LOGmanager a soulad s požadavky GDPR

Whitepaper ilustrující, jak nasazení platformy LOGmanager napomáhá zajistit dodržování požadavků NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 (GDPR). Toto nařízení stanovuje závazná pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů.

V roce 2012 Evropská komise navrhla důkladnou revizi Evropské Data Protection Direktivy 95/46/EC. To se stalo základem nové regulace obecně známé pod pojmem General Data Protection Regulation (dále jen GDPR), schválené v dubnu 2016. Harmonizuje doposud mnohdy rozdílné zákony týkající se ochrany osobních údajů a nakládání s nimi, a to napříč všemi státy Evropské Unie. Vejde v účinnost od 25. května roku 2018 a týká se všech organizací, které zpracovávají osobní údaje občanů EU, a to uvnitř i mimo Evropskou unii. Mezi základní požadavky GDPR patří zejména:

- Zvýšit práva občanů Evropské unie při nakládání s jejich osobními daty.
- Zahrnout do vývoje a nasazení software zpracovávajících osobní data požadavek na bezpečnost dat i vlastních systémů (privacy by design and by default).
- V maximální možné míře chránit osobní údaje, doporučeně za použití anonymizace, pseudonymizace a šifrování.
- Chránit data, jejich dostupnost, důvěrnost i vlastní proces zpracovávání osobních údajů.
- Vytvořit nové role a procesy v organizaci tak, aby byl posílen dohled nad bezpečností osobních údajů.
- Pravidelně testovat, posuzovat a hodnotit účinnost zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracovávání.
- Povinnost do 72 hodin nahlásit zjištění, týkající se porušení tohoto zákona nebo ztráty osobních údajů, příslušným regulačním orgánům.

S cílem posílit prosazování této regulace je v této právní normě obsaženo i ustanovení o sankcích včetně správních pokut, které mohou dosahovat astronomických částek. Bohužel nařízení Evropského parlamentu a Rady EU 2016/679 stanovuje, že tyto sankce je nutné v maximu uplatňovat, s možným náhradním opatřením jen ve vztahu k fyzickým osobám.

Protože tato regulace je napsaná ne zrovna srozumitelným úředním jazykem, mnoho organizací řeší otázku, jaká opatření a v jakých oblastech jsou dle požadavků GDPR 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 této právní normy zavedením vhodného systému centrálního sběru a řízení bezpečnostních událostí postaveného na platformě LOGmanager.

Stručný přehled pro vedoucí pracovníky na pozicích CISO/CIO
GDPR a platforma LOGmanager

LOGmanager a jeho vztah k GDPR: Stručně řečeno, LOGmanager umožnuje organizaci průběžně i nárazově auditovat a v případě zjištění porušení tohoto zákona i jednoznačně prokázat, **kdo, kdy a jakým způsobem přistupoval k datům a systémům, které jsou subjektem GDPR**.

LOGmanager je certifikovanou platformou pro pořizování auditních záznamů dle ISO/ČSN 27001:2014. Na šifrovaném* diskovém úložišti ukládá a dlouhodobě udržuje ve své centrální, indexované a kompresované databázi informace o událostech ze všech zdrojů, které ji svoje události předávají. Tyto události jsou normalizované pro snadné použití, ale současně uloženy i v původní podobě. A to s jednoznačným identifikátorem a důvěryhodným časovým razítkem. Ověřovací a autorizační mechanismy LOGmanageru i jeho vnitřní kontrolní mechanismy zajištují, že k uloženým datům mohou přistupovat jen pověřené osoby a data nelze žádným známým způsobem modifikovat nebo částečně odstranit.
** šifrování je dostupné pouze pro LOGmanager běžící na serverech HPE za využití HPE Secure Encryption.*

Přestože zavedení auditu je důležitým článkem v celém řetězci opatření, je nutné upozornit na to, že je to jen jedno z mnoha opatření. Na druhou stranu nelze jednoznačně konstatovat, že ani zavedení všech technických a organizačních opatření dle této regulace vyvazuje firmu ze zodpovědnosti za možné nedodržení cílů této regulace. (*Ano, takto vytvořená právní norma ve svých možných důsledcích vypadá opravdu děsivě. Ale není nutné předcházet a vytvářet katastrofické scénáře. Teprve budoucí rozhodnutí soudů za porušení GDPR ukážou, jaká bude skutečná realita.*)

Podrobněji pro pracovníky IT bezpečnosti organizace

V jakých oblastech GDPR dokáže LOGmanager pomoci specificky.

