



## » 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 spolehlivě 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, bankovníctví, 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).

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 nepřetržitě 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.

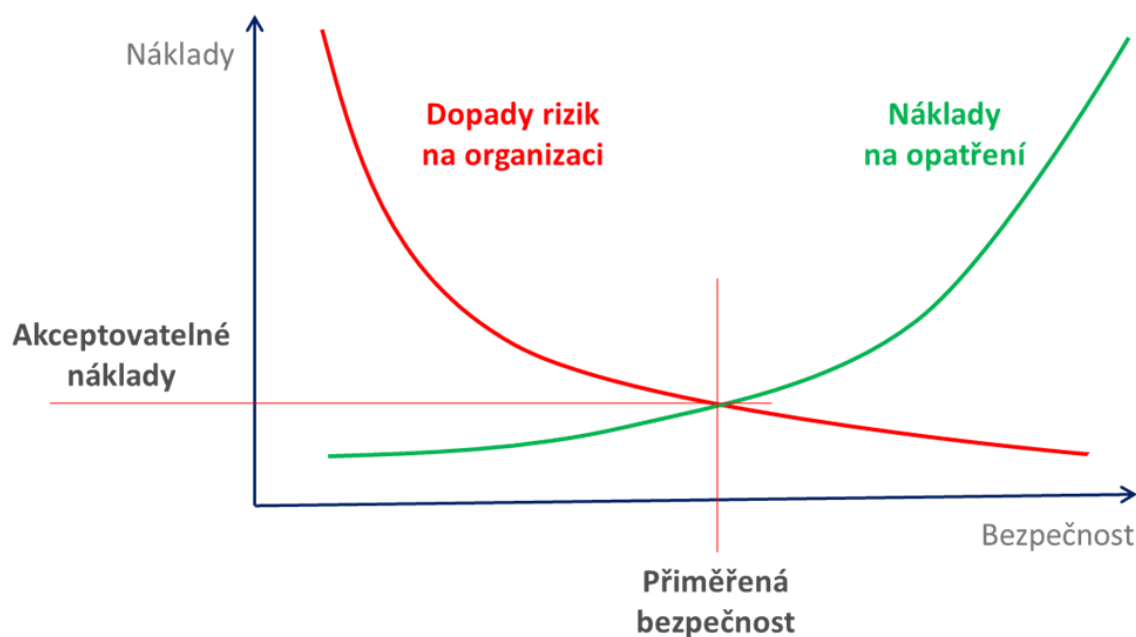
LOGmanager poskytne podporu při vytváření podkladů pro hlášení bezpečnostního incidentu v požadovaném formátu. Umožňuje organizaci poskytnout součinnost k posouzení bezpečnosti systémů, které jsou subjektem ZKB. Díky dostatečné retenci uložených strojových dat umožňuje vytvořit auditní záznamy a podklady 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<sup>1</sup> přenos logů do nástroje na zaznamenávání událostí.

<sup>1</sup>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 bezpečnost.

Autor: Ing. Miroslav Knapovský, CISSP, CEH, CCSK  
Security Solution Architect

Email: [knapovsky@logmanager.cz](mailto: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](http://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 bankovníctví 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.