# *PŘÍLOHA Č. 1: NABÍDKA*

# *PODROBNÁ SPECIFIKACE PŘEDMĚTU ZAKÁZKY*
# *ČÁST I. SOFTWARE*

# *KOMPONENTA LOG MANAGER*

## *2. NÁSTROJ PRO SLEDOVÁNÍ, VYHODNOCOVÁNÍ A UKLÁDÁNÍ UDÁLOSTÍ IS (LOG MANAGEMENT)*

Cílem dodávky a implementace je nástroj v podobě systému pro centralizované ukládání a správu logů z libovolných zdrojů, s možností analýzy a řešení bezpečnostních událostí (incidentů) ze systémů a aplikací zadavatele. Navržený systém musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně jeden rok zpět. Toto úložiště musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi.

Nutností je možnost procházení těchto logů vhodným grafickým nástrojem s předdefinovanými pravidly pro rychlé vyhledávání (např. jako jsou změny v systémech provedené administrátory; seznam nově vytvořených účtů v MS AD za zvolenou periodu; změny v přístupových právech pro zadaného uživatele nebo k zadané složce; monitoring privilegovaných účtů, sdílených účtů a změn konfigurací; sledování souborového systémů apod.) Dále musí systém umožňovat sledovat chování uživatelů a systémů s možností upozorňování na překročení pravidel, a to na základě limitů nebo korelací událostí stanovených administrátorem systému.

Zadavatel požaduje vytvoření jednotného úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučení možnosti modifikace logů ze strany administrátorů nebo uživatelů. Systém musí umožňovat tvorbu uživatelsky definovaných parserů bez účasti výrobce nebo dodavatele. Dokumentace v českém jazyce musí poskytnout jednoznačný návod, jak takovéto parsery vytvářet, včetně vzorových příkladů.

Popis požadované funkcionality:

- dashboard s centrálním přehledem s grafickou prezentací,
- korelace mezi jednotlivými událostmi,
- dlouhodobé bezpečné ukládání logů, pro případ bezpečnostního auditu,
- sběr logů pro řešení provozních problémů a bezpečnostních incidentů,
- ukládání logů ze všech síťových a bezpečnostních zařízení, serverů a stanic.

# A. POUŽITÁ TERMINOLOGIE

| pojem | význam |
|---|---|
| Bezpečnostní incident | Označuje nějakou nestandardní či nepříjemnou bezpečnostní událost, která vede k narušení pravidel bezpečnosti v organizaci. |
| Dashboard | Z anglického překladu „nástěnka“, se využívá u produktů, které mají za cíl integrovat informace z více složek do jednotného zobrazení. |
| MS AD | Microsoft Active Directory – řešení adresářové služby, ve které jsou uloženy popisy objektů (servery, stanice, uživatelé, aplikace), informace o členech sítě a vztahy mezi jednotlivými objekty. |
| Log událostí | Záznam (zpráva) jednotlivé události odehrávající se v systému pro poskytnutí informací o posloupnosti prováděných činností tak, aby je bylo možné sledovat a diagnostikovat problémy. |
| Parser | Část programu, která má na starosti tzv. parsing (syntaktickou analýzu) textu. |
| Syntaktická analýza | Proces zpracování textu v přirozeném či uměle vytvořeném jazyce za pomoci gramatických pravidel definovaných pro daný jazyk (např. při práci s XML). |
| SQL syntaxe | Strukturovaný programovací jazyk pro práci s daty v relačních databázích. |

# B. ZÁKLADNÍ INFORMACE – LOG MANAGEMENT

Předmětem zakázky je nasazení systému pro centralizované ukládání a správu logů z libovolných zdrojů, s možností analýzy a řešení bezpečnostních událostí (incidentů) ze systémů a aplikací zadavatele v prostředí Oblastní nemocnice v Mladé Boleslavi (Klaudiánova nemocnice).

Součástí předmětu dodávky bude poskytnutí demo verze nebo zapůjčení nabízeného systému pro účely testovacího provozu a ověření požadovaných funkčních vlastností na straně zadavatele. Zadavatel požaduje poskytnutí testovacích vzorků v místě plnění do deseti (10) pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný dodavatel poskytne testovací vzorky bezplatně a na dobu minimálně 30 kalendářních dnů.

V rámci testování budou ověřovány minimálně následující činnosti:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele.
- Konfigurace systémů Microsoft Windows zadavatele tak, aby posílaly logy do testovaného systému.
- Ověření funkčních a výkonových parametrů Windows agenta – viz. Technické požadavky, všechny body z tabulky „Sběr událostí z Microsoft prostředí“.
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům zadavatele.
- Vytvoření, konfigurace a odladění uživatelsky definovaného parseru – viz. Technické požadavky, tabulka „SW parametry“.

- Značkování událostí, vytvoření upozornění s limitem nebo korelací dle zadání zadavatele – viz. Technické požadavky, tabulka „SW parametry“ a tabulka „Alerty“ (příklad: pošli alert jen v případě, že se událost stala na skupině Windows serverů X-krát během 10 minut).
- Odeslat událost, která vyvolala alert na externí syslog server přes TCP protokol.
- Představení plnohodnotné dokumentace pro nabízený systém v českém jazyce.

Testování bude provádět dodavatel za součinnosti zástupců zadavatele. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou testovací vzorky dodavateli vráceny, přičemž si tyto vzorky vyzvedne dodavatel na vlastní náklady v místě plnění.

Testování bude zakončeno akceptační procedurou na jejímž základě bude vyhotoven Akceptační protokol potvrzený oběma stranami. Dodavatel pro tyto účely předloží zadavateli návrh minimálního rozsahu akceptačních testů ke schválení. V případě, že testovaný systém neprojde úspěšným otestováním, vyhrazuje si zadavatel právo neuzavřít s takovým uchazečem smlouvu.

## *C. TABULKY MINIMÁLNÍCH POŽADAVKŮ*

Níže jsou uvedeny minimální požadavky na nabízené řešení v jednotlivých strukturovaně členěných tabulkách. Uchazeč použije ve své nabídce tyto tabulky, ve kterých slovně uvede, zda požadavek je či není splněn (ANO / NE).

### A. Obecné požadavky

| | Požadavek | ANO / NE |
|---|---|---|
| **Systémové požadavky** | Podpora operačních systémů: Windows, Linux | Ano |
| | Jediné úložiště dat (repozitory) a to relační databázi, pro svůj provoz nevyžaduje LDAP server | Ano |
| | Podpora relačních databází - MySQL 5, MS SQL Server 2014, Oracle DB 12, PostgreSQL 9.4, nebo novější verze | Ano |
| | Řešení podporuje technologii Java 8 či .NET 4.5, nebo novější verze | Ano * |
| | Řešení je možné provozovat na jednom z aplikačních serverů: Apache Tomcat 8, Oracle Glassfish 3.1, Oracle WebLogic 12c, nebo novější verze | Ano ** |
| | Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC | Ano |
| **Licence** | Počet licencí bez omezení na počet uživatelů, koncových systémů, procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů | Ano |
| | Dodávka zdrojových kódů | Ano |
| | Možnost připojení budoucích nových systémů zadavatele a sběr provozních dat z těchto systémů do systému centralizovaného ukládání a správy logů bez dodatečných licenčních nákladů | Ano |

