HIRSCHMANN
A BELDEN BRAND

HOPF
PARTNER | SOLUTIONS | COMPONENTS

Sicherheit im Netzwerk

Entwurfsmuster für mehr Sicherheit in industriellen Netzwerken

Prof. Dr. Tobias Heer – CTO Office,
Hirschmann Automation and Control GmbH

Dr. Lars Geiger – Manager Advance Development,
Hirschmann Automation and Control GmbH

Die Zeiten, in denen industrielle Netzwerke physisch von allen anderen Netzwerken getrennt werden konnten, sind längst vorbei. Dies gilt ebenso für den Mythos der Sicherheit durch Inkompatibilität, der seit langer Zeit ein Gefühl der Sicherheit für industrielle Anlagen bot.

Die Verhältnisse haben sich jedoch nicht nur aufgrund von Entwicklungen wie des Industrial Internet of Things und von Industie 4.0, die zu einer starken Vernetzung und Homogenisierung der Netzwerkstrukturen industrieller Anlagen geführt haben, verändert. Bereits zuvor begannen die Hersteller von Industriekomponenten ihre vernetzbaren Komponenten auf Basis von Standard Industrie-PC-Systemen zu entwerfen.

Außerdem ersetzten sie zunehmend proprietäre Kommunikationsprotokolle mit den weltweit stark verbreiteten und akzeptierten Netzwerkprotokollen Ethernet und TCP/IP. Durch diese verstärkte Vernetzung entsteht jedoch eine größere Angriffsfläche für industrielle Anlagen.

Inhaltsverzeichnis

Be certain.
Belden.

Darüber hinaus werden viele Überwachungs- und Steuerungssysteme Jahre und Jahrzehnte lang eingesetzt, ohne dass sie rechtzeitig Sicherheits-Updates erhalten bzw. erhalten können. Entweder weil solche Patches nicht verfügbar sind oder weil eine Änderung der Software Risiken bergen oder auch bestehende Zertifizierungen ungültig machen kann. Dies führt zu zahlreichen sogenannten Soft Targets (weichen Zielen) in einer Anwendung mit industriellen Steuerungssystemen. Daher liegt es auf der Hand, dass diese wichtigen, aber anfälligen Systeme geschützt werden müssen. Viele Unternehmen setzen am Rand ihres industriellen Netzwerks sogenannte Perimeter Firewalls ein, um die Soft Targets in ihren industriellen Anwendungen vor Bedrohungen aus dem Internet oder aus Office-Netzwerken zu schützen. Obwohl dies ein unabdingbarer Schritt ist, erfordert moderne Netzwerksicherheit weit mehr als diese Perimeter-Sicherheit.

Konzepte für eine umfassende Netzwerksicherheit müssen sowohl unterschiedliche Angriffsmethoden als auch verschiedene Angreifer berücksichtigen. Dazu gehören etwa Szenarien, in denen die erste Verteidigungslinie bereits überwunden wurde, also die Firewall am Übergang vom Produktionsnetz zum Office-Netzwerk oder dem Internet. Sobald ein Angreifer in ein Netzwerk eingedrungen ist, kann er schnell großen Schaden anrichten, wenn die Architektur und die Konfiguration dieses Netzwerks ohne Berücksichtigung des Sicherheitsaspekts gewählt wurden. Die gute Nachricht: Ein Netzwerk zu realisieren, das einem eingedrungenen Angreifer widersteht, ist nicht so kompliziert, wie es zunächst scheinen mag. Jedoch muss die Sicherheit bereits in der Planungsphase eines Netzwerks berücksichtigt werden.

