Mittelstand-Digital Zentrum Chemnitz

IT-Sicherheit in 30 Minuten
Schutzschild Mensch

Andreas Neuenfels
Mittelstand-Digital Zentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

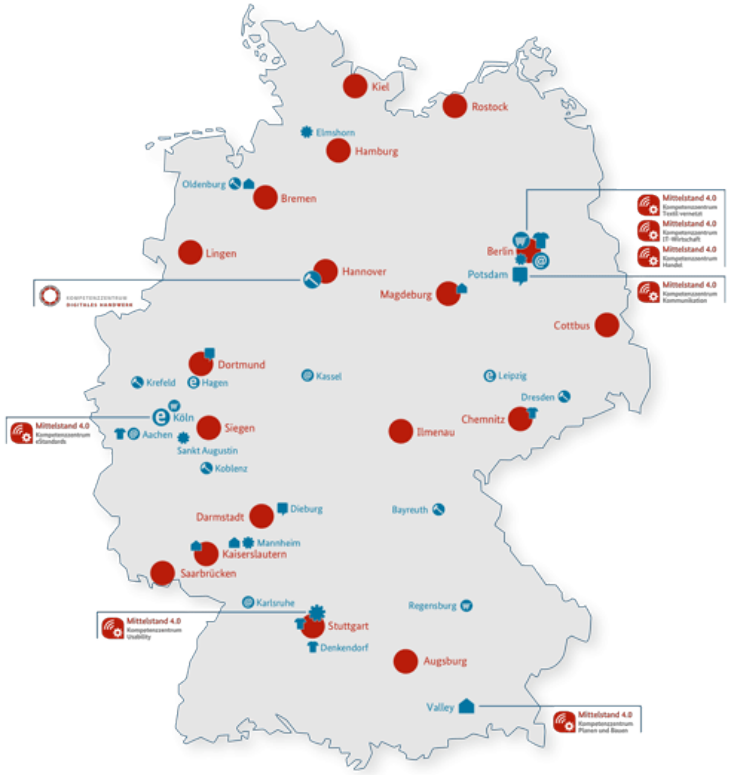
Mittelstand-Digital

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

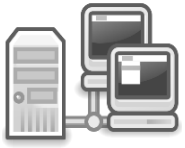
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Der Mensch & IT-Sicherheit

Ein Überblick

Umgang mit Informationen, Daten und Dokumenten



Benutzung von IKT - Geräten

Kommunikation mit anderen (soziales Wesen)

Optimierung von Arbeitsvorgängen

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Menschen als (Un-)Sicherheitsfaktor

Angriffsvektoren

Eigenes Verhalten

- Mobile Endgeräte & Schnittstellen
- Nutzung von Standard-Passwörtern
- Unachtsamkeit & „Work-Arounds“
- Sabotage

Social Engineering

- Manipulation der Mitarbeiter zur Informationsgewinnung
- Phishing, Spear-Phishing, CEO-Fraud
- Baiting (Ködern), Tailgating (Durchschlüpfen)

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

Mittelstand-Digital Zentrum Chemnitz

Menschen als (Un-)Sicherheitsfaktor bei Industrie-PCs

Top 10 Bedrohungen nach Bundesamt für Sicherheit in der Informationstechnik

Nr.	Top 10 - 2022	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 31.05.2022: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html?nn=128730

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Menschen als (Un-)Sicherheitsfaktor

Beispiele

19.09.2019

Unsicher konfigurierte Server leaken Daten von Millionen Patienten

Weltweit hätte im Grunde jedermann auf medizinische Daten wie Röntgenaufnahmen zugreifen können. Betroffen sind auch Patienten aus Deutschland. Zur Meldung

Falsch konfiguriert: Tausende Google-Kalender offen zugänglich

Weil Tausende Nutzer ihre Google-Kalender zu leichtsinnig konfigurieren, sind diese öffentlich zugänglich. Ein Sicherheitsexperte fand viele private Termine. Zur Meldung

Quelle: www.heise.de

IT-Sicherheit: Menschliche Datenschutz-Fails 2/5

Frankreich: TV5 Monde

Am 8. April 2015 wurde das Programm von TV5 Monde über mehrere Stunden hinweg blockiert, nachdem sich eine dem IS nahestehende Hacker-Gruppe namens „Cyber-Kalifat" Zugang zu den IT-Systemen verschafft hatte. Nur einen Tag nach der Cyberattacke erlebte der französische TV-Sender ein Datenschutz-Debakel – dieses Mal aufgrund menschlichen Versagens: Reporter David Delos enthüllte während eines Interviews unabsichtlich die Passwörter für Social-Media-Konten des Senders - darunter YouTube, Instagram und Twitter. Diesen waren auf dem Whiteboard hinter dem Pechvogel zu sehen. Auch wichtige Telefonnummern waren zu sehen. Darüber hinaus offenbarte die Wand auch, wie es zum vorangegangenen Hack durch die Islamisten-Hacker kommen konnte: Und zwar in Form des Passwortes für den YouTube-Account von TV5 Monde: "lemotdepassedeyoutube" („daspasswortfüryoutube").
Mehr Infos