Příloha č. 1c Smlouvy

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Servis a podpora** | *Implementátora* | Garance reakční doby | | Ano |
| | | Hlášení požadavků na telefonickou hotline a do helpdeskové aplikace režimu 5x8, pracovní doba od 9:00 hod do 17:00 hod | | Ano |
| | | Reporting o průběhu řešení požadavků v helpdeskové aplikaci provozované Dodavatelem | | Ano |
| | | 160 pracovních hodin (20 člověkodnů) na konzultace, případně drobný rozvoj řešení. Tyto hodiny bude možné využít libovolně v průběhu doby platnosti smlouvy | | Ano |
| | | Měsíční report o provedených službách | | Ano |
| | *Výrobce* | SW - Garance oprav jádra produktu | | Ano |
| | | SW - Přístup k novým verzím a patchům produktu | | Ano |
| | | HW - min. 5 letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady. | | Ano |
| | | SW - Podpora výrobce na aktualizaci systému a parserů na min. 5 let. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonická a emailová podpora s diagnostikou vzdáleným přístupem. | | Ano |
| | *Řešení vad* | P1 – kritické vady se zásadními dopady do běhu procesů Zadavatele | Reakce do 4 hod. v prac. době | Ano |
| | | | Odstranění do 8 hod. v prac. době | Ano |
| | | P2 – vady způsobující významné zhoršení funkčnosti systému | Reakce do 8 hod. v prac. době | Ano |
| | | | Odstranění do 24 hod. v prac. době | Ano |
| | | P3 – vady s nízkými dopady, ostatní požadavky | Reakce do 16 hod. v prac. době | Ano |
| | | | Odstranění dle dohody | Ano |

Obecné požadavky - pokračování

| Požadavek | | | ANO / NE |
|---|---|---|---|
| **Demo** | *Obecné* | V době podání nabídky on-line přístupné demo produktu bez nutnosti instalace jakéhokoliv SW či provedení konfigurace na straně zadavatele (např. VPN přístup) | Ano |
| | | Dostupnost po dobu minimálně 30 kalendářních dní od zpřístupnění | Ano |
| | Ukázková data | | Ano |

## B. Požadavky na funkcionalitu

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Technické požadavky** | *Obecné* | 1 | Systém pracuje jako appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací vyjma agenta pro sběr Windows logů. | Ano |
| | | 2 | Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware dle minimálního seznamu podporovaných zdrojů logů:<br><br>Apache httpd, Apache Tomcat, Amavis, Antivir AVG, Antivir Avast, Antivir Eset, Antivir Eset Remote administrator, Brocade FC switches, ArcSight CEF format all sources, Cisco ASA, Cisco Firepower, Cisco IOS, Cisco IronPort, Cisco Nexus, Cisco SMB, Cisco WLC, CompuNet GAMA (Volitelný), Dell Force10, Dell iDrac (Server OoB management), Dell PowerConnect, Dell SonicWALL, Dell W-series WiFi, Discard (Special distard rule), Dropbear SSH (mostly Embedded Linux), Extreme NAC, Extreme Networks XOS, FlowMon, FortiAuthenticator, FortiDDoS, FortiGate (FOS 5.2), FortiMail, FreeRADIUS, Qradar LEEF format all sources, HPE Aruba Instant AP (WLAN), HPE Aruba Mobility Controller (WLAN), HPE iLo 4 (Server OoB management), HPE IMC, HPE routers, HPE switches Procurve OS, HPE switches Comware OS, HPE Comware WLAN, Huawei USG, CheckPoint, ISC BIND, ISC DHCP, ISC DHCPD, JSON (format), Juniper SRX, Kaspersky Endpoint Security, Kaspersky Security Center, Kerio Connect, Kerio Control, Kernun Clear Web, Kernun web filter, Linux Cron, Linux Freeradius, Linux Iptables, Linux postfix, LOGmanager, Mikrotik, Microsoft Exchange log, Microsoft SharePoint, Microsoft SQL, Microsoft Windows DHCP log, Microsoft Windows firewall, Microsoft Windows IIS, MySQL, Nginx, Novell eDirectory, OpenSSH server, Oracle DB, Palo Alto Networks NGFW, PostgreSQL, Ruckuss wireless, SAP, Shorewall, SonicWall, Sophos, SpamAssasin, Synology NAS DSM, Trapeze, TrendMicro DeepDiscovery, TrendMicro TippingPoint NG-IPS, UBNT Rocket, UBNT UniFI, VMware, Windows - any logs from Event Viewer, Windows - any text log from file | Ano |
| | | 3 | Systém umožňuje dopsání parseru pro výše neuvedené zdroje logů uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce. | Ano |
| | | 4 | Parsery a alerty musí umožňovat použití matematických operací. | Ano |
| | | 5 | Parsery a alerty musí podporovat dekódování URL. | Ano |
| | | 6 | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožnovat příjem logů i na uživatelsky definovaných UDP a TPC portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. | Ano |
| | | 7 | Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje ji a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí. | Ano |
| | | 8 | Všechny pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. | Ano |
| | | 9 | Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159. | Ano |

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| | | 10 | Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. | Ano |
| | | 11 | Systém musí umožňovat přijatou zprávu rozhodnutím konfigurace nebo parseru zahodit. | Ano |
| | | 12 | Systém provádí konsolidaci logů na centrálním místě. | Ano |
| | | 13 | Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. | Ano |
| | | 14 | Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky. | Ano |
| | | 15 | Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období. | Ano |
| | | 16 | Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace. | Ano |
| | | 17 | Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám. | Ano |
| | | 18 | V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB. | Ano |
| | | 19 | Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení. | Ano |
| | | 20 | Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením. | Ano |
| | | 21 | Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. | Ano |
| | | 22 | Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk. | Ano |
| | | 23 | Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. | Ano |
| | | 24 | Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem. | Ano |
| | | 25 | Konfigurační a systémové rozhraní a dokumentace musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce. | Ano |
| | | 26 | Systém nabízí kapacitní i výkonovou škálovatelnost. | Ano |
| | | 27 | Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB. | Ano |
| | | 28 | Požadujeme, aby ze systému bylo možné vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště. | Ano |
| | | 29 | Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog. | Ano |
| | | 30 | Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožnoval autorizovaný přístup ke strukturované databázi logů. | Ano |
| | | 31 | Dodavatel jako součást dokladů dle čl. 4.9. Smlouvy o dodávce a implementaci software v rámci předání plnění doloží prohlášení o | Ano |

