Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha 3.d Technická specifikace – Část 3

Technické požadavky na serverovou technologii

k Zadávací dokumentaci projektu „Komplexní ochrana celonemocničního informačního systému ONK vůči kybernetickým hrozbám“

Obsah

1. Zkratky a pojmy

(1) Zkratky a pojmy užité v ZD jsou uvedeny v Příloze 3.a. ZD, specifické zkratky a pojmy poplatné zejména této části VZ jsou v následující tabulce.

(2) Jedná se o podpůrnou informaci, kterou Zadavatel poskytuje pro zachování jednoznačného výkladu textu dokumentu.

Zkratka	Význam
EPP	End Point Protection Platform
EDR	Endpoint Detection and Response
SW	Software
HW	Hardware
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name Server
SNMP	Simple Network Management Protocol
VLAN	Virtual Local Area Network
BYOD	Bring Your Own Device
OS	Operační systém
LAN	Local Area Network
VPN	Virtual Private Network
MDM	Mobile device management
CA	Certifikační autorita
PKI	Public Key Infrastructure
NAT	Network Address Translation
HTTPS	Hypertext Trasfer Protocol Secure
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SPF	Sender Policy Framework
DKIM	Domain Key Identified Mail
VRRP	Virtual Router Redundancy Protocol
DHCP	Dynamic Host Configuration Protocol

2. Místo plnění

Oblastní nemocnice Kladno, a.s., nemocnice Středočeského kraje, Vančurova 1548, 272 01 Kladno.

3. Doba plnění

(1) Dodávka bude zahájena po nabytí účinnosti smlouvy a bude řízena milníky uvedenými v tabulce Milníky.

(2) Milníky Fáze A instalace a implementace dle Smlouvy.

Id	Činnosti	Termín
01	Podpis Smlouvy	Zadavatel předpokládá 02. 01. 2024
02	Zahájení realizace projektu	do 01. 04. 2024 (navazuje na Část 1 - Zabezpečovací technologie pro 2 serverovny)
Instalace a implementace technologií		
03	**Zpracování a akceptace Detailního realizačního konceptu** Výstupem bude dokument Detailní realizační koncept Předání dílčího plnění a Akceptace dílčího plnění	do 1 měsíce od zahájení realizace projektu
04	**Dodávka a instalace technologií**	do 2 měsíců od zahájení realizace projektu
05	**Zkušební a testovací provoz, migrace stávajících dat objednatele** Akceptace Testovacího provozu	do 4 měsíců od zahájení realizace projektu
06	**Produkční provoz** Akceptace produkčního provozu, akceptace Fáze A Dodávka licencí Ukončení Fáze A,	do 5 měsíců od zahájení realizace projektu

(3) Fáze B – HW a SW maintenance výrobce technologií a bezpečnostních systémů dle Smlouvy bude zahájena ukončením Fáze A (ukončení projektu akceptací produktivního provozu).

(4) Termín ukončení se může změnit z objektivních příčin, způsobených třetími stranami nebo jinými okolnostmi, nezávislými na vůli smluvních stran.

4. Způsob prokázání splnění požadavků minimálního plnění

(1) Zadavatel požaduje, aby Dodavatelem nabízená dodávka splňovala veškeré dále uvedené požadavky (funkcionality a parametry) a tyto byly zahrnuty v nabídce Dodavatele a v celkové nabídkové ceně.

(2) Dodavatel ve své nabídce jednoznačně deklaruje splnění, popřípadě absenci každého níže uvedených požadavků v tabulkách označených jako „Minimální požadavky …“, a to vyplněním příslušného pole „Splněno“ jedno ze dvou nabízených možností:

„**ANO**“ v případě že dodávka Dodavatele (Nabídka) minimální požadavek **splňuje**

nebo **„NE“** v případě že dodávka Dodavatele (Nabídka) minimální požadavek **nesplňuje**

Zadavatel požaduje po Dodavatelích, aby uvedli informaci o skutečné funkcionalitě nabízeného řešení, kterou bude možné ověřit v testovacím provozu, např. v rámci školení administrátorů.

(3) Nesplnění kteréhokoli ze stanovených minimálních požadavků bude znamenat vyloučení účastníka ze zadávacího řízení.

(4) Tato kapitola 4 platí pro následující kapitoly 5 až 7.

5. Požadavky na jednotlivé položky páteřní infrastruktury

(1) Předmětem této části VZ je dodávka a instalace HW, SW a souvisejících služeb dále specifikovaných v kapitolách 5.1 až 5.7.

5.1. Technická specifikace řízení mailového provozu na perimetru sítě

(1) Perimetrová emailová brána skenuje veškerou příchozí poštu a stává se tak kritickým bezpečnostním prvkem infrastruktury celé organizace.

(2) Systém emailové brány bude plnit především funkci ochrany komunikace v roli mail transfer agenta. Výjimkou je možná definice karanténní oblasti pro zadržené maily čekající na uživatelské rozhodnutí.

(3) Emailová brána bude řešit jak ochranu provozu na úrovni dodržování standardů SMTP protokolu, seznamů spamových serverů a odesílatelů apod., tak i na úrovni obsahu těla mailu ať už při vyhledávání příznaků nevyžádané pošty, nebo přímo i jako další antivirový prvek blokující malware.

(4) Minimální požadavky na technickou specifikaci emailové bezpečnostní brány jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Nasazení v MTA režimu na perimetru sítě, vstupní a výstupní komunikační bod mailového provozu mezi internetem a sítí ONK	ANO
2	Možnost rate limitingu mailového provozu jak na bázi počtu spojení, tak i na bázi počtu zaslaných mailů	ANO
3	Možnost greylistingu	ANO
4	Kontrola compliance SMTP protokolu	ANO
5	Kontrola příchozího spojení na bázi DNS záznamů (existence MX, A, reverzních záznamů)	ANO
6	Použití blacklistů/whitelistů (client IP, sender apod.), buď udržovaný vlastní korpus, nebo napojení na dobře hodnocené blacklisty/whitelisty třetích stran	ANO
7	Možnost udržování vlastního blacklistu/whitelistu, tj. výjimky z přebíraných seznamů	ANO
8	Kontrola SPF	ANO
9	Kontrola DKIM	ANO
10	Napojení na AD jako zdroj seznamu validních příjemců	ANO
11	Odmítání mailu pro neexistující příjemce už na úrovni SMTP protokolu, zamezení backscatteringu	ANO

Id	Požadované parametry	Splněno
12	Aplikace validních ochran také pro odchozí provoz	ANO
13	AS/AV kontrola na bázi jak hlaviček, tak i těla zprávy, tak i příloh	ANO
14	Kontrola obsahu mailů vůči dobře udržované databázi vzorku spamů/malware	ANO
15	Aktualizace AS/AV databází několikrát denně, rychlé zařazení 0-day spamů/útoků	ANO
16	Akce výsledku kontroly definovatelná v kategoriích: – propuštění mailu beze změny, – přidání definované mailové hlavičky s výsledkem kontroly, – úprava Subjectu mailu (vložení definovaného upozornění/kategorie), – zachycení mailu v karanténní oblasti/schránce/změna příjemce, – odmítnutí/zahození mailu.	ANO
17	Podpora obvyklých typů příloh pro AS/AV scan, minimálně textové soubory, rtf, xml, pdf, ms office dokumenty, obrázky (jpg, gif, png), spustitelné soubory	ANO
18	Možnost definice chování pro neznámé/kryptované soubory	ANO
19	Kontrola archivů/komprimovaných příloh	ANO
20	Možnost definice maximální hloubky, velikosti a počtu souborů pro archívy a chování při překročení limitu	ANO
21	Blokace na základě reálného typu souboru, ne pouze jeho názvu	ANO
22	OCR analýza obrázků	ANO
23	Kontrola vložených odkazů dle reputační databáze	ANO
24	Podpora nějaké formy automatizovaného učení pravděpodobnosti spamu (bayesiánské filtry, neuronové sítě apod.)	ANO
25	Možnost správy vlastní karanténní oblasti pro uživatele, přístup přes jednoduché webové GUI	ANO
26	Konfigurace a administrace minimálně přes webové GUI	ANO
27	Možnost nasazení v některém z režimů vysoké dostupnosti (Active/Active přes MX, Active/Passive v rámci HA clusteru nad jednou VIP apod.). Řešení vysoké dostupnosti musí z hlediska administrace sdílet nastavení a informace pro správu mailového provozu (logy, databázi apod.) nezávisle na uzlu, na kterém se administrace provádí.	ANO
28	Schopnost zpracovat alespoň 2000 mailů za hodinu	ANO
29	Podpora SNMP (alespoň v2c) pro poskytování provozních údajů a statistik mailové komunikace	ANO
30	Podpora logování do centrálního syslog serveru	ANO
31	Provozní licence alespoň pro 900 uživatelů	ANO
32	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.2. Technická specifikace zavedení segmentace sítě

(1) Pro zajištění vysoké dostupnosti služeb datového centra, respektive zvýšení dostupnosti a bezpečnosti informačních aktiv, je požadována obměna páteřních prvků, které představují výchozí bránu celé přepínané sítě organizace. Do těchto páteřních přepínačů jsou také připojeny stávající servery a datová úložiště. S ohledem na požadavky dalších vysokorychlostních portů určených pro modernizované datové centrum, při nutnosti zajištění redundance nových síťových prvků, bude vybudována nová páteřní vrstva. Stávající páteřní prvky budou doplněny o další přepínače. Páteřní a distribuční vrstva sítě bude umístěna ve 2 lokalitách, viz popis topologie v Příloze 3.a. V každé lokalitě bude instalován stoh páteřních a stoh distribučních přepínačů. Každý stoh páteřních přepínačů bude sestaven ze 2 přepínačů propojených dvěma 100Gbps spoji. Je preferováno v rámci stohu oddělení control plane přepínačů a sdílení data plane. Žadatel preferuje řešení, které nebude závislé na jednom výrobci. Stoh distribučních přepínačů bude sestaven z minimálně dvou přepínačů propojených 40Gbps, nebo 50Gbps spoji. Stohy páteřních a distribučních přepínačů budou propojeny agregovanými spoji sestavenými z minimálně dvou 25Gbps spojů. Přístupové přepínače budou připojeny do distribučních přepínačů agregovanými porty sestavenými ze dvou 10Gbps spojů. Obě lokality a jejich páteřní stohy budou propojeny agregovanými spoji sestavenými ze 100Gbps spojů.

(2) Z důvodu zachování úrovně přehledu jsou technické požadavky rozděleny do 4 následujících podkapitol 5.2.1 až 5.2.4.

5.2.1. Technická specifikace datové síťové infrastruktury

(1) Z důvodu zajištění vysoké dostupnosti datových služeb a zvýšení kybernetické bezpečnosti je požadováno dodání 4 ks páteřních 25 Gigabit Ethernet síťových přepínačů (2 stohy sestávající ze 2 ks přepínačů), 6 ks distribučních 10 Gigabit Ethernet síťových přepínačů a 81 ks 48-portových a 32 ks 24-portových 1Gigabit Ethernet přístupových přepínačů pro komunikaci aplikací a zajištění dostupnosti v případě výpadku.