Zones und Conduits als Basis für sichere industrielle Netzwerke

Beim Entwurf von Netzwerken können verschiedene Architekturmuster für die Ausgestaltung des Netzes zugrunde gelegt werden. Die Wahl dieser Muster hat einen starken Einfluss auf die Sicherheit des Netzwerks und bestimmt den Unterschied zwischen einem leicht anzugreifenden Netzwerk und einem widerstandsfähigen Netzwerk. Da die Architektur und die Topologie die Grundpfeiler eines sicheren Netzwerks sind, wurden industrielle Sicherheitsstandards - wie die Normenfamilie der ISO/IEC 62443-Richtlinien [1] - für den Entwurf von Netzwerken definiert, um Anlagenbetreibern und Systemintegratoren einen Weg hin zu effektiveren Netzwerkstrukturen aufzuzeigen.
Eine der wichtigsten Leitlinien für den Entwurf von Netzwerken ist das Prinzip der „Zones and Conduits“ (Zonen und Leitungen). Es sieht vor, dass ein industrielles Netzwerk in verschiedene funktionale Zonen segmentiert wird und die Verbindungen zwischen diesen, also die Leitungen, nur zulässigen Datenverkehr von einer Zone in eine andere Zone weiterleiten. Beispielsweise könnte eine Maschine oder ein Teil einer Maschine eine Zone sein, in der unterschiedliche Geräte ungehindert kommunizieren müssen und können. Dagegen müssen nur wenige Geräte mit Geräten in anderen Zonen kommunizieren. Ein Beispiel hierfür wäre ein Protokollserver, der Ereignisprotokolle aller Systeme im Netzwerk sammelt. Dieser sollte auch über die Zonengrenzen hinweg aus verschiedenen Zonen heraus erreichbar sein. An den Zonenübergängen sollte außerdem genau geregelt werden,

