

Volle Präzision auch beim Netzwerkschutz

HERAUSFORDERUNG

Die Leitz GmbH & Co. KG ist mit rund 2.900 Mitarbeitern weltweit und Niederlassungen sowie Vertriebspartnern auf allen Kontinenten als Marktführer in der Produktion von Holzbearbeitungswerkzeugen etabliert – mit einem weiteren wichtigen Standbein in der Kunststoffbearbeitung. Klar, dass auf dem Schutz der Kunden- und Produktivdaten ein besonderes Augenmerk liegt. Insgesamt sind 36 Vertriebsgesellschaften, 6 Produktionsstandorte und weitere 120 Servicestationen an das zentrale Rechenzentrum in Oberkochen angeschlossen, von dem aus ein 15-köpfiges Team alle erforderlichen Services über eine virtualisierte Server-Umgebung bereitstellt. Hinsichtlich der Anbindung gab es bisher unterschiedliche Ansätze: Bei der Mehrzahl der Außenstellen erfolgte der Zugriff seit jeher über abgesicherte VPN-Tunnel auf Basis von WatchGuard-Plattformen. Bei den größeren Niederlassungen garantiert nach wie vor eine MPLS-Umgebung der British Telecom den Zugang. Der Wunsch nach einheitlichen Prozessen und Kostenoptimierung führte jedoch dazu, sich mit dem aktuellen Status quo auseinander zu setzen. Darüber hinaus galt es, spezifischen Herausforderungen hinsichtlich der Absicherung von Produktionsanlagen oder bei der elektronischen Abwicklung von Zollangelegenheiten zu begegnen.

LÖSUNG

Zur Entlastung des zentralen Rechenzentrums in Oberkochen, das den gesamten Datenverkehr der Standorte abwickelte, wurde ein Local-Breakout-Konzept geprüft: „Der Servicequalität unseres zentralen Netzwerks kommt es deutlich zugute, wenn der allgemeine Internetverkehr direkt vor Ort erfolgen kann, ohne den Schritt über das Rechenzentrum in Oberkochen“, so Roland Berndt, Mitarbeiter der Technischen EDV bei Leitz. Nach und nach wird jetzt auf Basis moderner WatchGuard-Plattformen unternehmensweit umgesetzt.

KUNDE

Leitz GmbH & Co. KG

ANZAHL MITARBEITER

Rund 2.900

BRANCHE

Fertigung

REGION

Deutschland

WATCHGUARD PRODUKTE

- Firebox T10-W
- Firebox T30-W
- Firebox T50-W
- Firebox M200
- Firebox M300
- Firebox M4600
- Basic Security Suite
- APT Blocker



So laufen künftig ausschließlich die unmittelbar relevanten, internen Prozesse auf Basis gerichteter VPN-Tunnel über die Zentrale, beispielsweise der ERP-Zugriff. Weniger geschäftskritische Anwendungen via Internet erfolgen parallel dazu direkt vor Ort über lokale Provider – natürlich mit entsprechenden Sicherheitsvorkehrungen und MultiWAN-Möglichkeit für zusätzlichen Ausfallschutz. Im Zuge dessen spielen die Möglichkeiten der zentralen Verwaltung und Konfiguration über Templates eine entscheidende Rolle. Je nach Größe und Anforderung der Niederlassungen kommen unterschiedlichste Hardware-Modelle von WatchGuard zum Einsatz, die sich über den System Manager jedoch alle gleich und zentral von Oberkochen aus bedienen lassen. Dank der Funktion RapidDeploy stellte auch der Rollout keinen größeren Aufwand dar. Schließlich muss die Hardware nur an den jeweiligen Standort verschickt und verbunden werden. Die Konfiguration erfolgt automatisch entsprechend der zentral hinterlegten, individuell anpassbaren Einstellungsvorgaben.

Auch für die Lokationen mit MPLS-Anschluss stehen die Zeichen auf Veränderung: Im Frühsommer 2017 wurde in der österreichischen Vertriebszentrale Riedau – gleichzeitig eine der Hauptproduktionsstätten – das erste WatchGuard UTM-Hochverfügbarkeitscluster jenseits des zentralen Rechenzentrums in Oberkochen in Betrieb genommen. Die darüber erzeugte VPN-Verbindung mit dem Rechenzentrum in Oberkochen inklusive der Option lokaler Breakouts läuft aktuell parallel, wird das MPLS-Konstrukt jedoch mittelfristig ersetzen.

Gleichzeitig wird bei Leitz den einschlägigen Gefahren im Rahmen von Industrie-4.0-Anwendungen Rechnung getragen und auf einen Segmentierungsansatz für das Netzwerk gebaut. „Da vernetzte Fertigungsanlagen immer öfter als Ziel für Übergriffe auserkoren werden, wollten wir hier eine zusätzliche Sicherheitsschicht einziehen“, so Berndt. Der Datenverkehr jeder einzelnen CNC-Maschine wird mithilfe der WatchGuard-Plattform über separate VLAN-Strukturen isoliert, zudem ist das Maschinennetz über Switches vollständig von anderen Bereichen abgetrennt. Der gesamte Traffic Richtung Produktivdaten muss erst die Firewall und weitere Scan-Module passieren. An den Übergabepunkten können zudem Benutzerberechtigungen auf Basis von Active Directory kontrolliert werden.

ERGEBNIS

Marko Bauer, Geschäftsführer der Fornax EDV-Service GmbH als IT-Partner von Leitz, verdeutlicht den Einspareffekt des Komplettumstiegs: „Unsere Kalkulation hat gezeigt, dass der Return-on-Invest bei diesem Wechsel bereits nach knapp einem Jahr erreicht ist. Dafür haben wir dann die Hardware inkl. der Lizenz für die eingesetzten Security-Services für drei Jahre.“

Neben der Bewältigung der grundsätzlichen Sicherheitsanforderungen konnte Leitz mit Unterstützung von WatchGuard auch ein weiteres Thema auf der Aufgabenliste abhaken: die Gewährleistung der verlässlichen Kommunikation im Rahmen von Zollanmeldungen über ATLAS (Automatisiertes Tarif- und Lokales Zollabwicklungssystem). Als einer der wenigen Sicherheitsanbieter verfügt WatchGuard seit Juni 2017 über eine entsprechende Zertifizierung und liefert für die VPN-Anbindung an das ATLAS-Zollverfahren sogar eine vollständige Dokumentation.

ÜBER WATCHGUARD

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Das umfangreiche Produktportfolio reicht von hochentwickelten UTM (Unified Threat Management)- und Next-Generation-Firewall-Plattformen bis hin zu Technologien für umfassenden WLAN-Schutz sowie weiteren spezifischen Produkten und Services rund ums Thema IT-Security. Mehr als 80.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

