case study

Dokonalé zabezpečení infrastruktury veřejného cloudu zvyšuje důvěryhodnost a renomé poskytovatele služeb Infrastructure as a Service.

České Radiokomunikace a.s.

Obor:
Technologie

Země:
Česká republika

Cíl projektu:
Zvýšit úroveň zabezpečení infrastruktury pro poskytování služeb Infrastructure as a Service.

Řešení:
Security Information and Event Management (SIEM).

Výsledky:

- Přehled nad událostmi z mnoha zařízení v reálném čase
- Možnost okamžité reakce na incidenty
- Možnost forensní analýzy nad událostmi z mnoha zařízení
- Automatické korelace událostí
- Nový komerční uživatel služby Infrastructure as a Service

Pro poskytovatele služeb veřejného cloudu je bezpečnost klíčovým parametrem, který ovlivňuje důvěryhodnost služeb a přivádí nové zákazníky. České Radiokomunikace patří k největším a nejúspěšnějším poskytovatelům na českém trhu. Spolu s rostoucí databází aktivních uživatelů služeb IaaS vzrůstají i jejich nároky na garance zabezpečení. **Technologie SIEM představuje účinnou cestu, jak vycházet vstříc i těm nejnáročnějším klientům.**

Shrnutí

České Radiokomunikace zavádí technologii SIEM, díky které získávají dokonalý přehled o všech zařízeních v infrastruktuře svého veřejného cloudu.

Plně automatizovaný sběr dat ze všech technologických entit v reálném čase, jejich korelace, analýza a srozumitelná intepretace dávají Českým Radiokomunikacím do ruky mocný nástroj, který představuje významnou konkurenční výhodu.

Profil klienta

České Radiokomunikace jsou předním hráčem na trhu provozování televizního a rozhlasového vysílání a nabízí široké portfolio profesionálních telekomunikačních a ICT služeb. Díky službám Cloud Computingu společnost pomáhá svým zákazníkům optimalizovat firemní IT infrastruktury a dosahovat podstatných úspor, ale i významného nárůstu bezpečnosti, flexibility a dostupnosti služeb.

Pozadí projektu

Poskytování služeb veřejného cloudu musí bezpodmínečně respektovat nároky zákazníků na škálovatelný výkon a vysokou dostupnost technologií. Ale je to především bezpečnost, která je alfou a omegou úspěchu poskytovatelů.

České Radiokomunikace svým zákazníkům naslouchají a plně respektují jejich rostoucí nároky na garance a bezpečnostní záruky. Tomu odpovídá i směrování investic do rozvoje vlastní cloud infrastruktury.

" Investice do bezpečnosti má obvykle strategický charakter a nepřináší přímé obchodní výsledky. **V našem případě se však díky investici do technologie SIEM podařilo bezprostředně navázat komerční spolupráci s velkým zákazníkem, pro kterého je právě garance pokročilé bezpečnosti rozhodujícím faktorem.**"

Marcel Jánský, Manažer zákaznických řešení společnosti České Radiokomunikace

Dodané řešení

SIEM technologie v reálném čase umožňuje analýzu bezpečnostních událostí, které generují síťová zařízení a aplikace. Mezi hlavní funkce SIEM patří:

Agregace dat
Seskupení vybrané části určitých entit za účelem vytvoření nové entity. Jednotlivé entity představují data z přepínačů, firewallů, serverů, IDS/IPS, aplikací a řada dalších.

Korelace
Nalézání vzájemných vztahů událostí a jejich významová intepretace. Technologie SIEM umožňuje provádět širokou škálu korelačních technik a využívat data z mnoha různých zdrojů.

Uchovávání historických dat
Dlouhodobé ukládání historických dat pro účelní forensního zkoumání.

Varování
Automatizovaná analýza korelovaných událostí a vytváření notifikačních varování o urgentních problémech. Informační panely, přehledové sestavy: zobrazování sebraných událostí na informačních panelech, odhalování nestandardních vzorců chování a událostí.

Reportování shod
Shromažďování dat a vytváření reportů, které porovnávají míru shody s existujícími bezpečnostními politikami a auditními procesy.

Pro implementaci technologie SIEM použila společnost Dimension Data pokročilé nástroje společnosti McAfee.

Hodnota dodaného řešení

Díky technologii SIEM mohou České Radiokomunikace úspěšně odhalovat nestandardní vzorce událostí ve své infrastruktuře, předcházet útokům a pružně reagovat na potenciální hrozby.

Svým zákazníkům garantují řádově vyšší úroveň zabezpečení pronajímané infrastruktury než konkurenční poskytovatelé.

Výhodou řešení je zároveň možnost přizpůsobit část systému požadavkům zákazníka, který tak dostává vlastní pohled na poskytovanou infrastrukturu a vzniklé události.