IT-Sicherheit in der Produktion

Vernetzung von Produktionsanlagen

Es ist eine zunehmende Verknüpfung von einzelnen Komponenten sowie ganzer Produktionsanlagen zu beobachten. Netzwerke ermöglichen die Kommunikation von der Geschäftsleitung bis in die Produktion. Ressourcenplanung, Fertigungssteuerung usw. werden miteinander verknüpft. Dezentrale Fertigungssysteme werden verbunden, Wartungs- und Serviceprozesse erfolgen online. Dies führt zu effektiveren Prozessen (z.B. Berichtswesen, Überwachung und Wartung). Es entstehen aber auch höhere Anforderungen an die Sicherheit.

Sicherheitsrisiko

Während die IT-Sicherheit im Büro mit der Entwicklung von Netzwerken und Internet gewachsen ist, wird sie in der Produktion erst seit kurzem stärker beachtet. Im Büro sind Viren und Schadsoftware weiterhin die größte Gefahr für die Kommunikation und Daten. In der Produktion liegt der Fokus auf der Verfügbarkeit von Informationen. Fallen Steuerungsprozesse aus, steht die Produktion still.

Durch die Vernetzung können sich Bereiche gegenseitig beeinflussen. Liegen zentrale Prozesse vor, schafft dies eine Abhängigkeit zwischen der Geschäfts- und der Produktionsebene. Bei unberechtigten Zugriffen können so Angriffe und Manipulationen erfolgen. Neben fehlenden Softwareaktualisierungen werden diese v.a. durch fehlerhafte Konfiguration verursacht und können zu einem Ausfall von Hard- und Software führen. Einen weiteren Schwachpunkt stellt der Umgang mit vernetzten Produktionsumgebungen und entsprechenden Regelungen dar.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote.
Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter:
www.mittelstand-digital.de

Mittelstand 4.0 – Agentur Prozesse

Die Aufgaben der Mittelstand 4.0-Agentur Prozesse liegen in der Organisation und Durchführung von Workshops und Seminaren, Fachvorträgen und Veranstaltungen, Webinaren und Online-Kursen, Themen- und Arbeitskreisen, interaktiven Planspielen und der Erstellung von Informationsmaterialien zu den Themen:

- Veränderungen in Montageprozessen durch informations- und softwaretechnische Komponenten
- Safety und Security bei der Digitalisierung von Produktionsprozessen (IT-Sicherheit)
- Prozessdatenerfassung und Analyse zur Gestaltung serviceorientierter Geschäftsmodelle

Weitere Informationen finden Sie unter:
www.prozesse-mittelstand.digital

Impressum

Text und Redaktion
Roland Hallau, Mittelstand 4.0-Agentur Prozesse

Herausgeber
Mittelstand 4.0-Agentur Prozesse
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9, 39108 Magdeburg
Tel.: +49 391 74435-20 • Fax: +49 391 74435-11
E-Mail: rhallau@tti-md.de
Geschäftsführer: Dr. Michael Klaeger, Marko Wunderlich
Amtsgericht Stendal, HRB 104429
Umsatzsteuer-Identifikationsnummer: DE 139 310 185

Grafische Konzeption und Gestaltung
toolboxx-media UG (haftungsbeschränkt)

Druckerei
KOCH-DRUCK

Bildnachweis
rvlsoft, sdecoret – Fotolia.com; Kinwun, Zapp2Photo – istock

Magdeburg, Mai 2018

Mittelstand 4.0
Agentur **Prozesse**

IT-Sicherheit in der Produktion

10 Goldene Regeln aus der Praxis

www.prozesse-mittelstand.digital

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

10 Goldene Regeln für die IT-Sicherheit in der Produktion

Digitalisierung der Produktion ja, aber sicher!

