Segmentierung umsetzen mit Mini-Firewalls

Netzwerkinseln in der Werks-IT

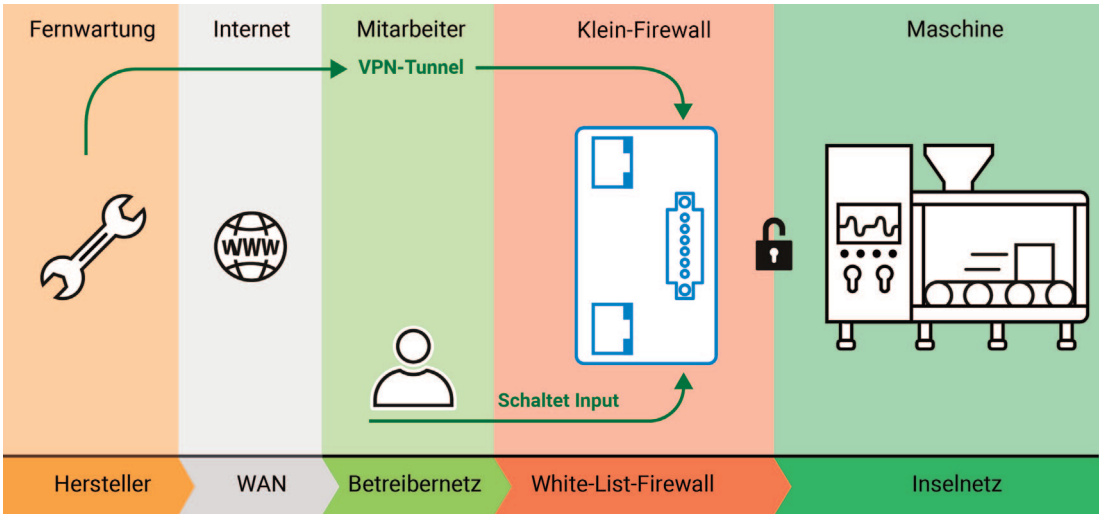

Bild: Wiesemann & Theis GmbH

Gerade in KMU fehlen oft grundlegende Konzepte für die IT-Sicherheit. Sorgen vor gestörten Produktionsabläufen und auch das 810-seitige IT-Grundschutz-Kompendium des BSI schrecken vom Einstieg ins Thema eher ab. Hier setzen Lösungen auf der Basis von Klein-Firewalls an. Sie sollen es jeder Firma ermöglichen, Netzwerkbereiche einfach und gezielt abzusichern.

Hardware-Produkte und -Lösungen für die Fabrik bringen heute fast ausnahmslos Netzwerkkonnektivität mit. Dazu zählen viele Sensoren und Aktoren, Anlagen und Maschinen ohnehin, Web-IOs, IPCs und diverse Gadgets. Die vermehrte Anbindung von Maschinen an Netzwerke erfordert schon zwecks Selbstschutz, gut dokumentierte Sicherheitskonzepte umzusetzen. Mit extra darauf abgestellten Klein-Firewalls etwa lässt sich die Sicherheit von werksnahen Netzwerken und den Systemen darin recht einfach auf ein vernüftiges Niveau heben. Dazu werden zusätzliche Firewallrouter innerhalb eines großen Netzwerks eingebunden, um mehrere isolierte Segmente zu bilden – die Netzwerkinseln. Die Router fungieren dabei als weitere Prüfstellen, die die Kommunikation zwischen den Subnetzen überwachen, steuern und protokollieren. Dabei werden notwendige Verbindungen zwischen Systemen auf der Netzwerkinsel und dem umgebenden Netzwerk im Vorfeld erfasst, auf ein Mindestmaß beschränkt und gezielt freigeschaltet. Angreifer und Schadsoftware, die über eine Maschine in ein Subnetzwerk eindringen, können so an einer Ausbreitung im übergeordneten Produktionsnetzwerk gehindert werden. Diese Maßnahmen können einfach dokumentiert und Berechtigten offengelegt werden.

Praxisbeispiel Sondermaschine

Am Beispiel einer Sondermaschine lässt sich das Prinzip des Ansatzes erklären: Diese soll gegenüber dem umliegenden Netzwerk abgesichert werden. Der Aufbau der Maschine besteht intern aus einem eigenen kleinen Netzwerk mit Sensoren, Aktoren und Steuerungen. Der Großteil der Kommunikation findet rein maschinenintern statt und erfordert keine Verbindung in ein übergeordnetes Netz. Es werden lediglich drei Verbindungen von und nach außen benötigt:

- Ein maschineninterner Industrie-PC muss aus dem umgebenden Netzwerk von zwei Teilnehmern per Browser und https erreichbar sein (Scada).