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| | | | shodě dle zákona č. 22/1997 Sb., o technických požadavcích na výrobky. Tento požadavek zadavatele je v zájmu garance uvedení SW jako výrobku na náš trh a je rovněž v souladu s požadavky kybernetické bezpečnosti dle Vyhlášky Národního úřadu pro kybernetickou a informační bezpečnost č. 82 / 2018 ze dne ze dne 21. května 2018 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“. | |
| | | 32 | Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému. | Ano |
| | | 33 | Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. | Ano |
| | | 34 | Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou výjimkou je monitorování systémů Windows, které přes WMI protokol neumožňuje monitorovat textové logy. | Ano |
| | | 35 | Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření z lokální databáze. | Ano |
| | | 36 | Součástí dodávky systému je administrátorská dokumentace. | Ano |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Technické požadavky** | *Minimální HW parametry požadovaného systému* | 36 | Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. | Ano |
| | | 37 | HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech. | Ano |
| | | 38 | 1 procesor (min. 10 jader), podpora HyperThreadingu. | Ano |
| | | 39 | Min. 64GB DDR-4. | Ano |
| | | 40 | Minimálně 12TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 2GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí. | Ano |
| | | 41 | Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/s. | Ano |
| | | 42 | Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. | Ano |
| | | 43 | Větráky v systému musí být vyměnitelné za provozu a redundatní. | Ano |
| | | 44 | 2x napájecí zdroje s redundancí napájení 1+1. | Ano |
| | | 45 | Virtuální KVM (tj. převzetí textové i grafické konsole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače. | Ano |
| | | 46 | Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod). | Ano |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Technické požadavky** | *Výkonnostní a SW parametry požadovaného systému* | 47 | Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli – viz. bod 32, není nutné editovat žádné konfigurační soubory včetně IP adresace systému). | Ano |
| | | 48 | Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli (viz. bod 32). | Ano |
| | | 49 | Systém musí podporovat downgrade, pro případ problémů s novou verzí systému po upgrade. | Ano |
| | | 50 | Průměrný trvalý příjem min. 2 tis událostí / s. | Ano |
| | | 51 | Špičkový příjem 4 tis událostí / s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později. | Ano |
| | | 52 | Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB. Integrovaná databáze musí mít čistou velikost nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat. | Ano |
| | | 53 | Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli (viz. bod 32). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |
| | | 54 | Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy. | Ano |
| | | 55 | Systém musí podporovat integraci externích informací. | Ano |
| | | 56 | Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení. | Ano |
| | | 57 | V centrální správcovské konzoli (viz. bod 32) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. | Ano |
| | | 58 | V centrální správcovské konzoli (viz. bod 32) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.). | Ano |
| | | 59 | Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | Ano |
| | | 60 | Podpora zrcadlení a clusteru – 2 nody v režimu active / active. | Ano |
| | | 61 | V případě rozšíření systému na cluster (2 nody) se dvou nodový cluster chová jako 1 celek. | Ano |
| | | 62 | V případě využití dvou nodů v clusteru se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru. | Ano |
| | | 63 | V případě rozšíření systému na cluster (2 nody) musejí zařízení odesílající události, odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi nody. | Ano |
| | | 64 | Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. | Ano |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Technické požadavky** | *Alerty* | 65 | Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert. | Ano |
| | | 66 | Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události. | Ano |
| | | 67 | Předpřipravené sety/vzory alertů výrobcem. | Ano |
| | | 68 | Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |
| | | 69 | Jako výstupní pravidlo alertu musí systém umět odeslat událost, která alert vyvolala na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. | Ano |
| | | 70 | V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě XY). | Ano |
| | | 71 | Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. | Ano |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Technické požadavky** | *Sběr událostí z Microsoft prostředí* | 72 | Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních Windows logů, tak monitoring textových souborových logů. | Ano |
| | | 73 | Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací. | Ano |
| | | 74 | Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole (viz. bod 32). | Ano |
| | | 75 | Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole (viz. bod 32). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |
| | | 76 | Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému (viz. bod 32). Správa a aktualizace Windows agenta se neprovádí z Group Policy. | Ano |
| | | 77 | Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.). | Ano |
| | | 78 | Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů. | Ano |
| | | 79 | Komunikace Windows agenta a centrálního systému musí být šifrovaná. | Ano |
| | | 80 | Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz. bod 32) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. | Ano |
| | | 81 | Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. | Ano |
| | | 82 | Počet instalací Windows agenta nesmí být licenčně omezen. | Ano |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | | ANO / NE |
|---|---|---|---|---|
| **Technické požadavky** | *Podpora pro sběr událostí* | 83 | Systém musí podporovat řešení, které sbírá události případně i na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. | Ano |
| | | 84 | Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat. | Ano |
| | | 85 | Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit. | Ano |
| | | 86 | Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí. | Ano |
| | | 87 | Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 50GB událostí. | Ano |
| | | 88 | Řešení pro sběr dat musí mít výkon minimálně 3 tisíce událostí /s. a to i v trvalé zátěži. | Ano |
| | | 89 | Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů. | Ano |
| | | 90 | Řešení musí podporovat dostupnost jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V. | Ano |
| | | 91 | Řešení musí podporovat komunikaci na centrálu i přes vícenásobný překlad adres (NAT). | Ano |

# *D. DETAILNÍ POPIS PLNĚNÍ*

Řešení je postaveno na produktu českého výrobce SIRWISA s názvem LOG MANAGER v konfiguraci M. Řešení je dodáváno ve formě HW appliance kryjící veškeré požadavky zadavatele na servis a podporu po dobu 5ti let. HW pro appliance je založen na certifikovaném HW výrobce DELL.

| Produktový kód (SKU) | Popis produktu | Množství (kusů) |
|---|---|---|
| LOGM-16TB-DELL-5Y | Malý LOGmanager, Dell,<br>LOGmanager M - DELL (5 roků HW záruka, 5 roků SW rnwl, 1x VF, 12TB databáze) | 1 |
| LOGM-INST | Instalace, Sirwisa, Instalace provedená technikem Sirwisa | 1 |
| LOGM-EDU-OUT | Školení,<br>Školení pro zákazníky (1 den, max 8 lidí. mimo Prahu) | 1 |

Detailní informace jsou uvedeny dále v datasheetu a ve whitepaperu věnovanému splnění podmínek pro ZoKB a VoKB.

Školení v rozsahu jednoho dne bude vycházet ze standardního školení definovaného výrobcem a bude customizované pro potřeby této konkrétní implementace. Technický popis je uveden v sekci datasheety dále.

Poznámka *)
Požadavek: Řešení podporuje technologii Java 8 či .NET 4.5, nebo novější verze
Vysvětlení: Dané technologie nejsou k vlastní činnosti LOGmanageru třeba. Uživatelské/administrátorské rozhraní využívá HTMLv5 podporované všemi moderními webovými prohlížeči. Komponenta „LOGmanager Windows Event Sender“ (agent pro sběr logů z Windows) vyžaduje ke svému běhu minimálně technologii .NET 3.5, ale samozřejmě doporučujeme použít poslední dostupnou verzi – .NET 4.8.x.

Poznámka **)
Požadavek: Řešení je možné provozovat na jednom z aplikačních serverů: Apache Tomcat 8, Oracle Glassfish 3.1, Oracle WebLogic 12c, nebo novější verze
Vysvětlení: Řešení LOGmanager je nabídnut v tomto výběrovém řízení zcela v souladu s požadovanou formou hardwarové appliance. Je tedy dodávané jako HW server s instalovaným operačním systémem a aplikacemi jako ucelený systém. Nevyžaduje k provozu žádný dodatečný zákaznický HW ani SW.

