4/18 www.digital-manufacturing-magazin.de D, A, CH: 9,50 Euro, weitere EU-Länder: 11,70 Euro

DIGITAL MANUFACTURING

AUFBAU UND OPTIMIERUNG IT-GESTÜTZTER PRODUKTIONSPROZESSE

Industrie 4.0 | Internet der Dinge

Digitalisierung in der Fertigung

Autonome Produktion durch kundenorientierte Automation

DMG MORI

S7-Firewall schützt SPS-Daten

Bei Industrie 4.0 ist eine der Grundvoraussetzungen die Anbindung aller Maschinen an die firmeninterne IT-Infrastruktur. Über diese sollen Prozessdaten von den Maschinen erfasst, Rezepturen eingegeben, Ferndiagnosen durchgeführt und Maschinen programmiert werden können. Eine Firewall sorgt dabei für die Daten- und Betriebssicherheit.

VON FABIAN TRÄGER

Die kompakte S7-Appliance eignet sich für die Hutschienenmontage im Schaltschrank.

DIE ANBINDUNG an Industrie-4.0-Plattformen betrifft nicht nur neue, sondern vor allem vorhandene Anlagen, die bereits in die Produktion integriert sind. Viele bestehende Anlagensteuerungen bieten die dafür notwendigen Schnittstellen. Allerdings sind nicht alle für eine direkte Angliederung an das häufig homogene Firmennetz gerüstet. Neben der technischen Umsetzbarkeit sollte bei solchen Vorhaben vor allem berücksichtigt werden, ob und wie sich die Daten- und Betriebssicherheit dieser Anlagen nach der Integration ins Netz aufrechterhalten lässt.

Ein weitverbreitetes und zugleich kritisches Exemplar ist die Speicherprogrammierbare Steuerung (SPS) Siemens S7 der Serie 300/400. Dieses Modell verfügt über eine TCP/IP-Schnittstelle, über die mittels des S7-Protokolls SPS-Daten ausgelesen und geschrieben werden können. Weder im Protokoll noch direkt in der SPS sind dabei Mechanismen vorhanden, die einen ausreichenden Schutz vor einer böswilligen oder unbeabsichtigten Manipulation der Prozessdaten und der SPS-Programme bieten.

Der im Jahr 2010 aufgetretene Computerwurm Stuxnet nutzte genau diese Sicherheitsmängel, um den Betrieb von spezifischen Anlagen, die mit S7-Steuerungen ausgestattet sind, gezielt zu stören oder sogar ganz zu zerstören.

Die Kommunikation mit der S7 wird über das sogenannte RFC-1006-Protokoll abgewickelt, das über den TCP/IP-Port 102 übermittelt wird. Der Zugriff auf die SPS-Variablen erfolgt mit Hilfe der Adressen der Datenbausteine, in denen sie gespeichert sind. Während diese Adressen in der Regel bekannt sind, können die Inhalte der Datenbausteine über das S7-Protokoll direkt ausgelesen und manipuliert werden. Eine Authentifizierung hierzu wird meist nicht verwendet und bietet selbst bei Einsatz keinen ausreichenden Schutz, da die Übertragung der Kommunikationspakete unverschlüsselt erfolgt und die Länge des Passworts unzureichend ist.

Das RFC-1006-Protokoll ist zwar nicht offengelegt, ist aber weitestgehend bekannt und in Form von Produkten wie S7-OPC-Server und Open-Source-Software verfügbar. Beispielsweise lässt sich mit dem Sniffing-Tool Wireshark der Datenverkehr zwischen zwei RFC-1006-Verbindungspartnern ohne weiteres aufnehmen und analysieren.

Jeder Netzwerkteilnehmer, der Zugriff auf den TCP/IP-Port der S7 und eine Implementierung des Protokolls besitzt, hat somit vollen Zugriff auf alle Funktionen in der SPS: Programmieren, Programme löschen, SPS starten, SPS stoppen, Prozessdaten lesen und schreiben. In der SPS lassen sich diese Funktionen weder einschränken noch wird der Absender der Telegramme überprüft. Jede Verbindung zur SPS ist gleichberechtigt.

Mit einer herkömmlichen IT-Firewall lassen sich Netzteilnehmer vom Zugriff auf die S7 aussperren. Die S7-Firewall erlaubt hingegen eine effiziente Zugriffskontrolle, bei der sich die Berechtigungen der Teilnehmer fein abstufen lassen. Bilder: Traeger Industry Components

Invalide Prozessdaten führen zu Fertigungsfehlern

Sollte diese Sicherheitslücke durch einen böswilligen Angriff ausgenutzt werden, können die daraus entstehenden Folgen alleine durch die Beschaffenheit der Anlage abgeschätzt werden. Im besten Fall stehen invalide Prozessdaten bereit, die im Produktionsverlauf zu Fertigungsfehlern führen und durch Fehlchargen Kosten verursachen. Darüber hinaus ist eine technische Schädigung der Anlage möglich, wie sie durch Stuxnet verursacht wurde. Produktionsausfälle und Wartungskosten wären hier die Folge. Im schlimmsten Fall ist sogar mit der Gefährdung von Menschen zu rechnen, insbesondere dann, wenn die Anlage im sicherheitskritischen Bereich eingesetzt wird.

