

# Unerlaubte Zugriffe blocken

**Industrielle Netzwerke schützen.** Volkswagen 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, Verbindungen oder Switches und Router sind die Gründe. Die Kehrseite ist ein erhöhtes Risiko von Störungen und Produktionsunterbrechungen durch Sicherheitslücken in industriellen Netzen.

Im Karosseriebau des Volkswagen-Werks Emden wurde deshalb im Produktions-Netzwerk 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 aufwendig und unwirtschaftlich ist.

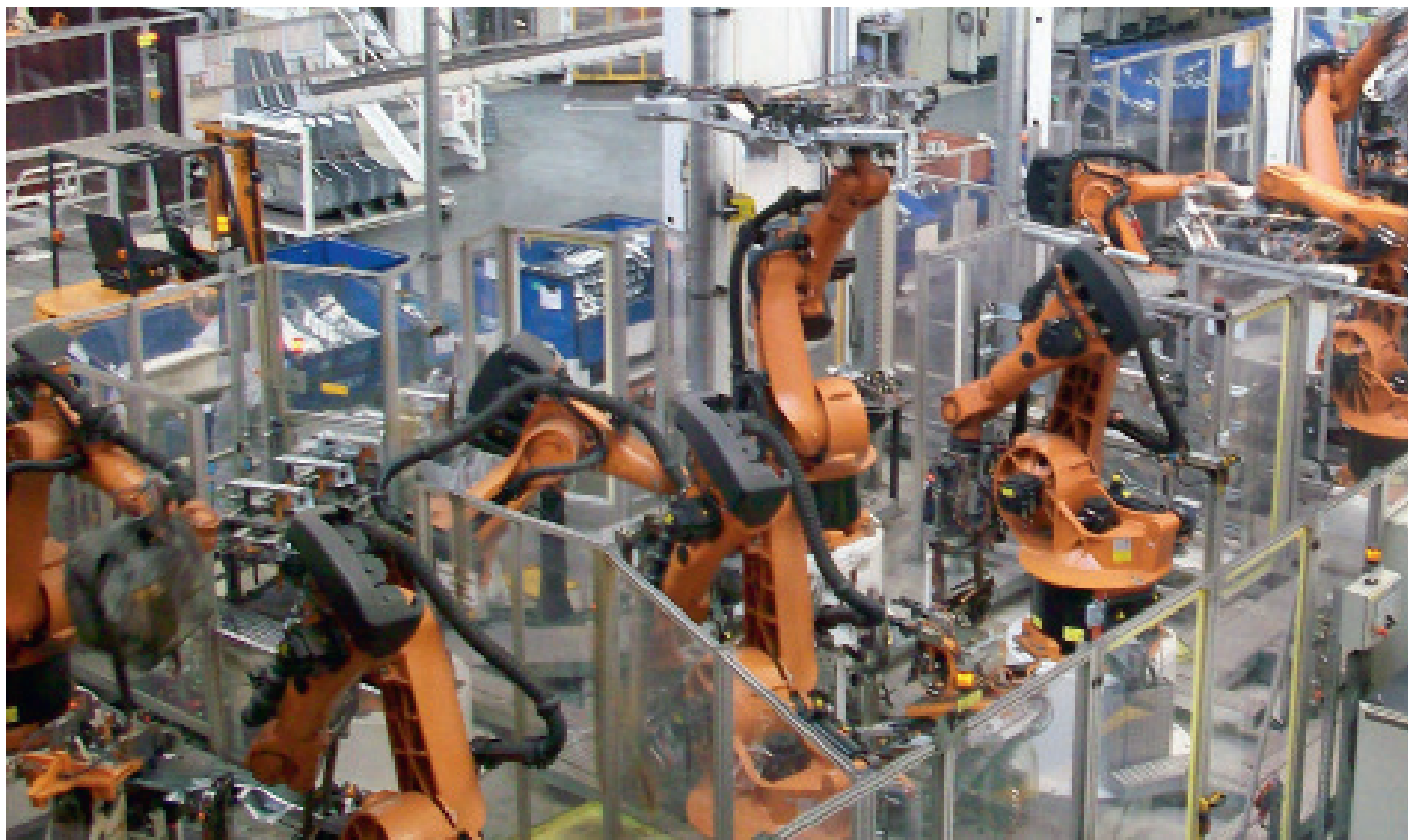
Als Gefährdungspotenzial gelten zum Beispiel Mitarbeiter von Fremdfirmen, die für Serviceeinsätze oder für Hard- und Softwareinstallationen mit ihrem Laptop auf das Netzwerk zugreifen und unbeabsichtigt Schadsoftware einbringen können. Auch unbeabsichtigte Fehleingaben wurden als problematische Schwachstellen identifiziert. „Ein typisches Beispiel ist die Installation eines Servers, der anschließend in kurzen Abständen