Akceptační testy před podpisem smlouvy:

Dodavatel v případě výzvy zadavatele zajistí akceptační testování zcela v souladu s požadavky části B uvedené výše. Předmětem akceptačního testování bude:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, a to ve formě zpřístupnění DEMO prostředí.
- Konfigurace systémů Microsoft Windows zadavatele tak, aby posílaly logy do testovaného systému, a to ve formě vzorového předvedení v rámci DEMO prostředí.
- Ověření funkčních a výkonových parametrů Windows agenta – viz. Technické požadavky, všechny body z tabulky „Sběr událostí z Microsoft prostředí“, a to ve formě vzorového předvedení v rámci DEMO prostředí.
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům zadavatele, a to ve formě vzorového předvedení v rámci DEMO prostředí.
- Vytvoření, konfigurace a odladění uživatelsky definovaného parseru – viz. Technické požadavky, tabulka „SW parametry“, a to ve formě vzorového předvedení v rámci DEMO prostředí.
- Značkování událostí, vytvoření upozornění s limitem nebo korelací dle zadání zadavatele – viz. Technické požadavky, tabulka „SW parametry“ a tabulka „Alerty“ (příklad: pošli alert jen v případě, že se událost stala na skupině Windows serverů X-krát během 10 minut), a to ve formě vzorového předvedení v rámci DEMO prostředí.
- Odeslat událost, která vyvolala alert na externí syslog server přes TCP protokol, a to ve formě vzorového předvedení v rámci DEMO prostředí.
- Představení plnohodnotné dokumentace pro nabízený systém v českém jazyce, a to ve formě zpřístupnění české dokumentace k předmětnému systému.

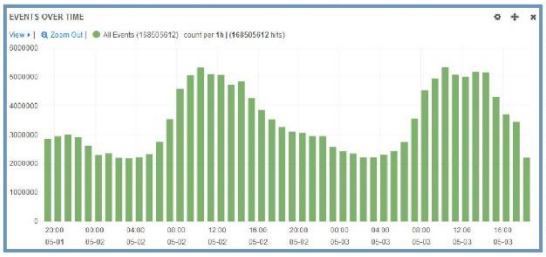
Příloha č. 1c Smlouvy

# *E. DATASHEET*

Datasheet produktu


## LOGmanager

V dnešním přetechnizovaném světě jsou informace kritickým zdrojem umožňujícím správné rozhodnutí ve správný čas. V protikladu k tomu konstatování stojí fakt, že důležité informace jsou distribuovány v nejrůznějších zařízeních a aplikacích napříč celou organizací, ne vždy ve snadno pochopitelném formátu a s rozdílnou dostupností. Sjednocení informací z mnoha zdrojů a jejich přeložení do lidsky srozumitelného tvaru, nastavení pevných pravidel pro nakládání s informacemi a jejich nezpochybnitelnost jsou proto klíčové požadavky pro efektivitu bezpečnostních i operativních činností každé organizace. Když se k tomu přidá i přehledná interpretace těchto informací v kompaktním a výkonném nástroji, získá IT organizace nástroj pro realizaci správných rozhodnutí. A tímto nástrojem je český systém LOGmanager.




## Určení systému LOGmanager

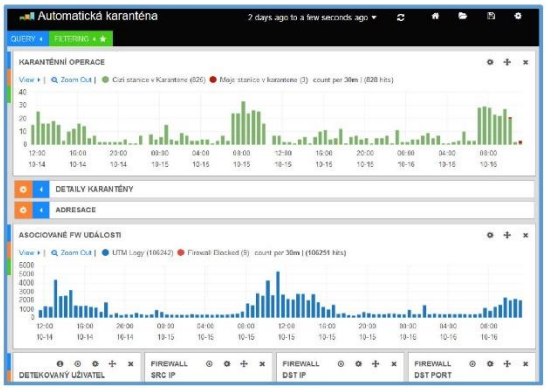
LOGmanager je HW řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Je založen na výkonné databázi s obrovskou kapacitou, rychlým vyhledáváním ve "velkých datech" a okamžitou vizualizací vyžádaných dat. Jeho podstatou je sběr, dlouhodobé nezpochybnitelné ukládání a analýza strojových dat organizace. Umožňuje prohledávat agregovaná data v reálném čase, vytvářet analýzy, reporty a upozornění na události korelované z dat více zdrojů. Nedílnou součástí řešení LOGmanager je taktéž podpora souladu s požadavky zákonných norem. Při správné implementaci pomůže organizaci k zajištění shody s ČSN/ISO 27001:2013 o pořizování auditních záznamů, plnění požadavků GDPR či Zákona o kybernetické bezpečnosti. LOGmanager však není určen pouze pro oddělení bezpečnosti IT. Při vývoji LOGmanageru je kladen velký důraz na radikální jednoduchost užívání a jeho reálný přínos pro IT obecně. LOGmanager na jednom místě shromáždí provozní a diagnostická data ze všech důležitých systémů organizace. Operátor IT tak dostane možnost zjistit během několika sekund informace o provozních stavech a případných závadách, které by jinak musel hodiny komplikovaně vyhledávat v distribuovaných zdrojích. K tomu je i automaticky informován o sledovaných událostech a může tak předcházet kritickým IT nebo bezpečnostním incidentům.

## Podporovaná zařízení

LOGmanager nativně podporuje více než 125 zdrojů ze všech oblastí IT, od bezpečnostních řešení, přes sítě, virtualizace, operační systémy, databáze, až po cloud aplikace. Seznam zdrojů se každou aktualizací rozšiřuje. LOGmanager dále podporuje standardizované strukturované formáty logů jako jsou CEF, LEEF, RFC5424 a JSON. Pro unikátní zdroje dat umožňuje rychlé a snadné vytvoření zákaznických parserů.

## Klíčové vlastnosti

- ⇒ Centrální úložiště logů, událostí a strojových dat organizace
- ⇒ Sjednocení formátu zdrojových logů do lidsky srozumitelné formy
- ⇒ Zpracování a vizualizace přijímaných dat v reálném čase
- ⇒ Rychlé prohledávání dat bez nutnosti znalosti SQL jazyka
- ⇒ SIEM funkce. Alerty na základě podmínek s limity a korelacemi
- ⇒ Unikátní grafické konfigurační a programovací rozhraní
- ⇒ Radikální jednoduchost a uživatelská přívětivost
- ⇒ Snadné vytváření reportů a auditních zpráv za běhu
- ⇒ Umožní snadnější splnění požadavku na shodu s regulacemi pro:
  - GDPR
  - Zákon o kybernetické bezpečnosti a návazné vyhlášky
  - ČSN/ISO 27001:2013 pro pořizování auditních záznamů
  - PCI DSS 3.2
- ⇒ Bez licenčních omezení na množství zdrojů, výkon a uložená data
- ⇒ Úsporu na licencích při budoucím rozšíření směrem k SIEM/UBA




## Konkurenční výhody

- ⇒ Trvalý příjem až 10 000 událostí za sekundu
- ⇒ Řešení „vše v jednom" - Server, OS, Aplikace, DB na jedné platformě
- ⇒ V základu diskové úložiště pro až 100TB logů
- ⇒ Podpora velkého množství zdrojových zařízení, OS a aplikací
- ⇒ Centrálně řízený klient pro sběr logů z Windows OS
- ⇒ Možnost vysoké dostupnosti v Active/Active clusteru
- ⇒ Snadná integrace se SIEM/UBA systémy třetích stran
- ⇒ Rychlé nasazení a snadné zaškolení pro běžné operace
- ⇒ Rozhraní i kompletní dokumentace v českém jazyce
- ⇒ Rozsáhlá síť spolehlivých a technicky zdatných partnerů
- ⇒ Přímá technická podpora výrobcem a možnost testování zdarma

# Typické uživatelské případy

### Shoda s předpisy

Potřebujete vzhledem ke svému působení centrální systém pro správu, analýzu a dlouhodobé uložení auditních i provozních dat. Požadujete cenově efektivní řešení bez licenčních omezení, které naplní „tickboxy" ve Vašem auditním plánu a firemní bezpečnostní politice...

