



Halle 7
Stand 540



Schutz industrieller Netzwerke

Die Volkswagen AG hat im Produktionsnetz des Karosseriebaus im Werk Emden nach einer Risikoanalyse einen neuen Sicherheitsstandard eingeführt. Durch die Segmentierung des Netzes, die Installation industrieller Firewalls und strenger Zugriffsregeln sind die Anlagen jetzt gegen unerlaubte Zugriffe geschützt.

Ethernet-basierte Produktionssysteme setzen sich zunehmend durch. Die einfache Integration in Intranets und das Internet, die hohe Bandbreite bis hin zu Gigabit/s sowie sinkende Kosten für industriell spezifizierte Kabel, Verbinder oder Switches und Router sind die Gründe. Die Kehrseite ist ein erhöhtes Risiko von Störungen und Produktionsunterbrechungen durch Sicherheitslücken in industriellen Netzen. Im Werk Emden Karosseriebau der Volkswagen AG wurde deshalb im Produktionsnetzwerk eine interne Risikoanalyse durchgeführt und die Sicherheit der Anlagen einschließlich der Steuerungs- und Regelungstechnik untersucht. Das Ergebnis: Sensible Produktionsanlagen sind nicht ausreichend gegen unerwünschte Zugriffe geschützt, weil Angriffe durch Schadprogramme, ungewollte Zugriffe oder unbeabsichtigte Fehleingaben durch Aktivitäten im internen Netz ausgelöst werden können und der Schutz durch zentrale Firewalls sehr aufwändig und unwirtschaftlich ist. Als Gefährdungspotenzial gelten z.B. Mitarbeiter von Fremdfirmen, die für Serviceeinsätze oder für Hard- und Softwareinstallationen mit ihrem Laptop auf das Netzwerk zugreifen und unbeabsichtigt Schadsoftware einbringen können. Auch unbeabsichtigte Fehleingaben wurden als problematische Schwachstellen identifiziert.

„Ein typisches Beispiel ist die Installation eines Servers, der anschließend in kurzen Abständen Ping-Pakete in das gesamte Netzwerk schickt. Solche permanenten Abfragen können eine industrielle Steuerung stören oder sogar zum Absturz bringen“, benennt Jens Hoofdman, technischer Sachbearbeiter Instandhaltung Karosseriebau einen Problempunkt aus der Analyse.

Neue Sicherheitsregeln für das industrielle Netz

Auf Basis der Risikoanalyse wurde ein Maßnahmenplan entwickelt, der organisatorische Änderungen, die Segmentierung des Netzes und die Einführung dezentraler industrieller Firewalls umfasste. Bei der Auswahl geeigneter Härtungs- und Sicherheitsmaßnahmen hat sich die Volkswagen AG, Werk Emden für Industrial Router mit integrierter Firewall entschieden. Die dezentral eingesetzte Industrie-Firewall-/Router-Lösung sorgt im Bereich des Karosseriebaus Emden für die Segmentierung des Produktionsnetzwerks in 15 abgeschottete Subnetze. Für einen zentralen Schutz mit vergleichbarer Granularität müssten alle Systeme bzw. Subnetze sternförmig mit einer sehr leistungsfähigen und komplex konfigurierten zentralen Firewall verkabelt werden. Das ist bei den typischen Entfernungen in

einem Industrierwerk sehr teuer und unwirtschaftlich, weswegen in solchen Umgebungen praktisch nur baum- und linienförmige Verkabelungstopologien vorzufinden sind, zu denen der dezentrale mGuard-Ansatz besser passt.

Dezentrale Industrie-Firewall-/Router-Lösung

Bei den Vorgesprächen zur Umsetzung der neuen Struktur, der technischen Bewertung und Anlaufüberwachung war auch die zentrale IT beteiligt. Die produktionsnahe IT sorgte schließlich für die Planung, Installation, Inbetriebnahme und Verwaltung. Das Anlagenetzwerk wurde bereits erfolgreich mit dem Blomberger Automatisierungsspezialisten Phoenix Contact geplant und in Betrieb genommen. Die guten Erfahrungen aus diesem Projekt und das vorhandene Wissen um die Anlagen waren deshalb auch bei der Absicherung des Netzwerks willkommen. Eingesetzt werden die Industrie-Firewall-/Router-Module FL mGuard von Phoenix Contact und Innominate. Für ihre Auswahl waren die Industrietauglichkeit und die Verfügbarkeit eines zentralen Managements die maßgeblichen Kriterien. Die mGuard-Module basieren auf einem gehärteten Embedded Linux und integrieren vier aufeinander abgestimmte Sicherheitskomponenten: eine bidirek-



Bild 2: Sensible Produktionsanlagen sind meistens nicht ausreichend geschützt. Eingeschleppte Schadprogramme oder auch unbeabsichtigte Fehleingaben im internen Netz können durch zentrale Firewalls nicht verhindert werden.

tionale Stateful Inspection Firewall, einen flexiblen NAT-Router, ein sicheres VPN-Gateway sowie optional einen industrietauglichen Schutz vor Schadsoftware. Als Vorteil erwies sich, dass die MGuard Security Appliance autark ist und durch den sogenannten 'Stealth Mode' ohne Rückwirkungen auf das Produktionsnetz nachträglich integriert werden kann. Die Firewall verhält sich dabei routing-technisch transparent wie eine Bridge.

