

Globale Kontrolle für Zugriff auf IT- und OT-Netze

In der Industrie sind heute IT und OT miteinander verbunden. Dies kann zu Herausforderungen beim Thema Security führen. Die JOST-Werke haben nun mit Cisco-Lösungen eine weltweite Zugriffskontrolle für ihre IT- und OT-Netze eingeführt.



Zusammenfassung

Kunde

JOST Werke AG

Industrie

Produktion sicherheitsrelevanter Komponenten und Systeme für Nutzfahrzeuge

Standorte

Sitz in Neu-Isenburg, Vertriebs- und Produktionsstätten in über 20 Ländern auf allen fünf Kontinenten

Mitarbeiter

3.500 Mitarbeiter



Situation

Die JOST-Werke verfügten bereits über eine einheitliche Netzwerk-Infrastruktur für IT und OT.

Aufgrund steigender Sicherheitsbedenken sollte eine Lösung für den geschützten Zugriff auf die Netzwerke sorgen.



Herausforderungen

- Erfüllung von Anforderungen durch Audits und Penetration-Tests
- Weltweite Lösung mit lokalem und zentralem Management
- Kleines IT-Team in der Zentrale verantwortet globale Service-Bereitstellung
- Schrittweise Einführung von Network Access Control (NAC)
- Limitierte IT- und Finanz-Ressourcen
- Erkennung, Meldung und Isolation von Schatten-IT, vor allem Fremd-Hardware



Ziel

- Erhöhung der Transparenz gepaart mit kontrolliertem Zugang
- Verbesserte Sicherheit bei Zugriff durch Nutzer und Geräte
- Zentrales Management von Netzwerkrichtlinien
- Effiziente Einführung und einfacher Betrieb von Netzwerkzugriffskontrolle
- Erkennung von kabelgebundenen und drahtlosen Geräten
- Limitierte Freigabe des Zugriffs durch lokales IT-Team
- Finale Freigabe durch zentrales IT-Team

Das Team

Cisco Systems GmbH

Garching bei München, Gegründet: **1984**,

Mitarbeiter: **850** (Deutschland)

Ansprechpartner: **Jörg Kunel**

Cisco (NASDAQ: CSCO) macht das Internet möglich.

Wir vernetzen Menschen, Daten, Prozesse und Dinge sicher miteinander – so treiben wir Innovationen, von der Wirtschaft und Gesellschaft profitieren.

www.cisco.de

So hat Cisco das Problem gelöst

JOST ist ein weltweit führender Hersteller und Lieferant von sicherheitsrelevanten Systemen für die Nutzfahrzeugindustrie. Das Unternehmen setzt seit Jahren Netzwerk-Infrastrukturen auf Basis von Cisco ein. Um die einheitliche Infrastruktur für IT und OT besser abzusichern und damit Anforderungen durch Audits und Penetration-Test zu erfüllen, war JOST auf der Suche nach einer Lösung für den Zugriffsschutz. Die Plattform Cisco ISE (Identity Services Engine) wendet kontextbezogene Sicherheitsrichtlinien für den Zugriff auf alle Ressourcen im Netzwerk automatisch an. Ein Pilotprojekt in der ungarischen Niederlassung zeigte, dass sie alle Anforderungen erfüllte. Im ersten Schritt überwachte sie im Monitoring-Modus das Netzwerk. Im zweiten Schritt erkannte sie, welche Geräte im Netzwerk vorhanden waren. Im dritten Schritt wurde das System live geschaltet. Nun lassen sich unbekannte Geräte in der Produktionsumgebung zunächst vom Netzwerk isolieren und bei Bedarf nach einer limitierten Freigabe durch die lokale IT-Abteilung sowie einer finalen Freigabe durch die Zentrale im Netzwerk nutzen. Zudem ist ISE mit dem Active Directory integriert, um die Zugriffsrechte der Anwender umzusetzen.

Die Lösungen von Cisco

- ISE (Identity Services Engine)
- Catalyst 2960 Switches
- Nexus 9000 Data Center Switches
- Classic WLAN Access Points
- IE1000 und IE2000 Industry Switches

So profitieren die OT-Mitarbeiter

- Sichere Anbindung verschiedener Geräte wie Handscanner, Drucker, Maschinen, Industrie-PCs oder Werkzeuge in der Produktion
- Erfüllung der hohen Anforderungen im Bereich Rückverfolgbarkeit von hergestellten Gütern
- Im Servicefall erhalten externe Servicetechniker und Tools temporär Zugang
- Sicherer Netzwerkzugriff erhöht die Ausfallsicherheit
- Schnellerer Support durch höhere Transparenz

So profitiert das Unternehmen

- Erfüllung der notwendigen Sicherheitsstandards im Netzwerkbereich
- Einhaltung von Compliance-Vorgaben
- Nachweis der Zuverlässigkeit für Kunden durch Audits und Zertifizierungen
- Sichere Zusammenarbeit mit Partnern und anderen Firmen
- Qualifizierte und nachvollziehbare Antworten auf Sicherheitsfragen möglich

So profitiert die IT

- Überblick, welche Geräte an welchem Standort in welchem Netzwerk angeschlossen sind
- Einfaches Management der ISE-Plattform
- Schnelle, unternehmensweite Umsetzung von Richtlinien
- Zentrale Konfiguration für alle Niederlassungen
- Mögliche Schwachstellen und Gefährdungspotenziale lassen sich besser erkennen und schneller beseitigen
- Identifikation von Fremdgeräten wie Maschinen, Kameras oder Rogue WLAN Access Points
- Transparenz, welche Switches und Ports von einem Gerät genutzt werden

„Unsere Erfahrungen mit Cisco-Produkten in den Bereichen Switching, Data Center und Wireless LAN sind sehr gut. Die weltweite Präsenz von Cisco und seinen Partnern ist für uns ebenfalls wichtig. Durch Cisco ISE konnten wir unsere Infrastruktur nun mit einer umfassenden Lösung für die Zugriffskontrolle ergänzen, die unser Netzwerk zuverlässig vor unsicheren Geräten schützt.“

Martin Frischkorn

Team Manager IT Administration & Operations,
JOST-Werke Deutschland GmbH

www.cisco.de