Entlastung durch Local Breakouts

Sicherer Datentransfer rund um den Globus

Bild: Leitz GmbH & Co. KG

Die Leitz GmbH & Co. KG, ein Hersteller von Holzbearbeitungswerkzeugen, setzt beim Schutz der Kunden- und Produktivdaten auf eine IT-Sicherheitsstruktur, die vom Hauptsitz in Oberkochen aus administriert wird. Auf Basis der Unified-Threat-Management-Lösungen von Watchguard und zusammen mit dem IT-Dienstleister Fornax, wurden die Produktionsanlagen und die elektronische Abwicklung von Zollanmeldungen sorgfältig gegen ungewollte Zugriffe abgesichert.

Jeder Standort der Leitz GmbH & Co. KG – 36 Vertriebesgesellschaften, sechs Produktionsstandorte und 120 Servicestationen – ist an das zentrale Rechenzentrum des Unternehmens in Oberkochen angeschlossen. Von dort aus stellt ein 15-köpfiges Team alle erforderlichen Services über eine virtualisierte Server-Umgebung bereit. Für den Schutz des Netzwerks ist seit 2006 ein UTM(Unified Threat Management)-Cluster von Watchguard im Einsatz. Hinsichtlich der Anbindung der Standorte gab es bei Leitz bisher unterschiedliche Ansätze: Bei der Mehrzahl der Außenstellen erfolgte der Zugriff von Beginn an über abgesicherte VPN-Tunnel. Bei den größeren Niederlassungen kommt eine MPLS-Umgebung der British Telekom zum Einsatz.. Dieser Status quo wurde jedoch überdacht.

Das Rechenzentrum entlasten

Ein wichtiges Kriterium war dabei die Bandbreite: „Bei unseren VPN-Standorten lief der Datenverkehr vollständig über unser Rechenzentrum in der Zentrale, inklusive des externen Internet-Traffics der einzelnen Lokationen", berichtet Roland Berndt, Abteilung technische EDV bei Leitz. Um für Entlastung zu sorgen, 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."

Nur relevante Anwedungen

Zukünftig sollen ausschließlich unmittelbar relevante, interne Prozesse auf der Basis von VPN-Tunneln über die Zentrale laufen – beispielsweise der ERP-Zugriff. Weniger geschäftskritische Anwendungen via Internet sollen parallel dazu über lokale Provider ermöglicht werden – mit den entsprechenden Sicherheitsvorkehrungen

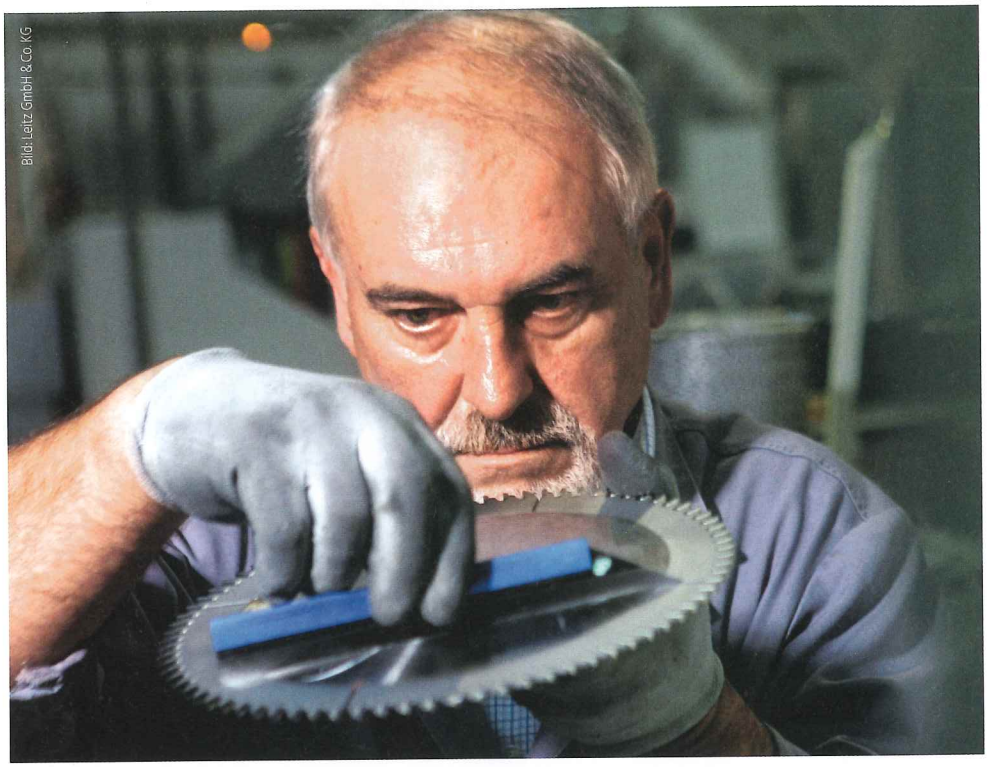
und Multi-WAN-Möglichkeit für zusätzlichen Ausfallschutz. „Im Rahmen der Breakouts ist es wichtig, dass alle Unternehmensvorgaben jederzeit erfüllt werden", sagt Marko Bauer, Geschäftsführer der Fornax EDV-Service GmbH. Sein Unternehmen unterstützt Leitz seit 2008 im Bereich der IT-Sicherheit.