(2) Minimální požadavky na technickou specifikaci síťových přepínačů jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
4 ks Páteřních síťových přepínačů		
1	Typ zařízení: L3 přepínač	ANO
2	Velikost zařízení: 1U	ANO
3	Minimálně 26x 1/10/25Gbps portů (volitelné fyzické rozhraní)	ANO
4	Minimálně 4x 40/100Gbps portů (volitelné fyzické rozhraní)	ANO
5	2x interní hot-swap AC napájecí zdroj	ANO
6	Redundantní hot-swap ventilátory	ANO
7	Směr proudění vzduchu zařízením: front-back	ANO
8	Maximální hloubka přepínače: 41 cm	ANO
9	Přepínací výkon: min. 2 Tbps	ANO
10	Forwarding rate: min. 1100 Mpps	ANO
11	Podpora rozdělení 40GE portů na 4x10GE a 100GE portů na 4x25GE	ANO
12	Podporovaný počet přepínačů ve stohu: 2	ANO
13	Kapacita stohovacího propojení: min. 400 Gbps	ANO

Id	Požadované parametry	Splněno
14	Podpora seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multi-Chassis LAG)	ANO
15	Podpora upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade)	ANO
16	Minimální počet aktivních VLAN: 4000	ANO
17	Minimální počet záznamů v tabulce MAC adres: 210 000	ANO
18	Minimální počet záznamů v tabulce ARP: 140 000	ANO
19	Podpora jumbo rámců včetně velikosti 9198 Byte	ANO
20	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
21	Minimální počet IPv4 záznamů ve směrovací tabulce: 600 000	ANO
22	Minimální počet IPv6 záznamů ve směrovací tabulce: 600 000	ANO
23	Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP	ANO
24	Podpora policy based routing	ANO
25	Podpora VRRPv2 a VRRPv3	ANO
26	Podpora virtuálních směrovacích instancí (VRF): min. 256	ANO
27	Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP	ANO
28	IGMP v2 a v3, IGMP snooping	ANO
29	Hardware podpora IPv4 a IPv6 ACL	ANO
30	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
31	Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace	ANO
32	Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace	ANO
33	Port security-omezení počtu MAC adres na port, statické MAC, sticky MAC	ANO
34	BPDU guard a Root guard	ANO
35	Podpora RADIUS CoA (RFC3576)	ANO
36	Podpora Radius over TLS (RadSec)	ANO
37	Podpora static a dynamic VXLAN s využitím BGP-EVPN	ANO
38	Podpora PBR VXLAN	ANO
39	Podpora Group based policy pro VXLAN (VXLAN GBP)	ANO
40	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ANO
41	Podpora Data Center Bridging (PFC 802.1Qbb, ETS 802.1Qaz)	ANO
42	IP Explicit Congestion Notification (ECN)	ANO
43	OOB management formou portu RJ45 s podporou ethernetu	ANO
44	CLI formou 1x USB-C console port	ANO
45	USB port pro přenos konfigurace a firmware	ANO
46	Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient	ANO

Id	Požadované parametry	Splněno
47	Podpora RSA s délkou klíče minimálně 4096 bitů	ANO
48	Podpora SNMPv2c a SNMPv3	ANO
49	Duální image-podpora dvou nezávislých verzí operačního systému	ANO
50	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů	ANO
51	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby	ANO
52	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	ANO
53	Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)	ANO
54	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování	ANO
55	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ANO
56	Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress	ANO
57	Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů	ANO
58	Podpora Cloud i On-Premise management software výrobce zařízení	ANO
59	Podpora Zero Touch Provisioning (ZTP)	ANO
60	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ANO
61	Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 20 GB	ANO
62	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO
63	Software aktualizace v minimální délce 60 měsíců.	ANO
64	Řešení musí být kompatibilní se stávajícími přepínači Aruba 6300M (JL658A)	ANO
6 ks Distribučních síťových přepínačů		
1	Typ zařízení: L3 přepínač	ANO
2	Velikost zařízení: 1U	ANO
3	Minimálně 24x SFP+ portů (volitelné fyzické rozhraní)	ANO
4	Minimálně 4x 50Gbps portů (volitelné fyzické rozhraní)	ANO
5	2x interní hot-swap AC napájecí zdroj	ANO
6	Redundantní hot-swap ventilátory	ANO
7	Maximální hloubka přepínače: 41 cm	ANO
8	Přepínací výkon: min. 880 Gbps	ANO
9	Forwarding rate: min. 850 Mpps	ANO
10	Minimální paketový buffer: 8 MB	ANO
11	Podporovaný počet přepínačů ve stohu: min.10	ANO
12	Podpora stohu na delší vzdálenost (min.100m)	ANO
13	Kapacita stohovacího propojení: 200 Gbps	ANO
14	Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)	ANO
15	Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)	ANO
16	Minimální počet aktivních VLAN: 4000	ANO
17	Minimální počet záznamů v tabulce MAC adres: 30 000	ANO

Id	Požadované parametry	Splněno
18	Minimální počet záznamů v tabulce ARP: 45 000	ANO
19	Podpora jumbo rámců včetně velikosti 9198 Byte	ANO
20	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
21	Minimální počet IPv4 záznamů ve směrovací tabulce: 60 000	ANO
22	Minimální počet IPv6 záznamů ve směrovací tabulce: 60 000	ANO
23	Podpora linkové agregace IEEE 802.1AX	ANO
24	Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ANO
25	Minimální počet LACP skupin/linek ve skupině: 256/16	ANO
26	IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w	ANO
27	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ANO
28	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
29	Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace	ANO
30	Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace	ANO
31	Port security-omezení počtu MAC adres na port, statické MAC, sticky MAC	ANO
32	Podpora RADIUS CoA (RFC3576)	ANO
33	Podpora Radius over TLS (RadSec)	ANO
34	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
35	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	ANO
36	Podpora LLDP-MED	ANO
37	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
38	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ANO
39	TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO
40	BPDU guard a Root guard	ANO
41	Statické směrování IPv4 a IPv6	ANO
42	Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP	ANO
43	OOB management formou portu RJ45 s podporou ethernetu	ANO
44	Podpora police based routing	ANO
45	Podpora VRRPv2 a VRRPv3	ANO
46	IGMP v2 a v3, IGMP snooping	ANO
47	ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4	ANO
48	DHCP snooping pro IPv4 a IPv6	ANO
49	Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM	ANO
50	Hardware podpora IPv4 a IPv6 ACL včetně podpory object group pro IP adresy a porty	ANO
51	ACL definice na základě skupiny fyzických portů	ANO
52	IN a OUT ACL aplikovatelný na interface, LAG, VLAN	ANO
53	CLI formou 1x USB-C console port	ANO
54	USB port pro přenos konfigurace a firmware	ANO
55	Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient	ANO
56	Podpora RSA s délkou klíče minimálně 4096 bitů	ANO

Id	Požadované parametry	Splněno
57	Podpora SNMPv2c a SNMPv3	ANO
58	Duální image-podpora dvou nezávislých verzí operačního systému	ANO
59	Podpora aktualizací běžícího software bez nutnosti restartovat systém – hot patching	ANO
60	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby	ANO
61	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů	ANO
62	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	ANO
63	Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)	ANO
64	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování	ANO
65	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ANO
66	Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress	ANO
67	Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů	ANO
68	Podpora Cloud i On-Premise management software výrobce zařízení	ANO
69	Podpora Zero Touch Provisioning (ZTP)	ANO
70	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ANO
71	Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 30 GB	ANO
72	Záruka garantovaná výrobcem na výměnu hardware NBD v délce 60 měsíců.	ANO
73	Software aktualizace v minimální délce 60 měsíců.	ANO
81 ks Přístupových síťových přepínačů		
1	Typ zařízení: L3 přepínač	ANO
2	Velikost zařízení: 1U	ANO
3	Počet 10/100/1000Mbit/s metalických portů:48	ANO
4	Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 4	ANO
5	Interní AC napájecí zdroj	ANO
6	Dostupný výkon pro PoE+ napájení:	ANO
7	Maximální hloubka přepínače: 33 cm	ANO
8	Podpora PoE přes kabely Cat3	ANO
9	Podpora PoE+ dle standardu 802.3at	ANO
9	Dostupný výkon pro PoE+ napájení: 370 W	ANO
10	Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ANO
11	Podpora Energy Efficient Ethernet (802.3az)	ANO
12	Přepínací výkon: min. 176 Gbps	ANO
13	Forwarding rate: min. 130 Mpps	ANO
14	Minimální paketový buffer: 8 MB	ANO
15	Podporovaný počet přepínačů ve stohu: min.8	ANO
16	Podpora stohu na delší vzdálenost (min.100 m)	ANO
17	Kapacita stohovacího propojení: 80 Gbps	ANO
18	Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)	ANO

Id	Požadované parametry	Splněno
19	Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)	ANO
20	Minimální počet aktivních VLAN: 4000	ANO
21	Minimální počet záznamů v tabulce MAC adres: 16 000	ANO
22	Minimální počet záznamů v tabulce ARP: 8 000	ANO
23	Podpora jumbo rámců včetně velikosti 9198 Byte	ANO
24	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
25	Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000	ANO
26	Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000	ANO
27	Podpora linkové agregace IEEE 802.1AX	ANO
28	Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ANO
29	Minimální počet LACP skupin/linek ve skupině: 32/8	ANO
30	IEEE 802.1s-Multiple Spanning Tree a IEEE 802.1w	ANO
31	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ANO
32	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
33	Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace	ANO
34	Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace	ANO
35	Port security-omezení počtu MAC adres na port, statické MAC, sticky MAC	ANO
36	Podpora RADIUS CoA (RFC3576)	ANO
37	Podpora Radius over TLS (RadSec)	ANO
38	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
39	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	ANO
40	Podpora LLDP-MED	ANO
41	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
42	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ANO
43	TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO
44	BPDU guard a Root guard	ANO
45	Statické směrování IPv4 a IPv6	ANO
46	Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3	ANO
47	Podpora VRRPv2 a VRRPv3	ANO
48	IGMP v2 a v3, IGMP snooping	ANO
49	ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4	ANO
50	DHCP snooping pro IPv4 a IPv6	ANO
51	Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM	ANO
52	Hardware podpora IPv4 a IPv6 ACL včetně podpory object group pro IP adresy a porty	ANO
53	ACL definice na základě skupiny fyzických portů	ANO
54	IN a OUT ACL aplikovatelný na interface, LAG, VLAN	ANO
55	OOB management formou portu RJ45 s podporou ethernetu	ANO
56	CLI formou 1x USB-C console port	ANO
57	USB port pro přenos konfigurace a firmware	ANO

Id	Požadované parametry	Splněno
58	Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient	ANO
59	Podpora RSA s délkou klíče minimálně 4096 bitů	ANO
60	Podpora SNMPv2c a SNMPv3	ANO
61	Duální image-podpora dvou nezávislých verzí operačního systému	ANO
62	Podpora aktualizací běžícího software bez nutnosti restartovat systém – hot patching	ANO
63	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby	ANO
64	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů	ANO
65	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	ANO
66	Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)	ANO
67	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování	ANO
68	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ANO
69	Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress	ANO
70	Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů	ANO
71	Podpora Cloud i On-Premise management software výrobce zařízení	ANO
72	Podpora Zero Touch Provisioning (ZTP)	ANO
73	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ANO
74	Software aktualizace v minimální délce 60 měsíců.	ANO
	32 ks Přístupových síťových přepínačů	
1	Typ zařízení: L3 přepínač	ANO
2	Velikost zařízení: 1U	ANO
3	Počet 10/100/1000Mbit/s metalických portů:24	ANO
4	Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 4	ANO
5	Interní AC napájecí zdroj	ANO
6	Dostupný výkon pro PoE+ napájení:	ANO
7	Maximální hloubka přepínače: 33 cm	ANO
8	Podpora PoE přes kabely Cat3	ANO
9	Podpora PoE+ dle standardu 802.3at	ANO
9	Dostupný výkon pro PoE+ napájení: 370 W	ANO
10	Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ANO
11	Podpora Energy Efficient Ethernet (802.3az)	ANO
12	Přepínací výkon: min. 128 Gbps	ANO
13	Forwarding rate: min. 90 Mpps	ANO
14	Minimální paketový buffer: 8 MB	ANO
15	Podporovaný počet přepínačů ve stohu: min.8	ANO
16	Podpora stohu na delší vzdálenost (min.100 m)	ANO
17	Kapacita stohovacího propojení: 80 Gbps	ANO
18	Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)	ANO
19	Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)	ANO

