LOGmanager

> SIEM
> Centrální úložiště logů

SPLŇUJE POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A ČSN ISO 27001

Případová studie

Úřad Městské části Praha 3

Městská část Praha 3 se nachází na východ od centra metropole, její území tvoří pražská čtvrť Žižkov a část Královských Vinohrad. Úřad městské části Praha 3 zajišťuje samosprávu městské části, správu majetku a v přenesené působnosti výkon státní správy.

MĚSTSKÁ ČÁST PRAHA 3

Výzva k řešení

Odbor informatiky Úřadu městské části Praha 3 spravuje informační systém městské části – řadu databázových systémů a aplikací pro provoz agend a počítačovou síť. To je více jak 300 počítačů, 40 virtuálních serverů, převážně Windows, 30 přepínačů a dalších zařízení.

Aplikace slouží především pro podporu výkonu státní správy a místní samosprávy. Celý informační systém pak komunikuje s dalšími informačními systémy veřejné správy, např. je integrován s IS Základních registrů nebo IS Datových schránek.

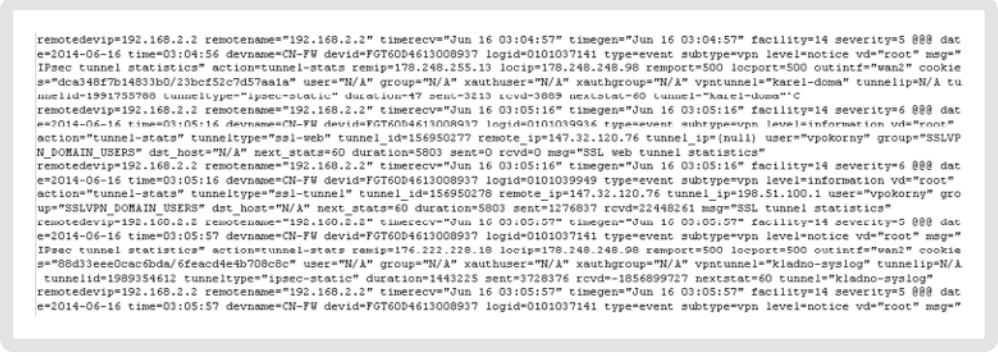
Všechny aplikace, systémy a zařízení generují logy. Logy byly umístěny lokálně na zařízeních, nebylo možné je nijak korelovat a archivovat. Pouze logy ze síťových zařízení byly uschovávány v aplikaci pro management a monitoring HP Intelligent management center.

Úřad městské části Praha 3 sice zatím nespadá pod působnost Zákona o kybernetické bezpečnosti 181/2014 Sb., ale odbor informatiky úřadu se snaží postupovat v souladu s tímto zákonem a odkazuje se na něj v Bezpečnostní politice úřadu. Bezpečnostní politika je zpracována na základě zákona 365/2000 Sb. o informačních systémech veřejné správy a podle ISO 27001:2005. Vyhláška k Zákonu o kybernetické bezpečnosti požaduje v §21 — „Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů“. V §23 je to pak „Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“.

Nutnost řešení centrálního úložiště logů si tak vynutil nejen provoz, ale i plnění legislativních požadavků a požadavků stanovených Bezpečnostní politikou.

Řešení – proč právě LOGmanager?

Výzvou řešení bylo zajistit centrální úložiště logů s dostatečnou kapacitou včetně vhodného nástroje pro vyhodnocování. Bylo vybíráno mezi několika velmi sofistikovanými nástroji SIEM velkých společností (ARCSight a QRadar) na jedné straně a mezi levnými nástroji postavenými na Open



LOGmanager

> SIEM
> Centrální úložiště logů

Field	Action	Value
@timestamp		2014-06-26T11:07:50.166Z
@version		1
_id		NHoa6hSBTWIRjaz_PINY_A
_index		lm-czu-2014.06.26
_type		fortigate
device_id		FGT1KC3912800628
devname		FGT1KC3912800628
dst_area_code		0
dst_city		Unknown
dst_country		Czech Republic
dst_country_code		CZ
dst_country_code3		CZE
dst_country_name		Czech Republic
dst_dma_code		0

Source řešeních (Splunk, Nagios).

Systém LOGmanager zaujal zlatý střed mezi nabízenými řešeními. Svojí výkonností v počtu přijatých EPS zdaleka převýšil zavedené SIEM systémy. Funkcemi pro analýzu, reportování a alertování se jim vyrovnal. Důležitým parametrem při výběru bylo licencování – systém LOGmanager není nijak licencován na počty zdrojů ani EPS.