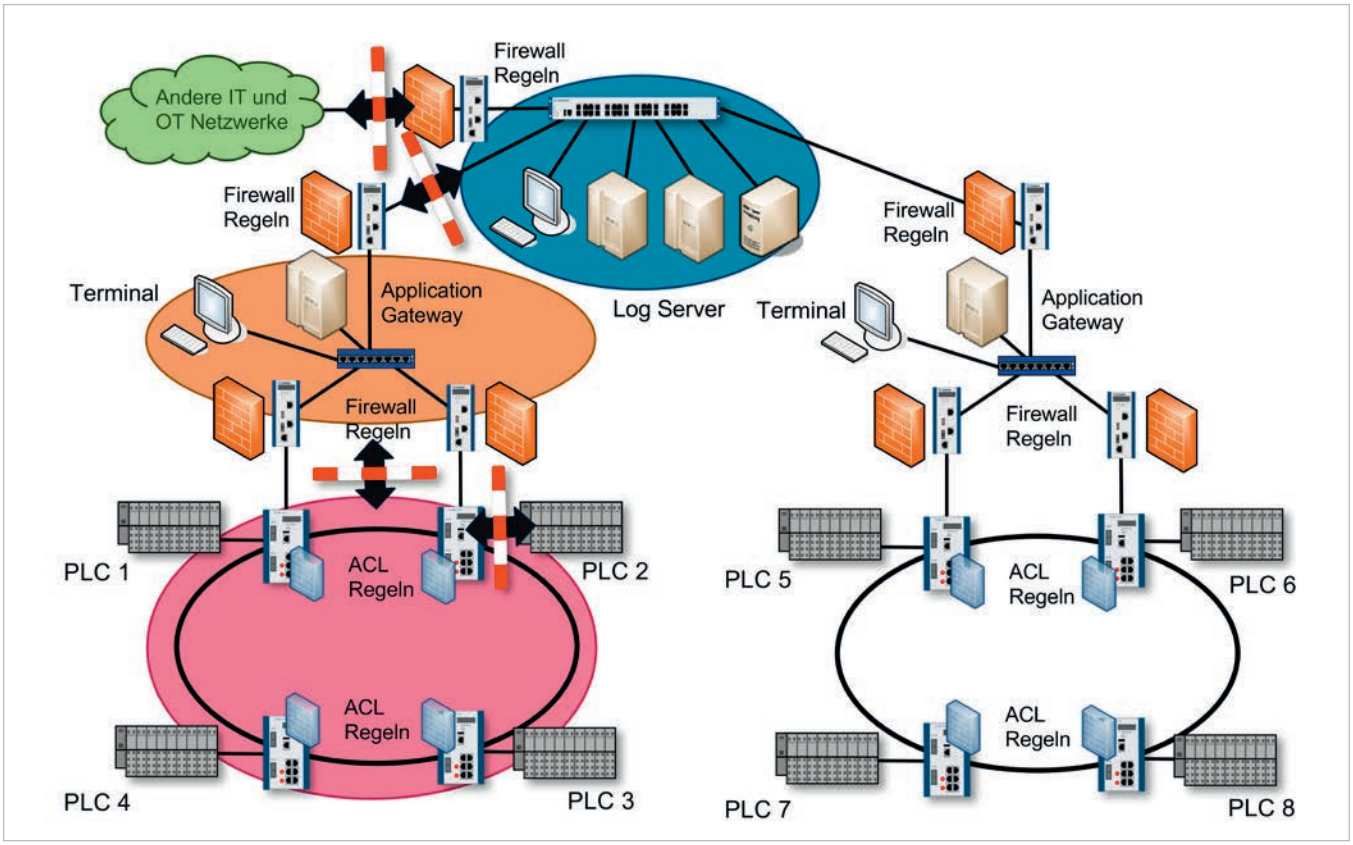

Abbildung 1: Unterschiedliche Zonen in einer industriellen Anwendung

EMEA +49 (0) 7127/14-1809 | beldensolutions.com ■ US 1-855-400-9071 | belden.com

welcher Verkehr die Zone verlassen darf (z. B. Verkehr an den Protokollserver) und welcher Verkehr nicht über Zonengrenzen weitergeleitet werden soll (z. B. der gesamte Verkehr, der nicht an den Protokollserver gerichtet ist).

Bei der Umsetzung von Zonen und Leitungen sind mehrere Dinge zu beachten. Zum einen müssen technische Maßnahmen für die Reglementierung des Zonenübergangs geschaffen werden. In den meisten Fällen sind hierfür Firewalls und Access Control Lists (ACLs) das geeignete Mittel. Abbildung 1 zeigt eine einfache industrielle Anwendung, die in verschiedene Funktionszonen unterteilt ist. Die Abbildung verdeutlicht, wie Firewalls mit restriktiven Regelsätzen den Verkehr zwischen den Zonen beschränken. Innerhalb einer Zone können Ethernet-Switches mit ACLs außerdem den Verkehr von und zu Geräten begrenzen.

Zusätzlich zur Aufteilung in Zonen muss der Zugang zu den einzelnen Zonen geschützt werden. Hierfür eignen sich Techniken wie IEEE 802.1X in Kombination mit einem Authentifizierungsprotokoll wie etwa RADIUS [3]. Schließlich muss auch innerhalb der Zonen dafür gesorgt werden, dass Angreifer den Netzwerkbetrieb nicht stören oder manipulieren können (z. B. durch Spoofing-Angriffe). Auf diese drei Bereiche wird in den folgenden Abschnitten eingegangen.

Unterteilung eines Netzwerks in Zonen und Leitungen durch Firewalls und Access Control-Listen

Die Segmentierung eines Netzwerks lässt sich mit Access Control-Listen auf verschiedenen Schichten des ISO/OSI-Schichtenmodells realisieren, und zwar auf Switches, über Firewalls oder über Application-Layer Gateways (ALGs). Da ACLs eine ähnliche Funktion wie zustandslose Firewalls haben und ALGs für spezielle Anwendungen angepasst sein müssen, wird im Folgenden vor allem auf die flexibel einsetzbaren Firewalls eingegangen. Firewalls und ACLs blockieren unerlaubten Verkehr anhand dessen Verbindungsmetadaten (z. B. MAC-Adressen, IP-Adressen, Port-Nummern und Protokoll-Flags).

Wenn nach dem Whitelisting-Prinzip (nur bekannter Datenverkehr ist erlaubt, jeder andere Verkehr wird blockiert) vorgegangen wird, so enthalten die Regelsätze einer Firewall nur die Merkmale von bekanntem und erwünschtem Verkehr. So kann im oben beschriebenen Beispiel jeder Verkehr über die Zonengrenzen hinweg pauschal verworfen werden, wenn er nicht an den Log-Server gerichtet ist. Eine Kommunikation mit anderen Geräten außerhalb der Zone ist daher nicht über die Zonengrenze (die Leitungen) möglich. Das Whitelisting trägt dazu bei, dass etwaige Angreifer ihren Einflusspielraum nur sehr begrenzt über eine Zonengrenze ausweiten können, da es für sie schwierig oder unmöglich ist, mit potentiellen Zielen über die Leitungen hinweg zu kommunizieren.

Um eine möglichst restriktive Konfiguration einer Firewall zu erlauben, muss bereits beim Entwurf der Netzwerkstruktur darauf geachtet werden, dass das Netzwerk in sinnvolle Zonen aufgeteilt wird. Die Zonen sollten möglichst klein sein, aber gleichzeitig sollte möglichst wenig Kommunikation über die Zonengrenzen stattfinden. Für die Aufteilung eines Netzwerks gibt es in der IT-Welt verschiedene - besser oder schlechter geeignete - Entwurfsmuster (Pattern und Anti-Pattern), die die Sicherheit eines Systems stärken bzw. schwächen können.

