NETZWERKSICHERHEIT IM WANDEL

Sicherheitsanforderungen für industrielle Ethernet-Netzwerke betreffen nicht mehr nur die Unternehmensebene, sondern zunehmend auch die Prozesssteuerung und andere industrielle Umgebungen. Nach den jüngsten Problemen durch die Stuxnet Malware muss das Thema Sicherheit in industriellen Netzwerken neu betrachtet werden. John Browett von der CLPA beleuchtet die möglichen Sicherheitsrisiken industrieller Netzwerke und zeigt auf, wie man ihnen begegnen kann.

Ethernet ist immer häufiger die erste Wahl bei industriellen Netzwerken. Der Aspekt der Netzwerksicherheit wurde dabei jedoch lange Zeit vernachlässigt. Das Risiko eines Angriffs von außerhalb wie auch von innerhalb eines Netzwerks ist allerdings nach wie vor hoch.

Es ist nicht einfach, sich vor vorsätzlichen Zugriffen Unbefugter zu schützen, denn hier besteht nicht nur ein Problem der Netzwerksicherheit, sondern auch der auf das Personal bezogenen Sicherheit. Die Möglichkeit, dass ein Mitarbeiter ein Gerät unbeabsichtigt mit einer falschen Stelle im Netzwerk oder mit unautorisierten Anwendern verbinden könnte, muss berücksichtigt werden. Nicht autorisierte Dritte können dann unter Umständen wichtige Prozessparameter ändern, ohne sich der Konsequenzen bewusst zu sein. Zwar schätzen Unternehmen die Vorteile des Fernzugriffs auf Anlagen, zum Beispiel in der Prozessüberwachung über einen Standard-Web-Browser, dies bedeutet aber auch, dass die Netzwerke dem potenziellen Missbrauch durch Dritte geöffnet werden.

Die Stuxnet-Problematik des letzten Jahres, in der der weit verbreitete Virus auch SCADA-Systeme (Supervisory Control and Data Acquisition Systeme) angriff, macht Sicherheitsschwachstellen der herkömmlichen Steuerungsarchitektur auf Werkebene deutlich. In Folge haben viele Betriebe die bislang üblichen Methoden zur Informationsübertragung zwischen Werk- und Unternehmensebene in Frage gestellt.

Das Stuxnet-Virus hat den Angriffspunkt im Unternehmensnetzwerk von der vermeintlich besonders sicheren obersten zur anfälligeren mittleren Ebene verlagert. Dort sind häufig PC-basierte Steuerungssysteme im Einsatz, die mit wenigen bis gar keinen Sicherheitsfunktionen ausgestattet sind und manchmal sogar trotz bekannter Angriffsanfälligkeit weiterverwendet werden.

Auf der mittleren wie auch auf Maschinenebene verschärfen sich Sicherheitsprobleme zusätzlich, da die Zusammenarbeit zwischen der IT-Abteilung und der Steuertechnik häufig eingeschränkt ist. Außerdem messen Kontroll- und Engineering-Abteilungen Sicherheitsgefahren in Automatisierungssystemen häufig nicht die nötige Bedeutung bei. Vor allem hat sich die Wirtschaftlichkeitsberechnung für die Sicherheit von Automatisierungssystemen noch nicht durchgesetzt, und das Risikoverständnis ist mangelhaft.

Offenen Netzwerktechnologien, allen voran das Ethernet, geben Unternehmen bei der Auswahl der bestmöglichen Steuerungssysteme große Freiheiten. Sie bergen aber auch hohe Sicherheitsgefahren. Einheitliche, offene Protokolle haben die Forderungen der Anwender nach Standardisierung, Flexibilität und Auswahlmöglichkeiten erfüllt. Die Folgen werden erst jetzt deutlich: Die offenen Protokolle sind weniger stabil und anfälliger für Angriffe. Im Gegensatz dazu waren die zuvor eingesetzten proprietären, also unternehmensspezifischen Netzwerke besonders stabil, aber auch wesentlich unflexibler und boten lediglich eine stark eingeschränkte Produktauswahl.

In einem optimalen industriellen Netzwerk wäre die Stabilität des alten mit der Flexibilität des neuen Systems kombiniert. Eine Ideallösung würde sich außerdem durch gewöhnliche Verkabelung, herkömmliche Anschlüsse, offene Standards, einfache Konfiguration, Flexibilität, höchstmögliche Sicherheit und reduzierte Angriffsanfälligkeit auszeichnen.