Id	Požadované parametry	Splněno
20	Minimální počet aktivních VLAN: 4000	ANO
21	Minimální počet záznamů v tabulce MAC adres: 16 000	ANO
22	Minimální počet záznamů v tabulce ARP: 8 000	ANO
23	Podpora jumbo rámců včetně velikosti 9198 Byte	ANO
24	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
25	Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000	ANO
26	Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000	ANO
27	Podpora linkové agregace IEEE 802.1AX	ANO
28	Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ANO
29	Minimální počet LACP skupin/linek ve skupině: 32/8	ANO
30	IEEE 802.1s-Multiple Spanning Tree a IEEE 802.1w	ANO
31	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ANO
32	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
33	Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace	ANO
34	Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace	ANO
35	Port security-omezení počtu MAC adres na port, statické MAC, sticky MAC	ANO
36	Podpora RADIUS CoA (RFC3576)	ANO
37	Podpora Radius over TLS (RadSec)	ANO
38	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ANO
39	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	ANO
40	Podpora LLDP-MED	ANO
41	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)	ANO
42	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ANO
43	TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO
44	BPDU guard a Root guard	ANO
45	Statické směrování IPv4 a IPv6	ANO
46	Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3	ANO
47	Podpora VRRPv2 a VRRPv3	ANO
48	IGMP v2 a v3, IGMP snooping	ANO
49	ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4	ANO
50	DHCP snooping pro IPv4 a IPv6	ANO
51	Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM	ANO
52	Hardware podpora IPv4 a IPv6 ACL včetně podpory object group pro IP adresy a porty	ANO
53	ACL definice na základě skupiny fyzických portů	ANO
54	IN a OUT ACL aplikovatelný na interface, LAG, VLAN	ANO
55	OOB management formou portu RJ45 s podporou ethernetu	ANO
56	CLI formou 1x USB-C console port	ANO
57	USB port pro přenos konfigurace a firmware	ANO
58	Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient	ANO

Id	Požadované parametry	Splněno
59	Podpora RSA s délkou klíče minimálně 4096 bitů	ANO
60	Podpora SNMPv2c a SNMPv3	ANO
61	Duální image-podpora dvou nezávislých verzí operačního systému	ANO
62	Podpora aktualizací běžícího software bez nutnosti restartovat systém – hot patching	ANO
63	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby	ANO
64	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů	ANO
65	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	ANO
66	Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)	ANO
67	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování	ANO
68	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ANO
69	Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress	ANO
70	Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů	ANO
71	Podpora Cloud i On-Premise management software výrobce zařízení	ANO
72	Podpora Zero Touch Provisioning (ZTP)	ANO
73	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ANO
74	Software aktualizace v minimální délce 60 měsíců.	ANO

5.2.2. Technická specifikace bezdrátové síťové infrastruktury

(1) Z důvodu modernizace a zajištění zabezpečení bezdrátové sítě s požadavkem na vysokou dostupnost datových služeb je požadováno dodání 50 ks bezdrátových přístupových bodů a 2 ks fyzických bezdrátových kontrolérů, určených pro řízení a zabezpečení bezdrátové sítě.

(2) Minimální požadavky na technickou specifikaci požadovaných komponent jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
	50 ks Bezdrátových přístupových bodů	
1	Indoor přístupový bod	ANO
2	Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax	ANO
3	Certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED 6E™ a WPA3™-Enterprise	ANO
4	Pracovní režim AP bez kontroléru (autonomní)	ANO
5	Pracovní režim AP řízené kontrolérem (lightweight)	ANO
6	Pracovní režim AP v roli kontroléru s možností správy až 120 AP	ANO
7	Minimální počet portů ethernet LAN: 2x 100/1000/2500 Mbit/s RJ45	ANO
8	Podpora multigigabit ethernet 2.5 Gbps IEEE 802.3bz na všech portech	ANO
9	Podpora standardů IEEE 802.3at (PoE+) a IEEE 802.3bt	ANO
9	Podpora linkové agregace LACP	ANO
10	Bezvýpadkový (hitless) PoE failover mezi ethernetovými porty	ANO
11	Podpora standardního PoE+ IEEE 802.3at 30W bez nutnosti redukce výkonu libovolného rádia	ANO
12	Podpora napájení z AC napájecího zdroje	ANO
13	Rozsah provozních teplot 0° až +50°C bez redukce vysílacího výkonu nebo omezení funkcí	ANO

Id	Požadované parametry	Splněno
14	Ochrana proti přehřátí - vestavěný teplotní senzor, který automaticky krátkodobě vypne AP	ANO
15	Vestavěná interní anténa MIMO, omni down-tilt	ANO
16	Radiová část: tri-band, současná podpora pásem 2,4GHz 5GHz a 6GHz	ANO
17	Minimální MIMO a počet spatial stream: 2x2:2	ANO
18	Podpora TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	ANO
19	Podpora DL-OFDMA a UL-OFDMA	ANO
20	Možnost nastavení vysílacího výkonu s krokem 0.5 dBm	ANO
21	Max data rate: 2400 Mbit/s pro 6GHz, 1200 Mbit/s pro 5GHz a 287 Mbit/s pro 2,4GHz	ANO
22	Minimálně 16 vysílaných BSSID na rádio	ANO
23	Nastavitelný DTIM interval pro jednotlivé SSID	ANO
24	Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ANO
25	Integrovaný TPM pro bezpečné uložení certifikátů	ANO
26	Podpora WPA3-CNSA, WPA3-SAE, OWE	ANO
27	Podpora 802.11ac explicitního beamformingu	ANO
28	Podpora airtime fairness	ANO
29	Prioritizace jednotlivých SSID na základě vysílacího času	ANO
30	USB port s podporou 3G/4G USB modemu jako WAN uplink	ANO
31	Vypínatelné indikační LED diody informující o stavu zařízení	ANO
32	Prioritizace 6GHz a 5GHz pásma – Band Steering či obdobné	ANO
33	Podpora automatická detekce Rogue AP	ANO
34	Mapování SSID do různých VLAN podle IEEE 802.1Q	ANO
35	VLAN Pooling	ANO
36	Podpora Layer-2 izolace bezdrátových klientů	ANO
37	HW podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu)	ANO
38	Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček	ANO
39	DHCP server, směrování a NAT pro bezdrátové klienty	ANO
40	Automatická identifikace připojeného zařízení a jeho operačního systému	ANO
41	Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming	ANO
42	Dynamické vyvažování klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP	ANO
43	Optimalizace provozu: multicast-to-unicast konverze	ANO
44	Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)	ANO
45	Podpora filtrování přístupu na web	ANO
46	Podpora RadSec (RADIUS over TLS)	ANO
47	802.11w ochrana management rámců	ANO
48	Podpora Kensington lock	ANO
49	Podpora MAC a 802.1X autentizace Wi-Fi klientů s využitím lokální databáze v AP	ANO
50	AP se ověřuje před připojením do LAN pomocí 802.1X - podpora PEAP a EAP-TLS suplicant	ANO

Id	Požadované parametry	Splněno
51	Volitelně možnost spravovat AP cloud management nástrojem	ANO
52	CLI formou serial konsole port a serial over bluetooth	ANO
53	SSHv2, SNMPv2c a SNMPv3	ANO
54	Podpora ZTP	ANO
55	Integrované Bluetooth 5.0 Low Energy (BLE) rádio	ANO
56	Integrované Zigbee 802.15.4 rádio	ANO
57	Podpora režimu SLEEP s max. spotřebou energie do 2W	ANO
58	Součástí AP je příslušenství pro montáž na zeď nebo strop	ANO
59	Software aktualizace v minimální délce 60 měsíců.	ANO
2 ks bezdrátových kontrolerů		
1	Bezdrátový kontrolér: HW appliance	ANO
2	Podpora standardu 802.11ax, a zpětná kompatibilita s 802.11a/b/g/n/ac	ANO
3	Specializovaná HW appliance (nepřipouští se virtualizovaný kontrolér)	ANO
4	Velikost: 1U	ANO
5	Napájecí zdroje: 2x interní AC hot-swap	ANO
6	Počet portů 1Gbps: 2	ANO
7	Počet 10Gbps SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 4	ANO
8	Podporovaný počet AP bez nutnosti přidávání hardware: min: 300	ANO
9	Minimální počet současně připojených klientů: min. 9000	ANO
9	Minimální výkon statefull firewallu: 20Gbps	ANO
10	Sdílení licencí mezi více kontrolery	ANO
11	Podpora clusterování kontrolerů v režimech: active-active a active-standby. Výpadek aktivního kontroleru v redundantním páru nemá dopad na provoz již připojených klientů (tj. bez potřeby opětovné autentizace)	ANO
12	Vzdálené lokality - podpora lokálního bridgování uživatelských dat per SSID přímo na příslušném AP, podpora roamingu přes AP na vzdálené lokalitě	ANO
13	Podporované režimy přenosu uživatelských dat: tunelovaní přes kontrolér a lokální AP bridging	ANO
14	Podporta ověření připojení AP ke kontroleru pomocí certifikátu	ANO
15	Minimální počet aktivních VLAN: 4000	ANO
16	Minimální počet záznamů v tabulce MAC adres: 32000	ANO
17	Podpora linkové agregace IEEE 802.3ad	ANO
18	Podpora IEEE 802.1w - Rapid spanning Tree	ANO
19	Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ANO
20	Podpora detekce protilehlého zařízení LLDP	ANO
21	Podpora statického směrování IPv4 a IPv6	ANO
22	Podpora dynamického směrování OSPFv2 včetně podpory stub a NSSA	ANO
23	Podpora Multicast: IGMP a MLD	ANO
24	Podpora nastavení lokálního DHCP serveru pro IPv4 a IPv6	ANO
25	NTP klient pro IPv4 a IPv6 včetně MD5 autentizace	ANO
26	Podpora překladu adres NAT/PAT	ANO
27	VLAN Pooling	ANO
28	Podpora IPv6	ANO

