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. 316/2014 Sb. o kybernetické bezpečnosti (dále jen VKB) v aktuálním znění.

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 zavedením vhodného systému centrálního sběru a řízení bezpečnostních událostí postaveného na platformě LOGmanager.

Stručný 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 (ZKB) a jeho prováděcí právní předpisy – vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (VKB). Dále bylo novelizováno nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (tato novela je zveřejněna ve Sbírce zákonů pod číslem 315/2014 Sb.) a probíhá novelizace ZKB s předpokládanou účinností od září 2017.

ZKB specifikuje v §3 seznam povinných subjektů – poskytovatele služeb elektronických komunikací, správce a provozovatele Kritické Informační Infrastruktury (KII), správce a provozovatele Významného Informačního Systému (VIS), které se musí ZKB a VKB řídit. Po novelizaci zákona přibude ve struktuře povinných subjektů nově i Provozovatel Základní Služby (PZS) a Poskytovatel Digitální Služby (PDS). Touto novelizací se tak působnost ZKB rozšiřuje o informační systémy, jejichž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví. Provozovatel základní služby: energetice, dopravě, bankovnictví, infrastruktuře finančních trhů, zdravotnictví, vodním hospodářství, digitální infrastruktuře, chemickém průmyslu. Provozovatel digitální služby: on-line tržiště, internetové vyhledávače a cloud computing. Novelizace taktéž zavádí nové přestupky a zvyšuje sankce za správní delikty vyvozené ze ZKB a VKB až na 5.000.000 Kč.

ZKB v hlavě II dále specifikuje způsob zajištění kybernetické bezpečnosti. Pro účely tohoto dokumentu je důležité, jak definuje v kategoriích organizační a technická opatření. Příslušné prováděcí právní předpisy pak stanovují obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace a specifikují povinné subjekty a jejich určující kritéria.

Zájemcům o podrobné prostudování výše jmenovaných právních norem jsou tyto v úplném znění k dispozici na následující adrese:
https://www.govcert.cz/cs/legislativa/legislativa/.

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 specifikovaných ZKB. LOGmanager navíc poskytuje i výkonné aplikační rozhraní podporující integraci s dalšími nástroji používanými v organizaci pro účely monitorování i zabezpečení.

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
- Oznamovat incidenty
- Poskytovat regulační autoritě součinnost k posouzení bezpečnosti
- A specificky pro KII a VIS pak 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 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 27001:2014 na pořizování auditních záznamů. Potvrzení od autorizovaného auditora je na vyžádání u výrobce LOGmanager, firmy Sirwisa a.s. k dispozici.

Podrobněji k jednotlivým povinnostem vyplývajícím ze ZKB/VKB, kde LOGmanager poskytuje součinnost při realizaci opatření:

