

Netzwerk-Security in einem industriellen Kommunikationssystem

Ralf Moebus



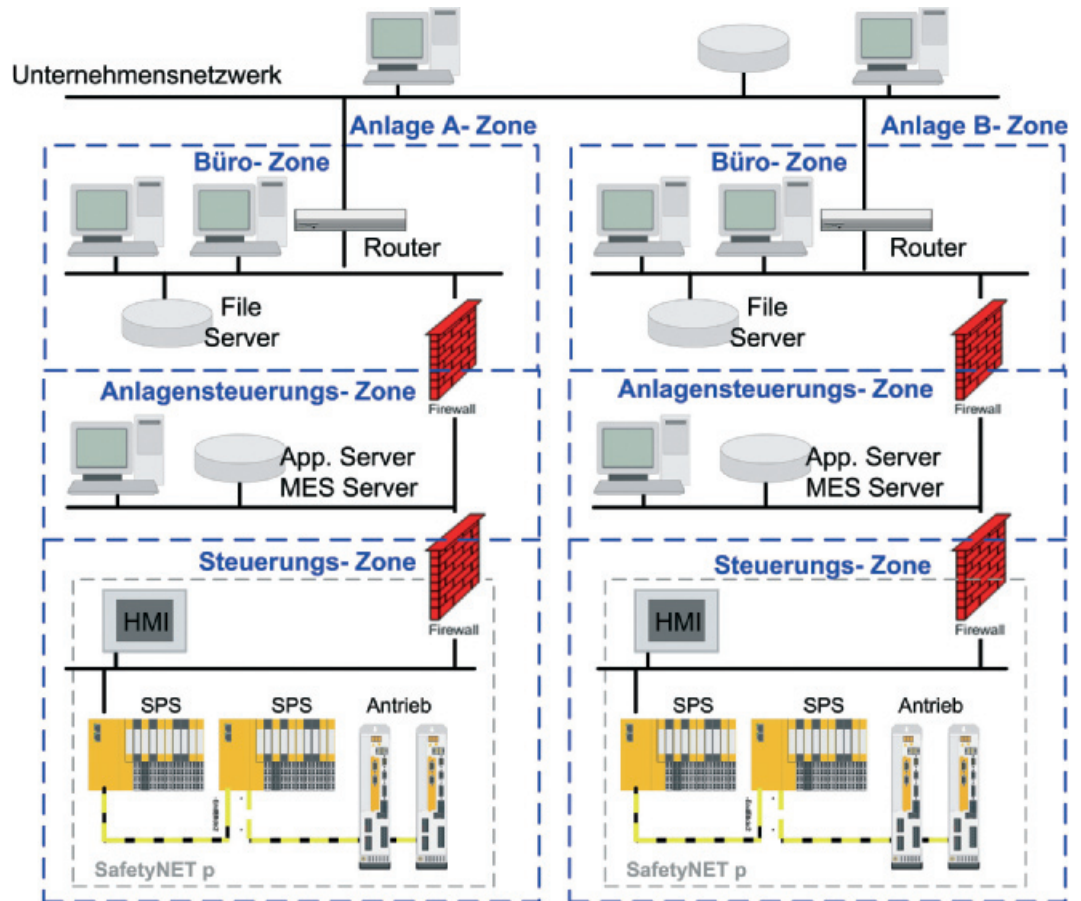
Ralf Moebus
Vorsitzender der
Security Arbeits-
gruppe
Safety Network
International e.V.
73760 Ostfildern
Kontakt: www.safety-network.de

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

Security – Sicherheit in der Automatisierung

Die proprietären Kommunikations- und Steuerungssysteme der Automatisierungstechnik werden mehr und mehr durch so genannte »offene Systeme« ersetzt. Boten die proprietären Systeme einen gewissen Schutz gegen böswillige oder auch unbeabsichtigte Angriffe auf das System, so sind diese Systeme heute durch die Verwendung von verbreiteten Technologien wie Ethernet und MS Windows vielfältigen neuen 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. Angriffe auf Computer durch Hacker gehören heute in der Office-Welt zum Alltag. Hier gehören Schutzmechanismen wie Firewalls oder Viren-Scanner zur gängigen Praxis.

Die 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 Robust-



Netzwerksegmentierung mit Industrial Firewalls.

Grafik: Safety Network International e.V.

heit der eingesetzten Geräte gegen Umwelteinflüsse. Echtzeit-Anforderungen der Systeme sind zu berücksichtigen.

Innerhalb der Nutzerorganisation Safety Network International hat sich eine Arbeitsgruppe formiert, welche ein Security-Konzept für das Ethernet basierte industrielle Kommunikationssystem SafetyNET p erarbeitet. Im Wesentlichen verfolgt die Arbeitsgruppe zwei Ziele: zum einen sollen Security-Anforderungen für SafetyNET p-Komponenten definiert und des Weiteren eine Guideline für Anwender von SafetyNET p entwickelt werden.

Im Folgenden wird der Prozess der Implementierung einer Security-Lösung und die bereits verfügbaren technologischen Lösungen für das Umfeld der industriellen Automatisierung aufgezeigt.

Lebenszyklus einer Security-Lösung

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

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.

