

Netzwerk-Security

Unberechtigte Zugriffe auf das Automatisierungsnetzwerk durch Hacker oder auch eigene Mitarbeiter können die Vertraulichkeit von Daten gefährden und die Verfügbarkeit des Systems beeinflussen. Daher spielen Security-Maßnahmen bei Industrial Ethernet eine wichtige Rolle.

TEXT: Ralf Moebus BILDER: Safety Network international e.V.

Die proprietären Kommunikations- und Steuerungssysteme der Automatisierungstechnik werden mehr und mehr durch so genannte „offene“ Systeme ersetzt. Insbesondere das aus dem Büro bekannte Ethernet soll die mehr oder weniger proprietären Feldbusse der Vergangenheit ablösen. Die Vorteile der neuen Kommunikationstechnologie sind vielfältig. Ethernet bietet genug Bandbreite, damit alle Automatisierungsgeräte in einem einzigen durchgängigen Netzwerk miteinander kommunizieren können. Des Weiteren ist eine direkte Kommunikation der Office- mit der Feldebene möglich. Das benötigte spezielle Wissen für viele verschiedene Feldbustechnologien kann auf eine Technologie reduziert werden. Durch die hohe Geschwindigkeit von Ethernet können Produktionsprozesse beschleunigt und die Qualität der Produkte gesteigert werden.

Allerdings müssen beim Einsatz von Ethernet auch einige Punkte berücksichtigt werden, damit eine hohe Produktivität von Maschinen und Anlagen gewährleistet ist. Boten die proprietären Systeme einen gewissen Schutz gegen bösartige oder auch unbeabsichtigte Angriffe auf das System, so sind diese Systeme heute durch die Verwendung von verbreiteten Technologien, wie Ethernet und Windows, vielfältigen neuen Gefahren ausgesetzt. Insbesondere durch die Forderung nach einem durchgängigen Netzwerk, das den Zugriff aus dem Büro oder gar dem Internet auf Geräte in der Feldebene ermöglichen soll, wird das Risiko von Angriffen erhöht. Angriffe auf Computer durch Hacker gehören heute in der Office-Welt zum Alltag und Schutzmechanismen wie Firewalls oder Virens Scanner sind gängige Praxis. In der Produktionsumgebung haben Ausfälle der Systeme weit dramatischere Auswirkungen. Produktionsausfälle von wenigen Stunden können bereits sehr hohe Kosten verursachen und sind nicht akzeptabel. In diesem Zusammenhang ist insbe-

sondere die Sicherheitstechnik zum Schutz von Menschen zu nennen. Sicherheitsgerichtete Kommunikation reagiert äußerst empfindlich auf Kommunikationsverzögerungen. Kommen sichere Daten nicht rechtzeitig beim Empfänger an, führt dies zum Abschalten der Anlage. Derartige Verzögerungen müssen nicht bösartig durch Hacker verursacht werden, sie können auch das Resultat eines unbeabsichtigten „Angriffs“ von eigenen Mitarbeitern sein. Unberechtigte Zugriffe aus dem Office können den Datenverkehr im Automatisierungsnetzwerk ausbremsen. Eine geeignete Netzwerkplanung, die Security-Aspekte berücksichtigt, kann die Risiken von Produktionsausfällen reduzieren.

Die bekannten Strategien aus dem Büro lassen sich jedoch nicht direkt auf das Automatisierungsnetzwerk übertragen, da die Anforderungen sehr verschieden sind. Im industriellen Umfeld herrschen höhere Anforderungen an die Robustheit der eingesetzten Geräte gegen Umwelteinflüsse. Desweiteren gelten wesentlich höhere Anforderungen an das Echtzeitverhalten der Systeme. Im Folgenden soll eine Vorgehensweise zur Implementierung einer Security-Lösung und einige einsetzbare Technologien vorgestellt werden.

Management einer Security-Lösung über den gesamten Lebenszyklus

Um die Wirksamkeit einer Security-Lösung zu gewährleisten muss deren gesamter Lebenszyklus betrachtet werden. Der Lebenszyklus einer Security-Lösung besteht im Wesentlichen aus drei Phasen:

1. Beurteilung. In der Beurteilungsphase wird das Unternehmensnetzwerk in Security-Zonen eingeteilt, die Zonengrenzen und der benötigte Security-Level festgelegt.

2. Entwicklungs- und Implementierungsphase. In dieser Phase werden Prozesse und Regelwerke definiert, sowie die Technologien wie zum Beispiel Firewalls implementiert.
3. Betriebs- und Instandhaltungsphase. Security-Maßnahmen müssen in regelmäßigen Intervallen überprüft und bei Bedarf die Wirksamkeit wiederhergestellt werden.