Článek 32 – Zabezpečení zpracování
Článek 33 - Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu
Článek 34 - Oznamování případů porušení zabezpečení osobních údajů subjektu údajů
Článek 58 - Pravomoci

Sledovat zabezpečení zpracování dat a přístup k datům
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.

Dokonalá viditelnost do logů, událostí a ostatních strojových dat může být použita, mimo jiné, i pro plnění účelu opatření specifikovaných v GDPR. LOGmanager navíc poskytuje i výkonné aplikační rozhraní podporující integraci s dalšími nástroji používanými v organizaci pro účely monitorování i zabezpečení.

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 GDPR. 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 a proaktivní ochranu informačních systémů a elektronických sítí.

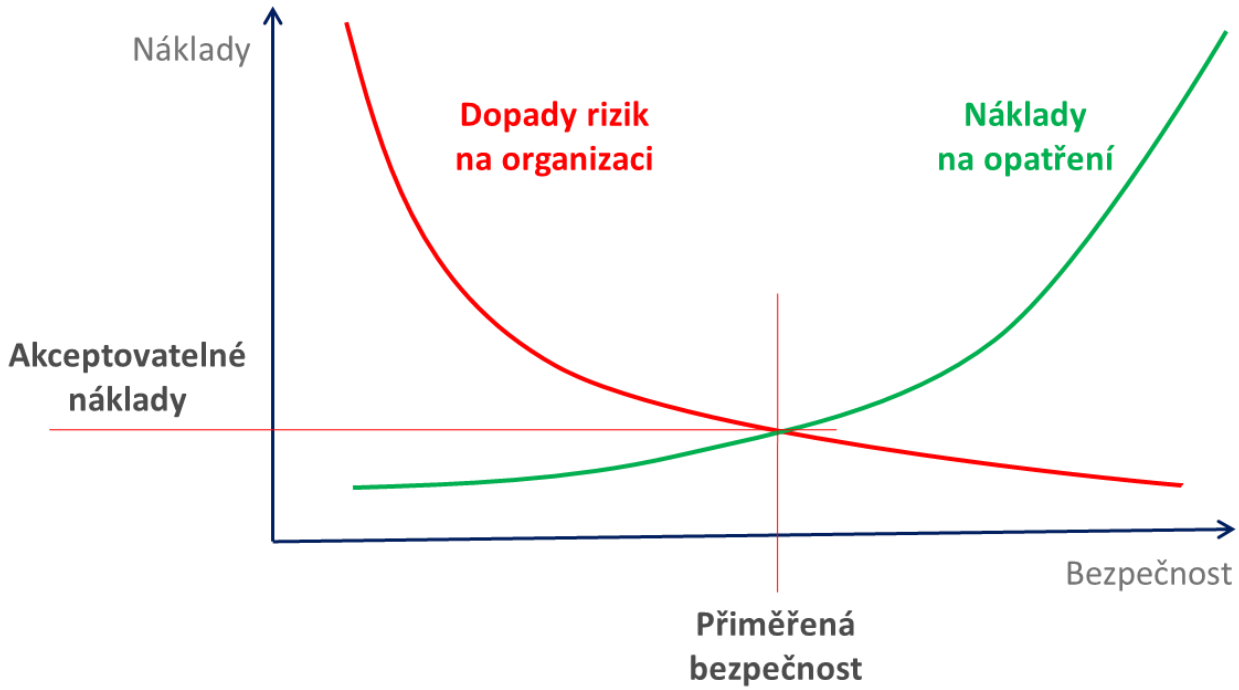
LOGmanager je tedy nástroj umožňující realizaci části opatření vyplývajících z GDPR. Poskytuje ale i podporu pro zvládnutí kybernetických událostí a kybernetických bezpečnostních incidentů. Operátorům bezpečnosti IT dává prostředky na kontrolu i audit. Jednoznačným a nezpochybnitelným způsobem zaznamenává činnost systémů, umožňuje detekci, sběr a vyhodnocení bezpečnostních událostí a dokáže ze získaných strojových dat průběžně monitorovat dostupnost informací.

Povinnost oznamovat incidenty a poskytovat dozorovému úřadu součinnost:
LOGmanager podporuje vytvoření podkladů pro oznámení bezpečnostního incidentu v požadovaném formátu a umožňuje organizaci poskytnout součinnost k posouzení bezpečnosti systémů, které jsou subjektem GDPR. 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.*

LOGmanager umožnuje předat, v přesně specifikovaném formátu tabulky, provozní údaje (strojová data) a informace, které v souvislosti s činnostmi, které jsou subjektem regulace, vznikly.

LOGmanager – správná volba pro dodržování souladu s GDPR

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 vybraných požadavků regulací.

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