Id	Požadované parametry	Splněno
29	Podporované typy autentizace: WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace, “captive portal”, 802.1X ověření s následným ověřením MAC	ANO
30	Podporované typy autentizace: Enhanced Open (OWE), SAE (Simultaneous Authentication of Equals), WPA3 Enterprise Basic, WPA3-Enterprise SuiteB	ANO
31	Podpora autentizace sdíleným klíčem s možnosti definovat několik různých PSK na jednom SSID (např. Identity PSK)	ANO
32	Podporované autentizační/autorizační zdroje: RADIUS, LDAP, RFC 3576 Change of Authorization	ANO
33	Funkce řízení a ochrany rádiového spektra s automatickou optimalizací sítě (přidělováni kanálů, fast roaming, rozdělení klientů na jednotlivá AP)	ANO
34	Aktivní scanování 802.11 kanálů pro výběr nejlepšího včetně automatického zastavení scanování v případě že probíhá časově senzitivní provoz (např. VoIP)	ANO
35	Klasifikace klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu	ANO
36	Vestavěný “captive portal” pro hosty s podporou nativních IPv6 klientů. s možností úpravy vzhledu a přídáním vlastního loga s, včetně vestavěného rozhraní pro vytváření dočasných guest účtů	ANO
37	Podpora pro 802.11u, 802.11v a 802.11k	ANO
38	Automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI a jejich SLA monitoring	ANO
39	Podporované úrovně oprávnění administrátorů: administrator, read-only, guest-provisoning	ANO
40	Podpora RestAPI pro automatizovanou konfiguraci kontroléru	ANO
41	Automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu	ANO
42	Grafický uživatelský dashboard zobrazující kvalitu a obsazenost kanálů, jednotlivé klienty, náhledy na VoIP přes WiFi síť a zobrazující informace o MOS (mean opinion score) aktivních hovorů. Možnost realtime analýzy kvality prováděných hovorů	ANO
43	Podpora rozpoznávaní aplikací na 7. vrstvě (aplikace typu: Youtube, Facebook, Dropbox, BitTorrent, Skype, Office365, apod.). Možnost jejich povolování, zakazování, prioritizace nebo omezování s možnosti vytvořit minimálně 20 souběžných aplikačních pravidel k omezení provozu konkrétních aplikací.	ANO
44	Centrální správa, aktualizace, konfigurace vč. bezpečnostních politik a QoS profilů pro všechna AP	ANO
45	Blacklist zařízení překračující nastavitelné prahy (opakovaná špatná autentizace, porušení bezpečnostní politiky)	ANO
46	Podpora RadSec (RADIUS over TLS)	ANO
47	Podpora Radius Accounting, roaming klienta mezi AP vyvolá Interim Update	ANO
48	Podpora tvorby bezpečnostních politik na základě časových pravidel	ANO
49	Podpora Bonjour services gateway, zpracování mDNS paketů, možnost filtrování služeb mezi subnety	ANO
50	Podpora L2 a L3 roaming bez nutnosti speciálního SW na klientovi	ANO
51	Podpora bezdrátových MESH sítí s protokolem pro výběr optimální cesty v rámci MESH stromu, podporovaná hloubka min. 8 hopů	ANO
52	Podpora Rogue Wireless detekce a containment	ANO
53	Podpora PKI	ANO
54	Možnost licenčního rozšíření o funkci VPN koncentrátor (SSL a IPsec VPN klienti)	ANO
55	Podpora WIPS pro detekci útoků na bezdrátovou síť	ANO

Id	Požadované parametry	Splněno
56	Spektrální analýza s možností časového záznamu do souboru a přehrávání záznamu	ANO
57	Podpora ochrany pomocí IDS signatur	ANO
58	Podpora wireless containment včetně Tarpitting	ANO
59	CLI formou RJ45 serial konsole port	ANO
60	Ethernet port pro out-of-band management	ANO
61	USB port pro přenos konfigurace a firmware	ANO
62	Podpora Dual boot flash	ANO
63	Podpora SSHv2, SCP a HTTPS web GUI	ANO
64	Podpora SNMPv2c, SNMPv3	ANO
65	Podpora SYSLOG s možností různé úrovně logováni do více syslog serverů	ANO
66	Podpora příjmu a filtrování zpráv z externího SYSLOGu (např. Firewall, IPS) s možností reakce na vybrané zprávy formou ACL nebo Blacklistu WiFi klienta	ANO
67	Podpora monitorování síťového provozu pomocí IPFIX	ANO
68	Integrované diagnostické nástroje: ping, traceroute, AAA test	ANO
69	Nástroj pro odchytávání WLAN datového provozu včetně 802.11 hlaviček a možnost jeho zasílání do Ethernetového analyzátoru	ANO
70	Podpora upgrade firmware pomocí: HTTPS, TFTP, FTP a USB	ANO
71	Podpora Pre-download Image AP s možností definovat konkrétní AP nebo skupinu AP	ANO
72	Plná kompatibilita s nabízenými přístupovými body	ANO
73	Záruka garantovaná výrobcem na výměnu hardware NBD v délce 60 měsíců.	ANO
74	Software aktualizace v minimální délce 60 měsíců.	ANO

5.2.3. Technická specifikace řízení přístupu do sítě

(1) Z důvodu zajištění zabezpečení drátové a bezdrátové sítě s požadavkem na ověření identity uživatele/ zařízení a nastavení přístupových oprávnění pro připojovaná zařízení je požadováno dodání 2 ks zařízení pro řízení přístupu do sítě (NAC).

(2) Minimální požadavky na technickou specifikaci požadovaných komponent jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
2 ks zařízení pro Řízení přístupu do sítě (NAC)		
1	Typ zařízení: virtuální	ANO
2	On premise řešení pro externí captive portál pro hosty a jejich rozšířenou autentizaci a pro BYOD	ANO
3	Appliance bez nutnosti dodatečných licencí	ANO
4	Podpora 802.1X autentizace pro LAN, WLAN a VPN	ANO
5	Podpora minimálně pro 2000 současně autentizovaných zařízení (pomocí 802.1X) s možností vytváření clusterů více virtuálních instancí. Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance. Cluster podporuje active-active režim pro ověřování.	ANO
6	Podpora RADIUS podle RFC3576 (CoA)	ANO

Id	Požadované parametry	Splněno
7	Podpora změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky (např. pro odpojení nebo karanténu koncových zařízení).	ANO
8	Podpora minimálně následujících metod autentizace: PEAP-MSCHAPv2, EAP-TLS, EAP-TEAP, EAP-TTLS, MAC autentizace	ANO
9	Podpora TACACS+ autentizace správců síťových zařízení	ANO
9	Využití dalších možností autentizace a autorizace. Minimálně: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta)	ANO
10	Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v Active Directory	ANO
11	Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období	ANO
12	Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (minimálně AirWatch, Citrix, MobileIron, JAMF)	ANO
13	Podpora REST API pro většinu základních úkonů AAA	ANO
14	Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.)	ANO
15	Podpora zpracování syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně (přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení).	ANO
16	Podpora vytvoření vlastního parseru/integrace syslog hlášení pro možnost uživatelské integrace se systémy třetích stran.	ANO
17	Podpora profilace zařízení na základě sběru dodatečných informací o připojených zařízeních jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.	ANO
18	Platforma obsahuje funkci otestovat autentizační politiky, včetně flexibilní volby typu autentizace, atributů klienta atd.	ANO
19	Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele – omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu.	ANO
20	SW záruka garantovaná výrobcem na výměnu hardware NBD v délce 60 měsíců.	ANO
21	Software aktualizace v minimální délce 60 měsíců.	ANO
22	Řešení musí být kompatibilní se stávajícími přepínači Aruba 6300M (JL658A)	ANO

5.2.4. Technická specifikace příslušenství k síťovým technologiím

(1) K navrženým síťovým technologiím je požadováno dodání transceiverů uvedených v následující tabulce. Zadavatel připouští dodání OEM kompatibilního HW.

(2) Minimální požadavky na technickou specifikaci požadovaných komponent jsou uvedeny v následující tabulce.

Id	Požadované parametry	Slněno
1	4 ks 100G QSFP28 MPO SR4 100 m 12-fiber MMF Transceiver	ANO
2	4 ks 100G QSFP28 LC CWDM4 2 km SMF Transceiver	ANO
3	4 ks 100G QSFP28-QSFP28 3 m DAC Cable	ANO
4	6 ks 50G SFP56 to SFP56 3 m DAC Cable	ANO
5	12 ks 25G SFP28 to SFP28 3 m DAC Cable	ANO
6	4 ks 25G SFP28 LC LR 10 km SMF Transceiver	ANO
7	381 ks 10G SFP+ LC LR 10 km SMF Transceiver	ANO
8	80 ks 25G SFP28 LC SR 100 m MMF Transceiver	ANO
9	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.3. Technická specifikace technologie dvoufaktorové autentizace

(1) Pro zajištění správy a ověřování identit bude zavedena dvoufaktorová autentizace, která bude plnit následující potřeby:

- více faktorové ověření zaměstnance nemocnice do informačních systémů a potřebných zařízení;
- autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb;
- zajištění kvalifikovaného elektronického podpisu, pečetě nebo časového razítka s využitím hybridní čipové karty, která je QSCD ready;
- šifrování dat pomocí certifikátu umístěného na kartě;
- identifikace zaměstnance v bezkontaktních systémech (docházka, zabezpečený tisk, stravování atd.,);
- vizuální identifikace držitele.

(2) Minimální požadavky na technickou specifikaci pro zavedení dvoufaktorové autentizace jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Hybridní čipová karta a ovladače: – Uložení elektronických certifikátů X.509 (a generování / uložení příslušných kryptografických klíčů) budou dodány hybridní čipové karty ve formátu ID-1 (velikost bankovní karty) – Kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací. – 2 000 Bezkontaktních čipů kompatibilních s dodávanou technologií.	ANO
2	Certifikované karty musí být v souladu: – S normou ČSN EN ISO 7816, část 1-4 a – Standardem EN 419 211 a profily: - BSI-CC-PP-0059 - BSI-CC-PP-0075 - BSI-CC-PP-0071 - BSI-CC-PP-0072 - BSI-CC-PP-0076	ANO
3	Vlastnosti kontaktního čipu a PKI aplikace: – Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty	ANO

Id	Požadované parametry	Splněno
	– Privátní klíč uložený na kartě nelze z karty vyexportovat – Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS – Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu. – Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány – Možnost uložení certifikátů různých certifikačních autorit – Generování RSA klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12 – Archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů – Podporované jsou minimálně kryptografické algoritmy: - Symetrické: 3DES, AES - Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. - RSA: 1024, 2048 bitů - Eliptické křivky: P-224, P-256, P-384, P-521 – Zablokování PIN, QPIN resp. PUK po opakovaném chybném zadání PIN, QPIN resp. PUK – Zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů) – Dvoufaktorovou autentizaci na bázi certifikátů X.509 (do PC v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.) – Vytváření elektronického podpisu na bázi certifikátů ve formě: - Kvalifikovaného elektronického podpisu, - Zaručeného elektronického podpisu, - Uznávaného elektronického podpisu a - Jiné formy elektronického podpisu. – Dvoufaktorovou autentizaci na bázi certifikátů X.509 do PC (prostředí Microsoft AD / Smartcard Logon, webových služeb, VPN, aplikací) – Možnost uložení certifikátů třetích stran – Generování a práce s RSA a ECC klíči v čipu – Algoritmy RSA, ECC a SHA-1, SHA-256, 384, 512 – Podpora PIN, QPIN, PUK pro odblokování PIN a QPIN – Hybridní čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů.	
4	Ovládací software karty: Čipové karty budou dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému. Vlastnosti ovládacího software: – Podléhá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší – Podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11 – použití na OS MS Windows 10 nebo vyšších verzích – Případné použití i na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11) – Instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), RPM, DEB – Distribuce ovládacího software přes službu MS Windows Update	ANO
5	Stav dodané karty: – Inicializovaná PKI aplikace s PIN, QPIN a PUK. – Předání seznamu personalizovaných karet, pro import do evidence. U každé karty uvedeno číslo kontaktního čipu.	ANO

