SICHERHEIT 4.0

GRAF Markus
Böhler Edelstahl GmbH & Co KG, Technik Center, Mariazeller Straße 25, 8605, Kapfenberg, AUT

1 Sicherheit

Der Begriff Sicherheit kommt aus dem Lateinischen und umschreibt einen Zustand, der als "frei von nicht zu vertretenden Risiken oder Gefahren" bezeichnet werden kann.
Im Bereich der Technik und insbesondere im Umfeld der Industrie bezog sich Sicherheit meist auf den Schutz der Arbeitnehmer und der Anlagen vor den Gefahren, die durch elektrischen Strom, Hitze oder mechanisch bewegliche Teile bestanden. So stand für Anlagen- und Maschinenbauer die Betriebssicherheit (safety) an erster Stelle.
Im Gegenzug findet sich im Bereich der Informationstechnologie seit Jahren das Wort "security" als Überbegriff für alle Maßnahmen, um EDV-Systeme und Daten sicher und immun gegen unbefugte Zugriffe und Manipulation zu machen.

1.1 Safety & Security

Die fortschreitende Automatisierung und Digitalisierung bringt neben vielen Vorteilen genau hier aber auch neue Gefahren mit sich, gegen die entsprechende Maßnahmen ergriffen werden müssen. Waren etwa Produktionsmaschinen und Anlagen in der Vergangenheit eigenständige Inseln, so sind diese heute Teil der vernetzten Welt. Neben der klassischen Betriebssicherheit (safety) gilt es nun, auch in diesem Bereich Maßnahmen der Informationssicherheit (security) zu ergreifen, um Anlagen gegen unbefugten Zugriff oder Manipulation zu schützen.

1.2 Schutzmaßnahmen aus der IT-Welt für Produktionsanlagen

Im Bereich der IT gibt es seit langer Zeit vielfältige Schutzmaßnahmen, um Server und Computer gegen Manipulationen, unbefugte Zugriffe bzw. Schadsoftware zu schützen. Virenscanner, Firewalls und Sicherheitsupdates für PC sind allgemein ein Begriff aus der Office-Welt.
Die nun an IT-Netzwerke angeschlossenen programmierbaren Steuerungen von Produktionsanlagen benötigen allerdings andere Schutzmaßnahmen als Office-Geräte. Programmierbare Steuerungen besitzen selbst oft nicht einmal die einfachsten Schutzmechanismen, wie Passwörter, um den Zugriff über das Netzwerk zu regeln, da deren Netzwerke ursprünglich nur als Produktionsinseln erdacht wurden.
So ist der naheliegende Einsatz einer Firewall zum Schutz der Produktionsanlagen nur ein kleiner Schritt in Richtung Sicherheit. Firewalls, wie sie in der klassischen IT zum Einsatz kommen, wissen mit industriellen Steuerungsprotokollen meist nicht umzugehen und können daher kaum „gute" von „bösen" Datenpaketen unterscheiden. Zudem sind in Produktionsanlagen oft PC mit veralteten Betriebssystemen im Einsatz, bei denen es aus diversen Gründen nicht möglich ist, Virenscanner zu betreiben oder Sicherheitsupdates einzuspielen, um bekannte angreifbare Lücken zu schließen.

1.3 Gewollte und ungewollte Zugriffe von außen

Sowohl durch die steigende Komplexität der Anlagen als auch durch den Umstand, dass (vor allem bei kleineren Unternehmen oder Außenstellen) vor Ort oft kein entsprechendes Fachpersonal vorhanden ist, werden immer häufiger Fernwartungszugänge für Produktionsanlagen eingerichtet, damit z.B. vom Hersteller der Anlage oder von der Firmenzentrale aus Ferndiagnosen erstellt oder neue Programme in die Anlagen eingespielt werden können.
Für die technische Realisierung von Fernwartungszugängen gibt es die unterschiedlichsten Ansätze (vom klassischen Telefonmodem über GSM-Lösungen oder auch von zentralen VPN-Lösungen über das Internet). Neben der Gefahr durch technisch unsichere Lösungen fehlt bei den Anlageneignern oft die Information über die tatsächliche Funktionsweise, oder es fehlt sogar das bloße Vorhandensein solcher Zugänge, was im Falle eines Angriffs fatale Auswirkungen haben kann. Während große Unternehmen an dieser Stelle ihre Standards vorgeben, bleibt vor allem KMU's nur das Vertrauen in den Hersteller, dass dessen Lösung entsprechend sicher ist.

2 IOT – das Internet der Dinge

Nicht nur im Unternehmensumfeld sondern auch im privaten Bereich gibt es ein ständig wachsendes Angebot an verlockenden Geräten und Diensten, die Abläufe erleichtern oder verbessern sollen. Im privaten Bereich kennt man eine Vielzahl von Geräten, die "mit dem Internet verbunden" sind und sich vom Smartphone abfragen lassen; dies beginnt bei der Kamera an der Haustür, der Heizungssteuerung, dem Türschloss….

Auch im kommerziellen und industriellen Umfeld gibt es immer mehr Anbieter, die mit Sensoren und Geräten Lösungen für Aufgaben aller Art versprechen, die einfach einzubauen und zu bedienen sind und ihre Daten ohne großen technischen Aufwand in die Cloud liefern, um diese dann z.B. „BigData Analysen" zuzuführen.

2.1 Sicherheit in der Cloud

Auch hier stellen sich sowohl im privaten Bereich als auch im Unternehmensumfeld dieselben Fragen:

- Wie sicher sind meine Daten in der Cloud?
- Wo auf der Welt liegen meine Daten?
- Welche Datenschutzgesetzte liegen zugrunde, und werden diese auch geachtet?
- Was passiert mit meinen Daten, wenn es meinen Anbieter einmal nicht mehr gibt, muss ich meine IOT-Geräte dann ersetzen, ist meine Investition dann wertlos?

Mit diesen Fragen sollten sich Unternehmen auseinander setzen, bevor sie Dienste von Anbietern in Anspruch nehmen und Daten ihres Unternehmens (vielleicht auch zwangsläufig) in die Cloud stellen. Die Wahl des richtigen, zuverlässigen und seriösen Anbieters von Cloud-Lösungen wird hier zukünftig ein wichtiges Thema sein.

So können etwa Daten aus IOT-Geräten sensibel oder unternehmenskritisch sein, Daten die in einer Web-Plattform von Kunden eingegeben werden, können personenbezogene Daten enthalten (Datenschutz). Temporäre Ausfälle oder die endgültige Einstellung von Cloud-Diensten können in weiterer Folge unmittelbare Schaden für das Unternehmen bewirken.