

Netzwerk-Security in industriellen Kommunikationssystemen

Innerhalb der Nutzerorganisation Safety Network International erarbeitet eine Arbeitsgruppe ein Security-Konzept für das industrielle, ethernet-basierte Kommunikationssystem SafetyNET p. Wie auf Anwenderspekte eingegangen wird, zeigen die Implementierung einer Security-Lösung, bereits verfügbare Technologien und der Stand der Normung.

TEXT: Ralf Moebus FOTOS: Safety Network International e.V.

Proprietäre Kommunikations- und Steuerungssysteme der Automatisierungstechnik werden zunehmend durch so genannte „offene“ Systeme ersetzt. Boten die traditionellen Systeme einen gewissen Schutz gegen bösartige oder auch unbeabsichtigte Angriffe auf das System, sind neue Lösungen durch die Verwendung von verbreiteten Technologien stärkeren Gefahren ausgesetzt. Insbesondere durch die Forderung nach einem durchgängigen Netzwerk, das die Kommunikation von der Office- in die Feldebene und direkten Zugriff aus dem Internet ermöglicht, wird das Risiko von Angriffen erhöht. Die Abwehr von Viren oder Hackern gehört in der Office- Welt heute zum Alltag. Schutzmechanismen, wie Firewalls oder Viren-Scanner sind gängige Praxis. Diese Strategien lassen sich jedoch nicht direkt auf das Automatisierungsnetzwerk übertragen. Im industriellen Umfeld herrschen höhere Anforderungen an die Robustheit der eingesetzten Geräte. Des Weiteren sind auch die Ansprüche an das Echtzeitverhalten der Systeme deutlich höher.

Um die Wirksamkeit einer Security-Lösung zu gewährleisten muss deren gesamter Lebenszyklus betrachtet werden. Dieser besteht im Wesentlichen aus drei Phasen. Hinweise zur detaillierten Vorgehensweise während dieser Phasen gibt die weiter unten im Text erläuterte Standard-Reihe ISA 99.

Beurteilung

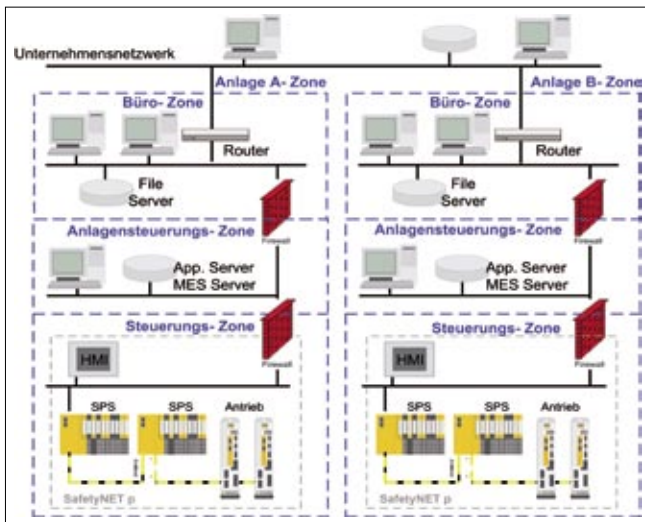
In der Beurteilungsphase wird das Unternehmensnetzwerk in Security-Zonen eingeteilt und die Zonengrenzen festgelegt. Außerdem wird das tolerierbare Risiko eines Unternehmens bestimmt: Welchen Security-Level möchte man überhaupt erreichen? Und wie viel ist einem diese Sicherheit wert? Also eine Abwägung von Aufwand und Nutzen.

Entwicklung und Implementierung

Wenn der Ziel-Security-Level einer Zone ermittelt wurde, müssen Maßnahmen implementiert werden, um diesen Level zu erreichen. Hierbei spielt neben den technologischen Lösungen, wie Firewalls, auch die Definition von Prozessen und Regelwerken eine wichtige Rolle. Bestandteil dieser Regelwerke ist eine Rollendefinition. Darin wird festgelegt, welcher Personenkreis im Netzwerk welche Aktionen ausführen darf.

Betrieb und Instandhaltung

Security-Maßnahmen verschlechtern sich im Laufe der Zeit. Deshalb müssen sie in regelmäßigen Intervallen über- >



Netzwerksegmentierung mittels Industrial Firewalls steigert Anlagenverfügbarkeit und sichert Vertraulichkeit der Daten

prüft und bei Bedarf die Wirksamkeit wiederhergestellt werden.

Zur Umsetzung solcher Maßnahmen stehen heute vielfältige technische Lösungen zur Verfügung, die einem ständigen technologischen Wandel unterliegen. Im Folgenden werden die Wichtigsten näher beleuchtet:

Industrial Firewalls

Eine Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden. So versucht sie das Netz vor unerlaubten Zugriffen zu schützen.

Die im Büroumfeld etablierten Firewalls sind nicht für den Einsatz im industriellen Umfeld geeignet. Denn die Projektierung und Handhabung in der Produktionsumgebung



Die Anforderungen des industriellen Umfelds unterscheiden sich von der Büroumgebung

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. Solche Plug&Play-Lösungen im robusten Hutschienengehäuse sind genau auf die Ansprüche in der Automatisierungstechnik zugeschnitten.

Eine dieser Aufgaben ist zum Beispiel, die sichere Fernwartung von Maschinen und Anlagen über das Internet zu ermöglichen. Um diesen Fernzugriff sicher zu gestalten, muss die Firewall VPN-Verbindungen (VPN = Virtual Private Network) unterstützen. Durch den VPN-Tunnel sind die Daten vor fremdem Zugriff geschützt. Desweiteren können Hardware-Eingänge 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.