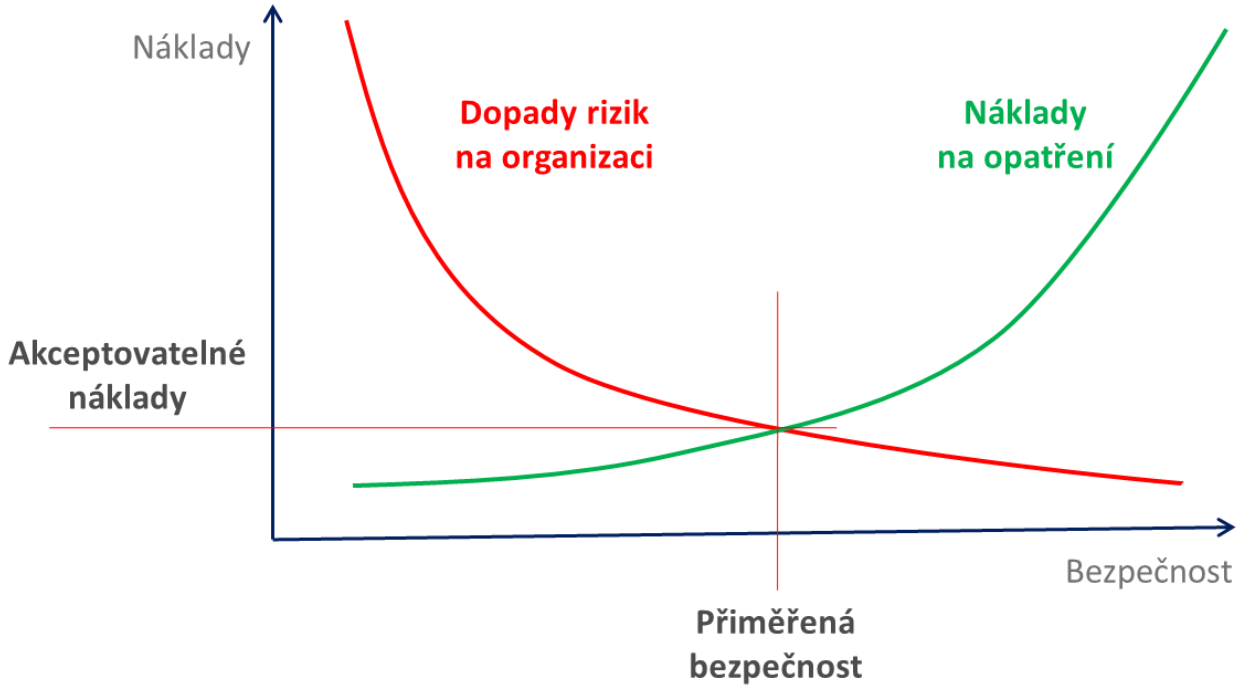
Bezpečnostní opatření a **opatření k předcházení incidentů** - §5 ZKB
Požadovaná organizační opatření:
2 k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
2 m) kontrola a audit kritické informační infrastruktury a významných informačních systémů
Požadovaná technická opatření:
3 f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
3 g) nástroj pro detekci kybernetických bezpečnostních událostí
3 h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
3 k) nástroj pro zajišťování úrovně dostupnosti informací

LOGmanager je nástroj umožňující realizaci těchto opatření. 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, za předpokladu správného nasazení LOGmanageru, v povinném subjektu minimálně v oblasti technických opatření konstatována plná shoda se zákonnými požadavky.

Povinnost oznamovat incidenty a **poskytovat regulační autoritě součinnost**:
LOGmanager podporuje vytvoření podkladů pro oznámení bezpečnostního incidentu v požadovaném formátu a umožňuje organizaci poskytnout součinnost k posouzení bezpečnosti systémů, které jsou subjektem ZKB. Díky dostatečné retenci uložených strojových dat umožnuje vytvořit auditní záznamy a podklady pro oznámení a následnou forenzní analýzu detekovaných bezpečnostních událostí, i když doba od vzniku bezpečnostní události a jejího zjištění se značně liší*.
** Retence dat je závislá na modelu LOGmanageru a množství a typu sbíraných strojových dat. U modelu XL LOGmanager s kapacitou databáze 100TB dosahuje při trvalém sběru 3500 událostí za sekundu průměrně 450 dní. Dle doporučení Národního centra kybernetické bezpečnosti (k dispozici zde:* https://www.govcert.cz/download/doporuceni/container-nodeid-1259/logmngmntfinal.pdf *) splňují všechny modely LOGmanager požadované retence dat, požadavky na kontrolu integrity, požadavky na šifrování logů a požadavky na šifrovaný přenos logů do log managementu.*

Povinnost provozovatele předat správci data, provozní údaje a informace (pro KII a VIS):
LOGmanager umožnuje předat, v přesně specifikovaném formátu tabulky, provozní údaje (strojová data) a informace, které v souvislosti s činnostmi které jsou subjektem regulace, vznikly.

Před realizací zákonem požadovaných opatření je třeba provést analýzu rizik a zhodnotit celkové náklady na různé varianty řešení, a to při maximálním zachování souladu s regulacemi.



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.
- 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 27001:2014, splnění požadavků regulací.

Závěrem: I když vaše organizace prozatím nepatří mezi povinné subjekty dle ZKB, můžete prokázat osobní zodpovědnost („due diligence“ and „due care“) za bezpečnost informací realizací výše uvedených opatření. Podobný přístup si nakonec od 28. května 2018 vyžádá i GDPR.

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