Bild: Baumüller

Muss kein Sicherheitsrisiko sein: Der Zugriff auf Maschinendaten...

Für die Fernwartung von Maschinen und Anlagen bietet Baumüller Ubiquity als verbesserte Sicherheitslösung an.

Bild: Fotolia – Leo Lintang

Kanal sicher?

Fernwartung in der vernetzten Produktion von morgen

Industrie 4.0 bringt neben einer hochflexiblen und intelligenten Produktion völlig neue Herausforderungen mit sich: zum Beispiel im Bereich Security. Für die Fernwartung von Maschinen und Anlagen bietet Baumüller jetzt eine sichere Lösung an – damit die Vorteile der Vernetzung nicht ins Gegenteil umschlagen.

Laut einer Studie von Pricewaterhouse Coopers (PWC) aus dem Jahr 2016 belegt Cyberkriminalität den zweiten Platz unter allen begangenen Wirtschaftsverbrechen und ist damit der am schnellsten wachsende Bereich. Folgt man einer Erhebung des Verbandes Bitkom, so waren 69 Prozent aller befragten Unternehmen schon Opfer von Datendiebstahl, Industriespionage oder Sabotage.

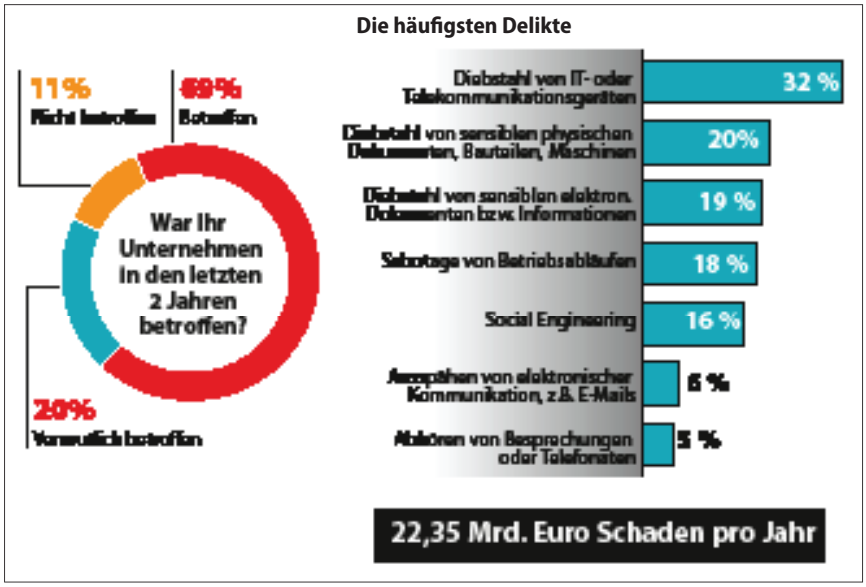
Betroffen sind hiervon auch Konzepte, die es schon lange vor Industrie 4.0 gab, zum Beispiel die Fernwartung. Wurde vor einigen Jahren Fernwartung noch mittels Modem und Wählleitung realisiert, so stehen heute mit Breitbandanschlüssen andere, leistungsfähigere Optionen zur Verfügung. Gleichzeitig steigt aber auch das Risiko, Ziel eines Angriffs zu werden.

Zertifikate und Verschlüsselungen

Mit Ubiquity bietet Baumüller seinen Kunden eine sichere Fernwartungslösung, die nach IEC 62443-3-3 zertifiziert ist und damit auch den Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnik) entspricht. Die Lösung besteht aus mehreren Komponenten, die in ihrem Zusammenspiel eine sichere Fernwartung gewährleisten: erstens das Control Center, die Zentrale von der aus die Fernwartungssysteme verwaltet, beobachtet und aktualisiert werden können; zweitens die Laufzeitumgebung, die auf dem Bediengerät installiert ist und ohne zusätzliche Hardware auskommt und drittens die Server- und Infrastruktur, über die der Austausch von Daten, Zertifikaten und Schlüsseln stattfindet.