### Dohled nad přístupem k síti

Plánujete nasadit centralizované řízení přístupu k drátové a bezdrátové síti a provoz IT potřebuje dohledový systém pro 802.1X. Spojit na jednom místě logy z ověřování na aktivních prvcích počítačové sítě, jednotného přihlášení přes Active Directory, zprávy z RADIUS serveru...

### Dohled nad souborovými servery

Kdo kopíroval nebo mazal citlivá data ze souborových serverů? Chcete mít pod kontrolou operace na souborových serverech a vědět kdy, kdo a jaké operace prováděl. Zasáhl vaši organizaci Ransomware a chcete cíleně obnovit pouze zašifrované soubory. Ale nevíte, co bylo zašifrováno...

### Monitoring bezpečnosti

Chcete monitorovat bezpečnostní systémy, ale používáte více platforem, ze kterých byste rádi sjednotili logy a audity do jednotného formátu. Specializované řešení je moc drahé a má omezenou podporu pouze pro některé výrobce. LOGmanager zpracuje a analyzuje logy ze všech zdrojů bez omezení...

### Sledování konfiguračních změn

Kdo, kdy a s jakým výsledkem prováděl konfigurační změny v aktivních prvcích, operačních systémech a aplikacích. Potřebujete vždy čerstvá auditní data a reporty ve své emailové schránce? Chcete mít možnost vědět, co konkrétní administrátor před půl rokem modifikoval napříč Vaším IT...

### Funkce i snadná integrace

LOGmanager obsahuje základní analytické funkce SIEM řešení. Pokud se však v budoucnosti rozhodnete pro nasazení dalšího nástroje, LOGmanager pomůže. Umožňuje selektivně sdílet strukturovaná data v mnoha formátech s produkty třetích stran. Šetří tak na licenčních poplatcích za tyto nástroje a zjednoduší jejich integraci...

### Kontrola pravidel

Chcete ověřovat, zda jsou pravidla v bezpečnostních systémech v souladu s firemní politikou...

### Sledování přístupu k aplikacím

Kdo, kdy a s jakým výsledkem prováděl operace ve Vašich aplikacích a databázích...

### Ochrana informací

Strojová data nelze modifikovat a díky certifikaci systému (dle ČSN/ISO 27001:2013) pro audit lze LOGmanager použít jako platformu pro vytváření reportů a forenzní analýzu...

## Technická specifikace jednotlivých produktů LOGmanager

| **LOGmanager Appliance se software 3.3.0 a výše** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Procesor | Paměť | Disk | RAID | Kapacita DB | Odhad retence EPS[1] - dní | Trvalé EPS[1] | Špičkové EPS[1] |
| **LOGmanager-XL** na HPE nebo DELL serveru 2U výšky s integrovaným Workload Akcelerátorem[2]. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF) | | | | | | | |
| 2x14core Intel Xeon@2.6GHz | 128GB | 12*10TB | 6 | 100TB | 5000EPS - 365dní | 10000 | 20000/10min |
| **LOGmanager-L** na HPE nebo DELL serveru 2U výšky. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF) | | | | | | | |
| 2x12core Intel Xeon@2.2GHz | 128GB | 12*4TB | 6 | 40TB | 3000EPS - 275dní | 5000 (6000[2]) | 10000/10min |
| **LOGmanager-M** HPE nebo DELL server 1U výšky. (3 roky NBD RMA, 1 nebo 3 roky SW aktualizace, 1x LOGmanager-VF) | | | | | | | |
| 1x12core Intel Xeon@2.2GHz | 64GB | 4*4TB | 5 | 12TB | 1000EPS - 230dní | 2000 | 4000/10min |
| **LOGmanager-S** DELL Tower server. (3 roky NBD RMA, 1 nebo 3 roky SW aktualizace, 1x LOGmanager-VF) | | | | | | | |
| 1x2core Intel G5500@3.8GHz | 32GB | 2*4TB | 1 | 4TB | 250EPS - 310dní | 500 | 1000/10min |
| **LOGmanager-Demo** ve formátu Intel NUC - pouze jako neprodukční box pro lab nebo na PoC. (3 roky NBD RMA, 1 nebo 3 roky SW aktualizace, 1x LOGmanager-VF) | | | | | | | |
| 1x2core Intel i5@2.6GHz | 32GB | 1*500GB | N/A | 490GB | 250EPS - 30dní | 500 | 1000/10min |
| **LOGmanager Forwarder** (řešení pro bezpečný a spolehlivý sběr logů ze vzdálených poboček a z Internetu/DMZ) | | | | | | | |
| Procesor | Paměť | Disk | RAID | Kapacita DB | Odhad retence | Trvalé EPS[1] | Špičkové EPS[1] |
| **LOGmanager-VF** Virtuální forwarder s 8, 16 nebo 128GB diskového prostoru ve verzi pro HyperV a VMWARE. (1 rok SW aktualizace) | | | | | | | |
| 2*vCPU | 4GB vRAM | 8/16/128GB vDisk | N/A | 8/16/128GB | N/A; pracuje pouze jako mezipaměť | 9000 | 18000/10min |
| **LOGmanager-HF** Fyzický forwarder ve formátu Intel NUC. (3 roky NBD RMA, 1 rok SW aktualizace) | | | | | | | |
| 1x2core Intel i3@2.4GHz | 8GB | 120GB | N/A | 120GB | N/A; pracuje pouze jako mezipaměť | 9000 | 18000/10min |
| **LOGmanager Workload Accelerator**[2] (Nativně integrován v LOGmanager-XL nebo jako volitelné rozšíření pro LOGmanager-L) | | | | | | | |
| **LOGmanager-A** Přídavný 3.2TB NVMe modul k akceleraci zpracování near-realtime operací **LOGmanager-XL** a **LOGmanager-L**. | | | | | | | |
| EPS[1] - očekávané množství událostí za sekundu, Log mix s RAW velikostí logů průměrně 700Byte. Odhad retence pro 24hodinové zpracování daného objemu EPS. | | | | | | | |

## Informace o výrobci a reference

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto produktového listu nalezl LOGmanager více jak 160 spokojených zákazníků a na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější reference přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.

Příloha č. 1c Smlouvy

Soulad s požadavky ZoKB a VoZK


## LOGmanager a soulad s požadavky Zákona o kybernetické bezpečnosti

Whitepaper ilustrující, jak nasazení platformy LOGmanager napomáhá zajistit dodržování požadavků Zákona č. 181/2014 Sb. o kybernetické bezpečnosti (dále jen ZKB) a Vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti (dále jen VKB).

Mnoho organizací řeší otázku, jaká kontrolní opatření a v jakých oblastech jsou dle požadavků ZKB a VKB povinny dodržovat. Také se zamýšlejí nad tím, jaké systémy a řešení jim mohou spolehlivé dodržování těchto požadavků zajistit. Tento dokument popisuje, jak lze dosáhnout splnění některých důležitých požadavků těchto právních norem, a to zavedením vhodného systému centrálního sběru a řízení bezpečnostních událostí postaveného na platformě LOGmanager.

