Fachbereich AKTUELL

FBHM-102

DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

Sachgebiet Maschinen, Robotik und Fertigungsautomation

Safety und Security in der vernetzten Produktion

Stand: 01.10.2018

Die Sicherheit von Produktionssystemen ist eine zentrale Voraussetzung für den Erfolg der vierten industriellen Revolution „Industrie 4.0“. Im Gegensatz zum englischen Sprachgebrauch wird im deutschen Sprachgebrauch der Begriff „Sicherheit“ für zwei verschiedene technische Arbeitsgebiete verwendet. Zum einen ist dies das Gebiet der Arbeitssicherheit beziehungsweise der technischen Sicherheit, zum anderen aber auch das Gebiet der IT- oder Cyber-Sicherheit. Eine klare Unterscheidung in zwei Begriffe „Safety“ und „Security“ wie im Englischen sieht der deutsche Wortschatz nicht vor.

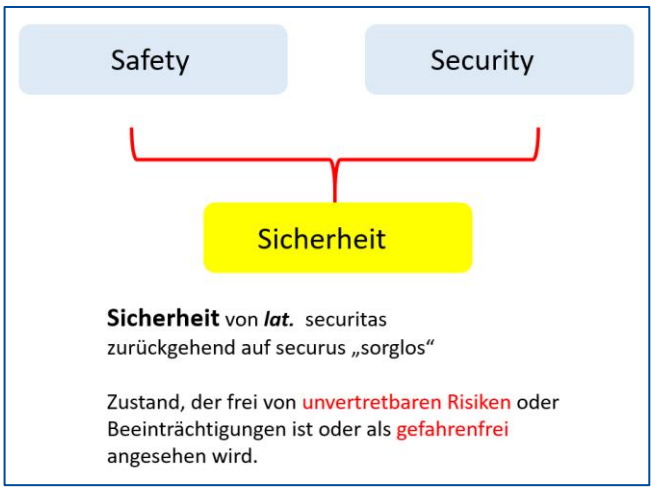

Bild 1: Der Begriff „Sicherheit“

Bisher wurden diese beiden Bereiche getrennt bearbeitet, eine gemeinsame, interdisziplinäre oder abgestimmte Vorgehensweise existierte nicht. Diese Informationsschrift stellt die beiden Begriffe Safety und Security einander gegenüber, erläutert sie und beschreibt mögliche Auswirkungen von IT-Sicherheitsbedrohungen für Maschinen und Anlagen, sowie daraus folgenden Gefährdungen mit hohem Verletzungsrisiko von Mitarbeitern. Es werden grundlegende Vorgehensweisen und Maßnahmen formuliert, um das Bewusstsein für die rechtzeitige Berücksichtigung von möglichen negativen Auswirkungen für Produktionsanlagen und die Arbeitssicherheit aufzuzeigen.

Eine umfassende Beschreibung von Schutzmechanismen gegen ungewollte oder unerlaubte Zugriffe auf technische Anlagen ist für jede Anlage oder Maschine spezifisch und demnach auch nicht Ziel dieser Informationsschrift.

> Definitionen oder Erläuterungen zu Begriffen, Formulierungen und Abkürzungen sind als Glossar auf Seite 8 dieser Schrift angeführt.

Inhalt

1 Einführung 1
2 Mögliche Gefährdungsfaktoren und deren Folgen 2
3 Analyse von bestehenden Maschinen oder Anlagen 3
4 Ansatzpunkte möglicher Schutzmaßnahmen 5
5 Zusammenfassung und Anwendungsgrenzen 7
Anlage 1: Checkliste Firmennetzwerk 9
Anlage 2: Beispiel-Beurteilung 12

1 Einführung

In den letzten zwanzig Jahren stieg der Automatisierungsgrad von Maschinen und Anlagen immer schneller und umfassender. Speziell die Anwendung von programmierbaren elektronischen Steuerungen und Rechnersystemen mit ständig größerer Verarbeitungsgeschwindigkeit, Komplexität und erweiterten Schnittstellen zur

Sensorik und Aktorik ermöglichen permanent neue Applikationen. Unter dem Aspekt der technischen Sicherheit war das in der Vergangenheit wenig problematisch, da zwar der Automatisierungsgrad von Maschinen und Anlagen zunahm, die Maschinen jedoch überwiegend im „Standalone-Betrieb“ oder lediglich mit einer Vernetzung innerhalb einer Produktionsanlage betrieben wurden. Eine übergeordnete Verknüpfung mit Anlagen und Maschinen in anderen Fertigungsstraßen oder -stätten fand in der Regel nicht statt. Somit konzentrierte sich die Betrachtung sicherheitstechnischer Aspekte bisher nur auf den störungsfreien und anwendungssicheren Betrieb von Maschinen und Anlagen. Diese betrachtet Gefahren durch Ausfälle, die ohne Fremdeinwirkung auftreten. Hierzu zählen insbesondere Hardware- oder Softwarefehler sowie Bedienungsfehler. Die Anforderungen wurden in der Europäischen Maschinenrichtlinie **2006/42/EG** sowie in verschiedenen harmonisierten Normen unter der Überschrift „funktionale Sicherheit“ spezifiziert und werden allgemein dem Begriff „Safety“ zugeordnet.

