Mittelstand-Digital
Zentrum
Chemnitz

IT-Sicherheit in 30 Minuten

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

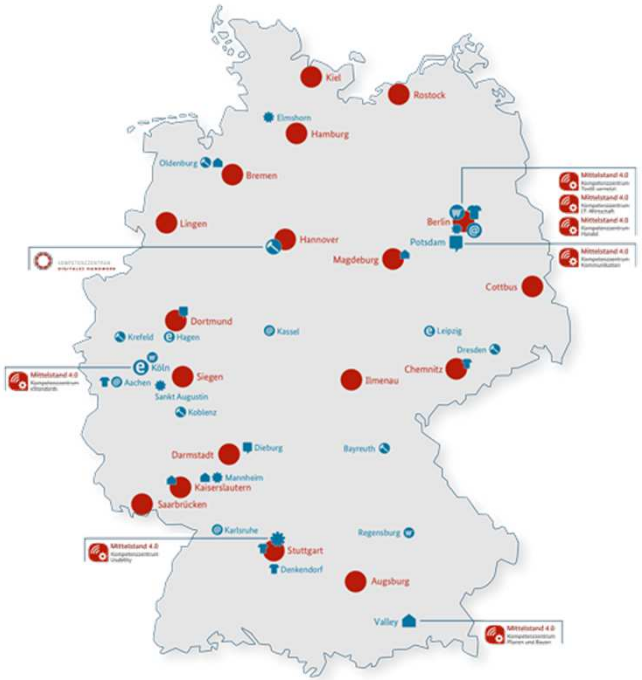
Mittelstand-
Digital

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

Mittelstand-Digital
Zentrum
Chemnitz

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



Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

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

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

Mittelstand-Digital Zentrum Chemnitz

Beispiel: Einsatz vernetzter 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%3bjsessionid=31D99F123864924D07605528E1B40837.2_cid369?__blob=publicationFile&v=4

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

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)

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

Mittelstand-Digital
Zentrum
Chemnitz

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

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

Mittelstand-Digital
Zentrum
Chemnitz

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

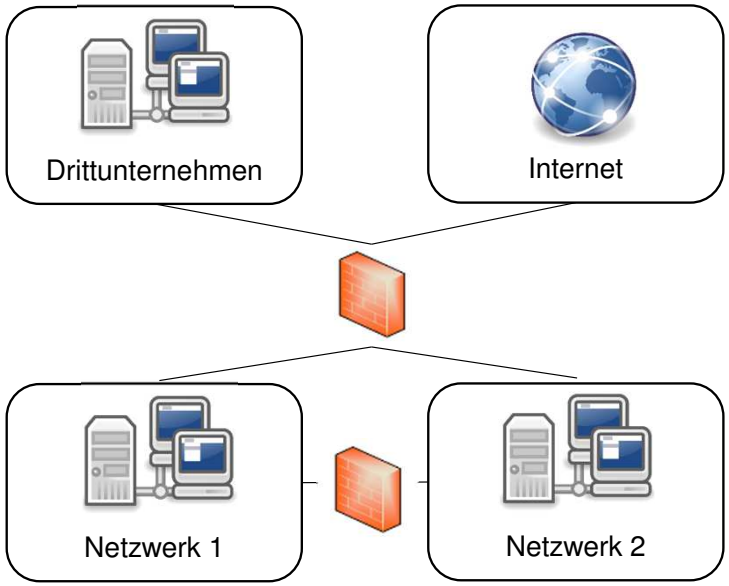
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

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 Schutzmaßnamen
  - Firewalls und/oder Gateways
- regelmäßige Überwachung und Updates
  - Monitoring
  - Updatemanagement



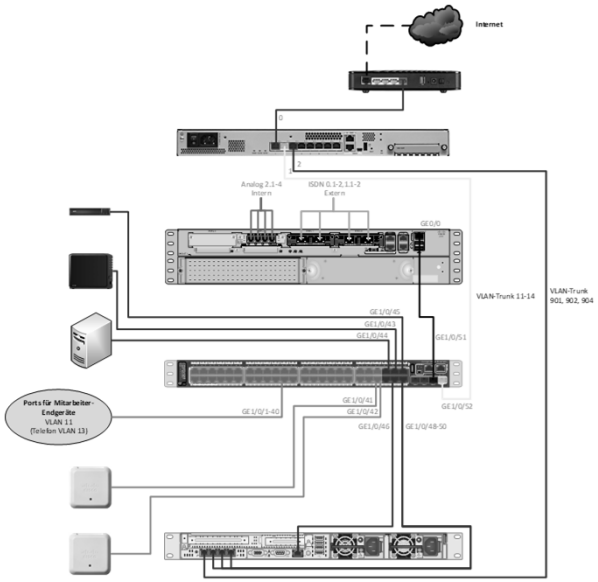
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

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



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

Mittelstand-Digital Zentrum Chemnitz

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

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

Mittelstand-Digital
Zentrum
Chemnitz

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)

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

Mittelstand-Digital
Zentrum
Chemnitz

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

ISO

Bundesamt
für Sicherheit in der
Informationstechnik

TISAX®

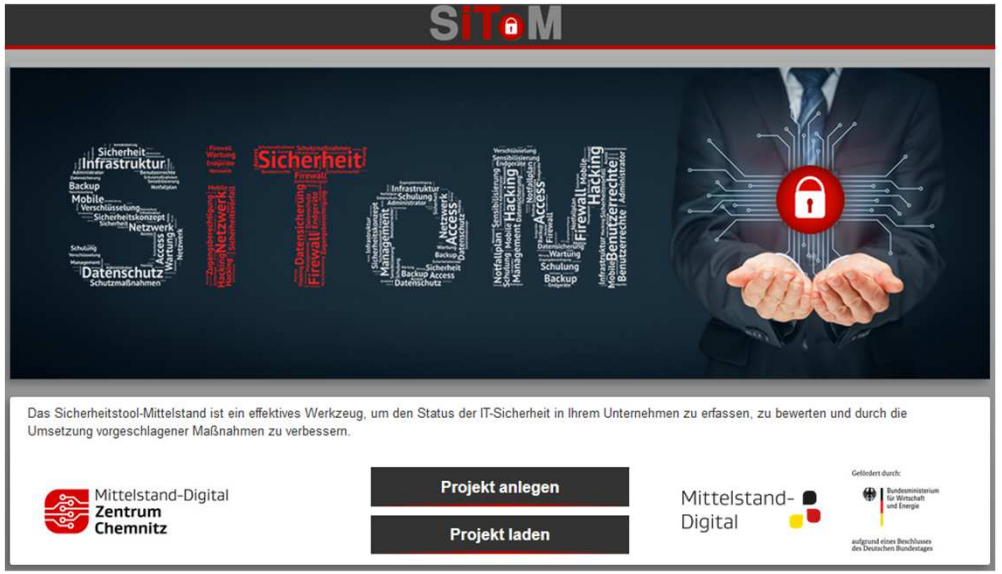
Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

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 oder www.check-it-sicherheit.de (Quick-Check)
- Selbstanalyse des IT-Sicherheitsniveaus im Unternehmen
- Empfehlungen geeigneter Maßnahmen zur Steigerung des IT-Sicherheitsniveaus im Unternehmen



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

Mittelstand-Digital
Zentrum
Chemnitz

VIELEN DANK

für Ihre Aufmerksamkeit!

Mittelstand-
Digital

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

Mittelstand-Digital
Zentrum
Chemnitz

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

Mittelstand-Digital

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