## Přehled pro vedoucí pracovníky na pozicích CISO/CIO – požadavky ZKB / VKB a platforma LOGmanager

Dne 1. ledna 2015 vstoupil v účinnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů - zkráceně ZKB a jeho prováděcí právní předpisy – vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích se změnami ve vyhlášce č. 205/2016 Sb. a vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - zkráceně VKB. ZKB i VKB jsou průběžně novelizovány a doporučujeme sledovat jejich aktuální znění. Tento dokument pracuje s aktuálním zněním ZKB k 7.březnu 2018 a VKB k 28.květnu 2018.

Stručně k ZKB a povinným subjektům - ZKB v §2 vymezuje jednotlivé pojmy a v §3 specifikuje seznam povinných subjektů takto:

a) **Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací** - specifikováno dle Zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

b) **Orgán nebo osoba zajišťující významnou síť** - významná síť zajišťuje přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťuje přímé připojení ke kritické informační infrastruktuře.

c) **Správce a provozovatel informačního systému kritické informační infrastruktury** - kritickou informační infrastrukturou je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti dle § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů a Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

d) **Správce a provozovatel komunikačního systému kritické informační infrastruktury.**

e) **Správce a provozovatel významného informačního systému** - významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Významné informační systémy jsou specifikované vyhláškou č. 314/2014 Sb., která byla novelizována vyhláškou č. 205/2016 Sb. s novou jmennou specifikací významných informačních systémů.

f) **Správce a provozovatel informačního systému základní služby -** informačním systémem základní služby je informační systém, na jehož fungování je závislé poskytování základní služby.

g) **Provozovatel základní služby** - základní službou je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl.

h) **Poskytovatel digitální služby a zástupce poskytovatele digitálních služeb** - digitální službou je služba informační společnosti podle zákona upravujícího některé služby informační společnosti dle § 2 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

www.logmanager.cz

ZKB v hlavě II specifikuje způsob zajištění kybernetické bezpečnosti. Příslušné prováděcí právní předpisy, zejména VKB, pak detailně stanovují obsah bezpečnostních opatření, postup při kybernetickém bezpečnostním incidentu a realizaci reaktivních opatření.

Zájemcům o podrobné prostudování výše jmenovaných právních norem jsou tyto v úplném znění k dispozici na následující webové adrese: https://www.govcert.cz/ v menu ZKB / Legislativa a v menu ZKB / Povinné osoby. Pro účely tohoto dokumentu je důležité, jak ZKB a VKB stanovují organizační a technická opatření a jakým způsobem LOGmanager může přispět k naplnění požadavků na realizaci některých z těchto opatření.

## LOGmanager - stručný popis

LOGmanager byl vyvinut jako systém pro centralizovanou správu protokolů událostí (logů) poskytující jednoduché zobrazení všech strojově generovaných dat v organizaci. V prvním kroku LOGmanager shromažďuje, sjednocuje a dlouhodobě uchovává protokoly událostí a záznamy o událostech z aktivních síťových prvků, bezpečnostních zařízení, operačních systémů a aplikačního softwaru. Následně v „téměř reálném čase" (near real-time) převádí shromážděná data do dobře definované výkonné databáze, ke které mohou IT bezpečnostní specialisté přistupovat prostřednictvím předdefinovaných řídicích panelů a strukturovaného i fulltextového vyhledávání s grafickým zobrazením výsledků. To může být použito, mimo jiné, i pro plnění účelu bezpečnostních opatření podrobně specifikovaných vyhláškou o kybernetické bezpečnosti. LOGmanager dále poskytuje základní SIEM funkce, jako jsou upozornění s limity a jednoduché korelace. Pro nasazení za účelem získání souladu s ZKB/VKB jsou tyto integrované SIEM funkce dostatečné. Pokud však zákazník požaduje pokročilé analytické a korelační funkce, LOGmanager poskytuje snadnou integraci s dalšími nástroji používanými v organizaci pro účely monitorování, zabezpečení nebo analýzy dat.

## LOGmanager a jeho vztah k ZKB/VKB

LOGmanager pomáhá všem povinným subjektům (ve vztahu ke KII, VIS, PZS a PDS) především s dodržováním povinností vyplývajících z následujících požadavků ZKB/VKB:

- Přijmout organizační a technická opatření k řízení rizik.
- Přijmout opatření k předcházení incidentů narušujících bezpečnost.
- Vést bezpečnostní dokumentaci.
- Hlásit kybernetické bezpečnostní incidenty.
- Poskytovat regulační autoritě součinnost k posouzení bezpečnosti.
- Specificky pro KII a VIS povinnost provozovatele předat správci data, provozní údaje a informace, které v souvislosti s provozem KII a VIS vznikly.

Pro výše uvedené povinnosti LOGmanager poskytuje mechanismy protokolování, upozorňování a zajišťuje schopnost zpětně dohledat aktivity systémů i uživatelů a provádět jejich průběžný i nárazový audit. To je kriticky důležité pro prevenci, odhalování nebo minimalizaci dopadů narušení (kompromitace) dat i systémů, které jsou subjektem ZKB/VKB. Vzhledem k tomu, že LOGmanager v rámci jednoduchého zobrazení poskytuje přístup ke všem strojovým datům, lze v případě, že je zjištěn problém, provádět podrobné sledování, aktivovat výstrahy a zajistit podrobnou analýzu. Ve zkratce se jedná o aplikaci pro shromažďování, ukládání a analýzu protokolů událostí, která umožňuje nákladově efektivní automatizaci bezpečnostních opatření specifikovaných v ZKB a VKB a proaktivní ochranu informačních systémů a elektronických sítí.

LOGmanager splňuje bez výhrad požadavky normy ČSN ISO/IEC 27001:2013 na pořizování auditních záznamů. Potvrzení od autorizovaného auditora je na vyžádání u výrobce LOGmanager řešení k dispozici.

## Podrobněji pro specialisty bezpečnosti

Soupis oblastí, kde LOGmanager poskytuje součinnost při realizaci povinností a opatření vyplývajících ze ZKB/VKB. Bezpečnostní opatření a opatření k předcházení incidentů - paragrafy VKB.

### Požadovaná organizační opatření:

§ **10 Řízení provozu a komunikací.** LOGmanager sleduje kybernetické bezpečnostní události a zajišťuje ochranu přístupů k vzniklým záznamům.

§ **12 Řízení přístupu.** LOGmanager umožňuje sledovat, zda uživatelé a administrátoři pro přístup k prostředkům informačního a komunikačního systému využívají jedinečné, nikoliv sdílené identifikátory.

§ **14 Zvládání kybernetických bezpečnostních událostí a incidentů.** LOGmanager pomáhá při detekci a vyhodnocování bezpečnostních událostí a incidentů a zlepšuje možnosti koordinace při řešení IT incidentů obecně. Z hlediska koordinace - všechna důležitá strojová data se nacházejí v lidsky srozumitelném formátu v jednom strukturovaném úložišti, čímž zrychluje provedení analýzy základních příčin incidentu (RCA—Root cause analysis) a následné provedení nápravy.

§ **16 Audit kybernetické bezpečnosti.** LOGmanager je nástroj podporující provedení nárazového i periodického auditu dodržování bezpečnostních politik a poskytuje platformu pro roli auditora kybernetické bezpečnosti.