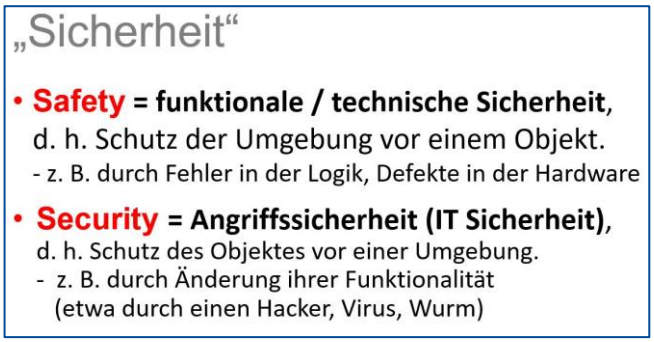

Bild 2: Definition „Safety and Security“

Unter Berücksichtigung technischer Weiterentwicklungen werden die Verbindungen von einzelnen Maschinen und kompletten Fertigungsstraßen nicht mehr nur auf die Vernetzung innerhalb einer Produktionsstätte, sondern auch regional und global übergreifend auf Produktionsstätten an weit auseinanderliegenden Fertigungsstandorten erfolgen. Das bedeutet jedoch auch, dass man nicht mehr von sogenannten gekapselten Produktionssystemen sprechen kann. Vielmehr ist zu berücksichtigen, dass der Datenaustausch von Maschineninformationen über Datenwege erfolgt, die auch einen **ungewollten** Zugriff auf Sicherheitsparameter und andere produktions- aber auch sicherheitsrelevante Daten ermöglichen. Ein Schutz der Daten, die über Datennetzwerke ausgetauscht werden, ist demnach unabdingbar. Der Schutz gegen mögliche bewusste Angriffe durch nicht autorisierte Personen wird als Informationssicherheit bezeichnet. Informationssicherheit hat das Schutzziel, die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherzustellen und wird allgemein auch als Security, IT-Security oder Cyber-Security bezeichnet. Security-Aspekte sind derzeit weder in der Europäischen Maschinenrichtlinie 2006/42/EG noch in harmonisierten Normen für die Sicherheit von Maschinen und Anlagen enthalten.

In der Vergangenheit bestand im Bereich Safety nur ein geringer Bedarf Security-Aspekte zu betrachten. Die Angriffsszenarien aus dem Bereich der IT-Security zeigten in den letzten Jahren, dass diese Thematik auch für den Safety-Bereich (im Rahmen der Arbeitssicherheit) beachtet werden sollte. Unter dem Aspekt der notwendigen Entwicklung von Maschinen- und Anlagensteuerungen wird schon heute eine gleichzeitige Betrachtung von Safety und Security auch in Automatisierungssystemen von Maschinen und Anlagen dringend erforderlich.

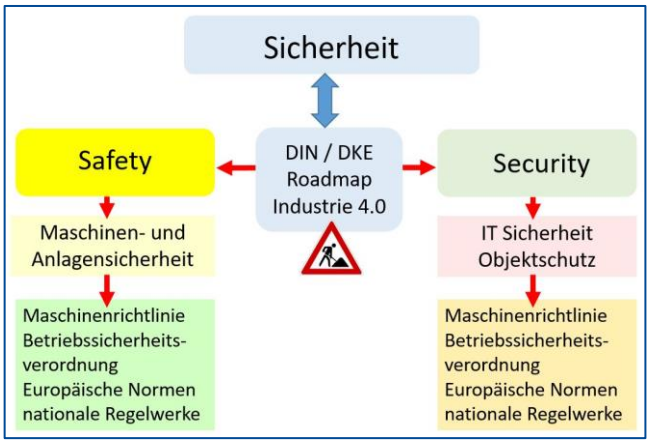

Bild 3: Anwendungsbereich von Safety und Security

2 Mögliche Gefährdungsfaktoren und deren Folgen

IT-Manipulationen bei denen Menschen gefährdet wurden, waren beispielsweise Angriffe auf Steuerungssysteme von Eisenbahnen, Stromversorgungssystemen, Verkehrsampeln oder auch komplexen Hochofensteuerungen in einem Stahlwerk. In diesem Kontext ist es eine Frage der Zeit bis weitere Vorfälle mit Körperschäden von Beschäftigten in der Öffentlichkeit bekannt werden.

Dies zeigt, dass Manipulationen von Industriesteuerungen durchaus im Fokus von Hackern stehen, die sich schon lange nicht mehr auf den Diebstahl von Kreditkarten- oder Kontoinformationen beschränken. Ziel der Angreifer ist es in solchen Fällen die Kontrolle über komplexe

Industrieanlagen zu erhalten. Mögliche Angriffe und Manipulationen können einerseits zu einem kompletten Produktionsausfall oder zu Diebstählen von Produktions-, Prozessdaten sowie von Know-How führen; andererseits können sie auch massive Auswirkungen auf die Maschinensicherheit und damit auf die Arbeitssicherheit haben. Veränderungen in Maschinenparametern können beispielsweise Sicherheitseinrichtungen des Personenschutzes betreffen. Sicherheitsfunktionen könnten dahingehend manipuliert werden, dass diese passiviert werden, dass Geschwindigkeiten verändert werden oder dass ein ungewollter Maschinenanlauf erfolgt. Hierbei kann es zu großen Gefährdungen mit schweren bis hin zu tödlichen Verletzungen von Beschäftigten kommen. Dies gilt es seitens der Akteure im Arbeitsschutz dauerhaft zu verhindern.

Der Schutz von vernetzten Industrieanlagen ist jedoch nicht mit den Werkzeugen beherrschbar, mit denen zum Beispiel Bürocomputernetze geschützt werden, denn Industriesteuerungen verfügen derzeit in der Regel nicht über Antivirenprogramme, Firewalls und andere Maßnahmen wie sie aus IT-Anwendungen bekannt sind. Hinzu kommt, dass auch die Betriebssysteme der programmierbaren Steuerungen heterogen sind und für bisher bestehende Anlagen, die zukünftig vernetzt werden sollen, jegliche Strategien eines Software-Updates fehlen.