Die 10 Goldenen Regeln sollen Ihnen helfen, die Digitalisierung der Produktionsprozesse im Unternehmen sicher zu gestalten. Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Anregungen rund um das Thema IT-Sicherheit finden Sie unter

www.mittelstand-digital.de

Regel 1: Den Zustand der IT-Sicherheit im Unternehmen erfassen
Sowohl für eine erste Bestandsaufnahme als auch für eine kontinuierliche Überprüfung des IT-Sicherheitsniveaus eines Unternehmens gibt es verschiedene Tools im Internet (siehe u.a. **www.bsi.de**). Im Rahmen der Arbeit der Mittelstand 4.0-Agentur Prozesse wurde insbesondere für kleine und mittlere Unternehmen das «Sicherheitstool Mittelstand SiToM» entwickelt. Unternehmen können unter **www.sitom.de** kostenfrei eine erste Ist-Analyse des eigenen IT-Sicherheitsniveaus durchführen und das Ergebnis inkl. möglicher Maßnahmen zum Aufbau bzw. zur Verbesserung der IT-Sicherheit nutzen.

Regel 2: IT-Sicherheit ist Chefsache
Die Geschäftsleitung eines Unternehmens ist nicht nur hauptverantwortlich für die IT-Sicherheit, sondern sie sollte sich auch tatsächlich mit dieser Aufgabe identifizieren. Wird dieses Engagement für die Mitarbeiter deutlich, ist eine wichtige Basis für eine erfolgreiche Umsetzung vorhanden. IT-Sicherheitsziele und Verantwortlichkeiten müssen sowohl für den Office- als auch für den Produktionsbereich klar in einem IT-Sicherheitskonzept zum Ausdruck gebracht werden. Der Aufbau und die Aufrechterhaltung von IT-Sicherheit ist ein kontinuierlicher Prozess und verlangt eine entsprechende Planung von Personal- und Zeitressourcen.

Durch die Geschäftsleitung ist ein IT-Sicherheitsbeauftragter zu benennen, welcher über das notwendige Wissen im Office- und Produktionsbereich verfügen sollte, ggf. muss Unterstützung bei externen Dienstleistern gesucht werden. In Abhängigkeit von der Größe des Unternehmens bzw. des Wissens können auch weitere Mitarbeiter eingebunden werden. Dieses Personal ist dann für die IT-Sicherheit inkl. der Maßnahmen bei Sicherheitsvorfällen verantwortlich.

Regel 3: Mitarbeiter regelmäßig sensibilisieren
Der größte Teil der IT-Sicherheitsvorfälle wird durch Mitarbeiter verursacht. Sind die eigenen Mitarbeiter für das Thema sensibilisiert und mit einem entsprechenden Wissen ausgestattet, ist das ein sehr wesentlicher Beitrag für die IT-Sicherheit. Neue Mitarbeiter müssen umgehend in die vorhandenen Datenschutz- und IT-Sicherheitsbestimmungen eingewiesen werden. Durch regelmäßige Schulungen muss das Wissen auf einem aktuellen Stand gehalten werden. Dabei sind evtl. IT-Sicherheitsvorfälle offen zu diskutieren und so für die Sensibilisierung zu nutzen. Für die Nutzung der Hard- und Software im Unternehmen inkl. der Produktionsbereiche sind Regeln zu definieren. So müssen z.B. alle Mitarbeiter wissen, dass das Aufladen des privaten Smartphones an einem evtl. vorhandenen Anschluss einer Maschine nicht zulässig ist. Schadsoftware könnte so auf die Maschinensteuerung übertragen werden und zu Störungen im Produktionsprozess führen. Weiterhin muss klar geregelt sein, wer für die Aktualisierung von Software verantwortlich ist und wie die Aktualisierung im Einzelnen zu realisieren ist. In Produktionsprozessen ist eine eingestellte automatische Aktualisierung unter Umständen mit einem zu hohen Risiko für einen störungsfreien Produktionsprozess verbunden.

Regel 4: Struktur der IT dokumentieren
Erfassen Sie alle IT-gestützten Prozesse, Anwendungen und relevante Informationen im Unternehmen und dokumentieren Sie diese. Erstellen Sie einen Netzplan von Office- und Produktionsumgebungen inkl. der Kommunikationsverbindungen unter Berücksichtigung der Räumlichkeiten, in dem die IT-Komponenten dargestellt sind. Zwecks Vereinfachung können dabei gleiche oder ähnliche Komponenten gruppiert werden.

