Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

IT-Sicherheit in Produktions-anlagen

ROLAND HALLAU

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

GESTALTUNG UND PRODUKTION
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL Roland Hallau (generiert mit Chat GPT)

VERÖFFENTLICHUNG November 2025

© Roland Hallau (generiert mit ChatGPT)

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 effizienteren 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

TIPP 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). Insbesondere für kleine und mittlere Unternehmen wurde der CYBERsicher Check entwickelt. Unternehmen können unter https://cybersicher-check.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.

TIPP 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 Mitarbeitenden 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 Mitarbeitende eingebunden werden. Dieses Personal ist dann für die IT-Sicherheit inkl. der Maßnahmen bei Sicherheitsvorfällen verantwortlich.

TIPP 3: MITARBEITENDE REGELMÄSSIG SENSIBILISIEREN

Der größte Teil der IT-Sicherheitsvorfälle wird durch Mitarbeitende verursacht. Sind die eigenen Mitarbeitenden für das Thema sensibilisiert und mit einem entsprechenden Wissen ausgestattet, ist das ein sehr wesentlicher Beitrag für die IT-Sicherheit. Neue Mitarbeitende 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 Mitarbeitenden 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.

TIPP 4: STRUKTUR DER IT DOKUMENTIEREN

Erfassen Sie im Unternehmen alle IT-gestützten Prozesse, Anwendungen und relevante Informationen 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.

TIPP 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 Sie die Ergebnisse. Ausgehend von diesen Untersuchungen können die optimalen Schutzmaßnahmen definiert werden.

TIPP 6: VERHINDERN SIE EINE WEITERE AUSBREITUNG

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.

TIPP 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 externen Zugriff.

TIPP 8: NOTFALLMANAGEMENT EINRICHTEN

Insbesondere in einer Produktionsumgebung sind schnelle und effiziente Reaktionen auf Störungen und Ausfälle von hoher Bedeutung, damit ein Produktionsprozess zeitnah wieder aufgenommen 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 die Auswertung bzw. Nachbereitung des Vorfalls.

TIPP 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 unerlaubtem Missbrauch abgesichert werden.

TIPP 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.

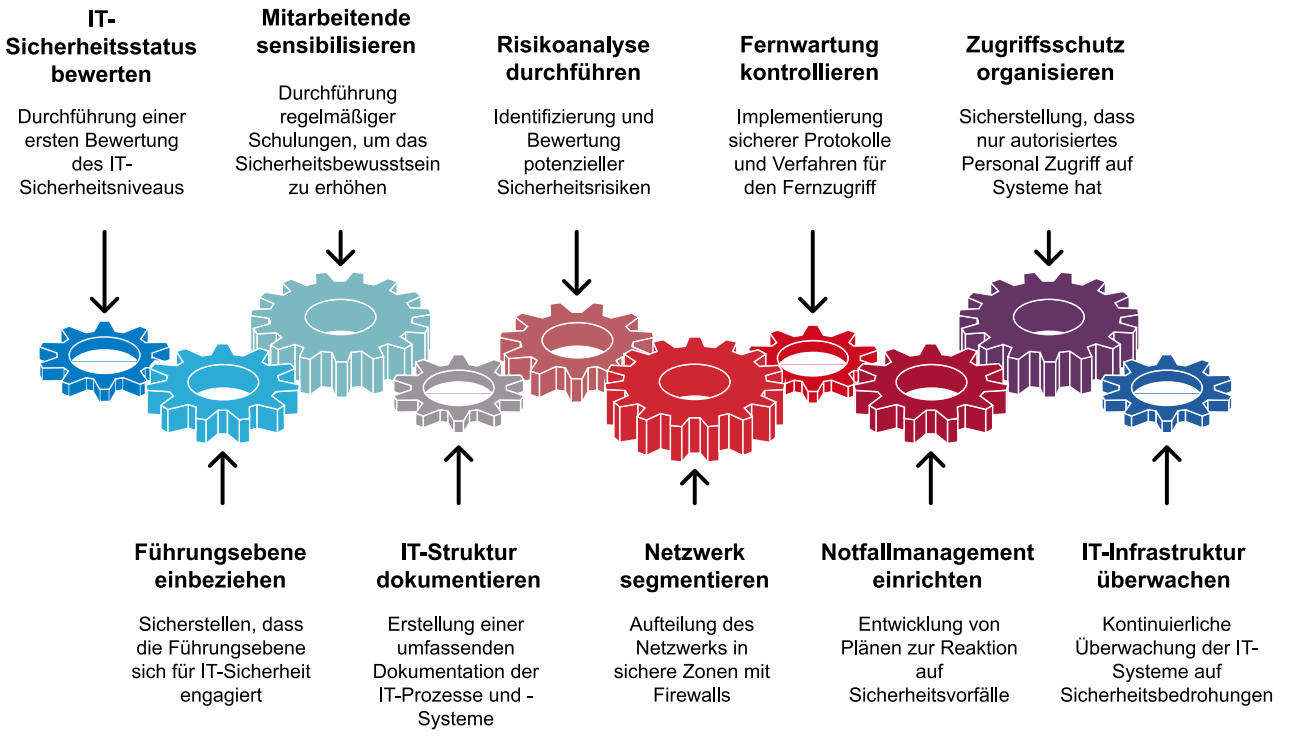

Abbildung 1: 10 Schritte für mehr IT-Sicherheit in der Produktion

Weiterführende Informationen

1. Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Home/home_node.html
2. Cybersicher Check https://cybersicher-check.de/

Verfasst von

ROLAND HALLAU ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er als Fachkoordinator im Bereich IT-Sicherheit tätig..
roland.hallau@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages