LOGmanager

> Central Log Repository
> Affordable SIEM

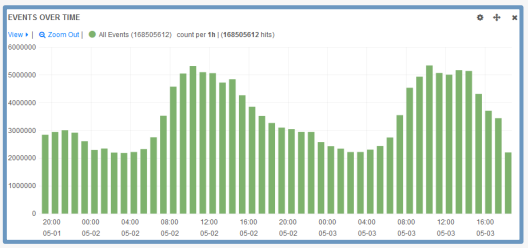
HELP TO RESOLVE CRITICAL IT INCIDENT

Případová studie ČD Cargo, a.s.

O zákazníkovi

ČD Cargo, a.s. (dále jen ČDC) je největší český nákladní železniční dopravce. Tato společnost je dceřinou společností národního dopravce České dráhy, a.s. Obě společnosti patří spolu s dalšími dceřinými organizacemi do Skupiny ČD. Společnost ČD Cargo, a.s. vznikla 1. prosince 2007 a zaměstnává 7 tis. zaměstnanců. K zajištění provozu má k dispozici 859 hnacích vozidel a více než 24 tisíc nákladních vozů. Z hlediska přepravených tun zboží patří mezi pět největších nákladních železničních dopravců v rámci Evropské Unie.

Co zákazník řeší a proč?



Informační systém ČDC je tvořen řadou dílčích provozně ekonomických a technologických systémů a aplikací s různou mírou vzájemné provázanosti. Celkem se jedná o několik desítek fyzických a virtuálních serverů, využívajících řadu technologických platforem předních výrobců, jako např. Microsoft, Oracle, SAP, ale i open-source řešení. Většina klíčových aplikací je provozována sesterskou společností ČD - Informační Systémy, a.s., některé dílčí systémy si ČDC provozuje vlastními silami na vlastních prostředcích nebo outsourcingově u dalších provozovatelů. Komunikační infrastrukturu ČDC z převážné většiny nevlastní, ale využívá ji formou poskytované služby ze strany sesterské společnosti ČD Telematika, a.s. Z důvodů složitosti ICT infrastruktury a smluvních vztahů mezi zákazníkem a dodavateli nemělo v řadě případů ČDC nad správou a provozem outsourcovaných systémů dostatečný přehled.

Cílem zákazníka bylo získat z ukládaných logů ucelený přehled o bezpečnosti a provozu informačního systému ČDC, schopnost reagovat na vzniklé události a incidenty, schopnost dohledat informace o činnostech a operacích s daty, uživatelskými účty a jejich oprávněními. Požadavkem bylo, aby úložiště logů zajišťovalo dlouhodobé uchovávání rychle dosažitelných informací v nezměnitelné podobě pro získání přehledu o stavu provozovaných systémů, přístupech k jednotlivým částem aplikací nebo přesně zmapované činnosti privilegovaných účtů v rámci informačních a komunikačních technologií. Zvolené řešení nemělo být licenčně omezeno maximálním počtem zpracovávaných událostí za časovou jednotku ani maximálním počtem sledovaných zařízení. Jako vhodné řešení byl vybrán nástroj LOGmanager.

Kromě centralizace logů a jejich dlouhodobého uchování z vybraných technologií a systémů, byla ze strany ČDC určena jako hlavní počáteční oblast sledovaných a vyhodnocovaných informací z nástroje LOGmanager oblast uživatelských účtů v jednotlivých úložištích identit.

U systému SAP sledování a vyhodnocování

- ⇒ Úspěšné i neúspěšné přihlášení uživatelů;
- ⇒ Provádění klíčových transakcí;
- ⇒ Pro účty zaměstnanců ČDC a externistů s přístupem do části ČDC akce: založení účtu, rušení účtu, přidělení role, odebrání role.

U LDAP serveru sledování a vyhodnocování

- ⇒ Úspěšné i neúspěšné přihlášení uživatelů;
- ⇒ Úspěšné i neúspěšné přihlášení privilegovaných účtů (včetně dodavatelských);
- ⇒ Pro účty zaměstnanců ČDC a externistů s přístupem do části ČDC akce: založení účtu, rušení účtu, povolení účtu, zakázání účtu, přidělení role, odebrání role.

U personální a mzdové aplikace

- ⇒ Úspěšné i neúspěšné přihlášení uživatelů;
- ⇒ Úspěšné i neúspěšné přihlášení privilegovaných účtů (včetně dodavatelských);
- ⇒ Provádění klíčových operací s osobními údaji.

U aplikace Active Directory

- ⇒ Úspěšné i neúspěšné přihlášení uživatelů;
- ⇒ Úspěšné i neúspěšné přihlášení privilegovaných účtů (včetně dodavatelských);
- ⇒ Provádění klíčových operací.