Zur Umsetzung von Security-Maßnahmen stehen heute vielfältige technische Lösungen zur Verfügung, die einem ständigen technologischen Wandel unterliegen. Aus diesem Grund werden im Folgenden nur die Wichtigsten näher erläutert.

Industrial Firewalls

Eine Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall, das Netzwerk oder Netzsegment vor unerlaubten Zugriffen zu schützen. Der Einsatz von Firewalls ist heute zum Schutz von Büronetzwerken gängige Praxis.

Die aus dem Büroumfeld bekannten Firewalls sind jedoch nicht für den Einsatz im industriellen Umfeld geeignet. Die Projektierung und Handhabung in der Produktionsumgebung ist eine wichtige Anforderung. Die einschlägigen Office-Security-Lösungen sind jedoch Systeme für Experten. In der Automatisierungstechnik kann nicht immer vorausgesetzt werden, dass tiefes Security-Knowhow vorhanden ist. Sogenannte Industrial Firewalls schaffen hier Abhilfe. Diese Geräte sind Plug&Play-Lösungen in einem robusten Hutschienengehäuse, deren Funktionalität genau auf die Aufgaben in der Automatisierungstechnik zugeschnitten sind. Eine dieser Aufgaben ist zum Beispiel, die sichere Fernwartung von Maschinen und Anlagen zu ermöglichen. Das heißt, eine Maschine an einem beliebigen Standort auf der Welt soll für den Maschinenhersteller für den Zweck der Fehlerdiagnose und -behebung über das Internet erreichbar sein. Um diesen Fernzugriff sicher zu gestalten, muss die Firewall VPN-(Virtual Private Network)-Verbindungen unterstützen. Durch den VPN-Tunnel sind die Daten vor fremdem Zugriff geschützt. Des Weiteren können Hardwareeingänge zum Anschluss von Tastern zum automatischen Verbindungsaufbau von der Maschine zum Hersteller vorhanden sein. Teilweise sind bei Industrial Firewalls auch ISDN-Modems für das Telefonnetz, oder GSM-Funkmodems integriert, womit eine vom Firmennetzwerk autarke Fernwartungslösung realisiert werden kann.

Virens Scanner

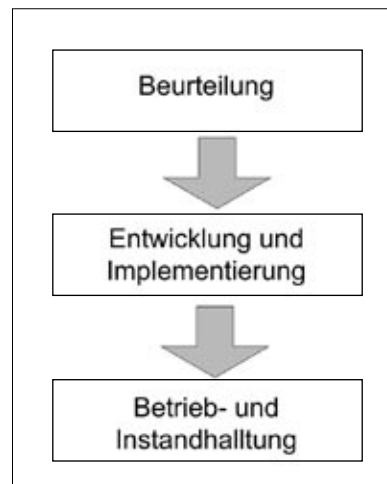
Das übliche Gegenmittel gegen Viren, Würmer und Trojaner sind Virens Scanner und regelmäßige Security-Patches. Was im Büroumfeld völlig normal ist, kann im Automatisierungsumfeld oft nicht umgesetzt werden. Automatisierungs-



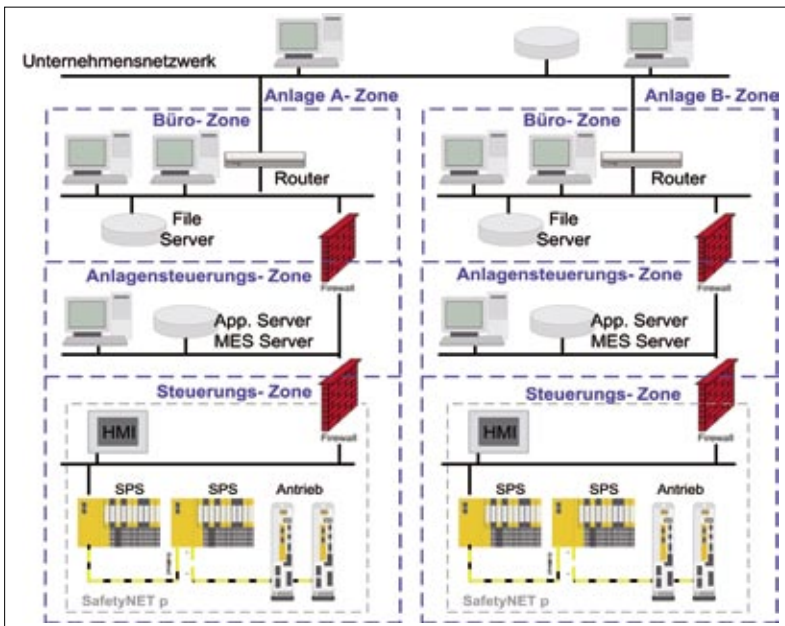
Die Anforderungen des industriellen Umfelds unterscheiden sich von der Büroumgebung

