Die Gefahr aus dem Netz

Schutz vor Hackerangriffen auf Maschinen und Anlagen / IT-Sicherheit in Zeiten von Industrie 4.0

Mit zunehmender Vernetzung der industriellen Produktion haben immer mehr Maschinen und Anlagen Internetzugang. Sie sind damit potenziellen Bedrohungen durch Hackerangriffe ausgesetzt. Inzwischen geht es nicht nur um Industriespionage, sondern auch um wirtschaftliche Schäden durch Sabotage von Produktionsanlagen und um Angriffe auf Maschinensteuerungen. Das kann auch Beschäftigte gefährden.

VON DR. OLIVER SCHMITT

[Dr. Oliver Schmitt ist Mitarbeiter der BGN-Prävention im Bereich Maschinen- und Anlagensicherheit.]

Ein bekanntes Beispiel eines Cyberangriffs in der Lebensmittelindustrie ist der Fall Mondelez. Im Lörracher Milka-Werk standen im Juli 2017 über mehrere Tage die Bänder still. Ein Erpressungs- und Verschlüsselungstrojaner hatte die Computersysteme infiziert. Die Gründe für solche Angriffe sind vielfältig. Oft kann nicht einmal ermittelt werden, wer dahintersteckt.

Denkbare Szenarien

Der Stillstand von Produktionsanlagen aufgrund gestörter IT ist aus Sicht des Arbeitsschutzes zunächst ein sicherer Zustand. Zusätzlich zu den Produktionsausfällen nehmen die Angreifer aber immer wieder auch die Gefährdung von Menschenleben in Kauf oder planen sie sogar gezielt mit ein. So könnte z. B. ein autonom fahrender Transportwagen plötzlich unerwartet mit voller Geschwindigkeit durch die Hallen fahren.

Ein weiteres denkbares Szenario entsteht durch die zunehmende Vernetzung der Maschinen im Zuge von Industrie 4.0. Mit den Vorteilen für die Produktionsplanung und -überwachung wachsen auch die Gefahren, dass ein Tor für Angreifer entsteht. Sie können dann z. B. vom anderen Ende der Welt Schutzeinrichtungen von Maschinen außer Kraft setzen, ohne dass es der Bediener bemerkt. Oder: Bei der Steuerung von Produktflüssen kann es zu Wechselwirkungen zwischen Produktbestandteilen kommen, die normalerweise keinen Kontakt haben dürfen. Die Folge können hohe Drücke oder explosive Gemische sein.

Es könnten auch Heizeinrichtungen großer Frittier-/Backstraßen so manipuliert werden, dass es zu Bränden oder Explosionen kommt. In diesen Szenarien können erhebliche Personenschäden die Folge sein. Dazu passt das Statement von Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI): „In produzierenden Branchen müssen nicht nur Produkte, sondern Leben, Gesundheit und Umwelt geschützt werden."

Grundlegende Maßnahmen der IT-Sicherheit

Die Erfahrungen der letzten Jahre haben glücklicherweise dazu geführt, dass Betriebe neben der traditionellen Maschinen- und Anlagensicherheit (Safety) der IT-Sicherheit (Security) mehr Beachtung schenken.

Große Betriebe sind bei der IT-Sicherheit oft im Vorteil. Sie können sich externe und interne IT-Mitarbeiter leisten, die sich hauptamtlich um die IT-Sicherheit kümmern. Sehr große Nahrungsmittel- und Getränkehersteller ab einer festgelegten Jahresproduktion zählen aufgrund ihrer herausragenden Stellung für die Grundversorgung in Deutschland sogar zur sogenannten Kritischen Infrastruktur (KRITIS) gemäß IT-Sicherheitsgesetz*.

[*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) von 2015]

Auch kleine und mittlere Unternehmen sind auf funktionierende IT-Systeme angewiesen. Allerdings haben sie oft nicht die finanziellen Mittel für entsprechende vorbeugende Maßnahmen. Glücklicherweise kann bereits mit wenigen grundlegenden Maßnahmen eine mögliche Gefährdung durch externe Eingriffe in die IT deutlich verringert werden. Der Kasten rechts enthält auch für Nicht-Experten verständliche Basisanforderungen an die IT-Sicherheit. Sie können Unternehmern auch bei der Gefährdungsbeurteilung der „Gefahren für den Arbeitsschutz, die von gestörter IT ausgehen“ helfen. []

Weitergehende Informationen, u. a. die BSI-Standards oder den Leitfaden zur Basis-Absicherung, finden Sie unter: www.bsi.de

BASISANFORDERUNGEN IT-SICHERHEIT

- → Bei den Mitarbeitern ein Bewusstsein für das Thema IT-Sicherheit schaffen, gerade beim Umgang mit E-Mails und sozialen Medien
- → Standardpasswörter gleich nach der Installation in neue, sichere ändern, danach regelmäßig
- → Firewall und Virenscanner auf den PCs verwenden
- → Regelmäßige Updates durchführen, insbesondere des Betriebssystems
- → Fernwartung/Remotezugang absichern, möglicherweise durch 2-Faktor-Authentifizierung
- → Zugriffsberechtigungen nur für entsprechende Nutzergruppen erteilen
- → Physischen Zugang zu Steuerungen von Maschinen/Anlagen beschränken
- → Verschlüsselung sensibler Daten sicherstellen
- → Verwendung privater/externer Datenträger auf Firmen-PCs verbieten
- → Regelmäßig eine gut dokumentierte Datensicherung durchführen