Alte Plattformen ausgetauscht

Insbesondere die Möglichkeiten der zentralen Verwaltung und Konfiguration über Templates spielten bei der Neuausrichtung der Sicherheitslandschaft eine entscheidende Rolle. Im Zuge dessen wurde auch der bisherige Hersteller auf Herz und Nieren geprüft und die allgemeine Anbieterlandschaft näher betrachtet. „Einen Schnitt brauchten wir in jedem Fall. Es stellte sich jedoch die Frage, ob wir auf die jüngste Modell-Generation von Watchguard bauen oder komplett wechseln", sagt Berndt. Am Ende entschied man sich für die Hardware des Herstellers und hat mittlerweile fast alle alten 120 Plattformen ausgetauscht. Je nach Größe und Anforderung der Niederlassungen kommen unterschiedliche Hardware-Modelle zum Einsatz. Diese lassen sich jedoch über den System Manager zentral von Oberkochen aus bedienen. Der Rollout erfolgte innerhalb kurzer

Bild: Leitz GmbH & Co. KG

Zukünftig sollen ausschließlich relevante, interne Prozesse per VPN-Tunnel über die Zentrale laufen.



Leitz liefert seine Produkte weltweit aus. Die Security Appliances sind daher Atlas-zertifitiert, um Zollanmeldungen zu erleichern.

Zeit. Die Hardware musste lediglich an den jeweiligen Standort verschickt und dort verbunden werden. Die Konfiguration erfolgt automatisch entsprechend der zentral hinterlegten, individuell anpassbaren Einstellungsvorgaben. Ein IT-Mitarbeier muss nicht vor Ort sein.

Aus für MPLS-Verbindungen

Im Zuge der Umstellung sollen nach und nach auch die kostenintensiven MPLS-Verbindungen abgelöst werden. Zu diesem Zweck wurde im Frühjahr 2017 in der österreichischen Vertriebszentrale in Riedau das erste UTM-Hochverfügbarkeitscluster jenseits des zentralen Rechenzentrums in Oberkochen in Betrieb genommen. Die darüber erzeugte VPN-Verbindung mit dem zentralen Rechenzentrum inklusive der Option lokaler Breakouts soll das MPLS-Konstrukt mittelfristig ersetzen. Nach erfolgreicher Pilotphase sollen so bis 2019 alle bestehenden MPLS-Anbindungen weltweit abgelöst werden. Marko Bauer verdeutlicht den Einspareffekt des Umstiegs: „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 inklusive der Lizenz für die eingesetzten Security-Services für drei Jahre."

Verschiedene UTM-Dienste

Neben der reinen Firewall-Funktionalität setzt das Unternehmen verschiedene UTM-Dienste wie Intrusion Prevention, Gateway Antivirus, Application Control, Spamblocker, Webblocker oder/und Reputation Enabled Defense ein. An ausgewählten Standorten greift darüber hinaus ein APT-Blocker als Sandbox-Technologie zum Erkennen und Blockieren von Malware und Zero-Day-Angriffen. Ein weiterer MPLS-Standort des Unternehmens befindet sich im holländischen Elst. Auch dort wird inzwischen ein UTM-Cluster eingesetzt. Aufgrund von Sicherheitsbedenken kommt dabei ein Segmentierungsansatz für das Netzwerk zum Tragen: „Bisher war in Elst nur die Verwaltung ansässig, jetzt kommt jedoch die Produktion hinzu", erläutert Roland Berndt. „Da vernetzte Fertigungsanlagen immer öfter als Ziel für Übergriffe auserkoren werden, wollten wir hier eine zusätzliche Sicherheitsschicht einziehen." Der Datenverkehr der CNC-Maschinen wird mit der Watchguard-Plattform über separate VLAN-Strukturen isoliert, zudem ist das Maschinennetz über Switches von anderen Bereichen abgetrennt. Der gesamte Netzwerkverkehr in Richtung Produktivdaten muss erst die Firewall und weitere Scan-Module passieren. An den Übergabepunkten können zudem Benutzerberechtigungen auf Basis von Active Directory kontrolliert werden. So kann nicht nur der Datenzugriff durch unautorisierte Nutzer unterbunden, sondern auch verhindert werden, dass sich von Produktionsanlagen ausgehende Gefahren im ganzen Netzwerk ausbreiten. Zudem wird durch unterteilte Netzwerkbereiche eine schnellere Identifizierung von Schwachstellen möglich. Nach Test der Netzwerksegmentierung soll das Konzept in allen weiteren Produktionsstandorten Einzug halten und sukzessive verfeinert werden.

Zertifiziert für Atlas

Leitz konnte mit seinem IT-Security-System ein weiteres Problem lösen und die Kommunikation im Rahmen von Zollanmeldungen absichern: „Leitz liefert seine Produkte in nahezu jeden Winkel der Erde, entsprechend hoch ist der Aufwand der Zollabfertigung", sagt Berndt. Um die damit einhergehenden Prozesse zu verschlanken, sollte Atlas (Automatisiertes Tarif- und Lokales Zollabwicklungssystem) genutzt werden. Dabei handelt es sich um eine vom Informationstechnikzentrum Bund bereitgestellte Lösung zur elektronischen Abwicklung und Überwachung des grenzüberschreitenden Warenverkehrs. Die Übermittlung der Daten erfolgt via VPN-Tunnel – jedoch nur, wenn der dafür verantwortliche Hersteller entsprechend zertifiziert ist. Diese Zertfizierung erhielt der Hersteller der Security-Appliances im Juni 2017 und liefert für die VPN-Anbindung an das Atlas-Zollverfahren auch eine vollständige Dokumentation. „Natürlich lässt sich hier und da immer noch weiter optimieren, aber da arbeiten wir ja gemeinsam mit Fornax konsequent dran. Mit den Möglichkeiten, die uns Watchguard in dem Zusammenhang bietet, sehen wir uns auch langfristig auf der sicheren Seite", sagt Berndt.

Die Autorin Rebecca Hasert ist Redakteurin bei Press'n'Relations in Ulm.

www.watchguard.de