Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

# IT-Sicherheit in Unternehmen: 10 Tipps für den Basisschutz

ROLAND HALLAU


Mittelstand-Digital

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

# Impressum

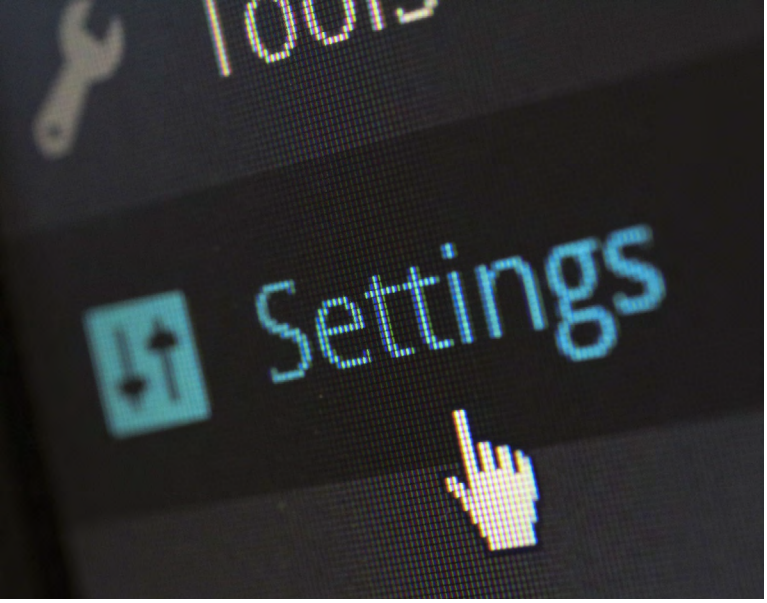
**HERAUSGEBER**
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

**REDAKTION** Diana Falke

**GESTALTUNG**
PUNKT191 – Marketing und Design
www.punkt191.de

**BILDNACHWEIS TITEL**
sdecoret – Fotolia.com

**VERÖFFENTLICHUNG** November 2022




© Pixabay on Pexels.com

Fast täglich berichten die Medien über Cyberangriffe – Datenbestände werden gestohlen oder verschlüsselt, die Betroffenen daraufhin erpresst, Prozessabläufe manipuliert oder ganz stillgelegt. Dabei sind sowohl Unternehmen als auch alle sonstigen wirtschaftlichen oder öffentlichen Organisationen Opfer solcher Angriffe. Diese Aktivitäten der Cyberkriminellen sind nur die eine Seite. Ebenfalls müssen Ausfälle von Hardware bzw. der allgemeinen IT-Infrastruktur, Bedienfehler und menschliches Versagen u.v.m. betrachtet werden. Im Grunde geht es darum, dass die Unternehmen auf Vorfälle, die zu massiven Störungen in den Arbeitsprozessen oder gar zu einem Totalausfall der unterstützenden IT-Infrastruktur führen, vorbereitet sind.

In diesem *Nachgelesen* haben wir ausgehend von den IT-Sicherheitsschutzzielen Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität (VIVA-Prinzip) die wichtigsten Maßnahmen und Regelungen zusammengestellt, wie sich ein Unternehmen schützen und gleichzeitig auf einen Sicherheitsvorfall vorbereiten sollte.

## Tipp 1: Verantwortlichkeiten festlegen

In jedem Unternehmen sollte für die IT-Sicherheit mindestens eine verantwortliche Person einschließlich einer Vertretung festgelegt werden. Für die Bewältigung der Folgen eines Sicherheitsvorfalles kann zusätzlich ein Notfallmanager eingesetzt werden.

## Tipp 2: Ressourcenplanung

Die Geschäftsleitung muss gemeinsam mit dem IT-Verantwortlichen anhand der zur Verfügung stehenden fachlichen und zeitlichen Ressourcen im eigenen Unternehmen definieren, welche konkreten Leistungen bei einem Sicherheitsvorfall durch das eigene Personal erbracht werden können. Die Leistungen eines IT-Dienstleisters sollten in einem IT-Instandhaltungsvertrag geregelt werden. Insbesondere ist hier bei einem eingetretenen Sicherheitsvorfall die festgelegte Reaktionszeit von hoher Bedeutung.