V konkurenci s levnými open-source systémy rozhodlo, že LOGmanager je odladěné ucelené řešení s jedním administračním rozhraním a řadou funkcí, která open-source řešení nenabízejí. Důležitou skutečností je, že není provozován ve virtuálním prostředí, ale jako samostatný server. Při havárii virtuálního serveru je logmanagement stále v provozu, logy se neztratí a je možné analyzovat důvody pádu hypervizoru. Současně nabízí vysokou úroveň zabezpečení uložených dat – veškerá data jsou uložena na diskovém poli RAID6 s akcelerovaným hardwarovým řadičem. Z bezpečnostního hlediska bylo klíčové, že administrátor nemá možnost mazat uložená data.

Jedním z hlavních požadavků byl sběr logů ze stanic a serverů Windows. Nejlépe s možností filtrování odesílaných událostí. Tento požadavek systém LOGmanager splnil, opět bez nutnosti zvláštního licencování. Navíc nabídnul specialitu – překlad chybových kódů Windows do srozumitelné formy, tedy doplnění chybové hlášky místo kódu.

Při výběru systému LOGmanager také rozhodlo, že systém LOGmanager je certifikovaný na plnění požadavků ISO 27001:2005.

LOGmanager

LOGmanager je systém pro centralizovanou správu, logmanagement eventů a logů a SIEM z libovolných síťových aktivních prvků, bezpečnostních zařízení i operačních systémů a aplikačního software. Nástroj, který je založen na novém typu databáze se škálovatelnou kapacitou a výkonným systémem prohledávání a prezentaci nalezených dat. Jeho podstatou je sběr všech relevantních eventů a logů organizace, jejich ukládání do centrálního zabezpečeného úložiště s předem definovanou retencí a možností prohledávat enormní množství dat v reálném čase. Výstupy prohledávání jsou prezentovány v textové i grafické podobě s vysokou mírou interakce vzhledem k nalezeným datům.

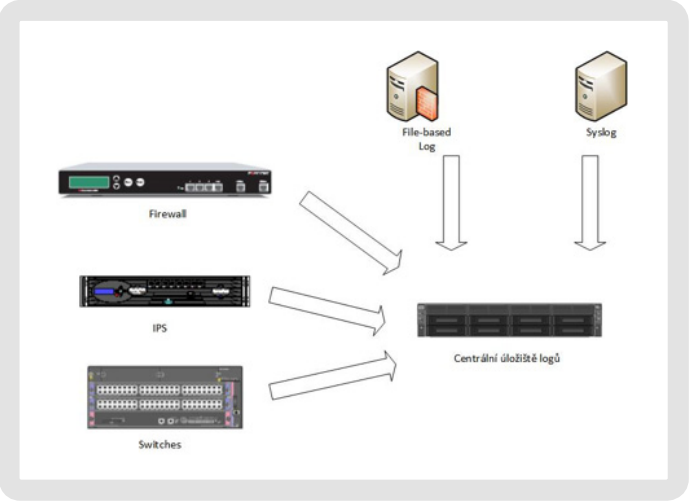
Dále systém umožňuje dlouhodobě ukládat data v nezpochybnitelné podobě pro potřeby shody s předpisy, požadavky pro forenzní analýzu a případné bezpečnostní audity.

Svým určením se však nejedná jen o systém pro bezpečnostní oddělení IT provozu firem. Velkým přínosem je i pro operační a provozní úseky, které mohou snadnou interakcí proti databázi událostí nalézt například podstatu nefunkčnosti systému, identifikovat možné závady a rychle dohledat události popisující příčinu konkrétního problému, ztráty dat nebo výpadku komunikace.

Součástí systému je Windows Event Sender – klient pro stanice a servery. Klient je centrálně spravovaný a umožňuje sběr logů z operačních systémů Windows. Tyto logy je možné filtrovat a kódované údaje v nich obsažené jsou překládány do srozumitelné formy.

Výhody řešení

Vybrané řešení, systém LOGmanager, zcela splnilo požadavky na centrální úložiště dat a nástroje na vyhodnocování logů. Obrovskou výhodou vybraného řešení je jeho výkon pro příjem událostí a kapacita pro ukládání logů. Systém je v provozu necelé dva roky a při současném množství přijímaných logů bude kapacita systému stačit na cca 5 let. To je naprosto dostatečná doba pro uložení logů bez nutnosti řešit jejich retenci. Důležitá je i skutečnost, že systém se spravuje z jednotného administračního rozhraní



a má propracovaný systém přístupových práv. Podstatným parametrem také bylo, že systém není provozovaný jako virtuální stroj a není tak závislý na jiných systémech.