Id	Požadované parametry	Splněno
	– Inicializovaná PKI aplikace s iniciálními hodnotami PIN, QPIN a PUK. Technickými prostředky bude vynuceno, aby si uživatel po přijetí karty změnil hodnotu PIN, kterou bude používat pro autorizaci operací kvalifikovaného podpisu.	
6	Bezpečné předání PIN a PUK je v okamžiku vydání karty uživateli zabezpečeno mimo jiné s využitím PIN formuláře a distribuční obálky.	ANO
7	PIN formulář disponuje diskrétní zónou pro bezpečné vytištění hodnot PIN a PUK, a obsahuje grafické instrukce pro správnou manipulaci s diskrétní zónou. Distribuční obálka bude sloužit pro zkompletování připraveného tokenu a PIN formuláře. Po vytištění hodnot PIN a PUK se token společně s PIN formulářem vloží do distribuční obálky. Obálka bude ve standardním tvaru DL v bílém provedení bez dalších dodatečných potisků.	ANO
8	Štítkovací tiskárna pro polepení karty držitelskými údaji	ANO
9	Zjednodušení správy životního cyklu karet a certifikátů	ANO
10	Automatizovaná obnova kvalifikovaných i komerčních certifikátů od externího poskytovatele. Automatizovaná obnova interních certifikátů z doménové CA	ANO
11	Implementace aplikace pro kvalifikované elektronické pečetění dokumentů prostřednictvím čipové karty	ANO
12	Implementace aplikace, které prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu	ANO
13	Implementace aplikace, která anonymizuje údaje o uživatelích, kteří ukončí pracovní poměr	ANO
14	Implementace aplikace, která do dokumentu připojí kvalifikovaný elektronický podpis + pečeť + vodoznak v rámci jednoho kroku	ANO
15	Implementace aplikace pro podporu činností spojených se správou životního cyklu čipových karet a certifikátů, zastřešení registračního místa doménové CA.	ANO
16	Implementace webové aplikace, určené správcům certifikátů. Možnost vyhledávat a prohlížet informace o certifikátech, odvolávat certifikáty, generovat a prohlížet reporty	ANO
17	Implementace nástroje zjednodušení práce s bezpečnostním kódem pro ochranu kvalifikovaných certifikátů	ANO
18	Návrh a implementace architektury hierarchie PKI, zprovoznění PKI v prostředí ONK	ANO
19	Vytvoření podkladů na implementaci šablon pro vydání certifikátů pro autentizaci uživatelů do domény, případně další uživatelské akce.	ANO
20	Předání podkladů na implementaci šablon pro vydání technologických certifikátů	ANO
21	Implementace šablon uživatelských a technologických certifikátů	ANO
22	Vytvoření definice distribučních bodů CRL	ANO
23	Ochrana a uložení klíče CA	ANO
24	Dodání havarijní a provozní dokumentace k vybudované vrstvě PKI	ANO
25	Operační systém pro multifaktorové ověření mobilní aplikací - Android a iOS	ANO
26	Lokalizace aplikace je čeština nebo angličtina	ANO
27	Nutnost podpory multitenantní použití	ANO
28	Požadované metody autentizace: mobilní/SW token s push notifikací, jednorázový autentizační kód (TOTP), SMS s autentizačním kódem	ANO
29	Možnost autentizace biometrickými prvky - otisk prstu (fingerprint), otisk obličeje (face ID)	ANO
30	Možnost zadání PINu pro autentizaci	ANO
31	Aplikace musí mít podporu podezřelého chování, potenciálního nebezpečí a stavu mobilního zařízení: Integrita systému, Integrita aplikace, Instalace z důvěryhodného	ANO

Id	Požadované parametry	Splněno
	zdroje, Runtime manipulace, Detekce překrytí obrazovky, Zámek zařízení, Zabezpečení biometrikou, Root operačního systému	
32	Prostřednictvím QR kódu funkční aktivace mobilní aplikace s identitou uživatele	ANO
33	Mobilní aplikace umožní zaručený elektronický podpis a autorizaci uživatele před podpisem - podpisový certifikát je vydán doménovou certifikační autoritou.	ANO
34	Portál pro uživatele s možností aktivace metody a portál pro administrátora, kde lze vyhledat všechny uživatele s potřebnými informacemi.	ANO
35	Informace z podezřelého chování v rámci mobilního telefonu musí být zobrazeny v náhledu pro administrátora - administrátorská konzole	ANO
36	Autentizace bez použití hesla (passwordless) do operačního systému MS Windows s použitím certifikátu uživatele (certifikát z certifikační autority).	ANO
37	Autentizace bez použití hesla (passwordless) do VPN s použitím certifikátu uživatele pomocí PKI (certifikát z certifikační autority Zadavatele).	ANO
38	Autentizace do interních webových aplikací prostřednictvím standardizovaných federačních protokolů OIDC, SAML2.0, OAuth2	ANO
39	Autentizace do aplikací prostřednictvím standardizovaného protokolu RADIUS	ANO
40	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.4. Technická specifikace technologie pro detekci a reakci na bezpečnostní události EPP a EDR

(1) Pro zajištění koncových stanic bude pořízen systém pro detekci a reakci na bezpečnostní události na uživatelské počítače a možností instalace bezpečnostního řešení i na klientské mobilní zařízení (telefony, tablety)

(2) Řešení bude nabízet možnost centrální správy klientů a v rámci logování a reportingu bezpečnostních incidentů

(3) Minimální požadavky na technickou specifikaci technologie pro detekci a reakci na bezpečnostní události na koncových stanicích jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Řešení musí být postaveno na modulární architektuře, která umožní zapnutí jednotlivých komponent ochrany	ANO
2	Možnost integrace s celou sadou řešení ochrany koncových bodů, jako je AV, DLP atd.	ANO
3	Řešení využívá jiný AV engine než systém pro ochranu síťové bezpečnosti (NGFW)	ANO
4	Klientský software s integrovanou funkci IPSec VPN kompatibilní s VPN koncentrátorem	ANO
5	Software na koncových stanicích nesmí vyžadovat instalaci programů nebo nástrojů s administrativními funkcemi	ANO
6	Software na koncových stanicích nesmí vyžadovat lokální administrátorská práva ke spuštění	ANO
7	Koncoví uživatelé nesmí ovládat a měnit nastavení klienta nebo zásad zabezpečení	ANO
8	Řešení musí mít zabudované kontroly/ochrany, které zabrání koncovým uživatelům provádět změny (odinstalace agenta, zastavit/spustit agenta nebo související služby…)	ANO
9	Podpora "Split tunnelling" (tj. možnost přístupu k Internetu mimo VPN, zatímco interní komunikace je směrována do vpn tunelu)	ANO
10	Podpora připojení VPN v prostředí za NAT zařízeními a bránami firewall, které neumožňují IPSec provoz (možnost tuneloval VPN přes HTTPS)	ANO

Id	Požadované parametry	Splněno
11	Podpora připojení v „hotspot“ prostředí (agent dočasně umožní přístup k captive portálu)	ANO
12	Podpora ověřování VPN pomocí uživatelského jména/hesla, klientského certifikátu, LDAP/AD	ANO
13	Podpora multi-faktorové autentizace VPN	ANO
14	Řešení schopné detekovat a odstranit viry, spyware a další malware na základě kombinace signatur, blokátorů chování a heuristické analýzy	ANO
15	Řešení schopné detekovat a identifikovat přítomnost virů v paměti systému, bootovacích sektorech, tabulkách oddílů a na všech formách dat uložených na pevném disku systému a jiných vyměnitelných médiích	ANO
16	Řešení schopné detekovat a zablokovat pokus o infekci známým malwarem	ANO
17	Koncový software musí informovat uživatele o pokusu infekce malwarem	ANO
18	Řešení schopné detekovat, identifikovat, blokovat a odstranit škodlivé aplikace v reálném čase. Skenování virů s minimálním dopadem na výkon koncové stanice	ANO
19	Uživatel má možnost provést AV kontrolu určitých jednotek, adresářů nebo souborů	ANO
20	Řešení schopné provést nápravná opatření k odstranění virového kódu z infikovaných souborů, zaváděcích sektorů nebo tabulek oddílů	ANO
21	Řešení schopné přesunout neopravený soubor infikovaný virem do karantény na místním pevném disku pro další kontrolu nebo akci	ANO
22	Řešení schopné provést karanténu souborů / procesů	ANO
23	Řešení schopné skenovat nejpopulárnější soubory a přílohy (dokumenty Microsoft Office, komprimované soubory a grafické soubory…)	ANO
24	Řešení schopné automaticky identifikovat vstupní bod malwaru	ANO
25	Řešení odolné proti "evasion" technikám moderního malwaru	ANO
26	Řešení podporuje technologii Content disarm and reconstruction (CDR) – proaktivní extrakce potencionálně škodlivého obsahu, min podpora grafických souborů, MS Office a pdf	ANO
27	Řešení blokuje útoky bez ohledu na to, zda jsou to webové, e-mailové, nebo z vyměnitelného média	ANO
28	Řešení detekuje a blokuje „Command & Control“ komunikaci	ANO
29	Řešení schopné detekovat zero-day útoky, detekcí a odesláním podezřelých souborů do prostředí sandboxu (cloud prostředí nebo lokální emulace)	ANO
30	Řešení podporuje emulaci spustitelných souborů, archivů, dokumentů, Java a flash souborů	ANO
31	Možnost emulovat soubory větší než 20 MB všech podporovaných souborových typů	ANO
32	Řešení chrání proti ransomware	ANO
33	Řešení schopné obnovit soubory při pokusu o zašifrování včetně automatické remediace systému	ANO
34	Řešení schopné rozpoznat post infekční komunikaci s řídícím centrem malware	ANO
35	Řešení schopné blokovat a zadržet soubor před rozšířením na všechny koncové body	ANO
36	Řešení schopné automaticky vygenerovat forenzní zprávu o provedení útoku	ANO
37	Řešení využívá detekci chování a technologie strojového učení pro detekci nových variant malwaru	ANO
38	Řešení schopné ověřit integritu updatu virových signatur před jeho aplikací	ANO
39	Řešení schopné inkrementální updaty virových signatur	ANO
40	Řešení schopné ukládat data do hostitelského zařízení bez přídavného nebo externího zařízení	ANO

Id	Požadované parametry	Splněno
41	Forenzní údaje shromážděné řešením jsou uloženy lokálně na samotném koncovém bodě. Uložená data jsou chráněna před neoprávněným přístupem nebo narušením struktury	ANO
42	Řešení shromažďuje probíhající informace o činnosti operačního systému. Shromážděné informace zahrnují procesní činnost, síťovou komunikaci, změny v registru, přístup k souborovým systémům	ANO
43	Možnost pozdržet download ve webovém prohlížeči	ANO
44	Podporované Internetové prohlížeče MS Edge, Google Chrome, Firefox	ANO
45	Podpora OS koncových stanic min Windows 7 SP1 (32-bit a 64-bit), Windows 10 (32-bit a 64-bit), Windows 11, Windows 2016, Windows 2019, MAC OS 11/12, Debian 10/11, Ubuntu 20/21/22	ANO
46	Podpora integrace s AD	ANO
47	Centrální správa bezpečnostních pravidel a nastavení koncových klientů	ANO
48	Centrální ukládaní logů	ANO
49	Komunikace mezi management serverem a koncovým klientem musí být autentizovaná a šifrovaná	ANO
50	Koncovým klient musí být schopen získat aktualizace signatur virů z centrálního management serveru i z internetu	ANO
51	Výrobce řešení by měl poskytovat aktualizované signatury. Nové signatury by měly být zpřístupněny alespoň jednou denně	ANO
52	Řešení umožňuje vytvořit a spravovat logické skupiny napříč několika funkčními (AD) skupinami	ANO
53	Administrátor schopen řídit politiku na úrovni uživatele a skupiny	ANO
54	Kontrola bezpečnostního stavu připojované stanice na úrovni předepsaných politik	ANO
55	Možnost ověřit „compliance klienta“ (verze OS, název a verze antiviru apod.)	ANO
56	Dashboard poskytuje možnost zobrazení všech souvisejících událostí	ANO
57	Identifikace škodlivé/podezřelé aktivity podle kategorií/přiřazení rizik	ANO
58	Možnost vyhledat infikované stanice podle zvoleného IOC (Indicator of Compromise)	ANO
59	Možnost vyhledávat jednotlivá IOC přes všechny koncové stanice	ANO
60	Možnost spuštění automatické analýzy z detekce incidentu síťového bezpečnostního prvku	ANO
61	Schopnost karantény nebo izolování celého počítače	ANO
62	Možnost generovat agregovaný report, který obsahuje data o koncových bodech a síťová data	ANO
63	Schopnost automaticky generovat podrobný forenzní report z detekovaných incidentů	ANO
64	Automatický report rozsahu vniknutí škodlivého softwaru	ANO
65	Reporty obsahují seznam zasažených souborů/dat v případě útoku	ANO
66	Možnost stažení reportů uživatelem i administrátorem	ANO
67	Řešení poskytuje úplný stromový přehled událostí a útoků	ANO
68	Řešení umožňuje automatizovanou analýzu událostí	ANO
69	Spouštění automatické analýzy od incidentů produktů třetích stran	ANO
70	Zobrazení reputace souboru ve forenzní zprávě	ANO
71	Možnost integrace se SIEM, SOAR - qRadar, ArcSight, Splunk, LogRhytm	ANO
	Ochrana mobilních stanic	
1	Detekce mobilního malwaru	ANO