## Tipp 3: Datensicherung

Nach Sicherheitsvorfällen geht es in erster Linie meistens darum, dass die eigenen Daten schnellstmöglich wiederhergestellt werden. Diese Datenbestände sind Grundlage für die Geschäftstätigkeit der meisten Unternehmen. Deshalb müssen auf jeden Fall die Daten gesichert werden, die selbst erzeugt wurden. Dazu zählen alle Daten, die durch Anwendungsprogramme (z. B. Textverarbeitung, Tabellenkalkulation, Präsentation, E-Mail, Rechnungswesen, Konstruktion, Lager und Finanzen) erstellt wurden. Ebenfalls gehören jene Daten dazu, die im Rahmen der Geschäftsbeziehungen mit Kunden (z. B. Artikeldaten, Preisangaben, Informationen zu den Angeboten und zum Auftrag) entstanden sind. Weiterhin ist es wichtig, dass auch produktionsspezifische Daten (etwa Auftrags- und Prozessdaten, Maschinenprogramme wie z. B. für die Steuerung von CNC-Maschinen) gesichert werden.

## Tipp 4: Passwörter und Authentifizierung

Im Zusammenhang mit der Authentifizierung bei der Anmeldung an Hard- und Softwaresystemen bzw. mit dem allgemeinen Einsatz von Passwörtern sollte in den Unternehmen eine regelmäßige Kontrolle durchgeführt werden, ob alle Systeme einen hinreichenden Zugangsschutz aufweisen und ob die verwendeten Standards den aktuellen Anforderungen genügen sowie ggf. auch eine Zwei-Faktor-Authentifizierung zum Einsatz kommen kann. Insbesondere ist hier ein periodischer Check (Leak-Check) aller dienstlichen E-Mail-Adressen hinsichtlich eines evtl. Identitätsdiebstahls empfehlenswert. Dazu können verschiedene Tools eingesetzt werden. (siehe Links)

## Tipp 5: Mobiles Arbeiten und Nutzung mobiler Endgeräte

Im Homeoffice oder beim mobilen Arbeiten müssen insbesondere Maßnahmen für den Zugriffs- und Zugangsschutz auf Daten und Geräte, für eine sichere Kommunikation (VPN, remote), für die Datensicherung sowie dem allgemeinen Umgang mit vertraulichen Unterlagen bzw. Informationen

definiert und umgesetzt werden. Beim Einsatz mobiler Endgeräte, wie Smartphones und Tablets, muss neben einem Basisschutz gegen Viren und Trojaner ein wirksamer Zugangsschutz (PIN, Passwort oder eine biometrische Lösung) eingerichtet sein, so dass die Unternehmensdaten geschützt sind. Für den Fall, dass Geräte verloren gehen, sollte ein Fernzugriff eingerichtet werden. Verschiedene Software-Tools bieten die Möglichkeit, dass der rechtmäßige Besitzer aus der Ferne Daten kopiert, löscht oder den Standort des Smartphones oder Tablets ermittelt.

## Tipp 6: Berechtigungskonzept

In jedem Unternehmen sollten die Zugriffsberechtigungen auf Hard- und Softwaresysteme sowie auf Datenbestände in einem Konzept definiert und ggf. im Rahmen eines Passwortmanagements umgesetzt werden. Dabei sind auch Produktionsbereiche sowie Fernzugriffe jeglicher Art zu berücksichtigen.

## Tipp 7: Dokumentation und Notfallplan

Eine gute, aktuelle Dokumentation der IT-Infrastruktur ist nicht nur für die laufenden Service- und Wartungsarbeiten sinnvoll, sondern insbesondere bei einem Sicherheitsvorfall sehr hilfreich. Müssen nach einem Vorfall Systeme und/oder Daten wiederhergestellt werden, sollte auch ein entsprechender Notfallplan in einem Unternehmen vorhanden sein. Ein Notfallhandbuch umfasst alle relevanten Dokumente, aus denen sich die notwendigen Maßnahmen und Handlungsanweisungen für eine entsprechende Wiederherstellung ableiten lassen. Dies beinhaltet vor allem Kontaktdaten relevanter Ansprechpartner, Dokumentationen der IT-Komponenten sowie Infrastruktur und Wiederanlaufpläne für IT-Komponenten.

