

LOGmanager

> Centrální úložiště logů



SPLŇUJE POŽADAVKY
ZÁKONA O KYBERNETICKÉ
BEZPEČNOSTI
A ČSN ISO 27001

Případová studie nasazení centrálního úložiště logů v České televizi



Česká televize

O zákazníkovi

Česká televize je poskytovatel veřejné služby v oblasti televizního vysílání a společenskou institucí, jejímž posláním je vytvářet a šířit programy a poskytovat vyvážené nabídky pořadů pro všechny skupiny obyvatel, dále také poskytovat objektivní, ověřené, vyvážené a všestranné informace pro svobodné vytváření názorů.

Co zákazník řešil a proč?

Česká televize spravuje informační systémy určené pro chod ČT, řadu databázových systémů a velmi rozsáhlou počítačovou síť. Obsluhuje více jak 3000 počítačů, 250 virtuálních nebo fyzických serverů (Windows, LNX, Unix) a přes 200 síťových prvků. Vzhledem k tomu, že v minulosti byl zakoupen logovací systém, který měl omezené možnosti správy a úchovy logů, bylo nutné najít cenově dostupné náhradní centralizované řešení.

Požadavek byl na dodávku a implementaci centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů, serverů a aplikací.

Nutností byla možnost procházení těchto logů vhodným grafickým nástrojem s před-definovanými pravidly pro rychlé vyhledávání (například jako jsou změny v systémech provedené administrátory, seznam nově vytvořených účtů v MS AD za zvolenou periodu, změny v přístupových právech pro zadaného uživatele nebo k zadané složce a monitoring privilegovaných účtů, sdílených účtů a změn konfigurací apod.)

Cílem bylo jednotné úložiště logů, ke kterému mají přístup pouze autorizovaní pracovníci ČT. Nutností bylo vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů.

Rozsah a popis projektu

Česká televize využívá systém Logmanager pro centrální správu a evidenci logů. IT technologií a SW. Momentálně je na Logmanager serveru využito 10 TB (za 1,5 roku) z cca 350 logovaných systémů.

Implementace ve spolupráci s dodavatelem pro základní využití nástroje trvala 14 dní. Vzhledem k tomu, že nástroj má velmi dobře vypracován manuál jak v anglickém tak v českém jazyce, tak si kompletní nasazení si ČT provedla vlastními silami.

Které vlastnosti zákazník nejvíce oceňuje?

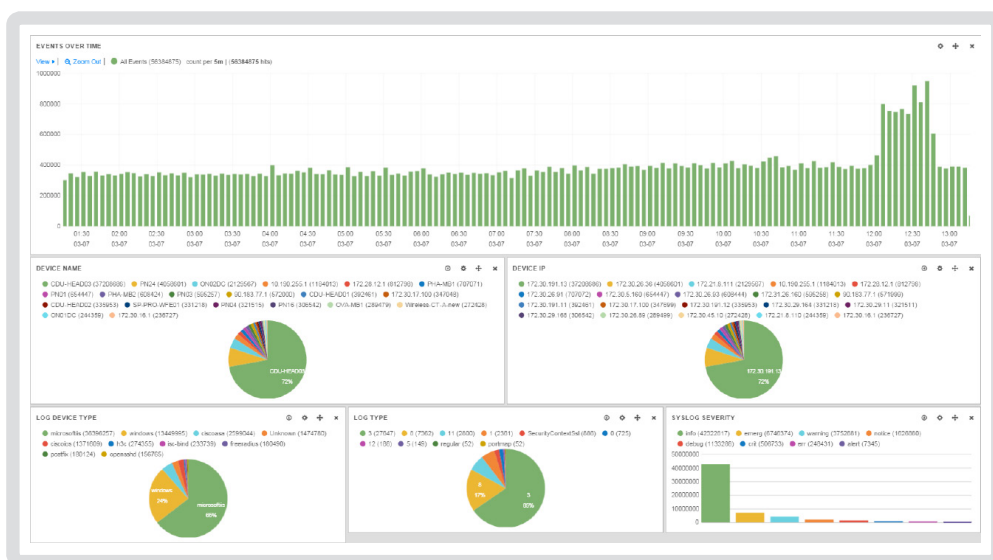
Česká televize oceňuje přehlednost, rychlost, úsporu času a rozsah možností uvedeného produktu

- > Zpracování událostí z předdefinovaných zdrojů logu napříč výrobci aplikací a operačních systému a síťového hardware
- > Otevřené řešení pro snadnou integraci systémů, které nejsou podporovány přímo výrobcem
- > Možnost sběru událostí minimálně ve formátech RAW, Syslog
- > Agent pro systémy Windows pro zajištění sběru nemodifikovaných událostí
- > Filtrování přijímaných a uložených zpráv administrátorem
- > Konsolidace logů na centrálním místě
- > Snadné vyhledávání událostí (ad hoc) bez nutnosti programování
- > Grafické znázornění událostí - grafy událostí
- > Grafické znázornění TOP událostí za určité časové období
- > Unifikované vyhledávání napříč všemi typy dat a zařízení
- > Možnost uložení filtrů, výsledků vyhledávání pro budoucí zpracování.
- > Reportovací nástroj s přednastavenými nejběžnějšími reporty a možnost vlastními úpravami vytvoření nových pohledů
- > Možnost dotazování externím monitorovacím systémem pro další zpracování alertů a prahových hodnot.
- > Webová konzole pro správu.

Přínos pro zákazníka

Aplikace Logmanager lze jednoduše nasadit do již běžícího provozu za využití jakéhokoliv systému a v jakékoli organizaci. Velmi snadná integrace je jedna z předností tohoto produktu.

Propojení s prostředím Microsoftu a ostatními platformami dává možnosti logovat (evidovat) a poskytovat eventy a logy z libovolných síťových aktivních prvků, bezpečnostních zařízení i operačních systémů a aplikačního software. Jednoduchost a přehlednost aplikace umožňuje poskytovat informace a zasílat alerty dle požadavků administrátorů ICT.



O společnosti Sirwisa a. s.

Společnost Sirwisa a. s. je čistě českou softwarovou společností zaměřující se na vývoj softwarových bezpečnostních řešení.

O společnosti Veracomp s. r. o.

Společnost Veracomp s. r. o. je Value Added distributorem IT produktů v oblasti síťové bezpečnosti, infrastruktury a open source software pro český a slovenský trh, jež klade důraz především na kvalitu, profesionalitu a flexibilitu nabízených řešení a služeb.