Die Fernwartung ist nur möglich, wenn die Laufzeitumgebung mit dem Control Center verbunden wurde. Dazu werden Zertifikate und eine Zwei-Faktor-Authentifizierung verwendet. Mit der Verwendung bestehender Internetverbindungen muss keine separate Verbindung aufgebaut werden. Ubiquity erkennt bestehende Verbindungen und konfiguriert sich automatisch. Auch der Einsatz von separater Hardware ist überflüssig, die Laufzeitumgebung ist auf den Bediengeräten bereits vorinstalliert. Mit Ubiquity werden höchste Sicherheits-Standards umgesetzt, indem automatisch das SSL / TLS Protokoll und Zertifikate genutzt werden, um eine

Datenklau, Spionage, Sabotage: Zwei Drittel der Industrie betroffen



Die Industrie im Visier von Cyberkriminellen (Quelle: Bitkom – Nachbau *antriebspraxis*)

Hintergrundinfo

Maschinenbau im Visier von Cyberkriminellen

Zwei von drei Industrieunternehmen (69 Prozent) sind in Deutschland in den vergangenen zwei Jahren Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden. Das hat eine repräsentative Umfrage im Auftrag des Digitalverbands Bitkom unter 504 Unternehmen des produzierenden Gewerbes ab 10 Mitarbeitern ergeben. Zum Vergleich: Im Durchschnitt der Gesamtwirtschaft sind nur 51 Prozent aller Unternehmen von entsprechenden Delikten betroffen. Der Schaden beläuft sich für die deutsche Industrie nach Berechnungen des Bitkom auf rund 22,4 Milliarden Euro pro Jahr. „Die deutsche Industrie mit ihren zahlreichen Hidden Champions ist ein attraktives Angriffsziel von Cyberkriminellen und ausländischen Nachrichtendiensten", sagte Bitkom-Präsidiumsmitglied Winfried Holz zum Start der Hannover Messe. Laut Umfrage ereigneten sich die kriminellen Vorfälle am häufigsten in der Produktion und Fertigung. Das berichten 36 Prozent der betroffenen Unternehmen. Bei 30 Prozent richteten sich die Angriffe auf die Bereiche Lager und Logistik, bei 29 Prozent auf die IT und bei 23 Prozent auf Forschung und Entwicklung. „Mit der Digitalisierung der Produktion und der Vernetzung von Maschinen über das Internet entstehen neue Angriffsflächen", sagte Holz. „Der Erfolg von Industrie 4.0 steht und fällt mit der Sicherheit der eingesetzten Systeme." Nach den Ergebnissen der Umfrage sind im Maschinen- und Anlagenbau 70 Prozent der Unternehmen von entsprechenden Delikten betroffen. ***(Quelle: Bitkom)***

hohe Sicherheit und Vertraulichkeit der Kommunikation sicherzustellen. Dabei kommen unterschiedliche Verschlüsselungsverfahren zum Einsatz: ein 256-Bit-Schlüssel nach dem AES-Verfahren und das asymmetrische Verschlüsselungsverfahren mit einem 1024-Bit-RSA-Schlüssel.

Kommunikation leicht gemacht

Mit einer integrierten Chat-Funktion wird der direkte Kontakt mit dem Kunden oder Supervisor ermöglicht. Dank integriertem Remote-Desktop-Service kann ohne die Installation von zusätzlichen RDP- oder VNC-Diensten auf das Remote-System zugegriffen werden. Mit dem File-Exchange-Dienst können Dateien ausgetauscht und Dateien direkt auf die dem HMI angeschlossenen Systeme – zum Beispiel PLC oder Umrichter – übertragen werden. Dabei registriert Ubiquity über eine Audit-Trail-Funktion alle auf dem System durchgeführten Remote-Zugriffe. *bf* ■

Autoren Susanne Aufmuth und André Zivny, Baumüller