**Požadovaná technická opatření:**

§ **22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů.** Zde je hlavní doména LOGmanageru. LOGmanager provádí nezpochybnitelné a dlouhodobé uložení zaznamenaných bezpečnostních a provozních událostí aktivit informačního a komunikačního systému. Spolupracuje při jednoznačné síťové identifikaci zařízení původce a zaznamenává požadované informace jak z hlediska obsahu, struktury, tak i činnosti. Dle modelu LOGmanageru a množství sbíraných strojových dat dokáže poskytnout dostatečnou retenci pro naplnění požadavku na nezpochybnitelné ukládání záznamů událostí po dobu 12 nebo 18 měsíců. A to bez nutnosti využívat externí datové úložiště.

§ **24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.** LOGmanager je nástroj, který provádí sběr a nepřetržité hodnocení kybernetických bezpečnostních událostí na základě upozornění a korelací. Poskytuje rychlé vyhledání a seskupení souvisejících záznamů. Dále poskytuje informace pro určené bezpečnostní role a umožní nastavení pravidel pro včasné varování o vzniklých bezpečnostních událostech.

§ **26 Kryptografické prostředky.** LOGmanager umožňuje upozorňovat na využívání méně odolných algoritmů, klíčů i protokolů, než je uvedeno v doporučení vydaném Úřadem.

**Kybernetický bezpečnostní incident:**

§ **32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů.** LOGmanager pomáhá splnit náležitosti hlášení bezpečnostního incidentu. A to zejména tím, že události zaznamenává v nezpochybnitelné podobě, s přesnou identifikací informačního a komunikačního systému, důvěryhodným časovým razítkem a poskytne potřebné informace k vytvoření podrobného popisu incidentu.

## LOGmanager - vlastnosti vzhledem k požadavkům ZKB/VKB

LOGmanager je nástroj umožňující nebo alespoň zjednodušující realizaci opatření uvedených na předchozí stránce. Poskytuje podporu pro zvládnutí kybernetických událostí a kybernetických bezpečnostních incidentů. Operátorům bezpečnosti IT dává prostředky na kontrolu i audit. Jednoznačným a nezpochybnitelným způsobem zaznamenává činnost systémů, umožňuje detekci, sběr a vyhodnocení bezpečnostních událostí a dokáže ze získaných strojových dat průběžně monitorovat dostupnost informací. V případě kontroly plnění povinností vyplývajících ze ZKB/VKB je obvykle v oblasti technických opatření, podporovaných LOGmanagerem, konstatována shoda. Samozřejmě za předpokladu správného nasazení LOGmanageru.

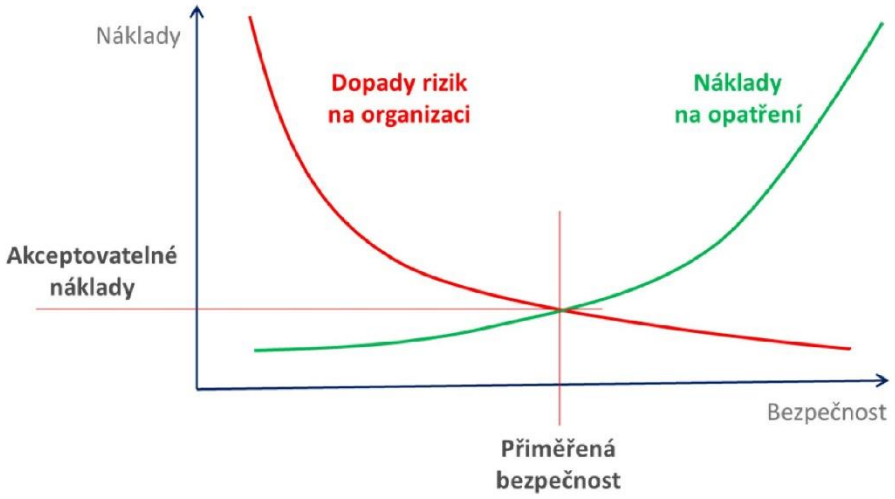
LOGmanager poskytne podporu při vytváření podkladů pro hlášení bezpečnostního incidentu v požadovaném formátu. Umožňuje organizaci poskytnout součinnost k posouzení bezpečnosti systémů, které jsou subjektem ZKB. Díky dostatečné retenci uložených strojových dat umožňuje vytvořit auditní záznamy a podklady pro hlášení a následnou forenzní analýzu detekovaných bezpečnostních událostí, i když doba od vzniku bezpečnostní události a jejího zjištění se značně liší*.

**Poznámka:** On-Line retence dat je závislá na modelu LOGmanageru a množství a typu sbíraných strojových dat. Například u modelu LOGmanager-XL s kapacitou databáze 100TB dosahuje při trvalém sběru 3000 událostí za sekundu, díky vylepšenému kompresnímu mechanismu, průměrně 2 roky. Dle doporučení Národního centra kybernetické bezpečnosti pro síťové správce v.2 (k dispozici zde: https://www.govcert.cz/cs/informacni-servis/doporuceni/2607-bezpecnostni-doporuceni-nckb-pro-sitove-spravce-nova-verze-2-0/) splňují všechny modely LOGmanager požadované retence dat, požadavky na kontrolu integrity, požadavky na šifrování logů a požadavky na **šifrovaný**[1] přenos logů do nástroje na zaznamenávání událostí .

[1] *pokud je podporováno zdrojovým systémem*

## LOGmanager - zhodnocení nákladů na řešení a přínosů pro organizaci

Před realizací zákonem požadovaných opatření je vhodné provést analýzu rizik a zhodnotit celkové náklady na různé varianty řešení, a to při maximálním zachování souladu s regulacemi. LOGmanager poskytuje vyvážený poměr na vynaložené náklady na řešení při dostatečném plnění bezpečnostních a technických opatření vyžadovaných ZKB/VKB.




Hlavní výhody LOGmanager řešení pro organizace hledající optimální poměr mezi dosaženou bezpečností a rozumnými náklady:

- Rychlá implementace. Pro dosažení souladu s regulacemi postačuje implementace v řádu dní.
- Obsahuje základní SIEM funkce a vzorové alerty i korelace pro typické uživatelské příklady.
- Snadné zaškolení obsluhy. Uživatelsky přehledné a intuitivní ovládání v češtině.
- Důsledná dokumentace v češtině i angličtině a návody pro vhodné nastavení zdrojů událostí.
- Nízké, a hlavně přesně definované náklady na provoz řešení. Hardware, software, služby v ceně.
- Žádné skryté licenční náklady, LOGmanager neobsahuje licenční omezení.
- Soulad s normou ČSN ISO/IEC 27001:2013, splnění požadavků regulací.

Závěrem: I když vaše organizace prozatím nepatří mezi povinné subjekty dle ZKB, může Vaše organizace prokázat zodpovědný přístup („due diligence“ and „due care“) k bezpečnosti informací a IT systémů realizací opatření uvedených v doporučeních Národního centra pro kybernetickou bezpečnosti.