IT&Production

Auszug aus IT&Production, Sonderheft Wissen Kompakt 2021

- Die Maschine schreibt Betriebsdaten auf einen im umgebenden Netzwerk befindlichen Datenbankserver.
- Der Hersteller der Maschine benötigt zu Service-Zwecken oder für Firmware- oder Programm-Updates Zugriff auf den internen Industrie-PC. Der Zugriff muss über einen separaten, externen Schalter (etwa ein Schlüsselschalter) durch den Betreiber freigegeben werden.

Das Management der installierten Lösung selbst soll ausschließlich dem Administrator des Betreiber-Netzwerks möglich sein.

Umsetzung mit einer Mini-Firewall

Die Anbindung der Maschine an das Betreiber-Netzwerk erfolgt über einen Mini-Router mit integrierter Whitelist-Firewall. Dieses Gerät hat zwei Aufgaben: den Schutz des Maschinennetzes vor schädlichen Ereignissen im Betreiber-Netzwerk (zum Beispiel Broadcaststürme, angriffsvorbereitende Port-Scans) und den Schutz des umgebenden Netzwerks vor schädlichen Ereignissen und Fehlern im Maschinennetz. Die Netzwerkkomponente reduziert zudem die Kommunikation auf das absolut Notwendige. Eine recht einfach zu erstellende Whitelist-Regel schränkt den Zugriff auf den maschineninternen Industrie-PC ein: Nur die beiden im Intranet befindlichen Scada-Arbeitsplätze und der verwendete TCP-Dienst können zugreifen. Eine zweite Regel erlaubt den Datenbank-Zugriff aus dem Inselnetzwerk heraus in das Intranet. Jeder hier nicht explizit freigegebene Datenverkehr wird unterbunden. Dadurch wird die Angriffsfläche für Attacken deutlich verringert.

Routing-Konzepte bleiben unberührt

Über Static-NAT in der Firewall wird das Maschinennetz darüber hinaus gegenüber dem Intranet verborgen. Aus Sicht der Intranet-Teilnehmer handelt es sich bei den Zugriffen in das Maschinennetzwerk um lokale Verbindungen. Eingriffe in das oft sensible Routing-Konzept des Betreiber-Netzes sind somit nicht erforderlich. Der Fernwartungszugriff des Herstellers wird verschlüsselt und authentifiziert über den VPN-Endpunkt der Klein-Firewall realisiert. Um dem Betreiber zusätzlich eine einfache Zugriffskontrolle zu ermöglichen, wird die Aktivierung des VPN-Endpunktes über einen digitalen Eingang mit einem Schlüsselschalter gesteuert. Auf diese Weise erteilt der zuständige Mitarbeiter des Betreibers dem Hersteller nur dann eine ausdrückliche Freigabe für den Zugriff, wenn er diesen konkret benötigt. ■

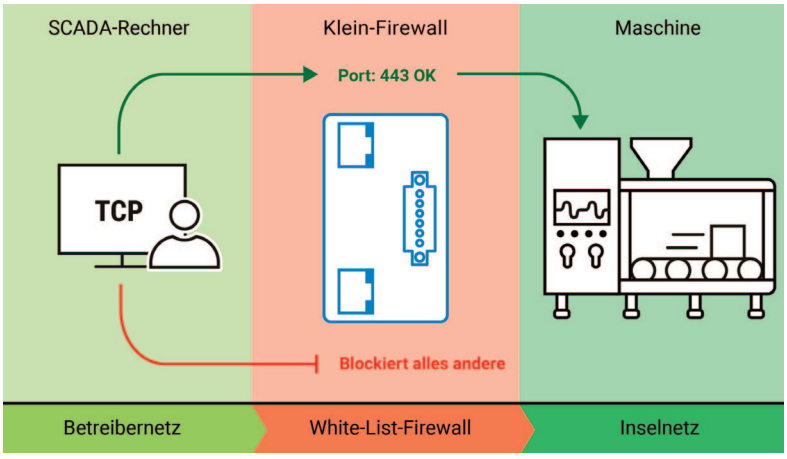

Bild: Wiesemann & Theis GmbH

www.wut.de

Autor

Thomas Clever ist Produktmanager bei der Wiesemann & Theis GmbH.