



Bild 1: Insgesamt wurden bei ZF Sachs 40 dezentrale Maschinennetze eingerichtet und jedes dieser Teilnetze durch eine mGuard Firewall von Phoenix Contact und Innominate abgesichert.



Industrie-Firewall schafft größere Sicherheit im Produktionsnetz

ZF Sachs, ein Automobilzulieferer für Antriebs- und Fahrwerkkomponenten mit Sitz in Schweinfurt, hat die Sicherheit seiner industriellen Netzwerke nachhaltig verbessert. Der Ansatzpunkt: eine dezentrale Sicherheitsarchitektur mit Industrie-Firewalls.

Ausgangspunkt für die stärkere Absicherung der Produktionsanlagen waren Virenprobleme im Office-Netz. Im Vergleich zum überschaubaren Schadensrisiko beim Befall von Office-Rechnern wurde das Gefährdungspotenzial für die Produktionsanlagen als wesentlich größer eingeschätzt. Um die Risiken möglicher Störungen oder gar von Produktionsausfällen durch fehlerhafte Zugriffe oder Schadsoftware zu reduzieren, wurden bei ZF Sachs zusätzliche Sicherheitsmaßnahmen beschlossen.

Dezentrale Sicherheitsphilosophie

Die Aufgabenstellung für die neue Sicherheitsarchitektur bestand darin, die Produktionsanlagen sowohl gegen unerwünschte externe und interne Zugriffe zu schützen als auch die Ausbreitung von eingedrungenen Schädigungen einzudämmen. Als geeignete Strategie wurde eine Trennung des Office-Netzes vom Produktionsnetz durch eine große Firewall und eine tiefengestaffelte Sicherheitsarchitektur (Defense in Depth) ausgewählt, mit der sich auch kritische Einzelsysteme absichern lassen. Eine Schlüsselrolle kam dabei der Kontrolle und Filterung des Netzwerkverkehrs durch Firewalls zu. Für eine de-

zentrale Architektur mit Firewalls sprachen der besser zu organisierende verteilte Schutz, die größere Flexibilität bei einem industrietypischen Netzwerk-Design und geringere Investitions- und Betriebskosten. Eine Segmentierung durch VLAN-fähige Switches in logisch getrennten Segmenten wurde geprüft und verworfen, da Virtual-LANs aus Sicherheitssicht als zu schlecht kontrollierbar bewertet wurden. Für die Umsetzung waren die Bereiche Automatisierungstechnik und Instandhaltung in Abstimmung mit der IT zuständig. Neben dem Einsatz von Virenschernern auch im Produktionsbereich wurde als wichtigste Maßnahme die Segmentierung des Produktionsnetzes in kleine, handhabbare Maschinennetze umgesetzt. Die Zuordnung erfolgte räumlich nach Gebäudebereichen und zusätzlich für einzelne Anlagen mit Profinet-Komponenten. Insgesamt wurden 40 dezentrale Maschinennetze eingerichtet und jedes dieser Teilnetze durch eine mGuard Firewall von Phoenix Contact und Innominate abgesichert. „Wir haben verschiedene Firewall-Security-Produkte vor allem nach zwei Kriterien geprüft. Die Industrietauglichkeit mit z.B. einem erweiterten Temperaturbereich war uns besonders wichtig. Außerdem brauchen wir eine Lösung, die sich möglichst

flexibel und mit geringem Aufwand in unser Umfeld von Automatisierungskomponenten einbinden ließ“, begründet Asmund Hey, bei ZF Sachs verantwortlich für die Automatisierungstechnik im Bereich technische Dienste, die Entscheidung für die mGuard Security-Lösung.

Die Einrichtung dezentraler Firewalls

Planungsgrundlage für die Umsetzung der dezentralen Sicherheitsarchitektur war der Netzstrukturplan. Er beschreibt die einzelnen Netzsegmente und enthält Angaben darüber, welches Gerät an welchen Port angeschlossen ist, welche IP-Adressen, MAC-Adressen, Firmwarestände und Produktkennzeichnungen vorliegen. „Damit die dezentrale Architektur mit 40 einzelnen Maschinennetzen nicht zu einer Vervielfachung des Einrichtungs- und Betriebsaufwands führt, haben wir zunächst für alle Teilnetze als Masterregelung einen Basissatz an gemeinsamen Firewall-Regeln entwickelt. Die Umsetzung war relativ einfach“, berichtet Asmund Hey. Für den Roll-out wurden die Masterregeln bei der Inbetriebnahme aus einem Speicherchip ausgelesen und auf das Teilnetz ange-

wendet. Damit waren bereits die meisten Anforderungen abgedeckt. Es mussten nur noch individuelle Regeln für spezielle Ausnahmefälle ergänzt werden, wie etwa für den Zugriff einer Steuerung auf Office-Servershares. Nach der Inbetriebnahme folgte eine dreimonatige Einführungs- und Lernphase, um nicht berücksichtigte Zugriffe oder Ports nachzubessern. „Dabei haben wir festgestellt, wie wichtig ein sorgfältiger Netzwerkstrukturplan ist. Je mehr Zeit hier investiert wird, umso geringer ist der spätere Korrekturaufwand. Außerdem haben wir die Vorteile eines zentralen Geräte-Managements erkannt“, benennt Asmund Hey die wichtigsten Erfahrungen aus der Inbetriebnahme.