ROZSAH A POPIS PROJEKTU

I. Fáze

Byly dodány appliance LOGmanager s kapacitou v řádech desítek TB pro ukládání logů. Tyto appliance byly nainstalovány do prostředí ČDC dle předaného adresního plánu. V rámci zajištění vysoké dostupnosti clusteru dvou LOGmanagerů byly appliance nainstalovány do dvou fyzicky oddělených lokalit. Ihned po nainstalování v jednotlivých datových centrech byly LOGmanagery nakonfigurovány do clusteru. Obě appliance v clusteru se ovládají přes jedno webové rozhraní. V rámci úvodní instalace došlo k napojení autentizace uživatelů LOGmanageru přes Active Directory.

II. Fáze

Byly nakonfigurovány vybrané aplikace a servery tak, aby zasílaly logy do LOGmanageru, který je kontinuálně sbírá a ukládá. V okamžiku, kdy byly v LOGmanageru logy dostupné, došlo k vytvoření specifických parserů. Parser je „Překladač“, to znamená, že z nestrukturovaného logu v nativní podobě udělá log ve standardizovaném formátu, ve kterém lze přehledně vyhledávat a dále využívat další pokročilé funkce jako je alerting, predikce chování systémů, korelace a vytváření reportů.

III. Fáze

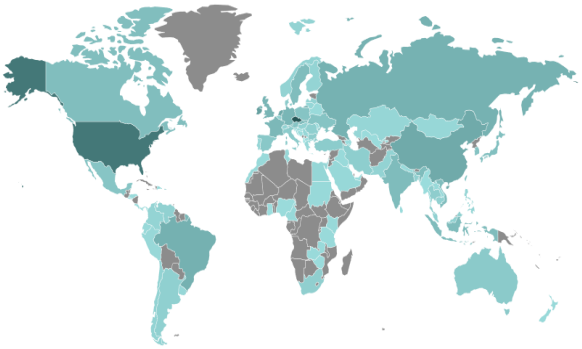
Bylo provedeno školení pro administrátory, techniky podpory IT a bezpečnostní pracovníky pro práci s nástrojem LOGmanager a tvorbu parserů.

PŘÍNOS PRO ZÁKAZNÍKA A OCEŇOVANÉ VLASTNOSTI

Systém splnil všechny očekávané cíle zákazníka. Slouží především jako podpůrný nástroj pro práci technikům podpory IT, administrátorům a bezpečnostnímu managementu. Úvodní implementací ale jeho nasazení nekončí, dalšími kroky bude postupné doplňování dalších aplikací a systémů, které nebyly součástí úvodního projektu. Toto průběžné rozšiřování je možné díky otevřenosti systému LOGmanager, která umožňuje snadné vytváření přehledných zobrazení potřebných informací pro jednotlivé systémy, činnosti nebo situace formou vlastních dashboardů, nebo doplnění zpracování logů z dalších aplikací pomocí vlastních parserů. Systém LOGmanager bylo možno snadno integrovat do stávajícího složitého a nehomogenního ICT prostředí ČDC. Zákazník velmi oceňuje kompletní vyčítání a zpracování rozšířených logů ze systémů Microsoft, možnost rychlého dohledání a filtrace potřebných informací z obrovského množství logů, možnost automatických upozornění na nestandardní stavy, a možnost vyčítání logů z části provozované síťové infrastruktury včetně bezpečnostních zařízení.

Zákazník oceňuje nejvíce následující vlastnosti

- Diagnostika pádů nebo provozních problémů jednotlivých aplikací IS ČDC,
- Predikce a předcházení vzniku havárií, narušení bezpečnosti dat, přehled nad neobvyklými a podezřelými transakcemi, přístupy apod.,
- Možné sledování konfiguračních změn prováděných externími i interními administrátory a operátory systému,
- Z pohledu bezpečnosti a zákona o kybernetické bezpečnosti pak dostupnost auditovatelných nezměnitelných logů z informačního systému ČDC v odděleném nezávislém úložišti, ze kterých lze sledovat a vyhodnocovat veškeré operace prováděné uživateli (autorizovanými i neautorizovanými) systému,
- Diagnostika a řešení bezpečnostních incidentů,
- Dohledání přístupů, uživatelských činností, plnění SLA, auditních požadavků apod.,
- Jsou k dispozici podklady pro forenzní analýzu při vyšetřování bezpečnostních incidentů,
- Monitoring a kontrola dodržování právních předpisů, regulací a norem.



INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto referenčního listu nalezl LOGmanager více jak 130 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.
Certifikovaným LOGmanager partnerem realizujícím tuto referenční zakázku je firma Caleum a.s.