Entwicklungs- und Implementierungsphase

Wenn der Ziel-Security-Level einer Zone ermittelt wurde, müssen Maßnahmen implementiert werden, um diesen Level zu erreichen. Hierbei spielen neben den verschiedenen technologischen Lösungen wie Firewalls auch die Definition von Prozessen und Regelwerken eine wichtige Rolle. Ein wesentlicher Bestandteil bei der Entwicklung eines Security-Konzepts für ein Netzwerk ist die Rollendefinition. Dabei wird definiert, welcher Personenkreis im Netzwerk welche Aktionen ausführen darf.

Betriebs- und Instandhaltungsphase

Security-Maßnahmen verschlechtern sich im Laufe der Zeit. Deshalb müssen sie 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 beleuchtet:

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

Industrial Firewalls und Schutz vor Viren, Würmern und Trojanern

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. Dies wird besonders bei der Projektierung, Inbetriebnahme und dem Pflegeaufwand im laufenden Betrieb deutlich. Die einschlägigen Office-Security-Lösungen sind allerdings Systeme für Experten, die entsprechende Kenntnisse erfordern. In der Automatisierungstechnik kann aber nicht immer vorausgesetzt werden, dass tiefes Security-Knowhow vorhanden und rund um die Uhr verfügbar ist. Industrial Firewalls sind Plug and 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, müssen VPN-Verbindungen unterstützt werden. 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. Oft möchten die IT-Abteilungen bei den Betreibern ihre Firewalls für bestimmte benötigte Protokolle nicht freischalten. Aus diesem Grund werden auch Industrial Firewalls mit ISDN-Modems für das Telefonnetz oder GSM-Funkmodems für das Mobilfunknetz angeboten, womit das Firmennetzwerk komplett umgangen werden kann.

Das probate Gegenmittel gegen jene Art von gefährlicher Software sind Virens Scanner und regelmäßige Security-Patches. Das, was im Büroumfeld völlig normal ist, kann im Automatisierungsumfeld oft nicht umgesetzt werden, denn Automatisierungsrechner müssen immer verfügbar sein und können nicht ohne Weiteres heruntergefahren und neu gebootet werden. Zusätzlich ist die verwendete Automatisierungssoftware oft nicht für Virens Scanner freigegeben, beziehungsweise die Virens Scanner reduzieren die Performance, so dass der Produktivdatenverkehr darunter leidet. Auch er-

fordern Virens Scanner ständige Pflege und sind so mit hohem Aufwand verbunden. Dennoch sind Viren, Würmer und Trojaner eine gefährliche Bedrohung für Automatisierungsrechner. Was also tun? 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. Bleibt nun noch die Gefahr durch firmenfremde Laptops, die zum Beispiel durch Service-Personal an dem betroffenen Netzwerksegment angeschlossen werden und deren Aktualität des Virens Scanners nicht garantiert werden kann. Eine mögliche Lösung ist, diesen Personen einen Laptop zur Verfügung zu stellen, welcher über einen aktuellen Virens Scanner verfügt.

Ein weiterer Schutzmechanismus gegen Viren, Würmer und Trojaner ist die Möglichkeit durch Schließen bestimmter Ports in der Industrial Firewall. Kommunikationsprotokolle werden gesperrt, die diese Schadsoftware benutzen, so dass diese nicht auf das Internet zugreifen oder sich weiter im firmeninternen Netz ausbreiten können.

Authentifizierung und Security Datasheets

Die Authentifizierung stellt sicher, dass nur ausdrücklich erlaubte Personen auf Netzwerksegmente oder auf einzelne Geräte zugreifen können. Ein wesentlicher Punkt ist dabei die Rol-

lendifinition, 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 nur mit einem geräteintegrierten Passwortschutz realisiert werden. Solche Mechanismen müssen durch den Hersteller des Automatisierungsgerätes zur Verfügung gestellt werden.

Um alle Security relevanten Eigenschaften dem Anwender zur Verfügung zu stellen, sollen Hersteller von SafetyNET p-Geräten der Bedienungsanleitung so genannte Security Datasheets beilegen. Diese beinhalten im Wesentlichen Informationen, die benötigt werden, um die Geräte in Betrieb zu nehmen, und Informationen darüber, welche Mechanismen für Security zur Verfügung gestellt werden. Wichtig für die Inbetriebnahme 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. In den Datasheets sind Angaben über eine vorhandene Benutzer-Authentifizierung enthalten. Damit weiß der Anwender, ob er die Authentifizierung gegebenenfalls durch andere Maßnahmen sicherstellen muss.

Security in der Normung

Verschiedene Normungsgremien befassen sich derzeit mit dem Thema Security. Bisher am weitesten fortgeschritten ist die Arbeit der Arbeitsgruppe innerhalb der nordamerikanischen ISA (International Society of Automation). Die so genannte ISA 99-Standard-Reihe ist ein sehr ganzheitlicher Ansatz, welcher sowohl den Prozess der Implementierung eines Security Management-Systems im Unternehmen als auch die technische Umsetzung berücksichtigt. Dieser Standard wird voraussichtlich aufgrund der umfangreichen Unterstützung eine hohe Bedeutung erlangen. Die ISA 99-Reihe besteht aus vier Normen-Teilen:

- 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 so genannten »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.

Neben den vier normativen Teilen wurden 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-Standard-Reihe befindet sich aktuell noch in der Entstehung. Voraussichtlich werden auch andere Normungsgremien wie die IEC höchstwahrscheinlich die Arbeit der ISA in Teilen oder sogar vollständig übernehmen. Auch die SafetyNET p-Security-Guideline wird sich dort wo anwendbar auf diesen Standard beziehen.