Mögliche Auswirkungen von Hackerangriffen
Produktionsausfall
Zerstörung von Maschinen
Diebstahl von Produktionsdaten
Verlust von „Know How“
Manipulation der Netzwerkkommunikation
Veränderung von Produktionsdaten ->Qualitätsmängel
Veränderung von sicherheitsrelevanten Informationen
Passivierung von Sicherheitseinrichtungen
Verlust der Verfügbarkeit durch Fremd-Aktivierung von Safety Prozeduren

Bild 4: Mögliche Folgen von Hackerangriffen

Insbesondere ist zu beachten, dass Gefahren hinsichtlich der Manipulation und des Datendiebstahls in vernetzten Industrieanlagen nicht nur durch Angriffe Dritter über das Internet bestehen. Auch direkte Tätigkeiten an der Maschine selbst durch externe Instandhaltungs- oder Wartungspersonal beinhalten Gefahren. Schon durch den Einsatz von zum Beispiel USB-Sticks oder Notebooks, die unmittelbar mit der Steuerung einer Maschine verbunden werden, können beispielsweise Viren, Trojaner übermittelt oder auch gewollt Daten (z. B. Prozessparameter) kopiert oder verändert werden

3 Analyse von bestehenden Maschinen oder Anlagen

Die bislang fehlenden gemeinsamen Betrachtungen von Safety- und Security-Anforderungen in der Industrieumgebung sind vor dem Hintergrund der fortschreitenden Vernetzung von Maschinen und Anlagen nicht weiter akzeptierbar. Maßnahmen, Strategien und Vorkehrungen, die zum Standard in der Bürokommunikation geworden sind, müssen sinngemäß auch in die Welt der Industrieanlagen transportiert werden. Die maßgebliche Frage ist somit: „Wie kann der Schutz von Produktionssystemen gegen ungewollte Angriffe von außen und innen erfolgen?“

3.1 Basismaßnahme

Die wichtigste Maßnahme ist, dass innerhalb eines Unternehmens das Bewusstsein für die Gefahr von Manipulationen und Industriespionage in Produktionsanlagen wächst und ein gemeinsames „Security-Safety-Management“ für Office- und Automatisierungsanwendungen umgesetzt wird. Der erste Schritt ist hierbei zunächst eine Analyse, aus der hervorgeht, welche Maschinen und Anlagen überhaupt betroffen sein können. Die Erfassung und grobe Bewertung der vorhandenen Maschinen und Anlagen kann im Sinne eines „Katasters“ vorgenommen werden. Dabei können grundsätzlich folgende Unterscheidungen und ersten groben Bewertungen vorgenommen werden:

3.2 Maschinen mit kontaktbehafteten Steuerungen

Maschinen, in denen die Steuerungen über kontaktbehaftete Bauteile realisiert wurden, sind unkritisch in Bezug auf Angriffe von außen und auch von innen, da sie nicht über programmierbare Bauteile verfügen. Ein externer Zugriff ist nicht möglich.

Security-Maßnahmen erübrigen sich.

3.3 Maschinen mit elektronischen Steuerungen

Maschinen, in denen die Steuerungen über elektronische, aber nicht über programmierbare Bauteile realisiert wurden, sind unkritisch in Bezug auf Angriffe von außen und auch von innen. Der Steuerungsablauf kann nur durch Veränderung der Elektronik bewusst geändert werden. Ein externer Zugriff ist nicht möglich.

Security-Maßnahmen erübrigen sich.

3.4 Maschinen mit programmierbaren Steuerungen

Maschinen, in denen die Steuerungen über programmierbare Komponenten (in der Regel SPS- oder Mikroprozessor-Systeme) realisiert wurden, sind in Bezug auf die Ausführung weiter zu differenzieren.

3.4.1 Maschinensteuerungen ohne Netzwerkverbindungen

Programmierbare Steuerungen ohne eine Datenverbindung zu einer anderen Steuerung oder zu einem übergeordneten Rechnersystem verfügen zumindest über eine Schnittstelle, über die ein Programm geladen oder gelesen werden kann. Durch den nachträglichen Anschluss eines Programmiersystems (z. B. Notebook, USB-Stick) besteht jederzeit die Möglichkeit, gewollt oder auch ungewollt eine Programmänderung durchzuführen. Diese Programmänderungen können auch durch das „Einschleusen schadhafter Software ausgelöst werden. Ein weiterer kritischer Aspekt ist das SPS- oder Mikroprozessorsystem selbst. In diesem kann bereits seit Auslieferung ein sogenannter „Schläfer“ vorhanden sein, der zeit- oder ereignisbezogen aktiviert werden und die Maschinensteuerung beeinflussen kann. Auch bei älteren Maschinen ist somit eine Analyse notwendig; mögliche Vorsichtsmaßnahmen sind zu treffen.

3.4.2 Maschinensteuerungen mit Netzwerkverbindungen, aber ohne Verbindungen zu übergeordneten Systemen

Programmierbare Steuerungen mit Datenverbindungen zu anderen Maschinensteuerungen, aber **ohne** Verbindung zu einem übergeordneten Rechnersystem verfügen über Schnittstellen, über die Programme geladen oder gelesen werden können. Zusätzlich erfolgt die Verbindung zu anderen Steuerungssystemen über weitere Schnittstellen (z. B. Verbindung mehrerer SPS-Systeme, dezentrale I/O) für einen gewollten Datenaustausch. Durch den Anschluss eines Programmiersystems (z. B. Notebook, USB-Stick) besteht jederzeit die Möglichkeit gewollt oder auch ungewollt eine Programm- und/oder Parameteränderung im gesamten vernetzten System durchzuführen. Diese Änderungen können durch das „Einschleusen“ von schadhafter Software ausgelöst werden, die nicht nur eine einzige Steuerung, sondern das gesamte Netzwerk einschließlich des übergeordneten Systems manipulieren kann. Ein weiterer kritischer Aspekt sind die SPS- oder Mikroprozessorsysteme selbst. In ihnen kann bereits seit Auslieferung ein sogenannter „Schläfer“ vorhanden sein, der zeit- oder ereignisbezogen aktiviert werden und die Maschinensteuerungen beeinflussen kann. Bei diesen Steuerungsarchitekturen ist besonders zu beachten, dass die angeschlossenen Systeme nicht von einem einzigen Hersteller stammen müssen, sondern durchaus auch von verschiedenen Herstellern sein können. Auch bei älteren Maschinen und Anlagen ist somit eine Analyse notwendig, mögliche Vorsichtsmaßnahmen sind zu treffen.

