Aus Erfahrung weiß man, selbst große Industriekonzerne sind vor Hackerangriffen nicht gefeit. Und dennoch gibt es hier noch immer Nachholbedarf, weiß André Zivny, Produktmanager Automatisierungstechnik bei Baumüller. Auch bei der Anlagenwartung aus der Ferne geht man teilweise noch recht leichtfertig mit der Sicherheit um. Dabei kann man schon mit einfachen Mitteln viel erreichen.

„Die Verlockung für Manipulation ist hoch“

Es heißt, der Grad der Vernetzung von Industrieanlagen und Infrastruktur wird mehr und mehr zunehmen. Welche Voraussetzungen müssen hierfür geschaffen und welche Vorsichtsmaßnahmen getroffen werden?

André Zivny: Um der stetig steigenden Vernetzung gerecht zu werden, muss eine entsprechende Infrastruktur zur Verfügung stehen. Es sollten standardisierte Schnittstellen und Protokolle verwendet werden, die auf einer breiten Basis aufsetzen und bei denen eine regelmäßige Weiterentwicklung sichergestellt ist. Das heißt also weg von proprietären Systemen. Des Weiteren kann bzw. sollte auch über eine Trennung der Produktivnetze von den „normalen“ Firmennetzen nachgedacht und ausreichend sichere Technik verwendet werden.

Wie ist es denn im Allgemeinen um das Sicherheitsbewusstsein in der Industrie bestellt?

André Zivny: Das Sicherheitsbewusstsein der Industrie hat in den vergangenen Jahren zugenommen. Allerdings muss das Thema Sicherheit in der Industrie weiterhin verstärkt thematisiert werden, denn hier gibt es nach wie vor großen Nachholbedarf. Noch ist nicht jedermann für die Bedrohung und Gefahren sensibilisiert. Angriffe auf Maschinen und Produktionsanlagen werden meiner Meinung nach zunehmen. Die Verlockung ist recht hoch mit relativ einfachen Mitteln, Schaden durch beispielsweise Manipulation und Erpressung zu verursachen.

Und was bedeutet die Weiterentwicklung der Kommunikationstechnologien für das Thema Fernwartung?

André Zivny: Es bedeutet einen größeren Funktionsumfang und mehr Möglichkeiten für das Thema Fernwartung. Bestand die „Fernwartung“ anfangs aus reiner Unterstützung

> *Als technische Lösung sollte über Mindestmaßnahmen nachgedacht werden, um die Fernwartung abzusichern. Dazu gehören beispielsweise eine verschlüsselte Kommunikation unter Einsatz sicherer VPN-Technologien, eine entsprechende Nutzer- und Berechtigungsverwaltung und die damit einhergehende Authentifizierung.*

am Telefon, so gab es recht schnell Modems, mit denen eine Maschine angerufen werden konnte. Mit der heutigen Technologie und Bandbreite können den Nutzern und Anwendern eine Vielzahl an Services zur Verfügung gestellt werden.

Sie sehen den Anwender als größtes Risiko, wenn Maschinen und Anlagen aus der Ferne gewartet werden. Wo sind Ihrer Meinung nach die (menschlichen) Schwachstellen?

André Zivny: Der Mensch an sich ist ein „Gewohnheitstier". Anstatt schwierige, lange Passwörter aus einer Kombination aus Zahlen, Zeichen und Buchstaben zu generieren, nutzt er lieber einfache Standard-Passwörter. Im schlimmsten Fall verzichtet er sogar auf Passwörter oder nutzt Begriffe oder Wörter, die in einem Wörterbuch zu finden sind. Diese Passwörter können leicht gehackt werden und stellen somit ein enormes Sicherheitsrisiko dar. Wichtig wäre auch die Vermittlung der entsprechenden Kenntnisse an die Mitarbeiter, um die Bedrohungen und Gefahren zu erkennen und zu vermeiden. Leider wird teilweise auch hier an Kosten für solche Schulungen oder Unterweisungen gespart, häufig aus Unwissenheit. Ebenfalls wichtig ist eine sichere Konfiguration der Fernwartung mit der dafür richtigen Hardware. Der Einsatz von sicheren Verbindungen mit ausreichend starker Verschlüsselung mag manchem als zu umständlich und schwer konfigurierbar erscheinen, ist aber unabdingbar. Darüber hinaus muss bei Bekanntwerden von kritischen Sicherheitslücken in den jeweiligen Systemen und Protokollen schnellstmöglich reagiert werden.