ANALYTICKÉ SCHOPNOSTI SYSTÉMU BYLY VYUŽITY NAPŘÍKLAD PRO:

> Audit přístupu uživatelů do informačních systémů.
> Audit spouštění a ukončování procesů ve Windows, monitoring využití aplikací.
> Identifikace komunikačních toků a konfigurace pravidel na firewallu,
> Monitoring chování uživatelů v internetu a přehledné výstupy z Webfilteru firewallu.

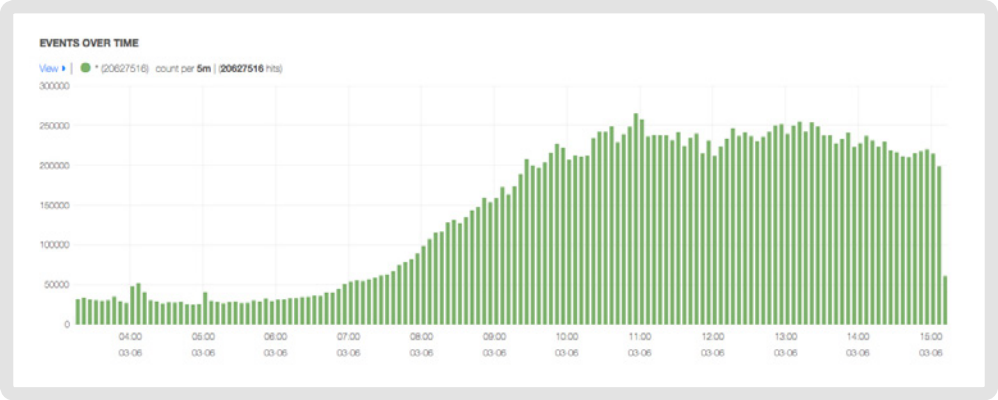
LOGmanager

> SIEM
> Centrální úložiště logů

- Monitoring komunikace s externími subjekty.
- Monitoring a řešení komunikačních problémů integračních můstků mezi informačními systémy.
- Řešení pracovně právních problémů – činnost uživatele.
- Kontrola činnosti uživatelů na návštěvnické WiFi a vytváření statistik.
- Kontrola nežádoucích služeb na počítačích – nezdařené či nekompletní odinstalace programů.

Pracovníci Odboru informatiky také využívají zasílání informačních alertů při přihlášení administrátorů nebo dodavatelů ke správě bezpečnostních zařízení – firewall a IPS. A také pří přístupu přes Remote desktop protokol na servery s aplikacemi.

„Nepotřebujeme drahý SIEM systém s řadou složitých funkcí. Chtěli jsme centrální úložiště logů s analytickými funkcemi a dostatečným výkonem. LOGmanager má přiměřenou cenu a jednoduchý, tedy žádný, systém licencování. A to nám naprosto vyhovuje.“ říká Tomáš Hilmar, vedoucí odboru informatiky Městské části Praha 3.

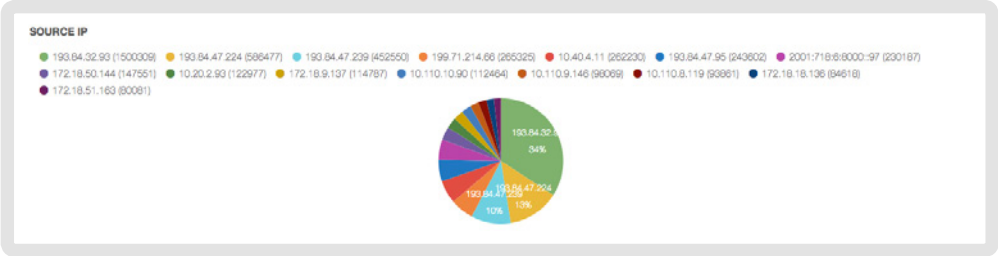


O společnosti Sirwisa a. s.

Společnost Siriwsa 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.



Kontakt:

VÝVOJÁŘ: Sirwisa a. s. www.sirwisa.cz **DISTRIBUCE:** Veracomp s. r. o. www.veracomp.cz

www.logmanager.cz