LOGmanager a dodržování požadavků bezpečnostních standardů PCI DSS v3.2

Whitepaper ilustrující, jak nasazení platformy LOGmanager napomáhá zajistit dodržování požadavků standardu PCI DSS

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

Stručný přehled pro vedoucí pracovníky na pozicích CISO/CIO – požadavky standardu PCI DSS a platforma LOGmanager

Standard **PCI DSS** (Payment Card Industry Data Security Standard) byl vyvinut s cílem podpořit a posílit bezpečnost dat držitelů karet a podpořit co nejširší zavádění jednotných opatření k zabezpečení těchto dat. PCI DSS stanovuje základní technické a provozní požadavky, jejichž cílem je zajistit ochranu zákaznických dat. Ve stručnosti se jedná o soubor požadavků, testovacích postupů a doporučení týkajících se postupů, které musí splňovat všechny subjekty zpracovávající údaje o platbách platebními kartami. Standard PCI-DSS pokrývá celkem 12 oblastí a zájemcům o jeho prostudováni je v úplném znění zdarma k dispozici na následující adrese: https://www.pcisecuritystandards.org/.

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 téměř v reálném čase převádí shromážděná data do dobře definované výkonné databáze, ke které mohou IT specialisté přistupovat prostřednictvím předdefinovaných řídicích panelů a strukturovaného a fulltextového vyhledávání s grafickým zobrazením výsledků. Poskytuje také výkonné aplikační rozhraní podporující integraci s dalšími nástroji používanými ve firmě pro účely monitorování a zabezpečení.

LOGmanager pomáhá organizacím především s dodržováním požadavku č. 10 standardu PCI DSS: “Sledovat a monitorovat všechny přístupy k síťovým zdrojům a datům držitelů karet”. Poskytuje mechanismy protokolování a zajišťuje schopnost zpětně dohledat uživatelské aktivity, což je kriticky důležité pro prevenci, odhalování nebo minimalizaci dopadů narušení (kompromitace) dat.

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 analýzu. Nemáte-li k dispozici kompletní databázi protokolů, jakou poskytuje např. LOGmanager, je stanovení příčiny narušení dat velmi obtížné nebo téměř nemožné. Ve zkratce se jedná o aplikaci pro shromažďování, ukládání a analýzu protokolů událostí, která umožňuje nákladově efektivní automatizaci auditů PCI a proaktivní ochranu dat držitelů karet.

Požadavky standardu PCI DSS a jak LOGmanager přispívá k jejich naplňování

OBLAST 1 – Vybudování a udržování bezpečné sítě a systémů

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
1.2.x	Vytvořit takovou konfiguraci firewallu a routerů, která zamezuje navázání spojení mezi nedůvěryhodnými sítěmi a jakýmikoli systémovými komponentami v prostředí dat držitelů karet.	Díky schopnosti systému LOGmanager parsovat a analyzovat protokoly generované na základě nastavení pravidel firewallu a protokoly obsahující záznamy o přístupu k routeru můžete s pomocí LOGmanageru zjistit, které síťové toky jsou blokovány nebo naopak povoleny. Poskytuje rychlou analýzu, na jejímž základě lze upravit nastavení příslušných zařízení, a zamezit veškerému provozu, který není generován důvěryhodnými operacemi.
1.4.x	Instalovat osobní firewall nebo systém zajišťující obdobnou funkci na veškerá přenosná výpočetní zařízení (včetně zařízení vlastněných firmou a/nebo zaměstnancem), která se připojují na internet mimo firemní síť (například notebooky používané zaměstnanci), a které se zároveň používají k přístupu do prostředí dat držitele karty. Konfigurace firewallů (nebo jejich ekvivalentů) zahrnuje následující kroky: - definování konkrétních nastavení, - zajištění aktivního běhu osobního firewallu (nebo systému zajišťujícího ekvivalentní funkci), - uživatelé přenosných výpočetních zařízení nesmějí mít možnost měnit nastavení osobního firewallu (nebo systému zajišťujícího ekvivalentní funkci).	Díky schopnosti LOGmanageru sledovat provoz osobního firewallu může tento systém napomoci při odhalování nežádoucích operací včetně poruch, změn v konfiguraci nebo odchylek od firemní politiky upravující používání osobního firewallu. Umožňuje také centrálně shromažďovat a analyzovat protokoly a záznamy o událostech z jednotlivých zařízení a systémů a generovat odpovídající výstrahy.