Wo sehen Sie hier Ansätze, dieses „Problem" zu beheben? Welche Lösung hat Baumüller hierfür parat?

André Zivny: Mit Ubiquity bietet Baumüller seinen Kunden eine sichere Fernwartungslösung an, die nach IEC 62443-3-3 zertifiziert ist und damit auch den Richtlinien des BSI, das heißt des Bundesamts für Sicherheit in der Informationstechnik entspricht. Die Lösung besteht aus mehreren Komponenten, die in ihrem Zusammenspiel eine sichere Fernwartung gewährleisten. Ubiquity ist standardmäßig auf allen Windows-basierten HMIs von Baumüller installiert. Die Authentifizierung erfolgt mittels Zertifikaten zwischen der Laufzeitumgebung und dem sogenannten Control Center, (das mit der Kunden-Domain verbunden ist), die erst bei erstmaligem Kontakt zwischen beiden Komponenten ausgetauscht werden. Ubiquity erkennt bestehende Verbindungen und konfiguriert sich automatisch für die sichere Fernwartung. Bei dieser Lösung fallen keine Kosten für zusätzliche Hardware oder Server-Infrastrukturen an. Mittels Audit-Trail-Funktion können alle Aktivitäten auf den Geräten, den Verbindungen und der Domain nachvollzogen werden. Mit der integrierten Firewall, dem Traffic-Monitor und weiteren Tools werden dem Nutzer hilfreiche Services zur sicheren Fernwartung zur Verfügung gestellt.

Wie lässt sich denn eine sichere Fernwartung realisieren respektive ein Netzwerk absichern?

André Zivny: Grundsätzlich muss zunächst die Wahrnehmung gegenüber der Bedrohung geschärft werden. Dies lässt sich durch eine intensive Schulung der Mitarbeiter und Maschinenbetreiber realisieren. Als technische Lösung sollte dann über Mindestmaßnahmen nachgedacht werden, um die Fernwartung abzusichern. Dazu gehören beispielsweise eine verschlüsselte Kommunikation unter Einsatz sicherer VPN-Technologien, eine entsprechende Nutzer- und Berechtigungsverwaltung und die damit einhergehende Authentifizierung. Es sollte vorher aber auch geklärt werden, wie und wo die Fernwartung zum Einsatz kommen soll: Die Überprüfung der eigenen Infrastruktur, wie ist das Produktivnetz aufgebaut, wie soll kommuniziert werden, welche Ports werden geöffnet, usw.

Gibt es Standards für einen sicheren Zugang zu Anlagen, Geräten und Daten, die unabhängig vom jeweiligen Standort oder Netzwerk der Maschinen sind?

André Zivny: Ein de-facto Standard in der Fernwartung sind die VPN-Verbindungen. Aber auch VPN-Verbindungen können attackiert, abgehört oder manipuliert werden (zum Beispiel sogenannte DoS oder Man-in-the-Middle-Angriffe). Diese Gefahr besteht vor allem dann, wenn bei der genutzten VPN-Lösung auf die Schließung bekannt gewordener Schwachstellen verzichtet wird oder die jeweiligen Updates nicht genutzt werden. Auch sollte auf den Einsatz einer ausreichend starken Verschlüsselung geachtet werden.

Welche Rolle spielt ein sicherer Fernzugriff im Kontext von Industrie 4.0?

André Zivny: Eine sehr große Rolle. Denn die Vernetzung von Maschinen und Anlagen führt zu immer größeren Datenmengen, die vor unbefugtem Zugriff von außen geschützt werden müssen. Gleichzeitig muss aber eine Fernwartung möglich sein, um die modernen, hoch spezialisierten und optimierten Produktionsanlagen warten, kontrollieren und steuern zu können.

Stellt die Sicherheit Ihrer Meinung nach eine Einstiegshürde für kleine und mittelständische Unternehmen in die Welt von Industrie 4.0 dar? Wie kann man diese Hürde nehmen?

André Zivny: Sicherheit ist das A und O. Sie muss immer gewährleistet werden können. In Zeiten von Industrie 4.0 hat Sicherheit einen größeren Stellenwert bekommen und kann so durchaus als Einstiegshürde bezeichnet werden. Mithilfe von sicheren Fernwartungslösungen, wie beispielsweise Ubiquity, kann die Hürde gut gemeistert werden. (agry)

KONTAKT

Baumüller Nürnberg GmbH, Nürnberg
Tel.: +49 911 5432 0 · www.baumueller.de