Zajištění kybernetické bezpečnosti - SIEM

Státní ústav pro kontrolu léčiv

ZÁKAZNÍK STRUČNĚ

Česká republika - Státní ústav pro kontrolu léčiv, organizační složka státu (zkráceně SÚKL) je správním úřadem s celostátní působností podřízeným Ministerstvu zdravotnictví.

Základním posláním SÚKL je:

- aby v ČR byla dostupná pouze farmaceuticky jakostní, účinná a bezpečná humánní léčiva
- aby byly používány pouze bezpečné a funkční zdravotnické prostředky
- přispívat k tomu, aby léčiva i zdravotnické prostředky byly racionálně používány

SÚKL

OBDOBÍ REALIZACE

květen 2017 - leden 2018

POUŽITÉ TECHNOLOGIE

IBM QRadar SIEM

„Produkt naplnil naše očekávání. Projekt SIEM hodnotíme jako úspěšný.“

Ing. Petr Koucký, ředitel oboru IT Česká republika
Státní ústav pro kontrolu léčiv, organizační složka státu

Výchozí situace a cíle projektu

SÚKL již dříve úspěšně zavedl a provozoval Systém pro řízení bezpečnosti informací (ISMS) dle ČSN ISO/IEC 27001. Hlavní důvody pro dodávku komplexního systému SIEM, zajišťujícího monitoring, sběr, centrální ukládání a vyhodnocování bezpečnostních událostí ze sítě, serverů, databází, aplikací a dalších zdrojů:

- součást komplexní bezpečnostní strategie SÚKL
- legislativa
- faktické potřeby zvýšení ochrany dat, včetně osobních údajů

Prioritou bylo v souladu se zákonem zavést konkrétní bezpečnostní opatření pro kritickou informační infrastrukturu a významné informační systémy:

- významný informační systém „Centrální úložiště elektronických receptů“ (dále jen „CÚER“) podle přílohy č. 1 vyhlášky č. 317/2014 Sb.
- významný informační systém „Registr léčivých přípravků s omezením“ (dále jen „RLPO“) podle přílohy č. 1 vyhlášky č. 317/2014 Sb.
- infrastruktura, která je nezbytně nutná pro provoz CÚER a RLPO

PŘÍNOSY

- zavedení konkrétních bezpečnostních opatření vztahujících se k zákonu o kybernetické bezpečnosti č. 181/2014 Sb. a vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
- zavedení automatického nástroje na hlášení kybernetických bezpečnostních incidentů a reaktivních opatření NÚKIB
- monitoring, zpracování, vyhodnocení a archivace bezpečnostních událostí napříč celou sítí = posílení bezpečnosti sítě
- monitoring manipulace s citlivými daty a aplikacemi = prevence před únikem dat a možnost zpětně rychle vypátrat konkrétního viníka
- normalizace událostí z bezpečnostních logů do srozumitelné podoby, jejich zpracování předdefinovanými pravidly, jednoduché uživatelské rozhraní SIEM, on-line grafické výstupy a reporting dle norem ISO
- služba vyšetřování bezpečnostních incidentů Security Operations Centrum (SOC) zajištěna specialisty AutoCont CZ a.s.

Popis řešení

Pro zhotovení díla byl použit produkt IBM QRadar SIEM. QRadar je hlavní produkt celé bezpečností platformy IBM QRadar Security Intelligence. Primárním úkonem je v reálném čase analyzovat (agregovat, korelovat) bezpečnostní události a toky generované zařízeními a aplikacemi v síti. Na základě tohoto vyhodnocení pak upozorňovat na bezpečností incidenty, poskytovat reporting a dlouhodobé uložení dat.

Architektura SIEM

Hlavním prvkem architektury je centrální server SIEM. Slouží pro management ostatních komponent, příjem flow, identifikaci bezpečnostních výjimek na základě korelačních pravidel a znalostní databáze, automatický reporting, poskytuje garantované úložiště dat a umožňuje přístup do grafické konzole SIEM. Centrální server zvládne zpracovávat kontinuálně 22.500 EPS a 65.000 FPM. Tuto hodnotu lze v době špiček několikanásobně překročit. HW je navržen na trvalý tok 40.000 EPS. Centrální server nemá žádná omezení velikosti garantovaného úložiště a aktuálně je dimenzován na více než 13 měsíců dat z logů a flow. Dále jsou instalovány dvě komponenty Event Collector. Ty tvoří cluster pro zajištění příjmu logovacích událostí v režimu vysoké dostupnosti HA. Dostupná síťová sonda Invea Flowmon zasílá exportované flow ve formátu IPFIX na server SIEM na dedikovaný síťový port. Jednotlivé servery mají připojený management port pro vzdálenou správu. Architekturu doplňují virtuální servery s Wincollect agentem, které slouží k lokálnímu vyčítání logovacích událostí z nejvíce zatížených doménových řadičů, vzdáleně pak z ostatních Windows Serverů. Veškeré logovací události jsou zasílány na Event Collector Cluster.

Implementace

Součástí implementace byla analýza, návrh cílového stavu a implementačního postupu, dodávka a instalace komponent systému, implementace, integrace s prostředím SÚKL, připojení logovacích zdrojů, konfigurace, parametrizace a ladění pravidel, dokumentace a školení. Proběhlo 41 funkčních testů, včetně vícedenního výkonového testu EPS.

V rámci implementace bylo do systému SIEM připojeno téměř 600 zdrojů logovacích událostí 64 různých typů (Avamar, Brocade, Cisco, f5, Oracle Invea Flowmon, Linux, Dell EMC, MS Widnows, Smart Card, Symantec, VMware, Synlogy, HP, Omnicast, zakázanické aplikace, a další). Celkem 189 připojených zdrojů tvoří prvky významného informačního systému.

Technická a servisní podpora

Zajišťuje kontinuální dostupnost řešení a zahrnuje službu vyšetřování bezpečnostních incidentů Security Operations Centrum (SOC). Součástí podpory je také produktová podpora výrobce, vedení dokumentace, provozní podpora, management změn, školení, proaktivní monitoring, identifikace a odstranění závad. Denně systém zpracuje a vyhodnotí více než 300 milionů událostí. Průměrně vzniká denně 10-15 bezpečnostních událostí, které vyžadují další analýzu.