OBLAST 2 – Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
2.1	Vždy změnit výchozí nastavení od dodavatele a odstranit nebo deaktivovat zbytečné výchozí účty před instalací systému do sítě.	LOGmanager může detekovat použití výchozích účtu, které by se neměly používat nebo které mají speciální nebo privilegovaná přístupová práva, jež nejsou pro dané systémy povolena, a může v takovém případě generovat výstrahu.
2.1.1	U bezdrátových technologií připojených k prostředí dat držitelů karet nebo přenášejících data držitelů karet je nutné změnit VŠECHNA výchozí nastavení od dodavatelů bezdrátových technologií včetně výchozích bezdrátových šifrovací klíčů, hesel a řetězců SNMP community strings.	LOGmanager je schopen parsovat strojová data generovaná bezdrátovými zařízeními od všech hlavních výrobců včetně SNMP TRAP zpráv. Dokáže detekovat změny konfigurace, neoprávněné úpravy a porušení politik týkajících se bezdrátového přístupu a vytvořit odpovídající výstrahu. Také dokáže detekovat útoky hrubou silou a upozornit na ně.
2.2.1	Implementovat na každém serveru pouze jednu primární funkci, aby se na jednom serveru zabránilo současné existenci funkcí vyžadujících různé úrovně zabezpečení. (Např. webové servery, databázové servery a DNS servery by měly být provozovány na oddělených serverech.)	LOGmanager může pomoci odhalit zdroje, na nichž je současně provozováno více služeb.
2.4	Spravovat inventář systémových komponent, na něž se vztahují požadavky PCI DSS.	LOGmanager dokáže vytvořit zprávu obsahující informace o systémech zjištěných v definované bezpečnostní zóně a upozornit na nové systémy, které se objeví v monitorovaných zónách, na něž se vztahují požadavky PCI DSS.

OBLAST 5 – Chránit všechny systémy proti malware a pravidelně aktualizovat antivirový software nebo programy

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
5.2	Zajistit, aby všechny antivirové mechanismy byly spravovány podle následujících bodů: - byly udržovány aktuální, - prováděly pravidelné skenování, - generovaly auditní protokoly (audit logs) uchovávané v souladu s požadavkem 10.7 PCI DSS.	LOGmanager dokáže detekovat případy, kdy soubory protokolu obsahují informace o nefunkčních nebo zakázaných funkcích běžného antivirového softwaru, a upozornit na ně. Lze vytvořit řídicí panel zobrazující téměř v reálném čase informace o aktuálním stavu antivirového softwaru nasazeného v prostředí podléhajícím požadavkům PCI DSS.
5.3	Zajistit, aby byly aktivní antivirové mechanismy a nemohly být deaktivovány ani změněny uživateli, pokud to není výslovně schváleno vedením, a to případ od případu a na omezenou dobu	Viz výše.

OBLAST 6 – Vyvíjet a udržovat bezpečné systémy a aplikace

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
6.2	Zajistit, aby všechny systémové komponenty a veškerý software byly chráněny před známými zranitelnostmi instalací příslušných bezpečnostních záplat dodávaných výrobcem. Instalovat kriticky důležité bezpečnostní záplaty do jednoho měsíce od jejich vydání.	LOGmanager dokáže detekovat dobu běhu jednotlivých serverových platforem, sledovat instalaci bezpečnostních záplat a vytvořit řídicí panel zobrazující nejméně aktulizované systémy.
6.3	Odstranit vývojové, testovací a/nebo běžné aplikační účty, uživatelská ID a hesla před uvedením aplikace do produkčního stavu nebo před jejím předáním uživateli.	LOGmanager dokáže detekovat použití testovacích nebo uživatelsky upravených aplikačních účtů, které by se v produkčních systémech neměly používat, a zobrazit příslušnou výstrahu.

OBLAST 10 – Sledovat a monitorovat všechny přístupy k síťovým zdrojům a datům držitelů karet.

Toto je oblast, kde může LOGmanager přispět k dodržování požadavků PCI DSS nejvíce.

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
10.1	Zajistit vytvoření auditních záznamů, které umožní u všech přístupů k systémovým komponentům určit konkrétního uživatele.	Pokud je jako cílový systém pro uchovávání auditních záznamů používán LOGmanager, mohou bezpečnostní technici rychle zjistit, jaké zdroje podléhají požadavkům PCI DSS, a získat informace o přístupu každého jednotlivého uživatele k systémovým komponentám podléhajícím požadavkům PCI DSS.
10.2.x	Zajistit u všech systémových komponent automatizované vytváření auditních záznamů, které umožní provést rekonstrukci následujících událostí: .1 všechny individuální přístupy uživatele k datům držitelů karet, .2 všechny činnosti jednotlivých uživatelů provedené s oprávněními administrátora nebo root, .3 přístup ke všem auditním záznamům, .4 neplatné pokusy o logický přístup, .5 použití a změny identifikačních a autentizačních mechanismů včetně vytváření nových účtů a zvyšování úrovně oprávnění a všechny změny, doplnění nebo odstranění účtů s oprávněními administrátora nebo root, .6 spuštění, zastavení nebo pozastavení vytváření auditních protokolů, .7 vytvoření a mazání objektů na systémové úrovni.	Při správné implementaci na zdroje poskytující informace o systémových událostech zajistí LOGmanager shromažďování, parsování a vhodné zobrazení informací o těchto událostech. Následně lze vytvořit výstrahy reagující na výskyt předem definovaných událostí, takže je o nich bezpečnostní technik bezodkladně informován.
10.3.x	Uchovávat u všech systémových komponent a jednotlivých událostí alespoň následující záznamy pro potřeby auditu: .1 identifikace uživatele, .2 typ události, .3 datum a čas, .4 informace o úspěchu či neúspěchu, .5 původ události, .6 identita nebo název dotčených dat, systémové komponenty či zdroje.	Při správné implementaci na zdroje poskytující informace o systémových událostech zajistí LOGmanager uchovávání těchto auditních záznamů.