Viren-Scanner

Das übliche Gegenmittel gegen Viren, Würmer und Trojaner sind Viren-Scanner und regelmäßige Security-Patches. Auch hier können Office-Lösungen nicht auf die Produktion übertragen werden, denn Automatisierungsrechner müssen immer verfügbar sein und können nicht ohne weiteres heruntergefahren und neu gebootet werden. Viren-Scanner reduzieren die Performance der Automatisierungsrechner, sodass der Datenverkehr darunter leidet. Außerdem erfordern Viren ständige Pflege und sind so mit hohem Aufwand verbunden. Hier kann ebenfalls die Segmentierung des Netzwerks mittels Industrial Firewalls helfen. Der Zugriff auf das Netzsegment wird dabei auf bestimmte Nutzer beschränkt. Wenn sichergestellt ist, dass diese Rechner einen aktuellen Scanner besitzen, können keine Viren ins Netz gelangen. Außerdem dürfen keine firmenfremden Laptops an dem betroffenen Netzsegment angeschlossen werden.

Authentifizierung

Die Authentifizierung stellt sicher, dass nur ausdrücklich erlaubte Personen auf Netzsegmente oder auf einzelne Geräte zugreifen können. Dabei wird auch festgelegt, wer welche Aktionen ausführen darf. Firewalls können die Zugriffe mittels Passwortschutz reglementieren. Oft sind innerhalb der Geräte verschiedene Passwort-Level notwendig. Beispielsweise möchte man dem Instandhaltungspersonal erlauben, das Programm einer SPS zu tauschen, aber nicht zu ändern. Oder aber man verhindert aus Know-how-Schutzgründen ein Auslesen der Programme. Dies kann mit einem geräteintegrierten Passwortschutz realisiert werden.



Für das Industrielle Kommunikationssystem SafetyNET p werden Security-Richtlinien für Gerätehersteller und Anwender definiert

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 Service-Personal dazu verleiten Ihren Laptop dort einzustecken. Wird durch diese Kommunikation der Prozessdatenverkehr ausgebremst, kommen Telegramme nicht mehr rechtzeitig bei deren Empfängern an und die Verfügbarkeit der Maschine kann beeinflusst werden.

Security Datasheets

Um alle securityrelevanten Eigenschaften dem Anwender zur Verfügung zu stellen, werden Hersteller von SafetyNET-p-Geräten angehalten, ihren Produkten sogenannte Security Datasheets beizulegen. Diese beinhalten Informationen zur Inbetriebnahme der Geräte und zu den Security-Mechanismen. Wichtig dafür sind in erster Linie die Protokolle, die zur Kommunikation verwendet werden. Für die Kommunikation über Firewalls müssen die entsprechenden Ports freigeschaltet werden. Daraus lassen sich auch Rückschlüsse über potenzielle Gefährdungen für die Netzwerksicherheit treffen.

Security in der Normung

Verschiedene Normungsgremien befassen sich derzeit mit dem Thema Security. Am weitesten fortgeschritten ist die Arbeit der Arbeitsgruppe innerhalb der nordamerikanischen ISA (International Society of Automation). Die Standard-Reihe ISA 99 ist ein ganzheitlicher Ansatz, der sowohl den Prozess der Implementierung eines Security-Management-Systems im Unternehmen, als auch die technische Umsetzung berücksichtigt. Die ISA 99 besteht aus vier Normteilen, die ersten beiden sind bisher veröffentlicht:

- ▶ ISA S99.00.01 – Models, Definitions, and Terminology: Teil 1 ist die Basis für ein einheitliches Verständnis und einheitliche Beschreibung von Security-Anforderungen und -Lösungen in Automatisierungsanlagen.
- ▶ ISA S99.00.02 – Establishing a Manufacturing and Control System Security Program: Teil 2 definiert ein Security-

Programm. Dabei wird ein vierphasiges Vorgehensmodell „Plan-Do-Check-Act“ mit 18 sogenannten „Key Elements“ spezifiziert.

- ▶ ISA S99.00.03 – Operating a Manufacturing and Control Systems Security Program: Teil 3 bezieht sich auf die Betriebsphase einer Security Lösung.
- ▶ ISA S99.00.04 – Specific Security Requirements for Manufacturing and Control Systems: Teil 4 befasst sich hauptsächlich mit unterschiedlichen Anforderungen zwischen der Büroumgebung und der Produktionsumgebung eingegangen.

Neben den vier normativen Teilen wurden von der ISA zwei technische Reports zum aktuellen Stand der Security-Technologieanwendungen im Automatisierungsumfeld erstellt:

- ▶ TR99.00.01 Security Technologies for Manufacturing and Control: Übersicht über verfügbare Security-Technologien die im industriellen Umfeld von Interesse sind
- ▶ TR99.00.02 Integrating Electronic Security in Manufacturing and Control Systems Environment: Hinweise zur Planung, Entwurf und Betrieb von Security-Maßnahmen in industriellen Anlagen

Die ISA-99-Standardreihe befindet sich aktuell noch in der Entstehung. Voraussichtlich werden auch andere Normungsgremien, wie die IEC die Arbeit der ISA teils oder sogar vollständig übernehmen. Auch die SafetyNET p Security Guideline wird sich dort wo anwendbar auf diesen Standard beziehen.

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. □

> MORE@CLICK.ADK90040