COMGUARD

cyber security masters

Případová studie

Zákazník: Ostravské vodárny a kanalizace a.s.

Ostravské vodárny a kanalizace a.s.

Partner: PCS®

PCS spol. s.r.o.

Případ:

Efektivní přístup ke kybernetické bezpečnosti společnosti Ostravské vodárny a kanalizace a.s. za pomocí technologií Trellix

COMGUARD

Informace o zákazníkovi

Společnost Ostravské vodárny a kanalizace a.s. zásobuje obyvatele města Ostrava pitnou vodou z veřejné vodovodní sítě. Ve své správě má vodovodní síť v délce cca 1 063 km, včetně vodovodních přípojek, a dopravuje pitnou vodu pro téměř 300 tisíc obyvatel města Ostravy. Zároveň spravuje i 946 km dlouhou kanalizační síť, která odvádí odpadní vodu jak od obyvatelstva, tak od podnikatelských a průmyslových subjektů.

K výraznému zlepšení životního prostředí se snaží přispět nejen odkanalizováním většiny ostravských nemovitostí, ale také řádným vyčištěním odvedených odpadních vod na některé z ostravských čistíren odpadních vod. Celkem provozují osm čistíren odpadních vod na území města.

Výchozí stav

250 pracovních stanic a 130 serverů bylo pod ochranou Microsoft Defenderu, který ale často reportoval falešně pozitivní nálezy. Tento jev byl už tak častý, že se Ostravské vodárny a kanalizace a.s. rozhodly pořídit dohled nad Microsoft Defenderem a volba padla právě na Trellix s jejich řešením EDR (Endpoint Detection and Response), které vhodně doplnili částí Device Control z rodiny Trellix DLP (Data Loss Prevention).

„Trellix jsme si zvolili na základě doporučení kolegů, kteří ve svých firmách využívají jejich technologie a jsou s nimi spokojeni. Zároveň pro nás bylo naprosto klíčové zachovat udržitelnost a kontinuitu činnosti naší organizace, hledali jsme řešení, které budeme moct implementovat bez odstávky systémů.“

Ing. Kamil Ružák,
Vedoucí oddělení informatiky

Implementace

V rámci implementace Trellix EDR a Trellix DLP proběhlo nasazení přes doménu za plného provozu, které bylo hladké a bezproblémové. Díky vhodné implementaci politik a jednoduchému provázání s Microsoft Defenderem získali administrátoři dohled nad antivirovým řešením od Microsoftu.

Provoz a začlenění Trellix EDR a DLP do agendy IT oddělení OVAK

Dnes je celý bezpečnostní provoz společnosti OVAK a.s. pod monitoringem Trellix EDR. O ochranu citlivých dat se stará Trellix DLP a vše je zastřešeno jednotnou správou z centrální konzole Trellix ePolicy Orchestrator, která poskytuje jednoduchou správu a přehlednost. I robustní bezpečnostní systém může být uživatelsky přívětivý.

Zákazník si pochvaluje soulad s pravidly blížící se NIS2 díky těmto technologiím a zároveň na otázku budoucích plánů s technologiemi EDR a DLP zmiňuje, že i když do budoucna nevylučuje rozvoj, aktuálně je spokojený na 100 %.

„Díky dobrému uživatelskému rozhraní a správnému nastavení politik v rámci implementace jsme si ušetřili zdlouhavou a náročnou práci při analyzování falešně pozitivních nálezů v naší síti. Díky týdenním reportům nad Microsoft Defenderem jsme získali dohled nad děním v síti. Řešení nám uvolnilo ruce k důležitějším činnostem v naší agendě. Samozřejmě přibyla povinnost podívat se na týdenní reporting, ale v porovnání s předchozím stavem je to zanedbatelný a hlavně účelně vynaložený čas. Bavíme se o ušetřených desítkách hodin týdně.“

Ing. Kamil Ružák,
Vedoucí oddělení informatiky