3.4.3 Maschinensteuerungen mit Netzwerkverbindungen und Verbindungen zu übergeordneten Systemen

Programmierbare Steuerungen mit Datenverbindungen zu anderen Maschinensteuerungen **und einer** Verbindung zu einem übergeordneten Rechnersystem verfügen über Schnittstellen, über die Programme und Daten geladen oder gelesen werden können. Zusätzlich erfolgt die Verbindung zu anderen Steuerungssystemen über weitere Schnittstellen (z. B. Verbindung mehrerer SPS-Systeme, dezentrale I/O) sowie zu den übergeordneten Rechnersystemen, die eine direkte Verbindung zum Internet haben können. Durch den Anschluss eines Programmiersystems (z. B. Notebook, USB-Stick) besteht jederzeit die Möglichkeit, gewollt oder auch ungewollt eine Programm- und oder Parameteränderung im gesamten vernetzten System durchzuführen. Dies kann entweder über den Anschluss an eine Schnittstelle des Steuerungssystemes oder aber auch über einen übergeordneten Rechner erfolgen. Auch eine Kommunikation über das Internet ist demnach möglich.

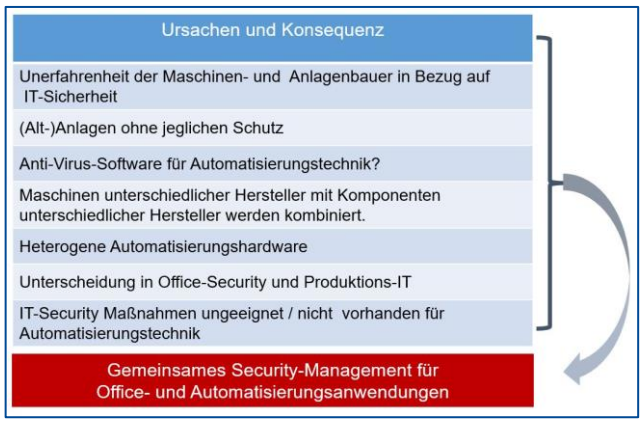

Bild 5: Aspekte, die Maschinenmanipulationen begünstigen

Programm- oder Parameteränderungen können durch das „Einschleusen“ von schadhafter Software ausgelöst werden, die nicht nur eine einzige

Steuerung, sondern das gesamte Netzwerk einschließlich des übergeordneten Systems manipulieren kann.

Außer in den SPS- oder Mikroprozessorsystemen können Gefährdungen somit auch in dem übergeordneten Rechnersystem selbst bestehen. Maschinensteuerungen und/oder Rechnersysteme können demnach sowohl über die „SPS-typischen Programme“ als auch über die in der Office-Welt verwendeten Programme manipuliert werden. Bei diesen Architekturen ist besonders zu beachten, dass die angeschlossenen Systeme nicht von einem einzigen Hersteller stammen müssen, sondern durchaus auch von verschiedenen Herstellern sein und demnach auch die verwendeten Betriebssysteme vielfältig sein können. In diesen Fällen darf sich die Analyse nicht nur auf die „Steuerungswelt“ beziehen, sondern muss auch die gesamte „Office-Umgebung“ einbeziehen. Dies gestaltet sich aufgrund der unterschiedlichen Betrachtungs- und Sprachweisen der Safety-Welt und der Security-Welt als äußerst schwierig und komplex.

4 Ansatzpunkte möglicher Schutzmaßnahmen

Die massiven Lücken in einer fehlenden „Security-Betrachtung“ von vernetzten Industrieanlagen sind nicht mit den Werkzeugen beherrschbar mit denen zum Beispiel Bürocomputernetze geschützt werden. Im Privatbereich sind zur Sicherung von Rechnern und Netzwerken Firewalls und Virenscanner allgemein bekannt und umgesetzt. Aus der Sicht von betrieblicher Security reicht es nicht aus, die Maßnahmen aus dem Privatbereich zu implementieren, um einen umfassenden Schutz von Daten und Maschinen zu erreichen. Das Projekt muss vielmehr systematisch bearbeitet werden, um einen möglichst hohen Schutz zu erreichen. Aus diesem Grunde wurde im Rahmen der internationalen und nationalen Normung die „Normungs-Roadmap Industrie 4.0“ [1] erarbeitet. Diese Normungs-Roadmap beschreibt bereits bestehende Normen, die für die Umsetzung im Rahmen von Industrie 4.0 relevant sein können und zeigt gleichermaßen auch die Lücken auf, die für eine erfolgreiche Umsetzung von zukünftigen Automatisierungsanforderungen zu schließen sind. Insbesondere die Entwicklung von technischen Anwendungen und neuen Arbeitsverfahren, der Bürokommunikation, der Visualisierung sowie der Integration von zukunftsorientierten Produkten und Methoden wird neue Konzepte und Technologien erforderlich machen.

Um in Industrieanlagen einen möglichst hohen Schutz gegen IT-Angriffe zu erreichen, ist eine systematische Vorgehensweise erforderlich. Die nachfolgenden Punkte zeigen eine beispielhafte Vorgehensweise.

4.1 Risikoanalyse

Zunächst sollte eine Risikoanalyse durchgeführt werden, die zuallererst schutzbedürftige Informationen und Komponenten identifiziert. Für die Auflistung muss die Wichtigkeit bewertet werden.

Dabei wird gekennzeichnet, ob zum Beispiel Daten garantiert verfügbar sein müssen, jederzeit eine Rückverfolgbarkeit möglich sein muss, oder sie nicht verändert werden dürfen (z. B. Maschinenparameter). Dabei sollte bewertet werden, was passieren kann, wenn Daten, Maschinenparameter oder Programme aufgrund des Zugriffs einer externen Bedrohung ausfallen oder verloren gehen.