Id	Požadované parametry	Splněno
2	Řešení schopné chránit proti hrozbám v síťové komunikaci (například SSL stripping, MiTM = Man in the middle apod.)	ANO
3	Řešení schopné chránit před útoky na integritu mobilních operačních systémů	ANO
4	Řešení schopné chránit před známými a neznámými škodlivými aplikacemi	ANO
5	Centrální správa a sledování stavu všech spravovaných zařízení a analýza rizika používaných mobilních aplikací	ANO
6	Možnost white a black listing mobilních aplikací	ANO
7	Detekce „rooting“ a „jailbraking“ zařízení	ANO
8	Uživatel nemůže změnit konfiguraci aplikace	ANO
9	Možnost integrace s MDM / EMM systémy třetích stran.	ANO
10	Řešení nesbírá a nevyužívá žádná privátní uživatelská data (zprávy, emaily, lokace, kontakty, historie…)	ANO
11	Možnost blokovat přístup na nevhodné stránky (URL filtering) podle kategorizace stránek	ANO
12	Řešení schopné detekovat phishing nejen na základě reputace IP/URL, ale také na základě analýzy obsahu stránky	ANO
13	Podpora OS Android a iOS	ANO
14	Podpora zařízení typu BYOD a firemních zařízení	ANO
15	Klient je dostupný v oficiálních obchodech Apple AppStore/Google Play store	ANO
	Licence a podpora	
1	Licence musí pokrýt ochranu 600 koncových stanic + 100mobilních stanic	ANO
2	Přenesení nastavení ze stávajícího prostředí na nový systém	ANO
3	Dokumentace, zaškolení administrátorů zadavatele	ANO
4	Podpora SW, dostupné aktualizace SW a bezpečnostních signatur v délce minimálně 5 let	ANO
5	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení.	ANO

5.5. Technická specifikace technologie pro centrální sběr logů

(1) Zadavatel dosud nemá implementovaný žádný centrální log management systém. Jsou provozovány pouze některé izolované technologie, které sbírají logy ze svých instancí pro své potřeby. Není tedy třeba přihlížet k existující funkcionalitě, nebo zachování investic pro existující technologii.

(2) Je požadováno řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Řešení by mělo využívat výkonnou databázi s velkou kapacitou, rychlým vyhledáváním ve “velkých datech” a okamžitou vizualizací vyžádaných dat.

(3) Minimální požadavky na technickou specifikaci technologie pro centrální sběr logů jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Řešení bude schopné příjmu a zpracování logů z většího množství zdrojů	ANO
2	Logy budou přijímány protokolem SYSLOG ve variantě UDP i TCP přenosu, velikost zpráv o velikosti minimálně 4 kB	ANO
3	Možnost přeposílání kopie nezměněných logů do dalších systémů	ANO
4	Možnost přeposílání kopie logů v některém z obvyklých strukturovaných formátů	ANO

Id	Požadované parametry	Splněno
5	Existence předpřipravených vstupních filtrů pro normalizaci logů z nejčastějších operačních systémů a síťových zařízení včetně jejich průběžné aktualizace	ANO
6	Možnost fulltextového vyhledávání v obsahu logů	ANO
7	Možnost vyhledávání na základě normalizovaných atributů	ANO
8	Možnost průběžného zobrazování příchozích logů (live-tail)	ANO
9	Možnost asynchronního vyhledávání (vyzvednutí výsledků dotazu v nezávislém spojení)	ANO
10	Web GUI s možností definice vlastního dashboardu	ANO
11	Přístupová práva definovatelná na bázi uživatelských rolí	ANO
12	Přístupová práva definují jak přístup k funkcionalitám, tak i k datům	ANO
13	Výsledky vyhledávání plně respektují uživatelské role	ANO
14	Možnost anonymizace vybraných atributů	ANO
15	Audit uživatelské aktivity	ANO
16	Možnost definice alertů na základě vlastních podmínek (výskyt výrazů i jejich četnost) včetně notifikací	ANO
17	Bohaté a dobře dokumentované API	ANO
18	Licenční model nezávislý na počtu připojených zdrojů logů	ANO
19	Perpetuální licence, nebo licence na provoz systému minimálně na 5 let	ANO
20	Schopnost zpracování 5000 EPS (events per second) ve špičkách	ANO
21	Data jsou uchovávána v lokálním úložišti, nedochází k přenosu mimo síť ONK	ANO
22	Retence logů minimálně 12 měsíců, s dostatečnou rezervou na plánovaný nárůst objemu během následujících 5 let	ANO
23	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.6. Technická specifikace technologie pro behaviorální analýzu síťového provozu

(1) Pro vybudování uceleného řešení na detekci kybernetických bezpečnostních událostí je požadováno dodání řešení, sestávající se z:

- 1 ks virtualizačního kolektoru pro monitorování a vyhodnocení datových toků
- 2 ks virtualizačních sond pro monitorování sítě na bázi datových toků
- automatického vyhodnocování NetFlow dat

(2) Jednotlivé položky řešení jsou specifikovány v následujících podkapitolách 5.6.1 až 5.6.3.

5.6.1. Technická specifikace virtualizačního kolektoru pro monitorování a vyhodnocení datových toků

(1) Minimální požadavky na technickou specifikaci 1 ks kolektoru jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Minimální nastavení 8 CPU cores	ANO
2	Minimální nastavení 16 GB RAM	ANO
3	Minimální nastavení 2000 IOPS	ANO
4	Minimální kapacita paměti 12 TB	ANO
5	Virtualizační prostředí VMware ESXi 5.5 a vyšší, Windows Hyper-V 2012 R2 a vyšší nebo KVM (KVM 3.10.0 a vyšší, QEMU 1.5.3 a vyšší, libvirt 4.5.0 a vyšší)	ANO
6	Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce	ANO
7	Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5minutových, 1minutových nebo 30sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků	ANO
8	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP	ANO
9	Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení	ANO
10	Snadná instalace do stávající síťové infrastruktury – šablony pro nasazení virtuálního stroje	ANO
11	Jednoduchá konfigurace pomocí dostupných konfiguračních šablon, které umožňují výběr z dostupných “Presets” a jejich aplikací vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace	ANO
12	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS	ANO
13	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí; Separace dat s omezením přístupu pro jednotlivé role/uživatele	ANO
14	Podpora autentizace vůči LDAP (Active Directory)	ANO
15	Podpora autentizace vůči TACACS+	ANO
16	Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce	ANO
17	Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP	ANO
18	Časová synchronizace zařízení proti centrálnímu zdroji času na síti	ANO
19	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky	ANO
20	Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232)	ANO
21	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	ANO
22	Podpora standardu Cisco AVC vč. položek HTTP hostname a URL	ANO
23	Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2	ANO

Id	Požadované parametry	Splněno
24	Podpora IPFIX položek proměnlivé délky	ANO
25	Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions	ANO
26	Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety	ANO
27	Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS)	ANO
28	Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů	ANO
29	Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů	ANO
30	Systém je schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat; Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně šesti měsíců	ANO
31	Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat	ANO
32	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků; Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik	ANO
33	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011	ANO
34	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování; O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu	ANO
35	Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat	ANO
36	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace; Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky	ANO
37	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie; Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory; Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele)	ANO
38	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).	ANO
39	Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu; Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů	ANO
40	Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat)	ANO

Id	Požadované parametry	Splněno
41	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem	ANO
42	Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami	ANO
43	Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru	ANO
44	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry; Různé formáty výstupů, minimálně PDF, CSV	ANO
45	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy; Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV; Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště	ANO
46	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem)	ANO
47	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu	ANO
48	Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT; Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace)	ANO
49	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu	ANO
50	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány; K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP apod.)	ANO
51	Možnost dohledat každý jednotlivý datový tok (flow záznam)	ANO
52	Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie	ANO
53	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení	ANO
54	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země)	ANO
55	Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.)	ANO

Id	Požadované parametry	Splněno
56	Monitorování dostupnosti zdroje flow dat pomocí SNMP	ANO
57	Kolektory NetFlow dat jsou schopné zpracovat 160 K toků za sekundu. Pro validaci tohoto požadavku budou provedeny akceptační testy	ANO
58	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků; Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik	ANO
59	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011	ANO
60	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování; O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu	ANO
61	Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat	ANO
62	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace; Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky	ANO
63	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie; Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory; Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele)	ANO
64	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel)	ANO
65	Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu; Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů	ANO
66	Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat)	ANO
67	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem	ANO
68	Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami	ANO
69	Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru	ANO
70	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV	ANO
71	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy; Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště	ANO
72	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem)	ANO

Id	Požadované parametry	Splněno
73	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu	ANO
74	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu	ANO
75	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány; K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP apod.)	ANO
76	Možnost dohledat každý jednotlivý datový tok (flow záznam)	ANO
77	Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie	ANO
78	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení	ANO
79	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země)	ANO
80	Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat; Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty apod.)	ANO
81	Monitorování dostupnosti zdroje flow dat pomocí SNMP	ANO
82	Kolektory NetFlow dat jsou schopné 200 K toků za sekundu; Pro validaci tohoto požadavku jsou provedeny akceptační testy	ANO
83	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.6.2. Technická specifikace virtualizačních sond pro monitorování sítě na bázi datových toků

(1) Pro monitorování sítě na bázi datových toků (NetFlow/IPFIX) je požadováno dodání 2ks monitorovacích sond.

