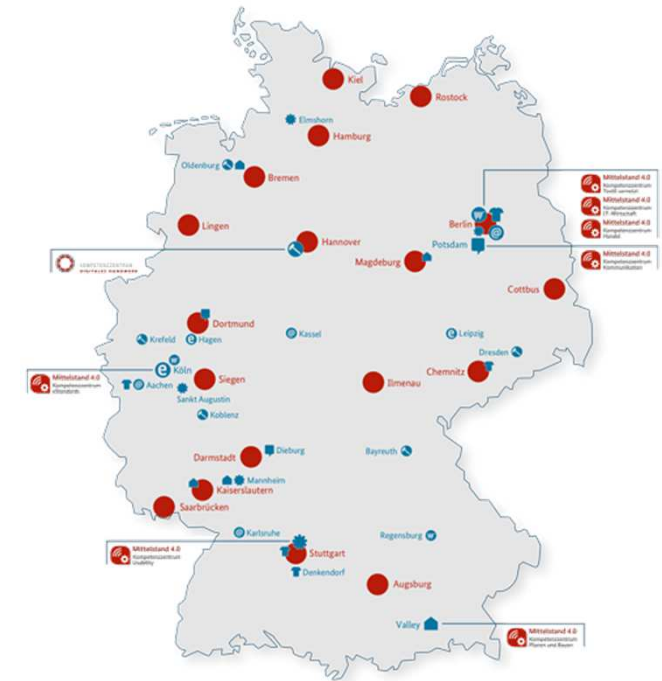


IT-Sicherheit in 30 Minuten Sichere Netzwerke

Roland Hallau
Mittelstand-Digital Zentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

Mittelstand-Digital Zentrum Chemnitz

- als Teil von Mittelstand-Digital unterstützen wir KMU und Handwerk bei der Digitalisierung
- der Mensch im Mittelpunkt - als Befähiger digitaler Produktions- und Arbeitswelten
- Expertise u.a. in den Bereichen Geschäftsmodell-Entwicklung, Produktion und Logistik, IT-Sicherheit und Datenschutz, Recht und Produktgestaltung



Mittelstand-Digital Zentrum Chemnitz

Kooperationspartner IHK Magdeburg und HWK Magdeburg



- **Annett Gröger-Rost**
Digitalisierungsberaterin
Tel: +49 391 5693-154
E-Mail: annett.groeger-rost@magdeburg.ihk.de



- **Karsten Gäde**
Betriebsberater
Tel: +49 391 6268-212
E-Mail: kgaede@hwk-magdeburg.de

IHK und HWK Magdeburg - Gemeinsame Angebote und Themen

- Wettbewerb „Digitale Erfolgsgeschichten aus Sachsen-Anhalt“
 - Bewerbungsschluss: 25. April 2022 - <https://digitale-erfolgsgeschichten-sachsen-anhalt.de>

- Monatliche Digitalisierungssprechstunde
 - gemeinsam mit der IHK Magdeburg, Handwerkskammer Magdeburg und Mittelstand 4.0-Kompetenzzentrum Magdeburg
 - **nächste Sprechstunde: 21.04.2022 von 09:00 – 13:00 Uhr**

IHK und HWK Magdeburg - Gemeinsame Angebote und Themen

→ Veranstaltungen

- **20.04.2022 Workshop: Vertrieb - Der Verkauf von Emotionen**
- **24.06.2022 Moderne & digitale Fachkräftegewinnung mit regionalen Best-Practises**
- **24.06.2022 3. Digitale Konferenz der Wirtschaft Sachsen-Anhalts**

- **Monatliche Workshops** aus der Reihe „*Pflanze und Ernte*“ für eine erfolgreiche Unternehmensführung
20.04.2022 von 10:00 – 12:00 Uhr: Vertrieb: Der Verkauf von Emotionen
- **Veranstaltungsreihe „Digital.Nachhaltig.Erfolgreich“** über nachhaltiges Wirtschaften im Unternehmen durch die Digitalisierung mit vielen Beispielen aus der Praxis

Detaillierte Informationen und Anmeldemöglichkeiten sind in den Veranstaltungskalendern der IHK Magdeburg und der HWK Magdeburg zu entnehmen.

IHK und HWK Magdeburg - Gemeinsame Angebote und Themen

→ Gemeinsame Themen, wie IT-Sicherheit im Mittelstand

→ IHK Magdeburg und HWK Magdeburg sind regionale Anlaufstellen der Transferstelle für IT-Sicherheit im Mittelstand (TISiM)

→ TISiM unterstützt mit dem Sec-o-Mat die Unternehmen bei der Erstellung eines Aktionsplanes, um die IT-Sicherheit im Unternehmen zu erhöhen.

→ Wie funktioniert der Sec-o-Mat?
Fragen aus Ihrem Unternehmen beantworten.