4.2 Zoneneinteilung

Als Ergebnis der Risikoanalyse kann im zweiten Schritt eine Zonenaufteilung vorgenommen werden. Dabei sollten Maschinen, Komponenten und Informationen ähnlichen Schutzbedarfs zusammengefasst werden. Diese Aufteilung hat viele Vorteile, wenn mit technischen Maßnahmen eine Netzsegmentierung, zum Beispiel durch Firewalls, abgeleitet wird. Fällt eine Zone zum Beispiel durch einen Hackerangriff, einen Virus oder interne Manipulation aus, sind andere Zonen nicht betroffen und arbeiten unbeeinflusst weiter. Diese Netzsegmentierung muss regelmäßig auf Aktualität und Effektivität überprüft werden.

4.3 Authentisierung und Autorisierung

Prinzipiell gibt es in gut strukturierten und gesicherten Netzwerken individuelle Benutzerkonten. Hierbei ist jeder Zugriff authentisiert und auch autorisiert. Durch individuelle Nutzerkennungen (Authentisierung) und Passwörter (Autorisierung) für alle am Netz Beteiligten können Rechte im Netz vergeben werden. Diese müssen im Vorfeld definiert werden und können auch in Gruppen zusammengefasst werden. Maschinen könnten so beispielsweise nur eine Leseberechtigung auf einen Netzwerkspeicher bekommen, wenn sie von dort ein Maschinenprogramm laden müssen. Programmierer und Programmiererinnen von NC-Steuerungen hingegen erhalten zusätzlich einen Schreibzugriff auf definierte Netzwerkkomponenten z. B. Maschinen

und Anlagen. Generell muss festgelegt werden, dass Passwörter personenbezogen sind, turnusmäßig geändert werden müssen und auch nur autorisierten Personen zugänglich sind. Um eine hohe Produktivität zu erreichen ist es heutzutage auch erforderlich, dass Fernzugriffe auf Maschinen, z. B. von Herstellern, ermöglicht werden. Auch für diesen Einsatz sind bei einem Netzwerk wechselnde Passwörter zu vergeben und sämtliche Zugriffe müssen überwacht werden. Im Sinne von Security darf es keinen anonymen Zugang zum Firmennetzwerk geben und alle Zugriffe müssen durch eine sichere Authentisierung abgesichert werden. Dies gilt auch für externe Schnittstellen wie USB-Ports (externe Monteureinsätze), Internet (Produktionsdatenerfassung und weltweiter Abruf im Sinne von Industrie 4.0), VPN (Maschinenfernzugriff). Nur durch diese Individualisierung ist es möglich, klare Rechte in Netzwerken zu vergeben und den Zugang auf das Nötigste einzuschränken.

Beispiel 1:

Eine Maschine wird bei einer Störung durch einen externen Monteur mit auf einem USB-Stick eingeschleustem Trojaner verseucht. Hat die „Maschine“ uneingeschränkten Zugriff auf das Firmennetzwerk, wird sich der Trojaner uneingeschränkt ausbreiten können. Werden USB-Sticks im Vorfeld auf einem autarken Rechner mittels Virensoftware gescannt und Maschinen haben als Netzwerkkomponente klar definierte Schreib- und Leserechte, wird der ungestörten Ausbreitung von Viren und Trojanern Einhalt geboten und der Schaden begrenzt.

Beispiel 2:

Speziell präparierte USB-Geräte sind in der Lage, ein System anzugreifen, ohne dass Benutzer und Benutzerinnen davon erfahren oder Virenscanner etwas wahrnehmen können. Ein Angreifer oder eine Angreiferin sorgt dafür, dass präparierte Hardware (geschenkte USB-Sticks auf Messen, Tastatur bei Werksführung neben SPS liegen lassen und abwarten…) unbewusst vom Technikpersonal angeschlossen wird.

4.4 Drahtlose Kommunikation

Im industriellen Umfeld findet die drahtlose Kommunikation, zum Beispiel über Tablets, Laptops und dergleichen, immer mehr Anklang. Sie findet in der Regel über WLAN (drahtloses lokales Netzwerk) oder Bluetooth statt. Die Standardpasswörter der Gerätehersteller sind oft bereits nach kurzer Zeit öffentlich bekannt. Eine Änderung der Standardpasswörter mit ausreichender Länge ist unabdingbar und auch die Begrenzung der Reichweite muss limitiert werden.

4.5 Fernwartung

Bei der Fernwartung von Maschinen und Anlagen werden Daten über das Internet zwischen Betreiber und Hersteller übertragen. Werden keine Vorkehrungen getroffen ergeben sich hierbei mehrere Schwachstellen in Bezug auf die Security. Es müssen Authentisierungs- und Autorisierungsmechanismen vorhanden sein. Erreicht werden könnte dies zum Beispiel durch eine manuelle Freigabe des erforderlichen Ports für die Fernwartung oder eine getrennte Kabelverbindung zur Maschine. Die Datenübermittlung über das Internet ist zu betrachten. Werden keine weiteren Maßnahmen gefordert, könnten Daten durch Dritte abgefangen und im Klartext gelesen werden. Hierzu bietet es sich an, eine VPN-Verbindung (virtuelles privates Netzwerk) aufzubauen und diese unter Security-Gesichtspunkten korrekt zu konfigurieren. Der Vorteil ist, dass durch diese Ende-zu-Ende-Verschlüsselung ausschließlich autorisierte Sender und Empfänger die Daten lesen können. Jegliches „Abfangen“ der Daten irgendwo im Internet ist wertlos, da die Informationen verschlüsselt sind. Für eine sichere Fernwartung muss weiterhin sichergestellt werden, dass der Rechner des Wartungspersonals nicht verseucht wurde (z. B. durch eine Schadsoftware, Verlust des Schlüssels) und eine sichere Verschlüsselung nach aktuellem Stand der Technik verwendet wird.