Bei der Suche nach Wegen, industrielles Ethernet so zu gestalten, dass es alle Anforderungen einer Ideallösung tatsächlich erfüllt, sollte man sich die Begriffsdefinition von Ethernet nochmal vor Augen führen. Denn nirgends in der Netzwerksprache wurde ein einziges Wort so häufig als Überbegriff für so viele unterschiedliche Standards, Technologien und Applikationen missbraucht wie im Fall des Ethernets. Im ersten Schritt ist die Betrachtung der sieben Schichten des Open System Interconnection Modells, kurz OSI-Modell, sinnvoll.

Schicht 1, die Bitübertragungsschicht (Physical Layer), definiert alle elektrischen und physischen Spezifikationen für Geräte und Netzwerkkomponenten. Vor allem bestimmt sie die Beziehung zwischen einem Gerät und dem Übertragungsmedium. Schicht 2 bezeichnet die Sicherungsschicht (Data Link Layer), die Funktionen und Verfahren für den Datentransfer zwischen Netzwerkkomponenten zur Verfügung stellt sowie Fehler der Bitübertragungsschicht erkennt und gegebenenfalls korrigiert. Auf dieser Ebene wird Ethernet als Netzwerkprotokoll gemäß IEEE-Norm 802.3 definiert.

Im Lauf der Jahre wurde der Begriff Ethernet zum Synonym für die TCP/IP Suite, was aber nicht immer korrekt ist. IP ist in Schicht 3 des OSI-Modells, der Vermittlungsschicht (Network Layer), festgelegt. Sie liefert die Funktionen und Verfahren zur Übertragung von Datensequenzen variabler Länge von einem Sender zu einem Empfänger über ein oder mehrere Netzwerke. Die Transportschicht (Schicht 4, Transport Layer) ermöglicht die transparente Datenübertragung zwischen Endanwendern und beschreibt Protokolle wie TCP und UDP.

Die Sitzungsschicht (Schicht 5, Session Layer) steuert die Computerverbindungen, die Darstellungsschicht (Schicht 6, Presentation Layer) wandelt Daten um und erstellt so eine Standardschnittstelle für die Anwendungsschicht (Schicht 7, Application Layer). Hier findet man typische Applikationen wie FTP, HTTP, RTP, SMTP und SNMP. Diese sieben übergeordneten Schichten bilden die Voraussetzung für den Einsatz von Ethernet als Kommunikationsarchitektur in industriellen Netzwerken.

Nicht alle industriellen Ethernet-Anbieter implementieren den Ethernet-Stack auf dieselbe Art. In der Anwendungsschicht verwenden die verschiedenen Entwickler ihre eigenen Kernels und Protokolle, die häufig die wesentlichen funktionalen Vorteile der jeweiligen Technologien ausmachen. Aus Sicherheitssicht sind jedoch die anfälligeren unteren Schichten besonders interessant.

Wird im OSI-Schichtmodell nur eine Schicht erfolgreich angegriffen, ist das gesamte Kommunikationssystem gefährdet. Dabei wird das Problem in den anderen Schichten gegebenenfalls gar nicht sichtbar. Die Sicherheit ist nur so stark wie das schwächste Glied des Systems.

Zwar gibt es eine Reihe diskreter, gut funktionierender Sicherheitsprodukte. Eines der größten Probleme im industriellen Bereich ist aber die Implementierung von nahtlos integrierten Sicherheitssystemen, ohne übermäßige Kosten zu verursachen und ohne eine Komplexitätsebene zu schaffen, die nur schwer aufrechterhalten und unterstützt werden kann. Außerdem erfüllen die standardmäßig verfügbaren Sicherheitslösungen selten die hohen Anforderungen anspruchsvoller industrieller Umgebungen.

Im Bereich der Netzwerktechnologie wurde viel getan, um Schicht 2 sicherer zu gestalten. Die Schwachpunkte der Vermittlungs- und der Transportschicht (Schicht 3 und 4) in industriellen Ethernet-Systemen finden in der Regel wenig Beachtung. Wie ein Office-Ethernet in der Büroumgebung sind auch die meisten industriellen Ethernet-Landschaften in Schicht 3 IP-gestützt, in Schicht 4 basieren sie oft auf TCP/UCP.

An Schnittstellen zu anderen Netzwerken sind industrielle Ethernet-Applikationen häufig mit äußeren Sicherheitsfunktionen wie Firewalls ausgestattet, um so den Schutz für diese leicht angreifbaren Schichten zu gewährleisten. Firewalls filtern nach Quell- und Ziel-IP-Adressen sowie Protokoll-Portnummern (zum Beispiel von TCP- und UDP-Ports) und schränken so zusätzlich die Zugriffe auf das Ethernet-Netzwerk ein. Paketfilter können sogar zwischen bekannten Netzwerk-Communities implementiert sein. In manchen Fällen sind die Filter auch auf spezifische Geräteadressen und Applikations-Ports ausgerichtet, um die Zugriffe zu sichern. Trotzdem sind in herkömmlichen industriellen Ethernet-Anwendungen die Schichten 3 und 4 weiterhin höchst anfällig für Angriffe.

