Umgehen der Schutzeinrichtungen unmöglich

Artikel vom **30. April 2019**
Security

Es gibt wohl kaum einen Maschinenbauer, der keine Fernwartungslösung für seine Maschine anbietet. Doch die Fernwartung wird nicht allein dadurch sicher, dass die relevanten Daten verschlüsselt über das Internet zwischen der im Produktionsnetzwerk des Betreibers installierten Maschine und der Servicezentrale des Maschinenbauers übertragen werden. Hier gilt es weitere Aspekte zu beachten.

Autor:
Frank Merkel
Business Development Manager
Phoenix Contact Deutschland GmbH

Bild: Phoenix Contact

Aufgrund der zunehmenden Vernetzung im Fertigungsbereich sollte zuverlässig sichergestellt werden, dass der Maschinenbauer im Rahmen der Fernwartung lediglich seine Maschine erreichen kann und nicht das gesamte Produktionsnetzwerk. Denn in

Abhängigkeit von der genutzten Lösung ist ein Missbrauch der Fernwartungsverbindung technisch möglich – sei es absichtlich oder nur aus Versehen. Das resultiert daraus, weil sich viele der Sicherheitsbarrieren, mit denen IT-Abteilungen ihre Netzwerke gegen Angriffe aus dem Internet schützen, von einer Fernwartungsverbindung umgehen lassen. Nachfolgend werden verschiedene Lösungen beschrieben, die den Anforderungen der Betreiber hinsichtlich einer umfassenden Absicherung ihrer IT- und Fertigungsinfrastruktur gerecht werden und den Maschinenbauern – bis auf den dritten Ansatz – die Beibehaltung ihrer bestehenden Fernwartungslösung erlauben. Als Ausgangssituation wird angenommen, dass das produzierende Unternehmen (Betreiber) mit zahlreichen Anbietern von Maschinen und Anlagen zusammenarbeitet. Diese nutzen jeweils unterschiedliche Fernwartungslösungen, deren Security-Parameter vom Betreiber nicht einheitlich administriert werden können.

Variante 1: Nachrüstung bestehender Lösungen durch eine Conditional Firewall

Als einfache und flexibel einsetzbare Variante erweist sich hier die Nachrüstung der vorhandenen hard- oder softwarebasierten Fernwartungslösung des Maschinenherstellers mit einer Industrial Firewall (Security Appliance), welche die Funktion einer zustandsbezogenen Firewall, also einer Conditional Firewall umfasst. Die Security Appliance wird zwischen der bestehenden Fernwartungslösung des Anbieters und dem Fertigungsnetzwerk installiert und lässt sich von den IT-Experten des Betreibers zentral administrieren. Die Conditional Firewall der Security Appliance kennt zwei Zustände:

1. Normalbetrieb/Produktion Alle notwendigen Kommunikationsverbindungen zwischen Maschine und Fertigungsnetz sind erlaubt. Der Verbindungsaufbau der Fernwartungslösung des Anbieters wird durch die Firewall blockiert.
2. Fernwartung Die Datenübertragung zwischen Maschine und umgebendem Produktionsnetzwerk ist auf ein Minimum beschränkt und im Extremfall sogar vollständig gekappt. In dem Fall stellt die Maschine/Anlage eine Insel im Fertigungsnetz des Betreibers dar. Der Verbindungsaufbau der Fernwartungslösung des Anbieters, die ihm den Zugriff auf seine Maschine/Anlage ermöglicht, wird gestattet. Die Security Appliance unterbindet einen Zugriff der Fernwartungslösung auf das Produktionsnetzwerk.

Funktionsprinzip einer Conditional Firewall: Aktivierung von Firewall-Regelsätzen mittels Schalter. Bild Phoenix Contact

Der Bediener vor Ort aktiviert den Fernwartungszustand der von Spezialisten konfigurierten Conditional Firewall über einen Hardware-Schalter. Für diese Tätigkeit benötigt er keine speziellen Security-Kenntnisse und muss auch keine Rücksprache mit den IT-Verantwortlichen des Betreibers nehmen. Nach der Beendigung der Fernwartung stellt der Bediener den Normalbetrieb wieder her, indem er den Schalter zurückdreht. Auf diese Weise wird die Fernwartungsverbindung unterbrochen und die Kommunikation zwischen der Maschine/Anlage und dem Fertigungsnetz wieder erlaubt.

Variante 2: Ergänzung der Conditional Firewall um eine VPN-Verbindung

Wenn neben den oben genannten Anforderungen des Betreibers zusätzlich eine zentrale Komponente zur Aktivierung der Fernwartung gefordert wird, lässt sich das durch eine Kombination der Conditional Firewall der Security Appliance mit VPN-

Verbindungen (Virtual Private Network) realisieren.