4.6 Monitoring

Wenn die oben beschriebenen technischen, organisatorischen und persönlichen Maßnahmen umgesetzt sind, ist es zudem unabdingbar, ein Monitoring zu implementieren. Es soll sicherheitsrelevante Informationen schreibgeschützt archivieren (Logfile). Dazu gehören erfolgreiche und fehlgeschlagene Logins mit Benutzernamen und Zeitstempel.

Manche Angriffe von intern und extern können in diesen Logfiles mit technischen Hilfsmitteln nachvollzogen werden. Daraus können gegebenenfalls erforderliche Gegenmaßnahmen eingeleitet werden. Auch das Verwenden neuester und stetig auf aktuellem Stand gehaltener Virenscanner ermöglicht ein frühzeitiges Erkennen von bekannten Viren im Firmennetzwerk.

4.7 Backup

Sollte trotz aller präventiven Anstrengungen dennoch eine Schwachstelle ausgenutzt worden sein, müssen auch Vorkehrungen für diesen Fall getroffen worden sein. Regelmäßige Backups sind hierfür eine wichtige Maßnahme. Abhängig von der Bedeutung der Daten und der erforderlichen Verfügbarkeit der gespeicherten Informationen sollte die Organisation des Backups erfolgen. Backups müssen auf Wiederherstellbarkeit geprüft werden und idealerweise redundant aufgebaut sein, zum Beispiel durch Datenträger, die nach dem Backup technisch getrennt werden. Sind einzelne Segmente betroffen, können Backups die Daten, Informationen und Prozessdaten schnell wiederherstellen.

4.8 Organisation

Für die Planung eines sicheren Netzwerks sowie die Umsetzung der Maßnahmen und die Prüfung der Aktualität muss in jeder Firma eine Person verantwortlich sein. Sie sollte zudem das System ständig auf Schwachstellen prüfen und ein Patchmanagement (Reparatur- bzw. Verbesserungsmanagement) organisieren. Auch überflüssige Software und Dienste sollten deinstalliert und nicht verwendete Hardwarekomponenten (z. B. USB-Ports) deaktiviert werden.

Es ist erforderlich, dass eine gute Übersicht über die Sicherheitsmaßnahmen vorliegt. Zu dieser Dokumentation gehören unter anderem sämtliche Schnittstellen, die Ergebnisse der Risikoanalyse, die Rechteverteilung, das Maschineninventar mit zugehörigen Nutzerinnen und Nutzern sowie Passwörtern (verschlüsselt).

5 Zusammenfassung und Anwendungsgrenzen

Der Erfolg von Industrie 4.0 wird wesentlich davon abhängen, ob es gelingen wird, die Sicherheitsaspekte gleichartig für Safety und Security anzuwenden. Hierbei spielen die technischen Anforderungen sowie das Verhalten der Maschinen- und Anlagenbetreiber eine gleichermaßen entscheidende Rolle. Schon jetzt darf sich der Begriff „Sicherheit“ nicht mehr nur allein auf den Aspekt „Safety“ beziehen, sondern muss gleichermaßen auch immer die „IT-Security“ beinhalten. Das zeigt, dass sich die Methoden zur Beurteilung der „Sicherheit“ bereits geändert haben und weiterhin an die Entwicklung neuer Produkte anzupassen sind.

Diese Fachbereich AKTUELL beruht auf dem durch den Fachbereich Holz und Metall, Sachgebiet Maschinen, Robotik und Fertigungsautomation der Deutschen Gesetzlichen Unfallversicherung DGUV zusammengeführten Erfahrungswissen.

Es soll insbesondere dazu dienen, neben Safety-Anforderungen auch Security-Aspekte bei der Beurteilung von Maschinen und Anlagen zu berücksichtigen und notwendige Sicherheitsmaßnahmen umzusetzen.

Die Bestimmungen nach einzelnen Gesetzen und Verordnungen bleiben durch diese Informationsschrift unberührt. Die Anforderungen der gesetzlichen Vorschriften gelten uneingeschränkt.

Um vollständige Informationen zu erhalten, ist es erforderlich, die in Frage kommenden Vorschriftentexte einzusehen.

Der Fachbereich Holz und Metall setzt sich unter anderem zusammen aus Vertretern und Vertreterinnen der Unfallversicherungsträger, staatlichen Stellen, Sozialpartnern, herstellenden und betreibenden Firmen.

Diese Fachbereich AKTUELL FBHM-102 ersetzt die gleichnamige DGUV Kurzinformation, herausgegeben als Entwurf 07/2018.

Weitere DGUV-Kurzinformationen bzw. Informationsblätter des Fachbereichs Holz und Metall stehen im Internet zum Download bereit [5].

Zu den Zielen der DGUV-Kurzinformation siehe DGUV-Information FBHM-001 „Ziele der DGUV-Information herausgegeben vom Fachbereich Holz und Metall“.

Literatur:

[1] Deutsche Normungs-Roadmap Industrie 4.0, DIN e.V. und DKE, März 2018

[2] Top 10 Bedrohungen für Industrieanlagen, 24.08.2016, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[3] Leitfaden Industrie 4.0 Security. Handlungsempfehlungen für den Mittelstand, VDMA-Arbeitskreis Industrial Security, Mai 2018

[4] Die Lage der IT-Sicherheit in Deutschland, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[5] Internet: www.dguv.de/fb-holzundmetall Publikationen oder www.bghm.de Webcode: <626>

Bildnachweis

Die in dieser Fachbereich AKTUELL gezeigten Bilder wurden freundlicherweise zur Verfügung gestellt von:

Bild 1, 2, 3, 4,5: FB HM, SG MRF, Heinke

Glossar

Begriff	Beschreibung
Antiviren-software	Sie versucht in Dateien und laufenden Prozessen die Muster von bekannten Viren zu erkennen, um diese zu beseitigen.
Backdoor	Sie erlaubt es Dritten, einen PC fernzusteuern und auch für kriminelle Zwecke zu verwenden.
Computer viren	Sind unerwünschte Programme, die sich in Computerprogramme einschleusen und nach dem Ausführen durch den Benutzer/die Benutzerin weiterverbreiten können.
Computer wurm	Malware, die sich im Gegensatz zum Virus selbständig verbreitet. Ein Computerwurm nützt sehr oft Sicherheitslücken zum Eindringen in ein System.
Daten-sicherheit	Die sichere Verarbeitung, Speicherung und Kommunikation der Informationen sollen durch Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet werden.
Firewall	Eine Software zwischen zwei Netzwerken, die anhand eines Regelwerks entscheidet, welche Datenpakete auf welchem Pfad übertragen werden dürfen.
Hacker	Hacker dringen wie Cracker in Computersysteme ein, behaupten aber von sich, dass sie damit nur Missstände und Sicherheitslücken aufzeigen wollen.
Integrität von Daten	Begriff zur Datensicherheit: Daten enthalten den korrekten Inhalt, stehen vollständig zur Verfügung und wurden nicht unbefugt verändert.
Key-logger	Programme, oder Geräte, die Tastatureingaben mitprotokollieren. So können Hacker an Passwörter gelangen.
Makro, Makro-viren	Makroprogrammiersprachen erlauben Automatisierungen in manchen Dokumentenformaten. Makroviren sind in diesen Sprachen geschrieben und werden in ein Dokument (z. B. als VBA Script in einer Tabelle im Excel-Format) eingebettet. Sie werden aktiv, wenn das schädliche Makro ausgeführt wird.
Malware	Oberbegriff für unerwünschte, schädliche Software. Malware kann einen Schaden am Computer und an den gespeicherten Daten anrichten.
Phishing	Hierunter versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers oder einer Internet-Benutzerin zu gelangen und damit Identitätsmissbrauch zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderungen oder Wirtschaftsspionage zu begehen und den entsprechenden Personen/Firmen zu schaden.
Pre-texting, Identitäts-diebstahl	Daten einer dritten Person (unter Vorgabe einer fremden Identität) besorgen. Pretexting ist ein anderer Begriff für Identitätsmissbrauch.
Spam / Junk E-Mails	Unerwünschte Werbemails. Das Verarbeiten und Aussortieren dieser E-Mails kostet Zeit und Geld. Spamfilter versuchen Spam zu erkennen und auszusortieren.
Spyware	Diese Malware forscht das Nutzungsverhalten aus und sendet die Daten an Hersteller der Malware.
Trojaner	Diese Malware ist in einem scheinbar nützlichen Programm versteckt und kann z. B. Passwörter auslesen oder auf Daten im Netzwerk zugreifen und diese an den Auftraggeber/die Auftraggeberin der Malware übermitteln.
Vertraulichkeit	Begriff zur Datensicherheit: Informationen sollen vertraulich behandelt werden und vor Missbrauch geschützt werden. Nur befugte Personen dürfen Zugang zu vertraulichen Informationen haben.
VPN	Virtual Private Network, verschlüsselte Verbindung, die zwei Netzwerke z. B. über das Internet verbindet.
WLAN	Wireless Local Network, drahtloses Netzwerk
LAN	Local Area Network, kabelgebundenes Netzwerk
Zugriff auf Daten	Auf Daten sollen nur befugte Benutzer und Benutzerinnen zugreifen können. • Benutzerauthentifizierung durch Eingabe von Benutzername und Passwort • Schutz von Dateien durch ein Passwort • Verschlüsselung von Daten erschwert unberechtigten Zugriff
SCADA	Supervisory Control And Data Acquisition (übergeordnete Steuerung und Datenerfassung)

Anlage 1: Checkliste für Betreiber von Firmennetzwerken

Diese Checkliste soll den Betreiber dabei unterstützen Firmennetzwerke zu beurteilen und sicherer zu gestalten. Sie erhebt keinen Anspruch auf Vollständigkeit.

Fragestellung	Ja	Nein	Nicht zutreffend	Wo/Wie
1. Grundsätzliches				
a) Werden Wechseldatenträger vor jeder (auch der ersten) Benutzung auf Viren gescannt?				
b) Wird das Bedienpersonal regelmäßig unter Security Aspekten unterwiesen?				
c) Werden für die Anlagenwartung und Programmierung nur Systeme eingesetzt, die aktuell auf Viren überprüft wurden?				
d) Werden regelmäßige Backups erstellt?				
e) Wird vor jeder Softwareänderung ein Backup erstellt?				
f) Werden Schutzmaßnahmen regelmäßig aktualisiert?				
2. Risikoanalyse				
a) Sind die schutzbedürftigen Informationen und Komponenten identifiziert und aufgelistet?				
b) Ist eine Risikobewertung durchgeführt in Bezug auf Wichtigkeit und Ableitung von Schutzzielen (z. B. garantierte Verfügbarkeit der Daten; jederzeit digitale Rückverfolgbarkeit von Produktionsdaten sichergestellt)?				
c) Sind mögliche Bedrohungen und ihre Folgen dokumentiert?				
3. Zoneneinteilung				
a) Maschinen, Komponenten und Informationen ähnlichen Schutzbedarfs wurden in Zonen eingeteilt?				
b) Sind einzelne Zonen untereinander durch technische Maßnahmen getrennt (Netzsegmentierung), z. B. durch Firewalls?				
c) Bei Ausfall einer Zone (z. B. durch Hackerangriff, Virus, Trojaner, …) sind möglichst wenig andere Zonen betroffen?				
d) Ist organisiert, dass die Netzsegmentierung auf Effektivität und Aktualität (Updates, Filterregeln, …) periodisch wiederkehrend geprüft wird?				
4. Ganzheitliche Organisation von Authentisierung und Autorisierung				
a) Gibt es für alle Nutzenden individuelle Benutzerkonten (Nutzer/Nutzerin + Passwort)?				
b) Ist definiert und umgesetzt, welche Nutzenden welche Rechte im Netz haben (Lesezugriff, Schreibzugriff)?				