Übersicht zum konkreten Sicherheitsbedarf mit konkreten Handlungsempfehlungen



Sichere Netzwerke

Netzwerkgeräte - Verbindung mit dem Internet

- Einbindung von Netzwerkkomponenten in das Internet stark zunehmend (Industrie/Wirtschaft 4.0, digitale Transformation)
- Systeme sichtbar für Suchmaschinen

Shodan

- <https://shodan.io>

Censys

- <https://censys.io>

Thingful

- <https://www.thingful.net>

Google

- <https://www.google.de>

Beispiel: Einsatz von industriellen Steuerungen

Top 10 Bedrohungen nach Bundesamt für Sicherheit in der Informationstechnik

Nr.	Top 10 - 2019	Top 10 - 2018
1.	Einschleusen von Schadcode über Wechseldatenträger / externe Hardware	Unberechtigte Nutzung von Fernwartungszugängen
2.	Infektion mit Schadsoftware über Internet und Intranet	Online-Angriff über Office-/Enterprise-Netze
3.	Menschliches Fehlverhalten und Sabotage	Angriff auf eingesetzte Standardkomponenten im ICS-Netz
4.	Kompromittierung von Extranet und Cloud-Komponenten	(D)DoS Angriffe
5.	Social Engineering and Phishing	Menschliches Fehlverhalten und Sabotage
6.	(D)DoS Angriffe	Einschleusen von Schadcode über Wechseldatenträger / externe Hardware
7.	mit dem Internet verbundene Steuerkomponenten	Lesen und Schreiben von Nachrichten im ICS-Netz
8.	Einbruch in Fernwartungszugänge	Unberechtigter Zugriff auf Ressourcen
9.	Technisches Fehlverhalten und höhere Gewalt	Angriffe auf Netzwerkkomponenten
10.	Kompromittierung von Smartphones im Produktionsumfeld	Technisches Fehlverhalten und höhere Gewalt

Quelle 18.03.2019: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/ /downloads/BSI-CS_005.pdf%3bisessionid=31D99F123864924D07605528E1B40837.2_cid369?_blob=publicationFile&v=4

Auswirkungen beim Eintreten von Bedrohungen

Folgen eines mangelhaften technischen und organisatorischen Schutzes

Beispiel: Netzwerkbereich der Produktion

- Produktionsausfall
- Manipulation der Produktqualität
- Verlust von marktbeeinflussendem Firmenwissen
- Schäden an Maschinen und Anlagen
- Auswirkungen auf die Arbeitssicherheit
- Folgeschäden / -angriffe



Quelle: Online Security and Hacking Alert © Anna (Fotolia)

Erhöhung der IT-Sicherheit

Kombination von technischen und organisatorischen Maßnahmen

Beispiel: Netzwerkbereich der Produktion

- Struktur der Produktions-IT dokumentieren
- Mitarbeiter regelmäßig sensibilisieren
- Technische Schutzmaßnahmen umsetzen
- Notfallmanagement einrichten
- Zugriffsschutz organisieren
- Monitoring durchführen



Quelle: <https://betrieb-machen.de/download/9761>

Maßnahmen zur Erhöhung der IT-Sicherheit

Schutz vor dem Einschleusen von Schadcode über Wechseldatenträger/externe Hardware

Hintergrund

USB-Sticks werden privat genutzt und dort infiziert

Wartungslaptops werden in anderen Netzen eingesetzt und dort infiziert

mögliche Maßnahmen

physischer Schutz verhindert Nutzung von USB-Sticks

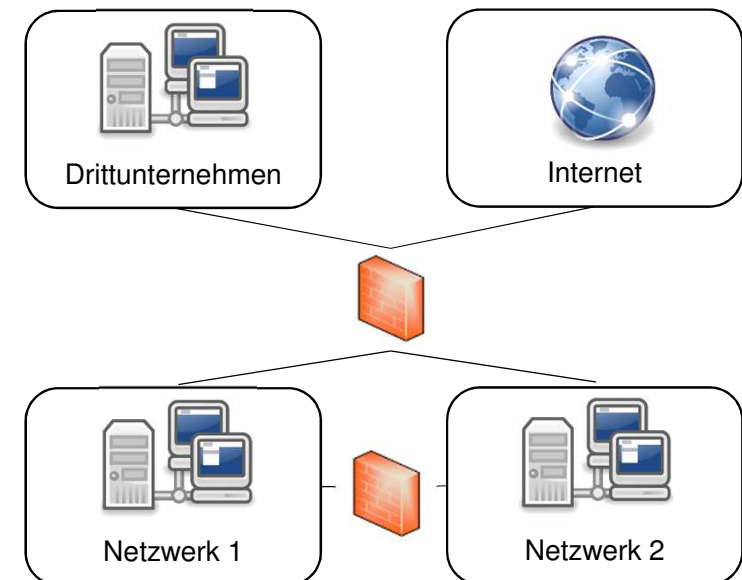
detaillierte Prüfung vor Einsatz im Unternehmen

Verbot der Nutzung der Hardware außerhalb des Produktionsnetzwerks

Maßnahmen zur Erhöhung der IT-Sicherheit

Wie lassen sich Netzwerke abschotten?