Pattern und Anti-Pattern in Netzwerken mit Firewalls

Firewalls können an verschiedenen Punkten eines Netzwerks platziert werden. Die Platzierung bestimmt häufig, ob ein mittels Firewall geschütztes System eine Bedrohung der Anlagen eines Standorts effektiv abschirmen kann. Das bereits erwähnte Whitelisting-Prinzip ist ein gutes Pattern, um danach Firewall-Regelsätze zu erstellen.

Das entsprechende Gegenmodell ist Blacklisting, das jeden unbekannten Datenverkehr erlaubt und nur den Verkehr blockiert, der als unsicher bekannt ist. Neben solchen Modellen für die Erstellung von Firewall-Regeln gibt es auch allgemeine Modelle für die Auslegung der Topologie, also der Struktur eines Netzwerks. Die beiden wichtigsten Anti-Pattern, die berücksichtigt werden müssen, sind das „Flat Network“und das „Screened Host“-Anti-Pattern. Ein deutlich effektiveres Modell ist das „Screened Subnet“-Firewall-Pattern.

Das erste Anti-Pattern für die Auslegung einer Netzwerktopologie ist das „Flat Network“-Entwurfsmuster. Eine solche Topologie entsteht, wenn beim Netzwerkdesign Sicherheitsaspekte nicht berücksichtigt werden. Ein Netzwerk mit flacher Topologie verbindet alle Geräte unabhängig von deren Funktion und Gefährdungspotenzial. Es schafft also eine einzige große Zone, die alle Geräte enthält. Der offensichtliche „Vorteil“ dieses Musters besteht darin, dass diese Struktur für alle Netzwerke funktional geeignet ist, da es bei den Verbindungen zwischen beliebigen Geräten keine Einschränkungen gibt.

Der Nachteil dieses Musters ist ein vollständiger Verlust der Kontrolle über die mögliche Kommunikation im Netzwerk. Da jedes Gerät im Netzwerk mit jedem anderen Gerät im Netzwerk kommunizieren kann, muss ein Angreifer lediglich irgendein Gerät eines „Flat Networks“ kompromittieren, um eine Verbindung zu allen Geräten herstellen zu können. Daher ist es unmöglich, Soft Targets (also potentiell verwundbare Geräte) oder unternehmenskritische Geräte besonders zu schützen. Trotz der Tatsache, dass dieses Muster offensichtlich ungeeignet ist, um einen Angreifer am Zugriff auf weitere Teile des Netzwerks zu hindern (und so das gesamte Netzwerk zu durchdringen), ist es in vielen Industrieanlagen leider noch immer weit verbreitet. Eine zu einfach gedachte Umsetzung von Zonen und Leitungen zur Absicherung des „Flat Network“-Anti-Pattern führt oft zu dem zweiten gefährlichen Entwurfsmuster: dem „Screened Host“-Anti-Pattern.

Wenn eine Firewall eingesetzt wird, um ein Netzwerk in mehrere Zonen zu unterteilen, muss weiterhin die Möglichkeit bestehen, dass eine bestimmte Kommunikation zwischen den Zonen durch die Firewalls fließen kann.

Dies liegt häufig an Diensten, die Geräte (Hosts) anderen Hosts in anderen Zonen anbieten. Ein Beispiel dafür könnte der oben erwähnte Protokollserver sein.

Angenommen, die Aufgabe dieses Servers besteht darin, die Protokolldaten aller Geräte einer Anlage zu konsolidieren, um ein vollständiges Bild über sämtliche Ereignisse in der Anlage zu liefern. Abbildung 2 zeigt dieses Szenario. Der Protokollserver (Host A) muss von außerhalb seiner Zone (Zone X) erreichbar sein. Um dies zu ermöglichen, kann der Netzwerkadministrator sozusagen ein Loch in die Firewall schlagen (eine erlaubende Regel einfügen), damit Geräte von außerhalb der Zone X nun den Server (Host A) erreichen können.

Vielleicht gibt es daneben einen weiteren Dienst B, der auch von außerhalb der Zone X zugänglich sein muss. Um diesen Dienst zur Verfügung zu stellen, wird ein weiteres Loch in die Firewall geschlagen, indem die Kommunikationsprotokolle und Kommunikationsendpunkte für diesen weiteren Dienst in der Firewall freigegeben werden.

In der Theorie ermöglicht die Firewall dann einen Zugriff auf A und B aus anderen Zonen und schützt gleichzeitig die weiteren Geräte (das Terminal und die Steuerung in Zone X) vor Angreifern. In der Praxis könnte ein Angreifer jedoch eine Software-Schwachstelle in den Diensten A und B ausnutzen, um den Protokollserver A oder den Host B zu übernehmen. In diesem Fall hat der Angreifer nun ein Standbein in Zone X und kann ungehindert über Host A auf die Dienste des Terminals oder die Steuerung zugreifen, um Schaden anzurichten.

Die Problematik beim „Screened Host"-Architekturmodell besteht darin, dass Zone X sowohl erreichbare und gefährdete Dienste (A und B) als auch weitere Dienste, deren Erreichbarkeit nicht gegeben sein sollte, enthält.
Die Lösung dieses Problems besteht darin, die gefährdeten Dienste A und B durch die Umsetzung des „Screened Subnet"-Architekturmodells von den anderen Geräten in Zone X zu trennen.

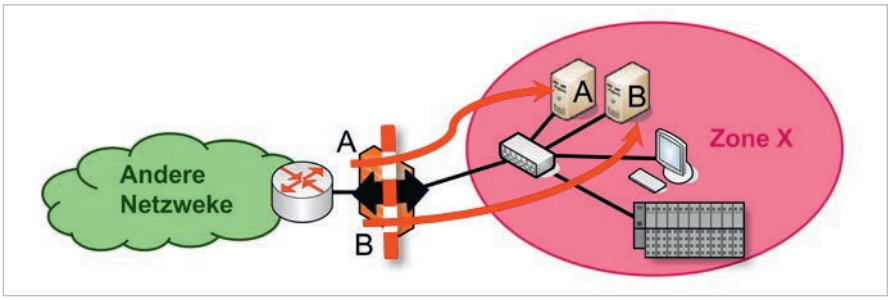

Abbildung 2: „Screened Host"-Gegenmodell

Eine gute Praxis in der IT-Sicherheit besteht darin, gefährdete Dienste in separate Zonen zu isolieren. Diese Zonen werden in der Regel als Demilitarized Zone (DMZ) bezeichnet und enthalten Dienste wie Web-Server, DNS-Server und E-Mail-Server. Typischerweise befinden sich diese Zonen am Rande des Unternehmensnetzwerks, also am Übergang in das Internet. Dieses Modell wird als „Screened Subnet"-Architekturmodell bezeichnet.

Abbildung 3 zeigt dieses Modell. Die Dienste A und B sind in der Zone Y isoliert, aber noch aus der Zone X und aus anderen Zonen der Anlage erreichbar. Allerdings ist die Kommunikation von den Diensten A und B zu den Geräten in der Zone X untersagt. Selbst wenn ein Angreifer die gefährdeten Dienste in der DMZ beeinträchtigen kann, sind die speicherprogrammierbare Steuerung (SPS) und das Terminal in der Zone X immer noch durch eine Firewall geschützt.

Die Umsetzung des „Screened Subnet"-Pattern erfordert eine Firewall, die mehrere Ports für mehrere Zonen unterstützt, oder zwei unterschiedliche Firewalls zwischen der DMZ und dem übrigen Netzwerk, wie in Abbildung 3 gezeigt. Die verbesserte Sicherheit rechtfertigt den zusätzlichen Aufwand jedoch in fast allen Fällen.

Kontrolle des Zugriffs auf eine Zone

Ein weiterer Faktor für die Effektivität eines Sicherheitskonzepts mit Zonen und Leitungen ist die Sicherung des Zugangs zu den Zonen. Die restriktivste Firewall an der Grenze eines kritischen Netzwerkteils ist nutzlos, wenn ein Angreifer sich direkt mit dem kritischen Netzwerkteil verbinden kann. Um den Zugriff auf eine Zone auf die dafür berechtigten Geräte zu begrenzen, bieten sich sowohl physische als auch protokolltechnische Schutzmechanismen an.

Die Grundlage eines Schutzes des Netzwerks sollte immer der physische Schutz des Netzwerk Equipments sein. Netzwerkgeräte wie Switches, Firewalls, WLAN Access Points etc. sollten für den Benutzer unerreichbar in abgeschlossenen Cabinets bzw. Schaltschränken untergebracht werden, damit kein unbefugter Akteur Kabel ein-, aus- oder umstecken kann, um so Zugriff auf das Netzwerk zu erlangen oder anderen Geräten den Zugriff zu verwehren.

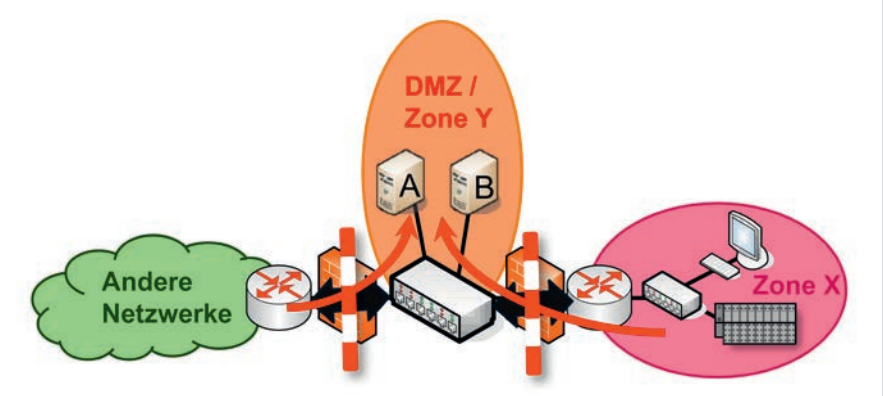

Abbildung 3: „Screened Subnet"-Architekturmodell

EMEA +49 (0) 7127/14-1809 | beldensolutions.com ■ US 1-855-400-9071 | belden.com

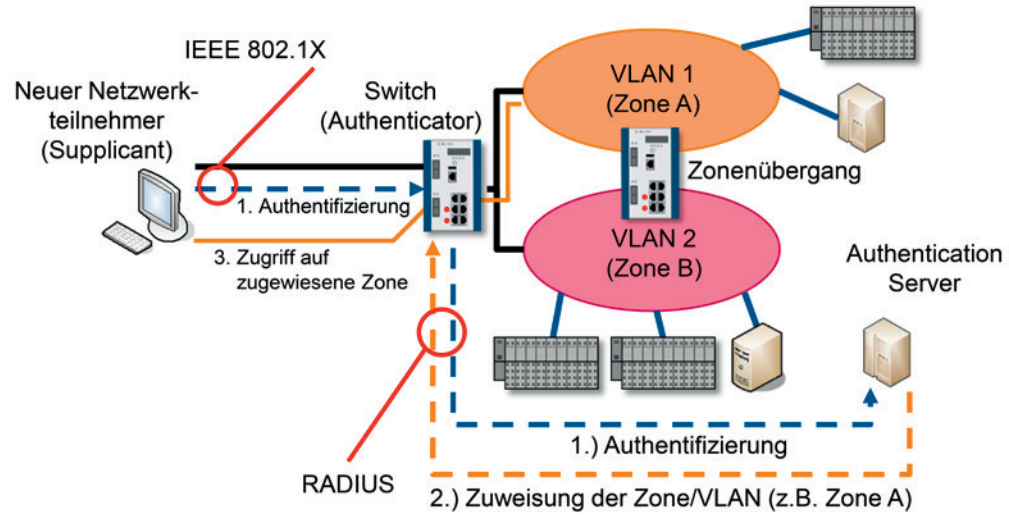

Abbildung 4: Authentifizierung eines neuen Netzwerkteilnehmers über IEEE 802.1X mit anschließender Zuweisung zu einer Zone.

Ebenso ist ein physischer Schutz nötig, um einen grundlegenden Schutz der Verfügbarkeit der Netzwerkkommunikation im Allgemeinen sicherzustellen. Sollte ein Angreifer ein Gerät stromlos machen, seine Konfiguration zurücksetzen oder anderweitig negativ auf das Gerät einwirken können, kann das Netzwerk stark gestört werden. Es mag zwar banal klingen, aber eine physische Trennung von Angreifer und Gerät bewahrt ein Netzwerk vor vielen Angreifertypen und Angriffen. Ebenso kann durch nicht frei zugängliche Netzwerkgeräte die Gefahr von versehentlichen oder fahrlässigen Beeinflussungen des Netzwerks deutlich gesenkt werden.

Nicht in allen Fällen kann ein physischer Schutz der Netzwerkgeräte realisiert werden oder ausreichend Sicherheit bieten. Beispiele dafür sind Geräte, die aus Platzgründen offen oder gemeinsam mit anderen Geräten, die zugänglich sein müssen, in Schaltschränken, die geöffnet werden können, untergebracht sind. Ebenso lässt sich der Zugriff auf Funksysteme nur äußerst schwierig und unzuverlässig durch physische Maßnahmen reglementieren – schließlich strahlen die Mikrowellen der WLAN Systeme, teilweise durchaus gewollt, auch durch Wände und Decken. Es sind daher protokolltechnische Verfahren zur Identifizierung und Authentifizierung der teilnehmenden Netzwerkgeräte notwendig, um den Zugriff auf das Netzwerk zu reglementieren. Einfache Verfahren, beispielsweise die Beschränkung der Netzwerkkommunikation auf einzelne Geräteidentifikatoren wie MAC-Adressen oder IP-Adressen, sind für Angreifer relativ leicht zu umgehen. Daher sollte bei der Beschränkung des Netzwerkzugriffs ein Schutz durch gute Passwörter bzw. Public-Key-Authentifizierungsmechanismen verwendet werden.

Sowohl im drahtlosen (IEEE 802.11 WLAN) als auch im drahtgebundenen Fall (IEEE 802.3 Ethernet) hat sich der Standard IEEE 802.1X [2] im Zusammenspiel mit einem Authentifizierungsserver (z. B. RADIUS) durchgesetzt. Jeder Netzwerkteilnehmer (z. B. eine Komponente oder Maschine) besitzt dabei eindeutige und einmalige Zugangsdaten (z. B. Benutzername und Passwort oder ein digitales Zertifikat), mit denen er sich gegenüber dem Switch oder WLAN Access Point, mit dem er verbunden ist, ausweisen kann.

Meldet sich ein neuer Teilnehmer am Netzwerk an, so gibt der Switch oder der WLAN Access Point die Anmeldenachrichten an einen Authentifizierungsserver weiter. Dieser vergleicht die Zugangsdaten mit seiner Benutzerdatenbank und instruiert den Switch daraufhin, die Verbindung des neuen Netzwerkteilnehmers entweder zuzulassen oder abzulehnen.

Abbildung 4 zeigt eine solche Anmeldung eines neuen Geräts. Die Verwendung von IEEE 802.1X im Zusammenspiel mit einem Authentifizierungsserver bietet aus Sicht der Sicherheit zwei entscheidende Vorteile:

- Jedem Gerät können unterschiedliche Zugangsdaten zugewiesen werden. Damit kann ein Zugriff auf das Netzwerk pro Gerät gesteuert werden, da die Geräte anhand ihrer Zugangsdaten voneinander unterscheidbar sind. Darüber hinaus muss beim Diebstahl oder Verlust eines Gerätes nur dieses eine Gerät aus dem Netzwerk entfernt werden. Dazu genügt eine einfach druchführbare zentrale Sperrung des Geräts am Authentifizierungsserver. Eine Neukonfiguration von anderen Geräten im Netzwerk (z. B. der Firewalls oder anderer WLAN Clients mit demselben WLAN-Schlüssel) ist nicht mehr nötig, da die Zugangsdaten nur speziell für dieses Gerät gesperrt wurden.
- Zusätzlich zur Zugriffssteuerung auf das Netzwerk kann das Gerät einer Zone in Form eines Virtual LAN (VLAN) zugewiesen werden. Nur Geräte im selben VLAN sind in der Lage miteinander zu kommunizieren. Die Übergänge zwischen den mit VLANs dynamisch zuweisbaren Zonen können dann wieder durch Firewalls realisiert werden.

Durch diese Vorteile kann eine Zugriffssteuerung für Netzwerkgeräte durch IEEE 802.1X, eine effiziente Aufteilung eines Netzwerks in Zonen sowie eine passgenaue Zuordnung von Geräten zu den Zonen erreicht werden. Durch die zentrale Konfigurierbarkeit der Gerätezugehörigkeit am Authentifizierungsserver bleibt der Aufwand bei Anpassungen und Sperrungen von Geräten zudem überschaubar.