Fragestellung	Ja	Nein	Nicht zutreffend	Wo / Wie
c) Werden Standardpasswörter von Maschinen und Anlagen turnusmäßig geändert und sind nur befugten Personen zugänglich?				
d) Werden Fernzugriffe überwacht und auch mit wechselnden Passwörtern geschützt?				
e) Wird jeder Zugriff von Maschinen auf das Netz oder von Personen auf das Netz/auf Maschinen authentisiert?				
f) Werden Zugriffe auf externe Schnittstellen (USB, Internet, VPN…) auch über sichere Authentisierung abgesichert?				
5. Absicherung von Funktechnologien				
a) Erstrecken sich die Reichweiten nur auf das Nötigste (Signalstärke oder Abschirmung)?				
b) Gibt es sichere Passwörter?				
c) Wurden ggf. voreingestellte Passwörter durch individuelle Passwörter ersetzt?				
d) Safety-relevante Parameter können nur über sichere Kommunikation geändert werden?				
e) Gibt es Regelungen zum Aufbau und Beenden einer Kommunikation?				
6. Fernwartung				
a) Gibt es Regelungen zum Aufbau und zum Beenden einer Fernwartung?				
b) Sind Fernwartungen generell über verschlüsselte Verbindungen aufgebaut (z. B. VPN, SSH)?				
c) Sind USB Ports bei Monteureinsätzen vor Ort gesichert und mit organisatorischen Maß-nahmen belegt (z. B. USB-Stick-Prüfung an Pforte mittels Virenscanner; Instandhaltung gibt USB Ports danach frei)?				
d) Änderungen, die Gefährdungen hervorrufen können (z. B. Maschinenanlauf), sind nur möglich, wenn zuvor vor Ort an der Maschine eine Bestätigung erfolgt ist?				
7. Monitoring und Hackerangriffserkennung				
a) Werden mindestens alle externen Zugriffe auf abgesicherte Netzwerke protokolliert?				
b) Werden verdächtige Ereignisse wie falsche Passworteingabe, Senden von Daten an unbekannte Empfänger gemeldet?				
c) Werden dann Gegenmaßnahmen eingeleitet?				
d) Sind Virenscanner im Netzwerk implementiert, die jeweils auf aktuellen Stand gehalten werden?				

Fragestellung	Ja	Nein	Nicht zutreffend	Wo / Wie
8. Backups				
a) Werden regelmäßig Backups durchgeführt?				
b) Wird jede Zone dabei unabhängig von anderen Zonen berücksichtigt?				
c) Sind die Backup-Datenträger abgesichert?				
d) Wird das Backup gegen Fremdzugriff und Abhandenkommen sicher aufbewahrt?				
e) Werden regelmäßige Prüfungen auf Wiederherstellbarkeit durchgeführt?				
f) Sind die Backup-Systeme redundant aufgebaut, sodass ein weiteres Backup bei Nicht-Wiederherstellbarkeit zur Verfügung steht?				
9. Organisatorische Maßnahmen				
a) Wurde eine geeignete verantwortliche Person für Security bestimmt?				
b) Wird das System regelmäßig auf Schwachstellen überprüft?				
c) Ist das Updatemanagement organisiert?				
d) Ist bei Initialisierung des Systems organisiert, dass alle individuellen Einstellungen wiederhergestellt werden (z. B. die Zugangsdaten bei Austausch eines Maschinenrechners)?				
10. Dokumentation der Sicherheitsmaßnahmen				
a) Sämtliche Schnittstellen (Ports) sind dokumentiert?				
b) Die Ergebnisse der Risikoanalyse sind dokumentiert?				
c) Wurde die Rechteverteilung dokumentiert?				
d) Das Maschineninventar mit zugehörigen Nutzenden und Passwörtern (verschlüsselt) ist dokumentiert?				
e) Sicherheitsvorfälle und deren Gegenmaßnahmen, bzw. daraus abgeleitete Strategien und Schutzmaßnahmen sind dokumentiert?				

Anlage 2: Beispiel-Beurteilung vorhandener Systeme

Bezeichnung der Maschine, Anlage, etc.	Steuerungen					
	Kontakt-behaftete	Elektro-nische	Program-mierbare ohne Netzwerk-verbindung	Programmier-bare mit Netz-werkverbindung, keine Verbin-dung zu über-geordneten Systemen	Programmier-bare mit Netz-werkverbindung, mit Verbindung zu übergeord-neten Systemen	Bemerkungen
Tischbohr-maschine		**X** Keine Maß-nahme erforder-lich				
Presse 12			**X** Maß nahme Siehe DOK ….			Kommunikation mit Maschine 1 und 3
CNC Fräse				**X** Maßnahme siehe DOK ….		
Automatik-Lagerkran					**X** Abstimmung mit Lagerrechner Maßnahme siehe DOK…	Austausch von Lageraufträgen mit Lagerrechner Y

Herausgeber

Deutsche Gesetzliche
Unfallversicherung e.V. (DGUV)

Glinkastraße 40
10117 Berlin
Tel.: 030 13001-0 (Zentrale)
Fax: 030 13001-6132
E-Mail: info@dguv.de
Internet: www.dguv.de

Sachgebiet „Maschinen, Robotik und Fertigungsautomation“
im Fachbereich „Holz und Metall“
der DGUV > www.dguv.de Webcode: d544722

An der Erarbeitung dieser Fachbereich AKTUELL haben mitgewirkt:

- Normenausschuss Maschinenbau (NAM) im DIN Deutsches Institut für Normung e. V
- Referat 5.2 Maschinen und Anlagen des Instituts für Arbeitsschutz der DGUV (IFA)
- Fachbereich ETEM der Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse (BG ETEM)