Aber auch ohne mutwillige Manipulation ist eine solche Betriebsfehler möglich. Eine unbeabsichtigte Fehlkonfiguration in der Anbindung eines SCADA kann ebenfalls zu invaliden Prozess- und Programmdaten in der SPS führen und verheerende Folgen haben.

Eine naheliegende Möglichkeit, die SPS vor Fremdzugriffen zu schützen, ist der Einsatz einer Firewall. Mit herkömmlichen, nichtspezialisierten IT-Firewalls können Verbindungen nach bestimmten Filterkriterien verboten oder zugelassen werden. Diese Verbindungskriterien sind die IP-/MAC-Adressen des Verbindungs-

initiators beziehungsweise des Verbindungsziels und der Ziel-Port. Mit einem solchen Filter lassen sich beispielsweise Office-Netzwerke und SPS-Netzwerke effektiv trennen. Somit können die Anlagen vor direktem Zugriff durch Viren-infizierte Büro-PCs geschützt werden.

Zugriff auf die Anlagensteuerung

Der Schutz zwischen SCADA-Netzwerk und SPS-Netz gestaltet sich als weitaus schwieriger. Einerseits benötigt man vom SCADA-System aus Zugriff auf die Steuerungen der Anlagen. Andererseits sollte dieser Zugriff für einen sicheren Betrieb nicht uneingeschränkt möglich sein. Hierbei sind die Filterkriterien einer solchen Firewall nicht anwendbar. Entweder ist eine Verbindung zur SPS möglich und der andere Kommunikationsteilnehmer besitzt die Berechtigung auf der SPS oder es ist keine Verbindung erlaubt. Für eine sinnvolle und dennoch geschützte Anbindung sind tiefergehende Filterkriterien notwendig, die eine feinere Granulierung der Zugriffsberechtigungen zulassen.

Die S7-Firewall bietet Deep Paket Inspection, eine Bit-genaue Zugriffskontrolle und SPS-Programmschutz.

Die S7-Firewall von Traeger führt eine sogenannte Deep Paket Inspection der durchgehenden Datenpakete in Echtzeit durch. Dabei untersucht sie die Pakete auf Protokollebene und filtert Pakete mit unerlaubten Zugriffen aus. Auf diese Weise ermöglicht sie eine effiziente Kontrolle der Zugriffe auf die jeweilige SPS.

Bei der Anbindung eines SCADA-Systems kann nur eine Lese- und Schreibberechtigung für die notwendigen Datenbausteine gesetzt werden. Das SPS-Programm wird geschützt und private Daten der SPS bleiben für den Kommunikationspartner unerreichbar. Wenn im Falle eines Datenloggers Daten von der SPS gelesen werden müssen, können hierfür nur lesende Zugriffe auf die benötigten Daten erlaubt werden. Die Konfiguration der S7-Firewall erfolgt über ein integriertes Web-Interface. Darüber kann Bit-genau festgelegt werden, welche Datenbereiche der SPS vom Partner geschrieben oder nur gelesen werden dürfen. Die Parametrierung erfolgt mit einer einfachen, regelbasierten Syntax, mit der sich die Datenbereiche exakt beschreiben lassen.

Nahtlose Integration der Firewall

Die S7-Firewall lässt sich ohne Änderung der Infrastruktur und der Konfiguration der jeweiligen Geräte in das vorhandene Netzwerk integrieren. Die Kommunikationsparameter in den Endgeräten bleiben unverändert. Bei Anfragen mit Zugriffen auf nicht freigegebene Daten werden nur die verbotenen Zugriffe herausgefiltert und eine protokoll-konforme Fehlerantwort generiert. Die erlaubten Zugriffe werden weitergeleitet und können von der SPS verarbeitet werden. In einem Logfile lassen sich abgelehnte Zugriffe anzeigen und Netzwerkteilnehmer mit Fehlverhalten aufspüren. Weiterhin verfügt die Firewall über eine integrierte Lernfunktion, mit deren Hilfe sich aus den erfassten abgelehnten Zugriffen Regeln erstellen lassen. So ist es möglich, Regeln hinzuzufügen, selbst wenn die konkreten Adressen der verwendeten Daten nicht bekannt sind.

Die S7-Firewall kann in einen sogenannten validierten Betriebsmodus versetzt werden. Dabei wird die aktuelle Konfiguration eingefroren und lässt sich nicht mehr bearbeiten. Erst nach dem kompletten Zurücksetzen der Firmware ist wieder eine Änderung der Konfiguration möglich. Dieser Modus wurde für den Einsatz in Anlagen, die einer Validierungspflicht unterliegen, zum Beispiel in der Pharmaindustrie, implementiert.

Weiterhin bietet die S7-Firewall die Möglichkeit, IP-Adressen von Anlagen auszutauschen. Mit diesem IP-Address-Swapping können Anlagen, die ab Werk eine nichtveränderbare identische IP-Konfiguration besitzen, im gleichen Netz betrieben werden, ohne Adresskonflikte zu verursachen. Um über außergewöhnliche Ereignisse informiert zu werden, lässt sich eine E-Mail-Benachrichtigung in der Firewall aktivieren. sg

Fabian Träger ist Senior Developer bei Traeger Industry Components.