den Ping-Pakete in das gesamte Netzwerk schickt. Solche permanenten Abfragen können eine industrielle Steuerung stören oder sogar zum Absturz bringen“, benennt Jens Hoofdmann, 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.

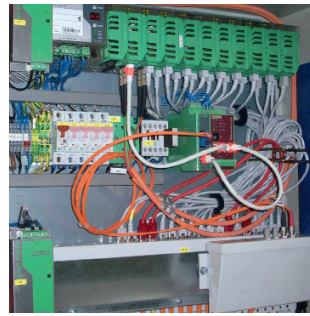
Bei der Auswahl geeigneter Härtings- und Sicherheitsmaßnahmen hat sich Volkswagen für Industrial Router mit integrierter Firewall entschieden. Die dezentral eingesetzte Industrie-Firewall-/Router-Lösung sorgt im Bereich des Karosseriebaus Emden für die Segmentierung des Produktionsnetzwerks in 15 abgeschottete Subnetze. Für einen zentralen Schutz mit vergleichbarer Granularität müssten alle Systeme oder 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 von Innominate sehr viel besser passt.





„Unsere Erfahrungen mit den mGuard-Industriefirewalls sind sehr gut.“

Jens Hoofdmann,  
Volkswagen



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

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 Anlagennetzwerk 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 bidirektionale 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.

### Einrichtung von Industriefirewalls

Die Installation, Einrichtung und Einbindung der Industriefirewalls war aus Sicht von Jens Hoofdmann eher einfach. Die Geräte wurden dezentral in jedem Uplink in Schaltschränken eingesetzt. Hardwaretechnisch konnten die 24-Volt Hutschienen-Geräte direkt in die Schaltschränke montiert und mit eigenem Personal auf Basis der vorhandenen Netzwerkstruktur und ohne Neuverkabelung 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.

### Zentrales Management-System

Das zentrale Management-System, der Innominate Device Manager (IDM), bietet einen Template-Mechanismus, mit dem alle mGuard-Devices 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 hoch geladen 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.

Im Produktionsnetzwerk vom Karosseriebau Emden wurden inzwischen Roboter, SPS, Panel-PC, Lasertechnik, Schweißanlagen, Steuerungen und das führerlose Transportsystem (FTS) durch dezentrale Firewalls abgesichert. Hoofdmann berichtet, dass es seit der Einrichtung der Firewalls keine Sicherheitsvorfälle mehr gegeben hat. Anhand der Log-Files konnten allerdings versuchte 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. „Die Erfahrungen mit den mGuard-Industriefirewalls sind sehr gut. Wir sind zu 100 Prozent zufrieden. Die Unterstützung von Innominate ist auch bei Problemen sehr professionell. Alle unerlaubten Zugriffe werden geblockt und die Anlagen sind jetzt gegen Schadsoftware besser geschützt“, berichtet Hoofdmann abschließend.



Sensible Produktionsanlagen sollten ausreichend gegen unerwünschte Zugriffe geschützt werden – so auch im Karosseriebau des Volkswagen-Werks Emden.

**Autor**

Martin Ortgies, freier Fachjournalist, für Innominate