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
10.4.x	S použitím technologie pro synchronizaci času synchronizovat všechny systémové hodiny a časy kritických systémů a zajistit, aby byly pro získání, distribuci a ukládání informací o času učiněny následující kroky.	LOGmanager ve svém výchozím nastavení nedůvěřuje časovým údajům poskytnutým jednotlivými zdroji a přidává k záznamům své vlastní časové razítko vytvořené na základě údaje o přesném čase získaného z redundantních NTP severů. Spolu s každou obdrženou událostí je uloženo také časové razítko poskytnuté zdrojovým systémem a časové razítko vytvořené LOGmanagerem.
10.5	Zabezpečit auditní záznamy proti změnám	LOGmanager nedovoluje jakékoli úpravy či mazání shromážděných logů a událostí. Po zápisu dat do databáze funguje v režimu umožňujícím pouze čtení. Jediná možnost, jak získaná data smazat, je prostřednictvím funkce „výchozí tovární nastavení“ přístupné pod právy super-admin při plném fyzickém přístupu k systému LOGmanager. Pokud je vyčerpána úložná kapacita dostupná v systému LOGmanager pro databázi, je o tom informován operátor systému LOGmanager a je zahájen proces přesunu uložených dat. LOGmanager je navržen tak, aby dokázal při zachování plného vstupního výkonu uchovávat data za období alespoň 12 měsíců.
10.5.1	Umožnit prohlížení auditních záznamů pouze osobám, které to potřebují k výkonu svých pracovních povinností.	LOGmanager umožňuje poskytnout uživatelům s omezenými oprávněními pouze omezený přístup k uživatelskému rozhraní i datovým zdrojům.
10.5.2	Chránit soubory s auditními záznamy před neoprávněnými úpravami.	Viz č. 10.5.
10.5.3	Bezodkladně zálohovat soubory s auditními záznamy na centralizovaný server pro uchovávání protokolů událostí nebo na médium, které se obtížně pozměňuje.	LOGmanager je řešením poskytujícím tuto funkcionalitu.
10.5.4	Zapisovat protokoly technologií, které jsou v kontaktu s vnějším prostředím, na bezpečný, centralizovaný, interní server pro uchovávání protokolů událostí nebo zařízení používající záznamová média.	LOGmanager je řešením poskytujícím tuto funkcionalitu.

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
10.5.5	Použít software pro ověřování integrity souborů a sledování prováděných změn na souborech protokolů s cílem zajistit, aby údaje obsažené v existujících protokolech nemohly být bez vygenerování výstrahy změněny (přidání nových dat by ale výstrahu spustit nemělo).	Viz č. 10.5.
10.6.x	Zkontrolovat protokoly a informace o událostech týkajících se bezpečnosti ze všech systémových komponent a identifikovat neobvyklé nebo podezřelé aktivity. *Poznámka: Pro účely splnění tohoto požadavku je možné použít nástroje pro sběr dat, jejich parsování a generování výstrah.*	LOGmanager je platforma určená pro tuto činnost.

OBLAST 11 – Pravidelně testovat bezpečnostní systémy a procesy

č.	Požadavek PCI DSS	Řešení požadavku produktem LOGmanager
11.1	Zavést procesy k otestování přítomnosti bodů bezdrátového přístupu (802.11) a čtvrtletně detekovat a identifikovat všechny autorizované a neautorizované body bezdrátového přístupu.	Moderní systémy pro bezdrátový přístup poskytují funkce umožňující detekovat a ukládat informace o neautorizovaných zařízeních. LOGmanager může tyto informace shromažďovat a vytvářet automatické výstrahy.
11.5	Nasadit mechanismus detekce změn (například nástroje monitorování integrity souborů) pro upozornění pracovníků na neautorizované úpravy (včetně změn, doplnění a odstranění) kritických systémových souborů, konfiguračních souborů nebo obsahových souborů a konfigurovat software k provádění porovnání kritických souborů alespoň jednou týdně.	LOGmanager shromažďuje upozornění na provedené změny a může vydat výstrahu určenou bezpečnostnímu technikovi. K dispozici je řídicí panel pro práci s protokoly o změnách konfigurace.

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