Foto: TV5 Monde

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

Menschen als (Un-)Sicherheitsfaktor

Beispiele

02.09.2021

35 Prozent der Mitarbeiter tricksen im Home-Office Sicherheitsmaßnahmen aus

Eine Umfrage zeigt, dass die meisten Unternehmen am hybriden Modell aus Homeoffice und Büropräsenz festhalten wollen. Allerdings hapert es mit der Sicherheit. Zur Meldung

17.02.2022

Firmenkonten nicht gelöscht: Ehemalige Mitarbeiter sind oft ein Security-Risiko

Soziale Medien, E-Mails und Dokumente – in fast allen Unternehmen können frühere Angestellte weiterhin auf interne Informationen zugreifen.

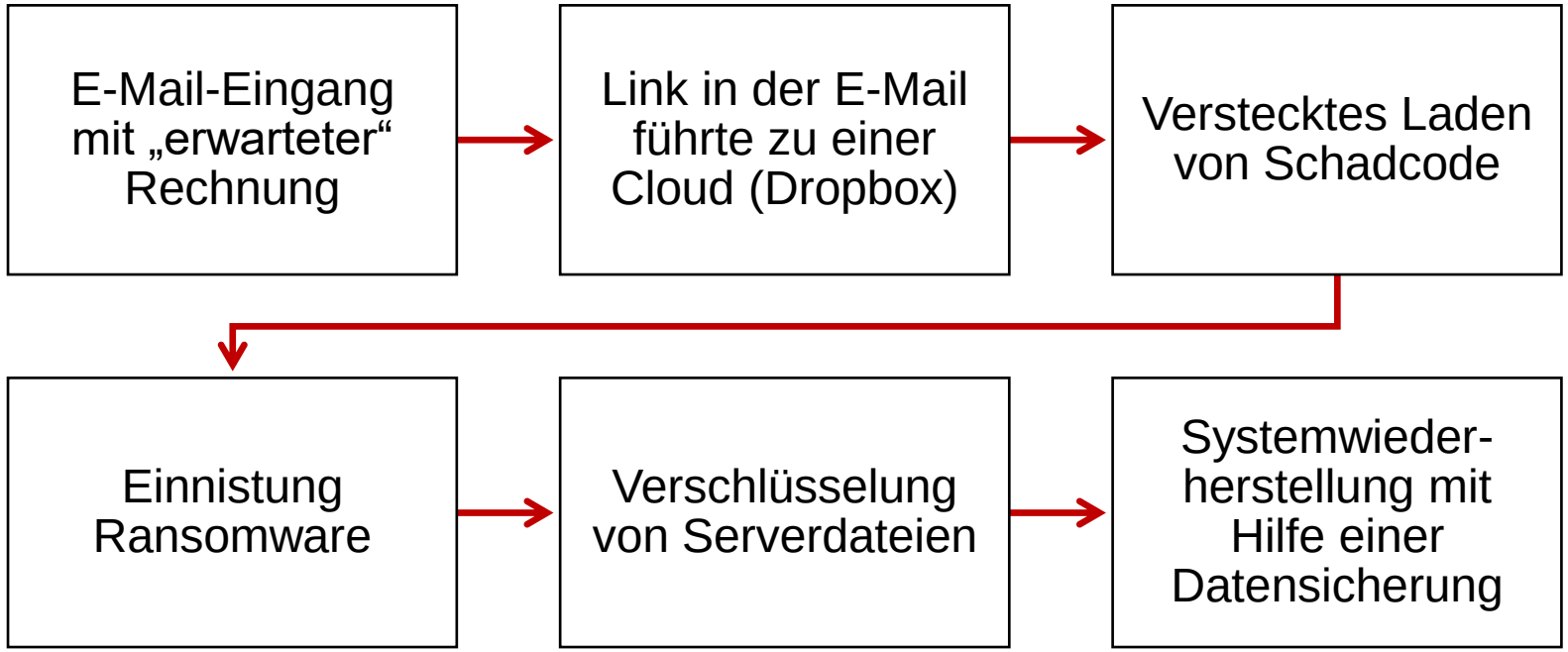
iX Magazin

Quelle: www.heise.de

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

Menschen als (Un-)Sicherheitsfaktor

Beispiel für Dienstleistungsunternehmen aus Magdeburg <20 MA



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

Menschen als (Un-)Sicherheitsfaktor

Auswirkungen von menschlichem Fehlverhalten und/oder Social Engineering

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

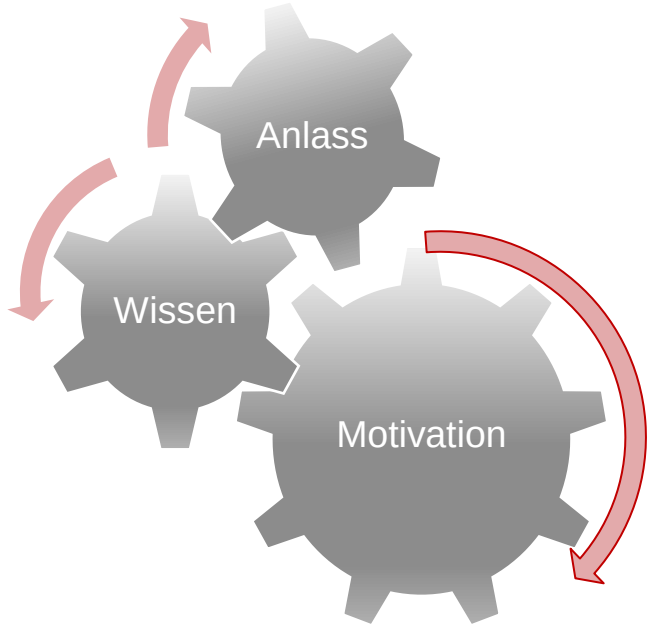
- Manipulation von Daten
- Verlust von Daten
- Abfluss von Daten an Dritte
- Vertrauensverlust bei Partnern und Kunden
- Folgeschäden / -angriffe
  (Advanced Persistent Threads APT)

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

Der Mensch & IT-Sicherheit

Psychologische Dimension der IT-Sicherheit

- Verhalten wird bestimmt durch das Zusammenspiel von Motivation, Wissen und Anlass
- Risiken der Informationssicherheit entstehen oft unbewusst durch Nichtwissen
- Thema der IT-Sicherheit wird oft unbewusst als selbstverständlich angesehen und führt dadurch zu Nachlässigkeiten im Umgang damit



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

Mensch als Sicherheitsfaktor!

Aufbau des „Schutzschild Mensch“

- Richtlinien zur IT-Sicherheit aufbauen und umsetzen
- Unterstützung durch technische Maßnahmen

- Wissen und Bewusstsein gegenüber Gefahren aufbauen
- Prozesse zur Verbesserung initiieren

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

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

Schutzschild Mensch

Vorgehens- und Verhaltensweisen für Mitarbeiter

- umfassende Regelungen zu den Themen
  - Einsatz mobiler Endgeräte
  - Telearbeit / Home-Office