## Tipp 8: Schutzsoftware

Im Sinne einer Prävention sollte in jedem Unternehmen mindestens eine Firewall als Absicherung gegenüber den Bedrohungen aus dem Internet eingerichtet sein. Weiterhin sollten alle Server- und Clientsysteme mit einem aktuellen Antivirensystem ausgestattet sein. Darüber hinaus ist es sinnvoll, die vorhandenen Hard- und Softwaresysteme im Netzwerk des Unternehmens dauerhaft zu überwachen und periodisch auf Schwachstellen zu überprüfen. Sowohl für die Analysen als auch für das Monitoring bzw. Überwachung gibt es hier zahlreiche Tools. (siehe Links)

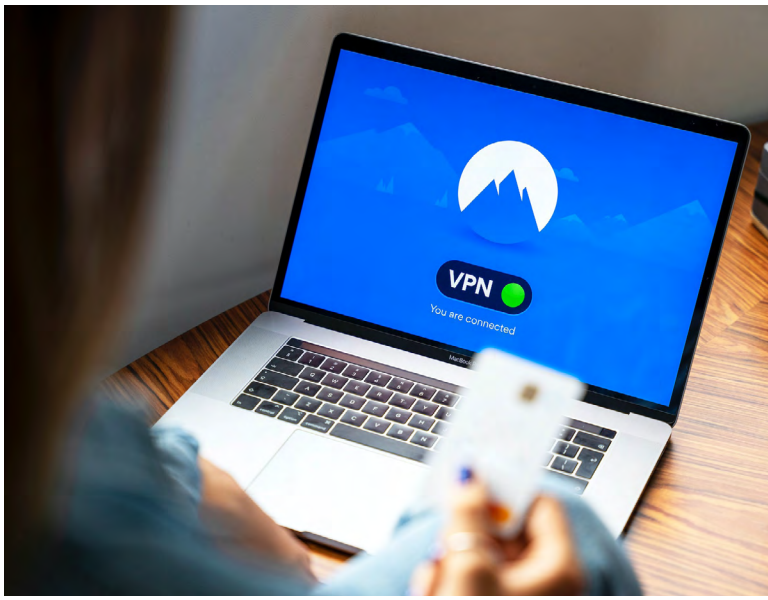
## Tipp 9: Schulung des Personals

Der Mensch wird beim Thema IT-Sicherheit oft als schwächstes, aber gleichzeitig als wichtiges Glied gesehen. Das grundlegende Verhalten von Mitarbeitenden wird dabei durch das Zusammenspiel aus Motivation, Wissen und Anlässen geprägt. Die Risiken in Bezug auf die IT-Sicherheit resultieren oft aus Unwissen. Phishing-Mails sind dafür ein gutes Beispiel. Das Personal muss hier durch eine Wissensvermittlung in die Lage versetzt werden, diese Art der E-Mails zu erkennen und entsprechend zu reagieren. Sensibilisierte und gut geschulte Mitarbeiter:innen haben einen wesentlichen Anteil am IT-Sicherheitsniveau in den Unternehmen.

## Tipp 10: Aktuelle Hard- und Softwaresysteme

Im Zusammenhang mit den Bedrohungen durch mögliche Cyberangriffe stellen veraltete Hard- und Softwaresysteme bzw. fehlende Sicherheitsupdates und Firmware-Aktualisierungen ein besonders hohes Risiko dar. Die Unternehmen sollten hier entsprechende Maßnahmen umsetzen, die für regelmäßige und nach Möglichkeit automatisierte Updates bei den Systemen sorgen bzw. ein sogenanntes Update- und Patch-Management einführen. Auch für diesen Bereich gibt es zahlreiche Tools, die diese Aufgaben unterstützen können. (siehe Links)





# Links mit weiterführenden Inhalten

**ALLGEMEINES**

- Selbsteinschätzung zum vorhandenen IT-Sicherheitsniveau: https://www.SiToM.de
- Feststellung des IT-Sicherheitsbedarfes: https://sec-o-mat.de
- https://www.secion.de/de/blog/blog-details/bsi-lagebericht-zur-cybersicherheit-2021-bedrohungslage-angespannt-bis-kritisch
- https://www.av-test.org

**CHECK VON E-MAIL-KONTEN**

- https://sec.hpi.de/ilc/search?lang=de
- https://haveibeenpwned.com
- https://monitor.firefox.com

**TOOLS FÜR SICHERE NETZWERKE**

- https://www.heise.de/download/products/netzwerk/monitoring#?cat=netzwerk%2Fmonitoring
- https://network-king.net/de/besten-netzwerkueberwachungstools/
- https://www.security-insider.de/die-besten-quelloffenen-schwachstellen-scanner-a-1072103/
- https://www.dnsstuff.com/de/network-vulnerability-schwachstellen-scanner
- https://www.dnsstuff.com/de/patch-management-verwaltung-software

**DATENSICHERUNG**

- https://digitalzentrum-chemnitz.de/wissen/unternehmensdaten-schuetzen

**SCHUTZSCHILD MENSCH**

- https://digitalzentrum-chemnitz.de/wissen/schutzschild-mensch/

# Autor

**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 Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

**WAS IST MITTELSTAND-DIGITAL?**

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt 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 Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages