

Netzsegmentierungen in Prozessleitnetzen

Thomas Gronenwald und Florian Thiessenhusen, Security Consultants bei der Admeritia GmbH

Netzwerksegmentierungen verhindern den ungefilterten Zugriff auf ein SCADA-System, wenn sich Corporate-LAN und Prozessleitnetz nicht strikt voneinander trennen lassen.

Firewalls teilen das Netzwerk auf und filtern den Verkehr zwischen den einzelnen Segmenten.

Automatisierungs- und Prozesssteuerungssysteme werden weltweit in nahezu allen Industrieunternehmen eingesetzt. Der Trend und die Entwicklung gehen dabei weg von proprietären und isolierten Feldbussystemen hin zu standardisierten und gekoppelten Netzwerken.

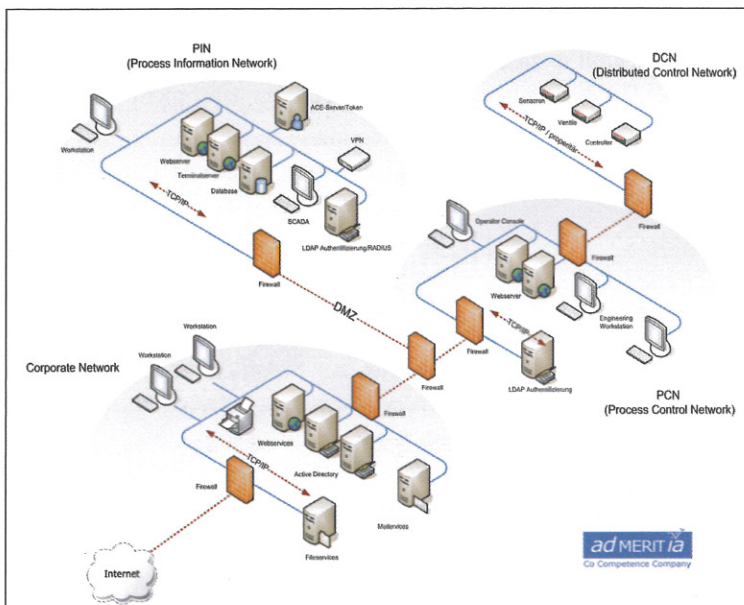
Doch welche Sicherheitsrisiken bergen solche Entwicklungen in der Automatisierungs- und Prozesssteuerungstechnik innerhalb von kritischen Infrastrukturen und wie können Unternehmen diesen entgegenwirken?

In der jüngeren Vergangenheit tauchten viele Schwachstellen in den Anlagen führender Industrieunternehmen auf. Dadurch rückt das Thema Sicherheit verstärkt in den Fokus von Verantwortlichen, Betreibern und Sicherheitsexperten. Einer der bedeutendsten Vorfälle war sicherlich der Stuxnet-Virus. Dieser Schadcode wurde von einer mutmaßlich kriminellen Vereinigung entwickelt, um Steuerungssysteme der Firma Siemens gezielt anzugreifen.

Im gegebenen Fall richtete sich der Schadcode gegen spezielle Frequenzrichter, die in verschiedenen Kraftwerken vorkommen. Das Ziel des Angriffs waren die Manipulation und somit die Zerstörung der Geräte. Einerseits basierte der Schadcode auf einer Schwachstelle innerhalb des Steuerungssystems, andererseits musste er sich bis an die entscheidenden Stellen weiterverbreiten. Dies kann nur dann funktionieren, wenn der Schadcode durch unsichere IT-Anlagen eingeschleust und durch fehlende Netzwerksegmentierungen weiterverbreitet werden kann. Beides ist selbst bei führenden Energieerzeugern noch heute möglich.

Die Anforderung der Bereitstellung von gesammelten Prozessdaten zu Abrechnungs- oder Überwachungszwecken bedingt eine Kopplung zum Corporate-LAN (Büronetz) und macht eine bestehende Netzwerkverbindung zu potenziell gefährlichen Netzen (Corporate, Internet) unausweichlich. Das BSI empfiehlt in seinen Maßnahmenkatalogen in solchen Fällen die strikte Trennung der Netze zumindest durch eine Firewall (Paketfilter). Jedoch ist dies in der Praxis vergleichsweise selten zu finden. Netztrennungen sind nicht vorgesehen oder gar mangelhaft implementiert. Ein direkter ungefilterter Zugriff vom Corporate-LAN zum SCADA-System ist so zumeist möglich.

Die wichtigste Maßnahme bei der Absicherung von Prozessleitnetzen ist somit die Absicherung der Basis, also des Netzwerks. Unter Zuhilfenahme von Firewalls wird dieses in Netzsegmente aufgeteilt. Die Firewall filtert den Verkehr zwischen diesen Segmenten.



Netzsegmentierung zwischen Corporate-LAN und Produktionsnetz

Dieser Netzplan zeigt eine Segmentierung der einzelnen aufgebauten Netzwerkstrukturen zwischen Corporate-LAN und Produktionsnetz. Ein so genanntes Zonenmodell kommt zum Einsatz, bei dem Systeme und Systemgruppen klassifiziert und anschließend segmentiert werden.

Der Netzübergang zum Corporate-LAN wird durch drei Firewalls abgesichert. Eine Firewall davon stellt eine DMZ (Demilitarized Zone) zur Verfügung. Diese dient als Transfernetz von Daten, die zwischen Produktionsnetz und Corporate-LAN ausgetauscht werden müssen (Messdaten u.a.). Ein direkter Zugriff aus dem Corporate-LAN ins DCN ist nicht möglich.

Zudem ist das DCN durch zwei Firewalls vom PCN getrennt. Die Besonderheit dabei ist, dass bei den Aktoren häufig proprietäre Protokolle zum Einsatz kommen. Das muss bei der Beschaffung und Implementierung der Firewall berücksichtigt werden.

In der Praxis sind solche Projekte nicht so einfach umzusetzen wie in vergleichbaren Büronetzwerken. Die Projekte sind wesentlich komplexer, dauern länger und bedingen eine größere Vorbereitung.