



Slovácké strojírný nasadily řešení Sophos XG Firewall a Intercept X Advanced na spolehlivé zabezpečení perimetru a koncových bodů.

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

O zákazníkovi



Slovácké strojírný, akciová společnost

Průmysl
Strojírnoství

Webové stránky

www.sub.cz

Počet uživatelů

400

Řešení Sophos

Sophos XG Firewall

Sophos Intercept X Advanced

Sophos Central

‘Kybernetické hrozby v podobě ransomwaru, phishingu či malwaru jsou velmi aktuální a my na ně musíme odpovídajícím způsobem reagovat – ať už kvůli zajištění kontinuity našeho provozu, nebo ochraně dat a zajištění souladu s GDPR.’

Ing. Petr Zálešák
CIO, Slovácké strojírna



Výzva

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

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

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 se zajištěním kontinuity provozu v případě kybernetického útoku, ale bylo nezbytně nutné, aby mělo nové bezpečnostní řešení nenáročnou správu, jelikož IT oddělení společnosti po snižování nákladů dlouhodobě pracuje s minimalizovaným personálním obsazením.

Společnost Slovácké strojírna 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 dvou let.

Technologické řešení

Jako základ nového bezpečnostního řešení společnosti Slovácké strojírna byly zvoleny firewally nové generace Sophos XG Firewall, konkrétně modely XG 310 v redundantní konfiguraci. Všechna podniková zařízení řady XG Firewall přitom poskytují extrémně vysokou úroveň ochrany, společně s vysokým výkonem. XG 310 Firewally Sophos ve formátu 1U rackového zařízení jsou určeny pro středně velké a distribuované organizace, kterým poskytují flexibilní možnosti bezpečného připojení do internetu.

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.



‘Řešení Sophos 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 strojírný

Současně ale XG Firewally spolehlivě rozpoznají podezřelé pakety a hrozby, které by mohly znamenat probíhající kybernetický útok.

S využitím technologie hloubkového učení dokážou XG Firewally identifikovat a zastavit i zcela nové hrozby, ještě než proniknou do sítě. Analýza podezřelých dat probíhá v izolovaném cloudovém prostředí, s využitím technologie Intercept X Advanced s umělou inteligencí.

Technologie Intercept X Advanced 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.

XG Firewally i zabezpečení koncových zařízení s technologií Intercept X Advanced jsou integrovány do řešení Synchronized Security, které v reálném čase sjednocuje a zjednodušuje ochranu všech zařízení před pokročilými hrozbami. Infikovaná zařízení jsou automaticky izolována a malware je okamžitě odstraněn, aby nemohl proniknout dále do podnikové sítě a napáchat škody.

Práci IT administrátorům společnosti Slovácké strojírný usnadňuje také platforma Sophos Central, prostřednictvím které jsou intuitivně spravovány všechny bezpečnostní produkty Sophos, nasazené v rámci firmy. Sophos Central je cloudová konzole, provozovaná bez vlastních serverů, ve které mohou administrátoři z jednoho místa nakonfigurovat zásady pro všechna koncová zařízení i řídit provoz XG Firewallů.

IT administrátoři společnosti Slovácké strojírný měli možnost vyzkoušet si práci s XG Firewally v rámci zápůjčky ještě před definitivním výběrem a spuštěním implementace nového bezpečnostního řešení. Výrazně se tím zrychlilo nasazení nových bezpečnostních produktů v rámci celé firmy, protože IT administrátoři již byli seznámeni s jejich funkcemi a ovládacím prostředím. Základní implementace XG Firewallů a řešení Intercept X Advanced na koncových zařízeních proběhla v rámci několika dní. Detailní nastavení pravidel XG Firewallů zabralo přibližně jeden měsíc.

Dosažené cíle

Slovácké strojírní získaly špičkové, moderní zabezpečení na perimetru své sítě i v všech koncových zařízeních. Nové řešení poskytuje potřebnou redundanci, je snadno spravovatelné prostřednictvím platformy Sophos Central a integrované v celém podniku v rámci Synchronized Security.

Pro IT administrátory Slováckých strojíren je i díky funkcím strojového učení a umělé inteligence velmi snadné celé řešení řídit a mohou se spolehnout, že jejich firmě zajistí maximální úroveň zabezpečení – i před zcela novými a zatím detailně neprozkoumanými hrozbami.

Kontrola Xstream TLS v XG Firewallch navíc řeší i problém se stále rostoucím podílem šifrovaného datového provozu, když bez poklesu výkonu dokáže i tento typ paketů prozkoumat na výskyt škodlivého kódu. Kybernetické útoky ani malware se díky této hloubkové inspekci paketů nemohou skrýt ani za šifrování.

Redundance nasazených bran XG 310 Firewall zajišťuje nepřetržitý provoz bezpečnostního řešení

a spolehlivé připojení do internetu i k podnikovým systémům a aplikacím Slováckých strojíren.

Řešení Intercept X Advanced, nasazené na koncových bodech, jako jsou stolní i přenosné počítače a mobilní zařízení, poskytuje zaměstnancům Slováckých strojíren bezpečné připojení k podnikovým systémům i aplikacím, stejně jako ochranu při používání internetu a dalších aplikací. Kromě ochrany v reálném čase detekuje Intercept X Advanced díky technologii umělé inteligence a hloubkového učení i nejnovější typy malware a automaticky blokuje podezřelá a potenciálně nebezpečná síťová připojení. Zabezpečení důležitých souborů je chráněno před napadením ransomwarem a technologie DLP (Data Loss Prevention) zajišťuje citlivá data Slováckých strojíren, uložená v koncových zařízeních zaměstnanců, před jejich odcizením či ztrátou. To vše s minimálním vlivem na výkon koncových bodů.

Pro Slovácké strojírní je zároveň velmi snadné v případě potřeby posílit výkon firewallů na vstupu do sítě a/nebo kdykoli rozšířit okruh koncových zařízení, zabezpečených řešením Intercept X Advanced.

AUTOCONT je českou soukromou společností, která v oblasti dodávek zboží, služeb a řešení na poli informačních a komunikačních technologií úspěšně působí od roku 1990. K rychlému rozvoji v prvních deseti letech přispěla výroba vlastní značky osobních počítačů a systematické budování rozsáhlé obchodní a servisní sítě. V druhém desetiletí své existence se AUTOCONT

zaměřil na poskytování komplexních IT řešení a služeb pro firemní klientelu a státní správu, čímž se postupně propracoval mezi nejvýznamnější společnosti v oblasti rozsáhlých a složitých ICT projektů.

AUTOCONT

Tel: +420 910 971 111
Email: obchod@autocont.cz
Web: www.autocont.cz

'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.'

Ing. Petr Zálešák
CIO, Slovácké strojírní

Zjistěte, jak vám můžeme pomoci chránit vaši organizaci.
Navštivte www.sophos.com