Případovka

AUTOCONT

Spolehlivé zabezpečení proti kybernetickým hrozbám pro Slovácké strojírny

PROFIL ZÁKAZNÍKA

Slovácké strojírny jsou jednou z nejvýznamnějších průmyslových společností Zlínského kraje s více než šedesátiletou tradicí vyspělé strojírenské výroby. V současnosti jsou moderní firmou, zaměřenou na kvalitu a flexibilitu výroby, zvyšování produktivity práce a s nastaveným procesem úspory vnitřních nákladů. Formou akvizic převzaly Slovácké strojírny řadu dalších strojírenských podniků v České republice. Podstatnou část své produkce exportují do dalších vyspělých zemí.

OBDOBÍ REALIZACE

02-03/2020

„S výsledkem implementace XG Firewallů a řešení Intercept X Advanced na ochranu všech koncových zařízení jsme velmi spokojeni. Díky pokročilým funkcím je naše síť chráněna i před nově vznikajícími hrozbami a celkový provoz zabezpečení nás nijak nezatěžuje. Řešení jsme měli možnost před pořízením vyzkoušet. Ukázalo se přitom, že nejen splňuje naše nároky na úroveň zabezpečení perimetru i koncových bodů, ale také jej lze velmi snadno konfigurovat a řídit v cloudovém ovládacím rozhraní."

Ing. Petr Zálešák, CIO Slovácké strojírny

Výchozí situace

Ochrana podnikové IT infrastruktury a dat Slováckých strojíren je plně v kompetenci IT oddělení, které má za úkol pohlížet na kybernetickou bezpečnost, stejně jako i jiné hrozby (požár, krádež, výpadky dodávek energií) a provádět i související revizní a preventivní kroky.

Zabezpečení IT infrastruktury společnosti bylo řešeno jedním a tedy neredundantním firewallem, dosahujícím limitu svého výkonu i konce své morální životnosti. Firewall nebyl vybaven žádnými z moderních bezpečnostních funkcí, které na detekci a zastavení hrozeb a útoků využívají například technologii umělé inteligence. Na koncových bodech bylo nasazeno antivirové řešení, které ale již neposkytovalo dostatečnou úroveň ochrany před aktuálním typy kybernetických útoků - především před ransomwarem a phishingem.

PŘÍNOSY

- Vysoká úroveň ochrany proti kybernetickým hrozbám
- Přehled o datových přenosech
- Identifikace hrozeb ještě než proniknou do sítě
- Analýza dat v izolovaném cloudovém prostředí
- Nenáročná správa

POUŽITÉ TECHNOLOGIE

XG 310 Firewall v HA

Sophos Central Intercept X Advanced

Management Slováckých strojíren si plně uvědomoval nutnost posílení ochrany perimetru, vstupní brány do podnikové sítě, stejně jako ošetření možné zranitelnosti zařízení koncových uživatelů, kteří často přistupují k podnikové síti i na dálku. Současně bylo nezbytně nutné, aby nové bezpečnostního řešení mělo nenáročnou správu, jelikož IT oddělení společnosti po snižování nákladů dlouhodobě pracuje s minimalizovaným personálním obsazením.

Společnost Slovácké strojírny volila z několika nabídek bezpečnostních řešení od různých výrobců, ale i díky možnosti zapůjčení a vyzkoušení zařízení Sophos se rozhodla právě pro Sophos XG Firewally a ochranu koncových bodů řešením Intercept X Advanced. Mezi další hodnotící kritéria výběru nového bezpečnostního řešení patřil rovněž jeho maximální výkon a rozsah funkcí za konkurenceschopnou cenu a předpokládaná doba udržitelnosti v délce nejméně tří let.

Cíle projektu

Slovácké strojírny potřebovaly špičkové moderní zabezpečení na perimetru své sítě i všech koncových zařízení. Nové řešení poskytující potřebnou redundanci, je snadno spravovatelné a integrované v celém podniku.

Popis řešení

Jako základ nového bezpečnostního řešení byly zvoleny firewally nové generace Sophos XG Firewall. Brány XG Firewall kompletně odkrývají provoz síťové infrastruktury, když poskytují přehled o datových přenosech s šifrováním TLS 1.3, provádějí hloubkovou inspekci paketů a jednoznačně identifikují legitimní aplikace a důvěryhodné přenosy dat, kterým poskytují optimalizovaný výkon. Současně, ale spolehlivě rozpoznají podezřelé pakety a hrozby, které by mohly znamenat probíhající kybernetický útok.

S využitím technologie hloubkového učení dokážou identifikovat a zastavit i zcela nové hrozby, ještě než proniknou do sítě. Analýza podezřelých dat probíhá v izolovaném cloudovém prostředí.

Technologie chrání rovněž koncová zařízení zaměstnanců Slováckých strojíren, kteří se mohou spolehnout na špičkovou ochranu před nejnovějšími typy malwaru, ransomwarem nebo phishingem. Systém inteligentní detekce hrozeb na koncových bodech a reakce na ně (EDR) kombinuje technologie umělé inteligence a strojového učení s informacemi o hrozbách od bezpečnostních specialistů ze SophosLabs.