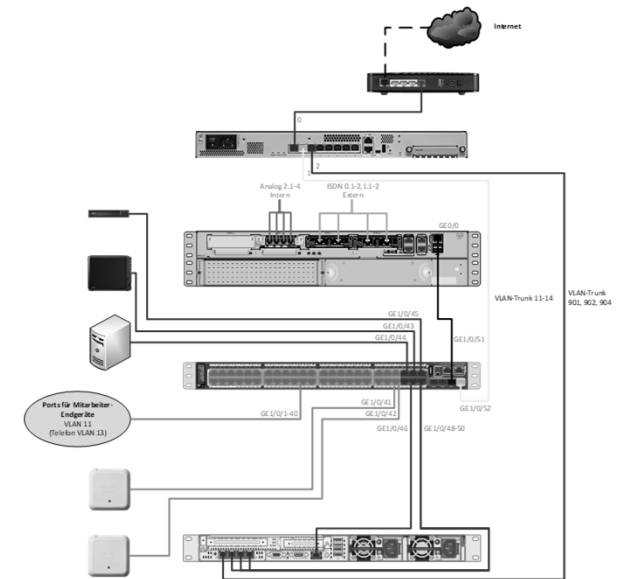
- Trennung von Office- und Produktionsnetzwerken
 - Netzwerksegmentierung
 - Demilitarisierte Zonen DMZ
- keine direkte Internetverbindung durch zusätzliche Schutzmaßnahmen
 - Firewalls und/oder Gateways
- regelmäßige Überwachung und Updates
 - Monitoring
 - Updatemanagement



Maßnahmen zur Erhöhung der IT-Sicherheit

Automatische Schwachstellenscanner als Teil des Update-Managements

- Überprüfung von Netzwerkstrukturen
 - Einbindung in eigene Umgebungen
 - Einrichtung über Weboberfläche
- Identifikation möglicher Schwachstellen
 - Prüfung auf Angriffsmöglichkeiten
 - Abgleich mit CVE-Datenbanken
- Management der Schwachstellen
 - Anpassung der Netzwerkstrukturen
 - Updates und Überwachung



Maßnahmen zur Erhöhung der IT-Sicherheit

Schwachstellen – Datenbanken als Informationsquelle

National Vulnerability Database - NIST

- <https://web.nvd.nist.gov/view/vuln/search>

CVE Details – MITRE

- <http://www.cvedetails.com>

Exploit-Database

- <https://www.exploit-db.com>

Datenbank für Angriffsanalysen des Hasso-Plattner-Instituts

- <https://hpi-vdb.de/vulndb>

ICS-CERT ICS-Cyber Emergency Response Team (NCCIC)

- <https://ics-cert.us-cert.gov>

Maßnahmen zur Erhöhung der IT-Sicherheit

Verhinderung des Missbrauchs von Fernwartungszugängen

Hintergrund

dauerhaft offene Fernwartungszugänge

Nutzung von Standardpasswörtern

direkter Zugang zu hochsensiblen Steuerungen

mögliche Maßnahmen

nutzerindividuelle Authentifizierung und Autorisierung

Einrichtung von Zugriffszeitpunkten für Fernwartung

weitere technische Maßnahmen (z.B. Firewall)

Maßnahmen zur Erhöhung der IT-Sicherheit

Zertifizierung nach IT-Sicherheitsstandards

- Zertifizierung als Teil des systematische Vorgehen zur Identifizierung und Umsetzung von Sicherheitsmaßnahmen
- Internationale Organisation für Normung
 - ISO 62.443, 27.000/27.001
- Bundesamt für Sicherheit in der Informationstechnik
 - BSI Grundschutz
- Automobilindustrie
 - Trusted Information Security Assessment Exchange TISAX



Wo steht mein Unternehmen in Bezug auf IT-Sicherheit?

Erstanalyse als IT-Sicherheitscheck mit dem Sicherheitstool Mittelstand SiToM

- Anwendung des Sicherheitstools Mittelstand unter <https://www.sitom.de>
- Selbstanalyse des IT-Sicherheitsniveaus im Unternehmen
- Empfehlungen geeigneter Maßnahmen zur Steigerung des IT-Sicherheitsniveaus im Unternehmen

Das Sicherheitstool-Mittelstand ist ein effektives Werkzeug, um den Status der IT-Sicherheit in Ihrem Unternehmen zu erfassen, zu bewerten und durch die Umsetzung vorgeschlagener Maßnahmen zu verbessern.

Mittelstand-Digital Zentrum Chemnitz

Projekt anlegen

Projekt laden

Mittelstand-Digital

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

Vielen Dank

für Ihre Aufmerksamkeit!

Mittelstand-Digital Zentrum Chemnitz

c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9
39108 Magdeburg

Roland Hallau
0391 74435-24
rhallau@tti-md.de

Andreas Neuenfels
0391 74435-23
aneuenfels@tti-md.de

David Wagner
0391 74435-28
dwagner@tti-md.de

Mike Wäsche
0391 74435-34
mwaesche@tti-md.de