Weiterer Schutz innerhalb einer Zone

Neben dem Schutz der Zonenübergänge und dem Schutz des Zugriffs auf einzelne Zonen ist es notwendig, dass Geräte sich innerhalb der Zone nicht als andere Geräte ausgeben können. Dieses Annehmen einer falschen Identität im Netzwerk wird als „Spoofing" bezeichnet. Dies ist vor allem dann von großer Bedeutung, wenn ein Angreifer Zugriff auf ein Gerät hat, das sich bereits in einer Zone befindet, und er sich durch das Vortäuschen falscher Identitäten Zugriff auf weitere Geräte oder Zonen verschaffen oder die Kommunikation innerhalb der Zone stören möchte. Spoofing kann im Netzwerk auf verschiedenen Ebenen mit verschiedenen Identitäten und mit sehr unterschiedlichen Auswirkungen erfolgen. Beim ARP Spoofing gibt ein Gerät vor, dass eine fremde IP-Adresse unter der eigenen MAC-Adresse im Ethernet-Netzwerk verfügbar wäre. Beim DHCP und DNS Spoofing antwortet ein Angreifer auf Anfragen eines Geräts mit gefälschten Informationen.

Diese Angriffe können dazu führen, dass Datenverkehr zum Angreifer umgeleitet wird und der Angreifer so Einfluss auf die Kommunikation anderer Geräte nehmen kann. In ihrer Initialkonfiguration sind Ethernet-Netzwerke diesen Angriffen weitgehend schutzlos ausgeliefert. Jedoch stehen mit Techniken wie „Port Security" und „Dynamic ARP Inspection" sowie „IP Source Guard" und „DHCP Snooping" effektive Sicherheitsmechanismen zur Verfügung, um Spoofing-Angriffe zu unterbinden. Diese Methoden sind auch in hochwertigen Industrie-Switches verfügbar und eignen sich dazu, die Möglichkeiten eines Angreifers im lokalen Netzwerk stark einzugrenzen. Wichtig ist jedoch, dass diese Techniken eine auf das Netzwerk abgestimmte Konfiguration benötigten und daher im Auslieferungszustand aller Switches nicht aktiviert sind. Ein zusätzlicher Schutz kann also nur nach einer Aktivierung erreicht werden.

Zusammenfassung und Schlussfolgerungen

Die Berücksichtigung der Sicherheit in der Anfangsphase eines Netzwerkdesigns ist ein wichtiger Schritt zu einem sichereren industriellen Steuerungssystem. Jedoch müssen auch bei der Umsetzung von Best Practices, etwa durch den Einsatz von Firewalls und des Zonen- und Leitungen-Konzepts, Aspekte wie gefährdete Dienste grundsätzlich mit einbezogen werden. Die Vermeidung der Architekturmuster des „Flat Network" und des „Screened Host"-Musters zugunsten der „Screened Subnet"-Architektur begrenzt die Bewegungsfreiheit eines Angreifers innerhalb des Netzwerks und schützt kritische oder anfällige Geräte besser vor gefährdeten Diensten. Bei der Begrenzung des Zugangs von Geräten zum Netzwerk und der Zuordnung der Geräte zu den einzelnen Zonen steht mit IEEE 802.1X eine effektive Technik zur Verfügung, die sowohl die Sicherheit erhöht und den Administrationsaufwand verringert. Schließlich gibt es weitere Methoden, um die Möglichkeiten eines Angreifers innerhalb einer Zone stark zu beschränken. Durch Anwendung dieser Methoden und Architekturen lassen sich sichere und robuste Netzwerke schaffen. Somit kann das Netzwerk nicht mehr als gefährliche Waffe eines Angreifers genutzt werden, sondern wird ein ernstzunehmendes Hindernis für Angriffe in industriellen Umgebungen.

Referenzen

[1] IEC 62443, Security for Industrial Automation and Control Systems (IACS)

[2] IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control

[3] IETF RFC2865 Remote Authentication Dial In User Service (RADIUS)

Über Belden

Belden Inc., ein weltweit führender Anbieter von hochwertigen Signalübertragungslösungen, bietet ein umfassendes Produktportfolio, das auf die Anforderungen unternehmenskritischer Netzwerkinfrastrukturen in den Branchen Industrie- und Gebäudeautomation sowie Broadcast zugeschnitten ist. Mit innovativen Lösungen für die zuverlässige und sichere Übertragung stetig wachsender Datenmengen für Audio- und Videoinformationen, die für moderne Anwendungen benötigt werden, übernimmt Belden eine Schlüsselrolle bei der globalen Veränderung hin zu einer vernetzten Welt. Das Unternehmen mit Hauptsitz in St. Louis, USA, wurde 1902 gegründet und betreibt Fertigungsstätten in Nord- und Südamerika, Europa und Asien.

Für weitere Informationen besuchen Sie uns unter www.belden.com und folgen Sie uns auf Twitter @BeldenIND.