Einrichtung von Industriefirewalls

Die Installation, Einrichtung und Einbindung der Industrie-Firewalls war aus Sicht von Jens Hoofdmann eher einfach. Die Geräte wurden dezentral in



Bild 3: „Die Erfahrungen mit den mGuard-Industrie-Firewalls sind sehr gut. Alle unerlaubten Zugriffe werden geblockt und die Anlagen sind jetzt gegen Schadsoftware besser geschützt“, berichtet Jens Hoofdmann, technischer Sachbearbeiter Instandhaltung Karosseriebau bei der Volkswagen AG im Werk Emden.

jedem Uplink in Schaltschränken eingesetzt. Hardwaretechnisch konnten die 24V-Hutschienen-Geräte direkt in die Schaltschränke montiert und mit eigenem Personal auf Basis der vorhandenen Netzwerkstruktur und ohne Neverkabelung in Betrieb genommen werden. Bei der Einrichtung der Firewall-Regeln sei man ganz pragmatisch vorgegangen, so Hoofdmann. Zunächst wurde jeder Datenverkehr zugelassen und die Zugriffe in die Subnetze nur mitgeloggt. Die Logfiles wurden anschließend ausgewertet und in Regeln festgehalten, welche Zugriffe künftig erlaubt sein sollten. Die Regeln wurden getestet, nochmals verbessert und schließlich so definiert. In dieser Phase wurden die Erfahrungen von Innominate, einer 100%-igen Tochter von Phoenix Contact, genutzt. Jens Hoofdmann: „Wir haben vom tiefgehenden Know-how von Innominate mit Industrie-Netzwerken, Protokollen und Firewall-Regeln intensiv profitiert und die Installationen so besser strukturiert und optimiert.“

Zentrales Management-System

Das zentrale Management-System, der Innominate Device Manager (IDM), bietet einen Template-Mechanismus, mit dem alle mGuard Geräte zentral konfiguriert und verwaltet werden können. Die Parameter für Firewall-Regeln und NAT-Einstellungen werden im IDM direkt konfiguriert, ohne dass abstrakte Security Policies definiert werden müssen. Über die Upload-Funktion werden

die Vorgaben auf alle aufgelisteten Devices hochgeladen und in einem Arbeitsgang konfiguriert. Mit dem IDM wurden auch spezielle Regeln zwischen den Subnetzen sowie Untergruppen und Usergruppen umgesetzt und dann auf alle Firewalls verteilt. Die Verwaltung der Geräte wurde durch das zentrale Management-System nach den Erfahrungen des Instandhaltungsbereichs bei VW Emden wesentlich erleichtert. Jetzt sei es kein Problem, innerhalb von fünf Minuten eine neue Firewall-Regel zu generieren, um etwa einem Servicemitarbeiter den Zugang zu erlauben.

Schutz für sensible Produktionsanwendungen

Im Produktionsnetzwerk vom Karosseriebau Emden wurden inzwischen Roboter, SPS, Panel PC, Lasertechnik, Schweißanlagen, Steuerungen und das führerlose Transportsystem (FTS) durch dezentrale Firewalls abgesichert. Jens Hoofdmann berichtet, dass es seit der Einrichtung der Firewalls keine Sicherheitsvorfälle mehr gegeben hat. Anhand der Log-Files konnten allerdings verseuchte Geräte aus anderen Produktionsbereichen identifiziert werden. Ein Virus hatte versucht, sich zu verteilen. Der Zugriff auf die geschützten Maschinen wurde aber abgeblockt und die anderen Bereiche konnten über die problematische Malware informiert werden. Jens Hoofdmann: „Die Erfahrungen mit den mGuard-Industrie-Firewalls sind sehr gut. Wir sind zu 100% zufrieden. Die Unterstützung von Innominate ist auch bei Problemen sehr professionell. Alle unerlaubten Zugriffe werden geblockt und die Anlagen sind jetzt gegen Schadsoftware geschützt.“

www.innominate.com



Autor: Martin Ortgies, Fachjournalist