Anforderungen der Automatisierungstechnik

Bei der Einrichtung der dezentralen Sicherheitsarchitektur mussten recht unterschiedliche Anforderungen berücksichtigt werden. Eine Produktionsanlage mit Profinet-Komponenten sollte gegen Störung aus dem Netz abgeschottet werden. Die '8HP' (ein Drehmomentwandler für 8-Gang-Automatikgetriebe) erfordert eine TCP/IP-Kommunikation auf der Ebene von Profinet-Protokollen. Dabei mussten sehr viele IP-Adressen gemanagt werden und für die Feldbuskomponenten war eine klare Segmentierung und Abschottung erforderlich. Da für das Antwortverhalten der Komponenten in Echtzeit ein Jitter kleiner einer Mikrosekunde vorgeben ist, mussten sie gegen Störungen wie den typischen Broadcast in einem Netz konsequent abgeschottet werden. Deshalb wurde für die 8HP ein eigenes Netzsegment reserviert. Eine weitere Anforderung war die 1:1 NAT (Network Address Translation) bei DNC-Maschinen (Distributed Numerical Control). Hier ging es um die Software zur Verteilung der DNC-Programme, die im Office-Netz läuft. Da die mGuard-Komponenten 1:1 NAT unterstützen, waren für die Software keine Anpassungen am internen Adressraum der Maschinen notwendig. Die Einrichtung von Portweiterleitungen war eine weitere wichtige Anforderung, weil von außen auf zentrale Datenbanken in den sogenannten Plant-Stationen zugegriffen werden muss. Außerdem ging es um strikte Ausgangsregeln. Durch die räumlichen Trennungen von Anlagen kommt es zu

einer Aufteilung der Software- und Prozessdaten, die zentral auf einem Server wieder zusammenlaufen müssen. Durch Regeln in den dezentralen Firewalls werden Zugriffe auf den zentralen Server erlaubt, aber andere unkontrollierte Zugriffe verhindert.

Dezentrale Firewalls haben die Sicherheit erhöht

Die mGuard-Security-Lösung ist bei ZF Sachs inzwischen seit zwei Jahren im Einsatz. Die dezentralen Firewalls werden bei neuen Anlagen oder bei Anlagen mit Profinet zum Schutz gegen Störungen eingerichtet. „Der Betrieb der dezentralen Netze läuft reibungslos. Es gibt nichts, was die Automatisierungstechnik ausbremst und der Betrieb läuft weitgehend ohne Wartung. Wir haben auch einzelne alte Maschinen ohne Virenschutz erfolgreich gegen Störungen und Angriffe geschützt. So konnte sich ein Virus, der von einem Techniker eingeschleppt worden war, dank der Segmentierung nicht weiter im Netz verbreiten“, fasst Asmund Hey die Erfahrungen zusammen. Er hat einen guten Vergleich, da im Office-Bereich oder bei alten Maschinen ohne Firewall-Schutz die Virenproblematik weiter vorhanden ist. Hey hebt hervor, dass der sichere Produktionsablauf auch dann sichergestellt ist, wenn andere Netzwerkkomponenten ausfallen. Die Firewall schützt die Anlagen in diesem Fall gegen störenden Broadcast oder vor fehlerhaften Paketen. „Die Erfahrungen mit der Einführung, dem Betrieb und dem erreichten Sicherheitsstandard durch die dezentralen Firewalls sind sehr gut. Das liegt sicher auch an der guten Betreuung durch Innominate. Die Reaktionszeiten sind kurz, und wenn wir Ideen oder Verbesserungsvorschläge haben, sind diese meistens in eine der nächsten Versionen eingebunden“, beurteilt Asmund Hey die Zusammenarbeit.

Weitere Verbesserungen sind geplant

Eine der geplanten Erweiterungen ist die Einrichtung einer zentralen Verwaltung der dezentralen Maschinennetze. Ziele sind die möglichst weitgehende Standardisierung, die einheitliche Konfiguration und die einfachere Administration der Netze. Dafür wird der Innominate Device Manager (IDM) einge-

führt, der die Status-Informationen aller verwalteten Komponenten für eine zentrale Überwachung verfügbar macht. Fertige Konfigurationen oder Updates können vom IDM auf die dezentralen Firewalls übertragen werden. Dabei lässt sich durch eine Vorlagen- und Vererbungstechnik ein hoher Automatisierungsgrad für die Konfiguration einzelner Geräte erzielen. Ein weiteres Projekt betrifft die Nutzung der mGuards zur Fernwartung. Bedarf für Fernwartungszugriffe gibt es durch die Anlagenbauer, aber auch intern durch den Prüfmittelbau. Erfahrungen mit der Fernwartung haben die Mitarbeiter von ZF Sachs seit Langem. Durch die neue Sicherheitsarchitektur mit den Maschinen hinter der Firewall muss allerdings eine andere Lösung entsprechend der geänderten Sicherheitsregeln gefunden



werden. Der sichere Remote-Zugriff über VPNs ist deshalb ein interessanter Zusatznutzen der mGuards, der jetzt zur Anwendung kommen soll.

Über ZF Sachs

Die ZF Sachs AG als Unternehmensbereich Antriebs- und Fahrwerkkomponenten der ZF Friedrichshafen AG hat ihren Hauptsitz in Schweinfurt und beschäftigt weltweit rund 16.500 Mitarbeiter. ZF Sachs ist seit über 100 Jahren ein angesehener Partner der Fahrzeugindustrie. Die Produkte kommen neben den klassischen Anwendungsbereichen Pkw, Nutzfahrzeuge, Bahn, Bau- und Agrartechnik auch im Motorsport zum Einsatz. ■

www.innominate.com



Autor: Martin Ortgies, freier Fachjournalist

Bild 2: Nach der Installation der mGuard-Systeme sind die Maschinennetze bei ZF Sachs besser geschützt. So konnte sich ein eingeschleppter Virus aufgrund der Segmentierung nicht weiter im Netz verbreiten.