Zweistufige Aktivierung einer Fernwartungsverbindung durch die Conditional Firewall und VPN. Bild: Phoenix Contact

In diesem Fall wird zwischen der vorhandenen Fernwartungslösung des Maschinenherstellers und dem Produktionsnetzwerk des Betreibers eine Security Appliance mit VPN-Funktion installiert. Das Gerät baut bei Bedarf eine interne VPN-Verbindung zu einem VPN-Gateway auf, das in der DMZ (Demilitarized Zone) des Betreibers montiert ist. Alle Fernwartungslösungen der Maschinenhersteller können sich nur mit dem Internet verbinden, nachdem der interne VPN-Tunnel zwischen Security Appliance und VPN-Gateway in der DMZ aufgebaut wurde. Jetzt ist eine zweistufige Aktivierung der Fernwartung möglich. Nach erfolgreicher Authentisierung kann zum Beispiel der für die Fertigung verantwortliche Mitarbeiter die interne VPN-Verbindung zwischen Security Appliance und dem in der DMZ installierten VPN-Gateway über eine Webanwendung einschalten. Eine Fernwartung lässt sich allerdings noch nicht durchführen, weil die Firewall im VPN-Tunnel die Nutzung der Fernwartungslösung des Maschinenherstellers blockiert. Diese wird erst durch den Bediener vor Ort über den bereits beschriebenen Schalter und die Conditional Firewall freigeschaltet. Es müssen also beide Berechtigungen erfüllt sein, damit die Fernwartung starten kann. Die beiden erläuterten Fernwartungsvarianten setzen so die folgenden Anforderungen um:

- Der Maschinenhersteller kann weiterhin seine eigene Fernwartungslösung einsetzen,
- die IT- und Security-Spezialisten des Betreibers können die Verbindungen zentral administrieren,
- die Aktivierung und Deaktivierung der Fernwartung erfolgt durch die Verantwortlichen/Mitarbeiter in der Produktion ohne nochmalige Rücksprache mit ihrer IT-Abteilung
    - entweder vor Ort mittels Schalter oder
    - vor Ort mittels Schalter in Kombination mit einer vorherigen Freigabe über eine Webanwendung.

Variante 3: Implementierung eines Fernwartungsportals beim Betreiber

Akzeptiert der Betreiber die unterschiedlichen Lösungen der Maschinenhersteller nicht, kann er diesen ein Fernwartungskonzept vorschreiben. Teilweise setzen die IT-Abteilungen der Betreiber dabei auf Ansätze, die sie aus der Office-IT kennen. Mit diesen Ansätzen ist aber keine einfache Aktivierung der Fernwartungsverbindung durch den Bediener möglich. Der Betrieb eines Fernwartungsportals in der DMZ des Betreibers erweist sich hier als praktikable Lösung.

Kontrolle von Fernwartungsverbindungen durch das Portal inklusive Session Recording und Inspektion der Anwendungsdaten. Bild: Phoenix Contact

Das Fernwartungsportal besteht aus einem Webserver für das Verbindungsmanagement sowie zwei VPN-Gateways, die jeweils die VPN-Verbindungen des Servicetechnikers des entsprechenden Zulieferers sowie der jeweiligen Maschinen als Serviceziel entgegennehmen. Zwischen den beiden VPN-Knoten liegen die Daten unverschlüsselt vor und können aufgezeichnet, gefiltert oder überwacht werden. Jede Maschine wird über eine Security Appliance inklusive VPN-Option mit dem Fertigungsnetz verbunden. Fordert der Maschinenbediener vor Ort in der Produktion eine Fernwartung an, aktiviert er die VPN-Verbindung von der Maschine

zum in der DMZ befindlichen Maschinen-Gateway über einen Schalter. Zusätzlich zu seiner VPN-Verbindung zum Service-Gateway wählt sich der Techniker über einen Browser in die Webanwendung des Fernwartungsportals ein. Diese zeigt ihm an, welche Maschinen online sind, und er kann sich per Mausklick mit der Maschine verbinden, welche die Fernwartung benötigt. Der Betreiber legt zudem über ein Berechtigungsmodell fest, welcher Techniker respektive Zulieferer welches Serviceziel, also welche Maschinen fernwarten darf. Auf Wunsch kann der Betreiber die drei beschriebenen Fernwartungslösungen auch kombinieren. Auf diese Weise lassen sich die vielfältigen Anforderungen im Hinblick auf eine sichere und trotzdem praktikable Fernwartung erfüllen und darüber hinaus bestehende unsichere Fernwartungslösungen nachrüsten.

Die robusten und industrietauglichen Security-Appliances beinhalten Firewall-, Routing- und VPN-Funktionalitäten. Bild: Phoenix Contact

Produktinfo

Bei den Geräten der Produktfamilie »FL mGuard« von Phoenix Contact handelt es sich um Netzwerkkomponenten, welche die Funktionen des Routers, der Firewall und des VPN-Geräts in sich vereinen. Das Ziel einer maximalen Sicherheit und Anlagenverfügbarkeit wird durch folgende Eigenschaften erreicht:

- sehr hohes Sicherheitsniveau mit IPsec-Protokoll auf dem Layer 3,
- bis zu zehn parallele VPN-Tunnel (optional bis 250),
- hoher VPN-Datendurchsatz von bis zu 70 MBit/s,
- Unterstützung aktueller Zertifikate wie x509.v3,
- Anschluss für VPN-Freigabetaster und VPN-Status-LED,
- Nutzung lediglich der ausgehenden User Datagram Protocol (UDP)-Verbindungen des Betreibernetzes,
- Stateful-Inspection-Firewall zur dynamischen Filterung.

Phoenix Contact GmbH & Co. KG
Infos zum Unternehmen

Direktkontakt

Kontaktformular folgt
Hersteller aus dieser Kategorie

Icon
DigiComm GmbH
Breite Str. 10
D-40670 Meerbusch
02159/69375-0
kkirstein@digicomm.de
www.digicomm.de
Icon
Innominate Security Technologies AG
Rudower Chaussee 13
D-12489 Berlin
030/921028-0
contact@innominate.com

www.innominate.com
Icon
Industrial Computer Source (Deutschland) GmbH
Marie-Curie-Str. 9
D-50259 Pulheim
02234/98211-0
oezcan@ics-d.de
www.ics-d.de