(2) Minimální požadavky na technickou specifikaci 2 ks sond jsou pro každou požadavky uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Minimální nastavení 4 CPU cores	ANO
2	Minimální nastavení 8 GB RAM	ANO
3	Minimální nastavení 25 GB HDD	ANO
4	Virtualizační prostředí VMware ESXi 5.5 a vyšší, Windows Hyper-V 2012 R2 a vyšší nebo KVM (KVM 3.10.0 a vyšší, QEMU 1.5.3 a vyšší, libvirt 4.5.0 a vyšší)	ANO
5	Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty)	ANO
6	Možnost zachytávat provoz přes ERSPAN nebo GRE tunel, který je zakončen na monitorovacím portu sondy	ANO
7	Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje	ANO

Id	Požadované parametry	Splněno
8	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS	ANO
9	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí	ANO
10	Sondu je možné integrovat do dohledového systému jako monitorované zařízení pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP	ANO
11	Časová synchronizace zařízení proti centrálnímu zdroji času na síti	ANO
12	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky	ANO
13	Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232)	ANO
14	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	ANO
15	Podpora autentizace vůči LDAP (Active Directory)	ANO
16	Podpora autentizace vůči TACACS+	ANO
17	Programové vybavení sondy musí umožnit export NetFlow dat ve formátech verzi 5 a 9, IPFIX	ANO
18	Zařízení umožňuje exportovat statistiky o síťovém provozu (toky) pomocí spolehlivého a zabezpečeného komunikačního kanálu dle standardu RFC 7011	ANO
19	Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor	ANO
20	Monitorování provozu v tunelu (dekapsulace) GRE, VxLAN, ESP, 4in6, DS-Lite a OTV	ANO
21	Zařízení je schopné detekovat a odstranit duplikované pakety	ANO
22	Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX pomoci kterých lze definovat exportované atributy	ANO
23	Monitorování a reportování MAC adres ve flow statistikách; Možnost použít MAC adresu jako položku klíče flow záznamu	ANO
24	Detekce aplikací dle standardu NBAR2	ANO
25	Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik; Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX)	ANO
26	Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname, stavový kód HTTP, dotazovací metoda; Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX)	ANO
27	Identifikace operačního systému vč. jeho verze; Identifikace internetového prohlížeče vč. jeho verze; Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX)	ANO
28	Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů; Použití standardní technologie reportování těchto rozšiřujících statistik IPFIX)	ANO
29	Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď; Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX)	ANO
30	Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace; Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX)	ANO

Id	Požadované parametry	Splněno
31	Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa; Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).	ANO
32	Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další; Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX)	ANO
33	Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další; Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX)	ANO
34	Schopnost monitorování a reportování různých charakteristik provozu šifrovaného pomocí SSL/TLS; To zahrnuje verzi protokolu, šifrovací algoritmus, cipher suite, detaily certifikátu a další	ANO
35	Podpora monitoringu nativních IoT a ICS/SCADA prostředí včetně protokolů IEC 61850 (Goose, MMS), DLMS, CoAP a IEC 104; Tyto statistiky jsou monitorovány pomocí standardní IPFIX technologie	ANO
36	Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů	ANO
37	Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port	ANO
38	Podpora pro nastavení času aktivní a neaktivní expirace toků (RFC 3954)	ANO
39	Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků; Lze konfigurovat pro každý monitorovací port zvlášť	ANO
40	Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě); Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX)	ANO
41	Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky)	ANO
42	Podpora vyplňování AS na základě vestavěného či dodaného seznamu	ANO
43	Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port	ANO
44	Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě pravidla záchytu definovaného uživatelem; Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace	ANO
45	Řešení podporuje sítě s rychlostmi 100 GbE (Gigabit Ethernet)	ANO
46	Minimální výkon virtuálního zařízení je 0,3 milionů paketů za sekundu pro 1GbE sondy a 0,7 milionů paketů za sekundu pro 10GbE sondy	ANO
47	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.6.3. Technická specifikace modulu na automatické vyhodnocování NetFlow dat

(1) Pro detekci anomálií v síti je potřebný systém pro automatické vyhodnocování IP toků umožňuje automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém je založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení

kybernetickým bezpečnostním incidentům. Detekované události je možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů výrazně zjednodušuje správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.

(2) Minimální požadavky na technickou specifikaci požadavků modulu na automatické vyhodnocování NetFlow dat.

Id	Požadované parametry	Splněno
1	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Podpora VPC flow logů z AWS, Azure a GCP.	ANO
2	Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií.	ANO
3	Systém detekce anomálií poskytuje veřejně dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).	ANO
4	Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí.	ANO
5	Systém pro automatické vyhodnocování NetFlow dat je schopné zpracovat 1K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy.	ANO
6	Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.	ANO
7	Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli.	ANO
8	Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním.	ANO
9	Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků.	ANO
10	Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události.	ANO
11	Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události.	ANO
12	Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií.	ANO
13	Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.	ANO
14	Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.	ANO
15	Detekce NATů v síti s využitím rozšířených informací z L3/L4.	ANO
16	Detekce P2P sítí a VPN komunikace.	ANO
17	Systém umožňuje detekovat závadnou komunikací na základě rozlišení legitimních domén (druhé úrovně) od náhodně generovaných domén.	ANO

Id	Požadované parametry	Splněno
18	Detekce použití TOR klientů v monitorované síti a detekce příchozí komunikace z TOR sítě na monitorované servery.	ANO
19	Systém umožňuje detekovat závadné komunikace monitorování JA3 otisků v síťovém provozu a jejich porovnáváním se seznamem známých závadných JA3 otisků.	ANO
20	Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci.	ANO
21	Systém lze napojit na MISP platformu a použít indikátory kompromitace (IoC) poskytované touto platformou k detekci závadných komunikací v monitorované síti.	ANO
22	Detekce nadměrné zátěže sítě, výpadků služeb, nových a cizích zařízení připojených k síti.	ANO
23	Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace.	ANO
24	Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování atd.).	ANO
25	Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí.	ANO
26	Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.).	ANO
27	Systém je schopen poskytnout přímý přístup k evidované události za pomoci ID události z externích systémů za pomoci unikátního URL, které je možné sestavit v externím systému při znalosti ID události.	ANO
28	Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě, kterých byla událost rozpoznána.	ANO
29	Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP/HTTPS.	ANO
30	Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP.	ANO
31	Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře.	ANO
32	Detekované události jsou mapovány na jednu nebo více MITRE ATT&CK taktik a technik pro poskytnutí širšího kontextu uživateli. Mapování je založeno na základě kontextové analýzy pro zajištění správného mapování taktiky a techniky na detekovanou událost. Stejný druh události tak může být mapován různě v závislosti na kontextu události nebo vývoji události v čase.	ANO
33	Systém poskytuje dashboard pro vizualizaci MITRE ATT&CK matice, která zobrazuje počet událostí detekovaných v jednotlivých taktikách a technikách čímž umožňuje	ANO

Id	Požadované parametry	Splněno
	poskytnout přehled nad stávající bezpečností situací a zobrazit útoky v jejich různých fázích dle MITRE ATT&CK frameworku.	
34	Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen.	ANO
35	Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ).	ANO
36	Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit.	ANO
37	Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry.	ANO
38	Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí.	ANO
39	Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu.	ANO
40	Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní.	ANO
41	Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu.	ANO
42	Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu.	ANO
43	Pravidla pro falešné poplachy je možné definovat pomocí čísel autonomních systémů (ASN) nebo pomocí plně kvalifikovaného doménového jména (FQDN), čímž lze označit provoz, který nebude zpracováván detekčními metodami.	ANO
44	Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management.	ANO
45	Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. Součástí exportu musí být event ID, které jednoznačně identifikuje danou událost.	ANO
46	Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap.	ANO
47	Události je možné exportovat do formátu CSV pro další zpracování.	ANO
48	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem.	ANO
49	Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě, kterých byla událost detekována k e-mailovému reportu.	ANO

Id	Požadované parametry	Splněno
50	Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. Tyto záchyty je možné uživatelsky spravovat.	ANO
51	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

5.7. Technická specifikace technologie virtualizačních serverů pro VDI a výpočetní farmu

(1) S ohledem na požadovaný výkon pro aplikace včetně VDI řešení, redundanci a zajištění vysoké dostupnosti je požadováno dodání 6 ks virtualizačních serverů.

(2) Minimální požadavky na technickou specifikaci 6 ks serverů jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	Montáž do standardního 19“ racku o maximální výšce 2 RU, chassis pro min. 8x 2,5“ disků	ANO
3	Interaktivní LCD display či obdobný systém indikující základní informace o serveru (min. IP adresa, stav serveru a výpis chybových stavů), možnost nastavení IP konfigurace OOB managementu na čelním panelu	ANO
4	Minimálně dva 32-jádrové procesory s hodnotou dle SPECrate®2017_int_base min. 410 a SPECrate®2017_fp_base min. 390 pro 2 CPU konfiguraci (údaje musí být k dispozici na www.spec.org)	ANO
5	Min. 512 GB RAM (min. 32GB moduly 3200MT/s s podporou ECC), server s celkem 32 DIMM pozicemi, každý paměťový kanál musí být osazen nejméně jedním modulem, všechny paměťové moduly musí být identické; Podpora rozšiřitelnosti až na min. 8TB RAM per server	ANO
6	Min. 2x 480 GB NVMe RAID1 úložiště nevyužívající 2,5“ diskovou pozici	ANO
7	Grafická karta s min. pamětí 24 GB určená pro provoz ve VDI prostředí osazená do PCIe Gen4 x16 slotu s výkonem (FP32) alespoň 10 TFLOPS	ANO
8	Min. 4x 10/25GbE SFP28 porty na dvou nezávislých síťových kartách	ANO
9	Management serveru nezávislý na operačním systému s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence	ANO
10	Management musí podporovat dvoufaktorovou autentizaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP, podpora Silicon Root Of Trust, Secure Boot a TPM 2.0	ANO
11	Pro management požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, REDFISH	ANO
12	Nejméně 2 redundantní, za chodu vyměnitelné napájecí zdroje s platinovou účinností min. 1500W každý	ANO
14	Dodání včetně 4x SFP28 twinaxial kabelů o délce 3m pro každý server	ANO
15	Certifikace pro VMware 6.7u3 a vyšší, Windows Server 2016 a vyšší, Citrix XenServer, Red Hat Enterprise Linux a SUSE Linux Enterprise Server	ANO
16	Schopnost napojení na dohledové centrum výrobce s funkcí automaticky generovat servisní události	ANO
17	Podpora výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou v místě instalace na 5 let	ANO
18	Licence na Microsoft Windows Datacenter 2019 na všechna CPU jádra	ANO

Id	Požadované parametry	Splněno
19	Licence VMware vSphere Enterpise Plus na všechna CPU jádra s podporou na 5 let	ANO
20	Licence pro dvě instance VMware vCenter Server Standard s podporou na 5 let	ANO
21	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

6. Fáze A - Instalace a implementace

(1) Instalace a implementace technologií popsaných v kapitolách 5.1 až 5.7 bude provedena v jednotlivých požadovaných krocích a termínech uvedených v kapitole 3.

(2) Minimální požadavky na Instalaci a implementaci technologií jsou uvedeny v následující tabulce.

Id	Plnění požadavku	Splněno
1	Kompletní instalace, konfigurace a montáž dodaného HW a SW v prostorách zadavatele	ANO
2	Instalace a konfigurace SW	ANO
3	Instalace a konfigurace všech požadovaných funkcionalit	ANO
4	Testování funkčnosti (provedení testů všech technologií a bezpečnostních systémů)	ANO
5	Základní uživatelské seznámení a proškolení administrátorů s dodanými technologiemi	ANO
6	Vypracování dokumentace realizovaného řešení zahrnující instalační protokoly a instalační postupy.	ANO

6.1. Zpracování a akceptace Detailního realizačního konceptu

(1) Dokument Detailní realizační koncept bude obsahovat minimálně:
   a) definici cílového stavu, která bude vycházet z požadavků na budoucí stav, viz tento dokument,
   b) akceptační kritéria cílového stavu;
      pro ověření plnění Dodavatele v rámci Smlouvy jsou uvedena v tomto dokumentu, a to v tabulkách označených „Minimální požadavky …“, kde Dodavatel bude deklarovat svoji připravenost poskytovat bezvadné plnění již v rámci Zkušebního (testovacího) provozu.
   c) detailní harmonogram realizace zakázky, který vychází z milníků uvedených v kapitole 3 a z Dodavatelem navrženého Harmonogramu projektu.

