

PŘÍPADOVÁ STUDIE:

Monitoring výkonnosti sítě v kritické infrastruktuře

EG.D je jedním z hlavních provozovatelů kritické infrastruktury v České republice, který spravuje rozsáhlou datovou síť pro řízení distribuce elektrické energie pokrývající třetinu země. „Provozní stav naší sítě má přímý dopad na více než milion domácností a podniků, o které se staráme,“ říká Martin Kepřt, Vedoucí správy kybernetické a fyzické bezpečnosti EG.D. „Jakékoli pochybení při dodávkách elektřiny by mohlo způsobit nevyčíslitelné škody.“

Aby bylo možné tato rizika řešit, bylo potřeba v rozvodnách zlepšit viditelnost do OT sítě a LAN. Proto bylo důležité, aby řešení podporovalo protokoly IEC 61850 a IEC 608-70-5-104 používané v OT sítích a umělo předávat data IPFIX do systému SIEM.

Řešení

EG.D nasadila řešení Kemp Flowmon, které tvoří přibližně 90 sond Kemp Flowmon sbírajících data v klíčových bodech sítě, zatímco stávající routery zajišťují další statistiky síťového provozu. Všechna data jsou pak ukládána a analyzována v centrálním virtuálním Kemp Flowmon kolektoru.

„Ihned po nasazení nám systém pomohl identifikovat několik chybně nakonfigurovaných zařízení. Umožňuje nám vidět veškerý provoz na jednom místě a dokáže nás varovat před případnými problémy. Poskytuje nám informace o využití sítě, poukazuje na potenciální úzká místa, odhaluje hrozby v síti a podává zprávy o různých anomáliích síťového provozu,“ říká Keprt.



Závěr

Díky zvolenému řešení získala společnost EG.D dokonalý přehled o celé své rozvodné síti zaručující dostatečnou transparentnost i povědomí o potenciálních problémech „Díky řešení Kemp Flowmon máme jistotu, že žádný problém neuniká naší pozornosti a vždy máme čas zakročit a věci napravit,“ upřesňuje Keprt. „Poskytuje nám poznatky, které nám umožňují proaktivní správu naší operační sítě a tím zajištění stabilní dodávky služeb našim zákazníkům.“



Martin Keprt

Vedoucí správy kybernetické
a fyzické bezpečnosti





kemp

kemp.ax