Regel 5: Eine detaillierte Risikoanalyse durchführen
Eine Risikoanalyse hilft Ihnen, die richtigen Schutzmaßnahmen zu bestimmen. Identifizieren Sie anhand der Struktur der IT-Umgebung die zu schützenden Werte, insbesondere der Datenbestände und Anwendungen, welche im Unternehmensalltag für einen funktionierenden Betrieb notwendig sind und klassifizieren Sie diese ggf. entsprechend der Wichtigkeit. Dokumentieren Sie dazu auch die Datenflüsse und beziehen Sie den Bereich der Produktion mit ein. Führen Sie in Bezug auf mögliche Schwachstellen sowie auf die sich daraus ableitenden Bedrohungen eine Analyse durch und dokumentieren die Ergebnisse. Ausgehend von diesen Untersuchungen können die optimalen Schutzmaßnahmen definiert werden.

Regel 6: Technische Schutzmaßnahmen umsetzen
Zur Absicherung der Maschinen und Anlagen sollte das Netzwerk der Produktions-IT in einzelne IT-Sicherheitszellen unterteilt werden, die jeweils mit einer Firewall gesichert werden (Netzwerktrennung-/segmentierung). In diesem Zusammenhang muss klar geregelt sein, welche Komponenten wie miteinander kommunizieren dürfen. Im günstigsten Fall ist jede Maschine bzw. Anlage durch eine separate Firewall geschützt.

Regel 7: Fernwartung kontrollieren
Der externe Zugriff auf die Produktions-IT ist ein besonders kritischer Vorgang. Ein Zugriff sollte deshalb nur über sichere Verbindungen (VPN) und Protokolle (z.B. IPsec, SSH, SSL) gezielt auf eine ausgewählte Komponente erfolgen, d.h. kein pauschaler Zugriff auf größere Netzbereiche. Dabei ist ein Verbindungsaufbau von innen nach außen empfehlenswert, so dass Sie auch hier die Kontrolle haben. Weitere wichtige Aspekte sind gute Passwörter, sichere Authentifizierungsverfahren, Verschlüsselung der Daten und die Definition von Zeitfenstern für den Zugriff.

Regel 8: Notfallmanagement einrichten
Insbesondere in einer Produktionsumgebung sind schnelle und effiziente Reaktionen auf Störungen und Ausfälle von hoher Bedeutung, damit ein Produktionsprozess zeitnah wiederaufgenommen werden kann. Es muss festgelegt und dokumentiert werden, welche Vorfälle an wen zu melden sind. Definieren Sie notwendige Maßnahmen und erstellen Sie Wiederanlaufpläne, auf die auch ohne IT-Systeme zugegriffen werden kann. Vergessen Sie nach der Wiederherstellung des ordnungsgemäßen Betriebes nicht die Untersuchung der Ursachen und eine entsprechende Dokumentation sowie Auswertung bzw. Nachbereitung des Vorfalls.

Regel 9: Zugriffsschutz organisieren
In der Produktions-IT ist es besonders wichtig, nur den berechtigten Personen Zugriff auf die Anlagen, Steuerungssysteme und Daten zu gewähren. Unbewusstes Fehlverhalten oder eine gezielte Manipulation können hier einen enormen Schaden zur Folge haben. Es ist also ein gutes Berechtigungs- und Passwortmanagement notwendig. Darüber hinaus müssen auch die Zugänge bzw. Schnittstellen (z.B. USB, LAN, WLAN) vor unerlaubten Missbrauch abgesichert werden.

Regel 10: Monitoring erstellen und betreiben
Auch unter Beachtung des Notfallmanagements sollten Sie in der Produktions-IT ein entsprechendes Monitoring durchführen. Das Monitoring der IT-Infrastruktur in Produktionsumgebungen hilft Ihnen, IT-Sicherheitsprobleme und deren Ursachen zeitnah zu erkennen. Dabei darf die Produktion jedoch nicht gestört oder verlangsamt werden. Prüfen Sie, welche Prozesse Sie in welchem Umfang protokollieren bzw. in Logfiles aufzeichnen können. Durch eine Datenauswertung und Mustererkennung können Vorfälle bzw. auch Angriffe ggf. erkannt und Maßnahmen ergriffen werden.

Weitere Informationen finden Sie unter nebenstehendem QR-Code oder unter: **www.prozesse-mittelstand.digital**