(2) Formálně bude tato oblast Fáze A završena dohodnutým a vzájemně odsouhlaseným Předávacím protokolem dílčího plnění (Dodavatel předává dokument Detailní realizační projekt) a Akceptačním protokolem dílčího plnění, kterým Zadavatel akceptuje splnění podmínek této části Fáze A ve Smlouvě.

6.2. Předání a převzetí plnění

6.2.1. Předání a převzetí dokumentů

(1) Dokumenty, které mají být vypracovány Dodavatelem a které se poskytují Zadavateli jako součást poskytování díla (zejména Detailní realizační koncept), budou nejdříve předloženy Zadavateli ve formě návrhu k posouzení.

(2) Dodavatel se zavazuje předat první verzi dokumentu Zadavateli k akceptaci ve lhůtě domluvené mezi Dodavatelem a Zadavatelem na základě Smlouvy, nebo jinak stanovené v souladu se Smlouvou.

(3) Zadavatel je oprávněn ve lhůtě pěti (5) pracovních dnů od doručení příslušného dokumentu písemně předložit Dodavateli své připomínky k návrhu.

a) Po diskusi o těchto připomínkách upraví Dodavatel příslušný návrh v souladu s dohodnutými změnami a se zapracováním těchto dohodnutých změn jej předá ve stejné lhůtě pěti (5) pracovních dnů Zadavateli.

b) V případě, že Zadavatel nemá k předaným dokumentům výhrady, považují se za převzaté k okamžiku doručení jejich konečné verze Zadavateli.

c) V případě, že Zadavatel připomínky ve lhůtě pěti (5) dnů nepředloží, má se za to, že s předloženým dokumentem souhlasí a dokument se považuje za řádně převzatý.

6.2.2. Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)

(1) V případě, že součástí poskytování plnění Dodavatelem dle Smlouvy je plnění, které podléhá akceptaci Zadavatelem, musí dojít k podpisu Předávacích protokolů ohledně tohoto plnění v termínech uvedených v harmonogramu, není-li výslovně uvedeno jinak.

Detailní kritéria akceptace a vymezení plnění, která podléhají akceptaci Zadavatelem, jsou uvedena v tomto dokumentu, případně v Detailním realizačním projektu.

Jestliže plnění nebo jeho jednotlivé části splní kritéria akceptačního řízení, považují se za řádně ukončené a Zadavatel je povinen jej převzít.

(2) Akceptační procedury zahrnují porovnání skutečných vlastností plnění se závaznou specifikací předmětu plnění dle Smlouvy.

a) Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů obsahující popis testů, testovací data, příslušné prostředí, pořadí provádění testů a akceptační kritéria.

Nedohodnou-li se smluvní strany jinak, vypracuje specifikaci akceptačních testů Dodavatel a předá Zadavateli k odsouhlasení v termínu pěti (5) pracovních dnů před zahájením akceptační procedury dle harmonogramu.

Odsouhlasení bude provedeno písemnou formou v termínu pěti (5) pracovních dnů před zahájením akceptační procedury. Jestliže se Zadavatel v této lhůtě ke specifikaci akceptačních testů písemně nevyjádří, má se za to, že specifikaci akceptačních testů odsouhlasil.

Jestliže Zadavatel specifikaci akceptačních testů v uvedené lhůtě neodsouhlasil, je povinen Zadavatel v této lhůtě sdělit připomínky k Dodavatelem předložené specifikaci akceptačních testů a poskytnout Dodavateli veškerou potřebnou součinnost k dokončení a odsouhlasení specifikace akceptačních testů.

Lhůta pro provedení akceptačních testů a lhůta pro předání plnění nebo jeho části se prodlužuje o dobu, o kterou se prodloužilo písemné odsouhlasení specifikace akceptačních testů z důvodu připomínek na straně Zadavatele oproti lhůtě stanovené.

b) Dodavatel bude písemně informovat Zadavatele, resp. jeho oprávněné osoby nejméně pět (5) dní předem o termínu zahájení akceptačních testů.

Zadavatel je oprávněn se těchto testů zúčastnit a osvědčit jejich konání, a to formou předávacího protokolu (nebo dílčích předávacích protokolů), podepsaného (podepsaných) oprávněnými osobami obou smluvních stran. Pokud se Zadavatel nedostaví v termínu určeném pro provedení akceptačních testů, ačkoli byl s tímto termínem řádně seznámen, je Dodavatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti.

Takto provedené akceptační testy se považují za provedené v přítomnosti Zadavatele. Kopie veškerých dokumentů vypracovaných v souvislosti s provedením těchto akceptačních testů budou Zadavateli poskytnuty do pěti (5) dnů.

c) Základním předpokladem pro řádné předání plnění (nebo jeho části) Dodavatelem a převzetí tohoto plnění (nebo jeho části) Zadavatelem, a to formou předávacího protokolu podepsaného oprávněnými osobami obou smluvních stran je skutečnost, že plnění splní kritéria akceptačních testů uvedená v dohodnutých kontrolních specifikacích a bude provedeno v souladu se závaznou specifikací předmětu plnění dle Smlouvy.

d) Jestliže plnění nebo jeho část splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje v den následující po ukončení akceptačních testů umožnit Zadavateli plnění nebo jeho část převzít a Zadavatel se zavazuje v tomto termínu plnění nebo jeho část převzít.

   Pokud Zadavatel plnění nebo jeho část v tomto termínu nepřevezme, ačkoli převzetí plnění nebo jeho části bylo Dodavatelem řádně umožněno, má se za to, že plnění nebo jeho část bylo řádně předáno a Zadavatelem převzato právě v den následující po ukončení akceptačních testů.

e) Jestliže plnění nesplňuje stanovená akceptační kritéria kteréhokoliv akceptačního testu, budou výsledky akceptačního testu (splněno/nesplněno/s výhradami) spolu s uvedením termínů pro nápravu uvedeny ve vyhodnocení Akceptačního protokolu.

   Dodavatel napraví tyto nedostatky a příslušné akceptační testy budou provedeny znovu.

   Tento proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně.

   Proces testování a následných oprav lze opakovat, dokud Dodavatel nesplní veškerá akceptační kritéria pro příslušný akceptační test, nejvýše však natřikrát (3x).

   V situaci, kdy by bylo nutné opakovat akceptační testy více jak třikrát (3x) pro konkrétní fázi projektu, je v takovém případě nutný souhlas nadřízeného orgánu projektu – tzn. řídícího výboru nebo ředitelů projektu dle použité metodiky řízení projektu.

f) Žádný akceptační test se však nebude považovat za nesplněný, jestliže daný nedostatek nebyl způsoben Dodavatelem, nebo byl zjištěn nebo měl být zjištěn Zadavatelem před nebo při předcházejícím akceptačním testu, ale nebyl v té době oznámen Dodavateli, nebo byl nepodstatný, tzn., neměl vliv na řádné poskytování funkčnost díla nebo jeho části tak, jak jsou vymezeny ve Smlouvě.

g) Při převzetí plnění nebo kterékoliv jeho části v souladu s tímto článkem je Zadavatel povinen podepsat potvrzení o přijetí plnění nebo dané části a Zadavatel i Dodavatel se zavazují podepsat příslušný předávací případně akceptační protokol (dílčí předávací případně akceptační protokoly), tj. potvrzení o předání a přijetí (převzetí) plnění nebo jeho určité části.

6.3. Školení

(1) Dodavatel poskytne školení pro administrátory IS tak, aby byli schopni řádně užívat, respektive administrovat, instalované technologické části specifikované v kapitole 5.

6.4. Dokumentace

(1) Dodaná dokumentace slouží k zachycení a vyhodnocování plánovaných činností a též k dokumentaci skutečného stavu.

7. Fáze B – provozní podpora dodaných technologií

(1) Požadavky, které musí dodavatel minimálně naplnit na provozní podporu dodaných technologií, jsou v níže uvedené tabulce.

Id	Plnění požadavku	Splněno
01	V rámci běžného rozvoje jednotlivých částí serverové, datové a komunikační infrastruktury Dodavatel zajistí poskytnutí aktualizovaných verzí SW nejpozději do 1 měsíce po uvolnění nové verze k distribuci.	ANO
02	Budou poskytovány informace o změnách a nových funkcích v aktualizovaných verzích instalované technologie.	ANO
03	Bude prováděna průběžná aktualizace dokumentace k programovému vybavení tak, aby u Zadavatele byla vždy aktuální dokumentace k provozované technologii.	ANO
04	Bude poskytována součinnost při zásadním upgrade softwarových částí instalované infrastruktury na vyšší verze.	ANO
05	Bude zajištěna udržitelnost SW třetích stran, dodaných Dodavatelem v rámci veřejné zakázky.	ANO
06	HW a SW maintenance výrobce budou poskytovány po celou dobu smluvního vztahu (min 60 měsíců ode dne protokolárního ukončení Fáze A dle Smlouvy).	ANO
07	Technická podpora a servis zařízení HW a SW budou zabezpečeny Dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.	ANO
08	Technická podpora a servis budou realizovány v místě Zadavatele. Výjimku tvoří činnosti realizované vzdáleným připojením Dodavatele, výrobce zařízení do prostředí Zadavatele.	ANO
09	Veškeré požadavky budou evidovány v systému servisní podpory Dodavatele nebo výrobce zařízení (HelpDesk).	ANO
10	Kontaktní místo umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím služby HelpDesk, popř. služby Hot-line.	ANO
11	Služba Hot-Line umožní příjem požadavku na servisní zásah v českém jazyce na telefonním čísle: (uvede dodavatel) v **režimu 5x8 (8 hodin v pracovní dny) v době od 09:00 do 17:00 hod**, příjem požadavku bude zajištěn lidskou obsluhou.	ANO
12	Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 (nepřetržitě vyjma nahlášených servisních zásahů Dodavatele při správě systému HelpDesk).	ANO
13	Služba HelpDesk umožní Zadavateli upřesnit nebo doplnit požadavek.	ANO
14	Služba HelpDesk bude Zadavateli poskytovat přehled o aktuálně nahlášených požadavcích, jejich stavu a aktuálním způsobu jejich řešení. Služba HelpDesk bude Zadavateli zasílat notifikace o změně stavu jeho požadavku (např. zadaný, v řešení, uzavřený atd.) a musí Zadavateli umožnit schvalování uzavření nahlášeného požadavku.	ANO
15	Služba HelpDesk bude poskytovat Zadavateli přístup i k uzavřeným požadavkům a způsobu jejich řešení, bude poskytovat podrobné údaje o historii požadavků od jejich nahlášení, po jejich vyřešení.	ANO

8. Požadavky na technický popis řešení v nabídce

(1) Specifikace předmětu plnění:

a) Přehled plnění požadovaných minimálních parametrů;

Dodavatel vloží vyplněný tento dokument doplněný u jednotlivých položek označených jako „Minimální požadavky …“.

b) Technický popis řešení - grafické schéma a podrobný popis nabízených technologií a bezpečnostních systémů;

(2) Dodavatel uvede detailní popis rozhraní jednotlivých technologií pro napojení jiných (stávajících) IS Zadavatele;

(3) Rozsah školení vč. uvedení počtu dní školení navrženého Dodavatelem;

(4) Návrh Metodiky řízení projektu a Harmonogramu projektu.