtu VIS jejich napojení do SIEM řešení případně napojení dalších informačních systémů provozovaných KÚ KHK.

1.18 Technická specifikace opatření ID11 Optický propoj přístupové a páteřní vrstvy sítě

Níže uvedené technické specifikace uvádějí parametry řešení pro realizaci optického propojení.

Jedná se o výměnu stávajícího optického MM spoje mezi přepínačem přístupové vrstvy sítě (umístění v rozvaděči RD08) a přepínačem páteřní vrstvy sítě (umístění v DC2) z důvodu velké vzdálenosti a tím nevyhovujících přenosových parametrů stávajícího MM spoje.

V rámci dodávky a instalace bude optický kabel položen do stávající trasy včetně realizace případných prostupů a protipožárních ucpávek, provedení případných optických svárů a oživení celého spoje. Součástí dodávky je i odpovídající dokumentace a měřicí protokoly přenosových parametrů.

Kompletní dodávka zahrnuje:

Číslo	Požadovaná funkcionality	Minimální požadavky	
1	1x Optický SM kabel s 24 vlákeny o délce 300 m včetně příslušenství pro kompletní realizaci	SPLŇUJE	
2	Záruka min. 5 let	SPLŇUJE	