Důvod nasazování systémů SIEM

Stále reálnější riziko zneužití informací zvenku či zevnitř, ale také IT audity a rostoucí legislativní požadavky jsou nyní téměř ze dne na den součástí života většiny společností, a to jak komerčních tak státní správy a samosprávy. Pod vlivem této zátěže vynakládají organizace mnoho času a energie prověřováním jejich zabezpečení. To s sebou přináší řadu problémů:

- **Příliš vysoké náklady a rizika**

Na trvale rostoucí požadavky na zvýšení rozsahu a řízení rizik společnosti reagují nasazením řady specializovaných nástrojů v kombinaci s „ručním“ reportingem. Takové řešení je nejen nákladné, ale také neefektivní a poskytuje často rozporuplné výsledky.

- **Chybí integrace**

Existuje mnoho i osvědčených postupů pro sledování a řízení událostí v ICT infrastruktuře, obvykle však s minimální nebo žádnou centralizací. Bezpečnostní události jsou distribuovány v různých databázích, souborových systémech a aplikacích. Chybí nástroj pro efektivní zvládnutí monitoringu bezpečnostních událostí, které jsou nepřetržitě chrleny síťovými prvky, firewally, IDS, IPS, servery, operačními systémy, databázemi a aplikacemi.

- **Stálé přibývání nových hrozeb**

Bezpečnostní opatření na perimetru podnikové ICT infrastruktury jsou téměř kontinuálně „testována“ útoky z prostředí Internetu. Mění a vyvíjejí se také hrozby potenciálního vnitřního ohrožení podnikových systémů. Je téměř nemožné udržet si před nimi náskok

- **Těžko dosažitelná plná shoda s legislativou**

Bez řešení pracujících v reálném čase se může společnosti nebo úřadu lehce stát, že bude doslova mimo soulad dřív, než se to dozví. Důvodem může být nejen absence systémů, ale i fakt, že řada společností musí splnit mnohé předpisy a nařízení v různých navzájem mnohdy nekorespondujících termínech.

Systémy SIEM (Security Information and Event Management – SIEM) automatizují identifikaci a řešení incidentů na základě předdefinovaných pravidel, což umožňuje včasné upozornění na kritické události. Systémy SIEM zajišťují soulad se zákonnými normami, ale především přispívají k reálnému řízení bezpečnosti napříč společností.

Přínosy využití systému SIEM

K využití SIEM systémů vedou společnosti hlavně tyto důvody:

- reálné řízení bezpečnosti napříč společností
- zvýšení účinnosti a efektivity provozu IT
- snížení počtu bezpečnostních událostí na úroveň, která je zvládnutelná
- oddělení reálných bezpečnostních incidentů od incidentů, které tak pouze „vypadají“ (false-positive).

Významným rysem nasazení SIEM je výše zmíněné zvýšení účinnosti a efektivity provozu IT, které se projevuje schopností rychle analyzovat provozní problémy a tím snížit dobu neplánovaných výpadků.