CC-Link IE (Control and Communication Link Industrial Ethernet) ist hingegen anders konzipiert. CC-Link IE wurde von der CLPA als erstes vollständig integriertes Gigabit-Ethernet-Netzwerk für die industrielle Automatisierung entwickelt. Dabei wurden neue Schwellenwerte für offene Standards im industriellen Ethernet definiert. CC-Link IE vereint die Vorteile bestehender Technologien und wendet sie auf einem optischen oder kupferbasierten industriellen Netzwerksystem mit einer redundanten Architektur an, die extrem schnelle und zuverlässige Datenübertragung zwischen Feldgeräten und anderen Steuerungen über Ethernet-Verbindungen ermöglicht. Mit der Datenübertragungsrate

von einem Gigabit pro Sekunde setzt CC-Link IE hohe Maßstäbe und definiert Systemfähigkeiten neu. Die Ansprüche an Echtzeitdatenübertragung der Fertigungsindustrie werden dabei mehr als erfüllt.

Um den Kontrollanforderungen auf sämtlichen Ebenen des Automatisierungsnetzwerks zu entsprechen, ist CC-Link IE in unterschiedlichen Varianten erhältlich. CC-Link IE Control ist für den Einsatz auf Steuerungsebene bestimmt, CC-Link IE Field und CC-Link IE Motion sind für die Geräteebene konzipiert. Die Integration mit dem CC-Link Feldbus funktioniert nahtlos.

Der wesentliche Unterschied zwischen CC-Link IE und konventionellen Implementierungen besteht in der Definition eines offenen „Echtzeitprotokolls" innerhalb der Schichten des Protokoll-Stacks. CC-Link IE erfüllt alle Anforderungen einer idealen Netzwerktechnologie, da es über Standard-Ethernet-Anschlüsse verfügt, einfach zu konfigurieren und besonders stabil ist. Als offener Standard verleiht es Anwendern volle Entscheidungsfreiheit bei der Wahl der „Best-of-Breed"-Komponenten. Zudem erfüllt es höchste Sicherheitsanforderungen und ist deshalb weniger anfällig für Angriffe. Die Vorteile gegenüber anderer industrieller Ethernet-Systeme sind offensichtlich. Das wesentliche Unterscheidungsmerkmal ist eine offene aber zugleich kontrollierte Wissensbasis für die Netzwerktechnologie. Unternehmen können also die Technologie auf einer offenen Struktur implementieren und dennoch wird es für potenzielle Angreifer schwieriger, in das Netzwerk einzudringen.

Sicherheitsanforderungen für industrielle Ethernet-Netzwerke entwickeln sich ständig weiter. Zunehmend müssen neben Unternehmensnetzwerken auch Prozesssteuerungen und andere industrielle Umgebungen hohe Sicherheitsanforderungen erfüllen. Bei Netzwerkinstallationen sollten Unternehmen stets mögliche Angriffsflächen und damit verbundene Risiken ermitteln und untersuchen. Netzwerksicherheit gewinnt zunehmend an Bedeutung und in jeder der sieben Schichten der Netzwerkarchitektur sollten potenzielle Risiken abgeschwächt, reduziert oder komplett ausgeschlossen werden. Basierend auf einem offenen Standard und proprietärer Kommunikationstechnologie stellt CC-Link IE eine besonders interessante Option dar, die Netzwerksicherheit zu maximieren und zu optimieren.

Über CLPA

Die CC-Link Partner Association (CLPA) ist eine internationale Organisation mit weltweit über 1.700 Mitgliedsunternehmen. Gemeinsames Ziel ist die Verbreitung und technische Entwicklung der offenen CC-Link-Netzwerktechnologien. Über 250 Hersteller bieten inzwischen mehr als 1.200 zertifizierte Produkte an. CC-Link ist der führende industrielle Feldbus in Asien und gewinnt auch in Europa und Amerika zunehmend an Bedeutung. Die Organisation hat ihren europäischen Hauptsitz in Deutschland und weitere Büros in anderen europäischen Ländern.

Editor Contact

DMA Europa Ltd. : Elke Davies

Tel: +44 (0)1299 405454
Fax: +44 (0)1299 403092
Web: www.dmaeuropa.com
Email: Elke.davies@dmaeuropa.com

Company Contact

CLPA Europe : John Browett

Tel: +44 (0)776 833 8708

Fax: +49 (0)2102 532 9740
Web: www.the-non-stop-open-network.com
Email: john.browett@clpa-europe.com