rechner müssen immer verfügbar sein und können nicht ohne weiteres heruntergefahren und neu gebootet werden. Virens Scanner reduzieren die Performance der Automatisierungsrechner, sodass der Produktivdatenverkehr darunter leidet. Zudem erfordern Virens Scanner ständige Pflege und sind so mit hohem Aufwand verbunden. Hier kann ebenfalls die Segmentierung des Netzwerks mittels Industrial Firewalls helfen. Der Zugriff auf das Netzwerksegment wird dabei auf bestimmte Nutzer beschränkt. Wenn sichergestellt ist, dass diese Rechner einen aktuellen Virens Scanner besitzen, ist sichergestellt, dass hier keine Viren in das Netzwerksegment eingeschleust werden. Außerdem muss sichergestellt werden, dass keine firmenfremden Laptops mit Schadsoftware an dem betroffenen Netzwerksegment angeschlossen werden.

Industrial Firewalls können durch Sperren bestimmter Ports verhindern, dass Viren, Würmer und Trojaner auf das Internet zugreifen. >



Prozess der Implementierung einer Security-Lösung



Netzwerksegmentierung mittels Industrial Firewalls steigert Anlagenverfügbarkeit und sichert Vertraulichkeit der Daten

Authentifizierung

Authentifizierung stellt sicher, dass nur ausdrücklich erlaubte Personen auf Netzwerksegmente oder auf einzelne Geräte zugreifen können. Ein wesentlicher Punkt ist dabei die Rollendefinition, worin festgelegt wird, wer welche Aktionen ausführen darf. Firewalls können die Zugriffe auf Netzwerksegmente mittels Passwortschutz reglementieren. Oft sind auch innerhalb der Geräte verschiedene Passwortlevels notwendig. Beispielsweise möchte man dem Instandhaltungspersonal erlauben, das Programm einer SPS zu tauschen, aber nicht zu ändern. Oder aus Knowhow-Schutzgründen ein Auslesen der Programme verhindern. Dies kann mit einem geräteintegrierten Passwortschutz realisiert werden. Solche Mechanismen müssen durch den Hersteller des Automatisierungsgerätes zur Verfügung gestellt werden.

Physikalische Schutzmaßnahmen

Besonders im industriellen Umfeld reichen oft einfache Schutzmaßnahmen aus, um die Verfügbarkeit des Automatisierungssystems zu erhöhen. Freie Ethernet-Ports an einem Switch können Servicepersonal dazu verleiten, ihren Laptop dort einzustecken. Wird durch diese Kommunikation jedoch der Prozessdatenverkehr, der über diesen Switch läuft, ausgebremst, kommen Telegramme nicht mehr rechtzeitig bei deren Empfängern an und die Verfügbarkeit der Maschine kann beeinflusst werden.

Security in der Normung

Verschiedene Normungsgremien befassen sich derzeit mit dem Thema Security. Am weitesten fortgeschrit-

ten ist die Arbeit der Arbeitsgruppe innerhalb der nordamerikanischen ISA (International Society of Automation). Die sogenannte ISA99-Standardreihe ist ein ganzheitlicher Ansatz, der sowohl den Prozess der Implementierung eines Security-Management-Systems im Unternehmen, als auch die technische Umsetzung berücksichtigt. Dieser Standard wird voraussichtlich aufgrund der umfangreichen Unterstützer eine hohe Bedeutung erlangen.

Innerhalb der Nutzerorganisation Safety Network International hat sich eine Arbeitsgruppe formiert, die ein Security-Konzept für das Ethernet basierte industrielle Kommunikationssystem SafetyNET p erarbeitet. Die Arbeitsgruppe definiert Security-Anforderungen für SafetyNET-p-Komponenten und definiert eine Guideline für Anwender.

Zusammenfassung

Security wird durch den durchgängigen Einsatz von Industrial Ethernet weiterhin an Bedeutung für die Automatisierungstechnik gewinnen. Hersteller und Betreiber von Maschinen und Anlagen sollten sich mit dem Thema vertraut machen, wenn sie die neuen Möglichkeiten der durchgängigen Kommunikation ohne Verfügbarkeitsverlust der Produktion oder Gefährdung der Vertraulichkeit Ihrer Daten nutzen möchten. Safety Network International erarbeitet für SafetyNET p die notwendigen Anforderungen für Gerätehersteller und Security Guidelines für Anwender. □

Literatur

Guide to the ISA-99 Standards Manufacturing and Control Systems Security,
<http://www.isa.org>

> MORE@CLICK SIK10106