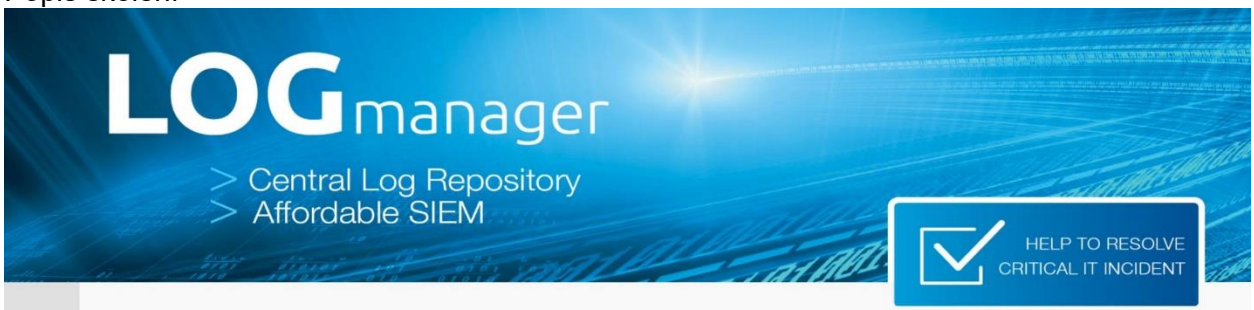
Autor: Ing. Miroslav Knapovský, CISSP, CEH, CCSK
Security Solution Architect
Email: knapovsky@logmanager.cz
Vytvořeno dne 19.6.2018

## INFORMACE O VÝROBCI A REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto whitepaperu nalezl LOGmanager více jak 120 spokojených zákazníků a na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější reference přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, Vám rádi předáme.

Příloha č. 1c Smlouvy

Popis školení




# Školení LOGmanager

## Popis školení

Výrobce řešení LOGmanager (Sirwisa a.s.) ve spolupráci s distributorem Veracomp nabízí tři typy školení. První dva typy školení jsou klasické, ve školícím středisku distributora – Dvoudenní **Technické certifikační** školení, jednodenní **Operátorské** školení. Tato školení mají nejen odlišný obsah, ale i cílového studenta – uživatele řešení. Obě školení kombinují lektorem vedené přednášky s praktickým cvičením uživatelských případů na demo zařízení. Maximální počet účastníků na těchto školeních je stanoven na 12 osob. Posledním typem školení je **Zákaznické** školení na objednávku v prostorách zadavatele. Všechna školení jsou uvedena v ceníku LOGmanager, termíny na klasická školení se pravidelně vypisují na stránkách autorizovaného distributora zde:

https://www.veracomp.cz/cz/kalendar-akci nebo https://www.veracomp.sk/kalendar/.

## Technické certifikační školení - obj. kód: LOGM-EDU-CERT

Technické certifikační školení je primárně určeno pro techniky partnerských společností prodávajících řešení LOGmanager. Jedná se o dvoudenní školení. Účast na tomto školení je, mimo jiné, povinná pro získání statusu Certifikovaný partner LOGmanager. Školení však není omezeno pouze pro partnery, ale je vhodné i pro administrátory řešení koncových zákazníků, kteří se zabývají instalací, implementací, případně integrací řešení v rámci infrastruktury dlouhodobě. Je vhodným startovacím můstkem pro ty, kteří se chtějí nebo potřebují dozvědět o LOGmanageru úplně vše a získat schopnosti nejen řešení využívat, ale aktivně vylepšovat pro potřeby dané účelem pořízení řešení. Technické certifikační školení je zakončeno certifikačním testem a vystavením certifikátu výrobce, který je platný na období dvou let.

## Obsah Technického certifikačního školení

**1. den školení (9:00-17:00)**

Seznámení se s LOGmanagerem
Co jsou to logy, události a strojová data
Architektura LOGmanageru a komunikační matice
První kroky v konfiguraci (quick start) s LMDemo
Upgrade/Downgrade systému, zálohování
Pokročilé možnosti nastavení síťového subsystému
Správa uživatelů a uživatelských oprávnění
Průběh toku logů uvnitř LOGmanageru
Tagování logů – jak jednoduše značkovat logy
Parsovací pravidla – vysvětlení činnosti a ukázka tvorby

**2. den školení (9:00-17:00)**

Zdroje – možnosti sběru logů ze systémů
Logování z Windows a Windows aplikací
Forwarder – vysvětlení činnosti a ukázka konfigurace
Dashboardy - jak „dolovat" data, vytvářet dashboardy a reporty
Alerty – princip činnosti, konfigurace a testování nových alertů
Šablony pro notifikaci alertů
Rekapitulace, test
Otázky a odpovědi

## Operátorské školení - obj. kód LOGM-EDU-OPER

Operátorské školení je pouze jednodenní a klade si za cíl seznámit operátora LOGmanageru s nejčastějšími postupy při využívání řešení. Operátorem je zde zamýšlen uživatel, který neprovádí kompletní nastavení a údržbu systému, ale ve své pracovní činnosti využívá LOGmanager k vyhledávání informací ze shromážděných strojových dat, provádí ad-hoc analýzy, audity, či chce vytvářet uživatelské dashboardy, pravidelné reporty, případně jednoduché alerty. Operátor se na školení seznámí se základní logikou řešení a naučí se LOGmanager uživatelsky ovládat se všemi aspekty tak, aby mohl být jeho aktivním uživatelem. Po školení obdrží účastník potvrzení o absolvování školení.

**Obsah Operátorského školení:**

Seznámení se s LOGmanagerem
Co jsou to logy, události a strojová data
Architektura LOGmanageru
Průběh toku logů uvnitř LOGmanageru
Vyhledávání v dashboardech, vytváření nových dashboardů, reporty a export dat
Základy vytváření a testování alertů
Otázky a odpovědi, rekapitulace.

## Zákaznické školení - obj. kód: LOGM-EDU

Zákaznické školení je na objednávku v prostorách zadavatele (doporučujeme rezervovat zasedací nebo školicí místnost) a na technickém vybavení zadavatele. Zákaznické školení se objednává na dny, Sirwisa a.s. provede návrh obsahu školení . Po odsouhlasení obsahu a termínu technik školení realizuje. Zákaznické školení je obvykle jedno až třídenní a doporučený počet účastníků je do 8 osob.

**Pár slov závěrem:** Hlavním cílem realizace školení je maximální spokojenost zákazníků. Přestože LOGmanager řešení se soustředí na radikální jednoduchost, doporučujeme nějakou formu školení vždy zvážit a následně absolvovat. Jakékoliv školení lze do určité míry nahradit školením v průběhu instalace certifikovaným partnerem nebo objednáním instalace LOGmanageru výrobcem, ale i tak doporučujeme s jistou prodlevou po instalaci se vybraného školení zúčastnit. Po účasti na školení je vhodné, aby se účastnici registrovali na uživatelském fóru LOGmanager – https://forum.logmanager.cz/, kde naleznou mnoho dalších užitečných rad a on-line návodů (typu krok za krokem), jak si snáze s LOGmanagerem poradit.

Zpětnou vazbu na školení, žádosti o vypsání nových termínů prosím adresujte na email: obchod@logmanager.cz
Případně nám zavolejte do kanceláře na telefon: +420 257 211 849

## INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.

# *F. SEZNAM NÁROKŮ NA SOUČINNOST*

Schválení implementačního plánu

Připravené redundantní napájení pro jeden 1U server s dvěma napájecími zdroji 230 V 50 Hz
Připravená síťová infrastruktura vč. adresování
Připravený prostor v datacentrovém rozvaděči, racku, o velikosti minimálně 1U

Zajištění přístupu – fyzického – při instalaci
Zajištění přístupu – vzdáleného – při konfiguraci