  - Authentifizierung und Verschlüsselung
  - Umgang mit personenbezogenen Daten
  - Notfälle und Schadensvorfälle
  - Verantwortlichkeiten bestimmen
- Umsetzung in Anlehnung an Erfordernisse gängiger Normen
  - IT-Grundschutz oder DIN ISO 27001

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

Schutzschild Mensch

Wissen und Bewusstsein

Informieren	• Newsletter • Intranet
Sensibilisieren	• Mitarbeitergespräche • Interne Workshops
Weiterbilden	• Angebote Mittelstand-Digital.de • Markt
Prüfen	• https://www.phish-test.de • https://www.knowbe4.de

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

Schutzschild Mensch

Umsetzung technischer Maßnahmen

Fehlverhalten verhindern	Gutes Verhalten unterstützen	Unregelmäßigkeiten erkennen
• Webproxy einsetzen • Ports und Schnittstellen sperren • Arbeiten in geschützten Umgebungen	• Passwörter nur nach bestimmten Kriterien + Einschätzung der Stärke • Automatisierung von Gefahrenmeldungen (z.B. bei Erkennung von Spam)	• Anomalieerkennung und Monitoring (aber keine Überwachung!) • automatischer Abgleich von Kontaktinformationen

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

Schutzschild Mensch

Beispiel: E-Mail-Nutzung

- https://www.computerweekly.com/de/tipp/E-Mail-Sicherheit-Gruende-fuer-eine-Security-Richtlinie
- https://blog.usecure.io/de/what-is-an-email-policy-and-should-my-company-have-it

Richtlinien

- Nutzung von Online-Angeboten oder Print-Materialien
- https://play.bakgame.de/PhishingQuiz/
- https://slideplayer.com/slide/11828718/ (BASF: Spot the Fish Quiz)

Sensibilisierung

- Mail-Proxy inkl. Spam-Filter
- Virenscan
- www.virustotal.com

Technische Unterstützung

- Beobachtung und Bewertung durch Leitung sowie IT-Verantwortliche
- Einholung von Feedback auf Mitarbeiterebene
- Überarbeiten der Regeln und Richtlinien

Kontinuierliche Verbesserung

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Schutzschild Mensch

Prozesse verbessern und Mitarbeiter schulen

Quelle: https://betrieb-machen.de/download/9767

- Feedback von Mitarbeitern zu Maßnahmen und Richtlinien einholen
- Schadensvorfälle analysieren und Lehren daraus ziehen
- Notfallmanagement aufbauen
- Wissens- und Bewusstseinsaufbau kontinuierlich erweitern sowie aktuell halten

Quelle: http://betrieb-machen.de/download/15019

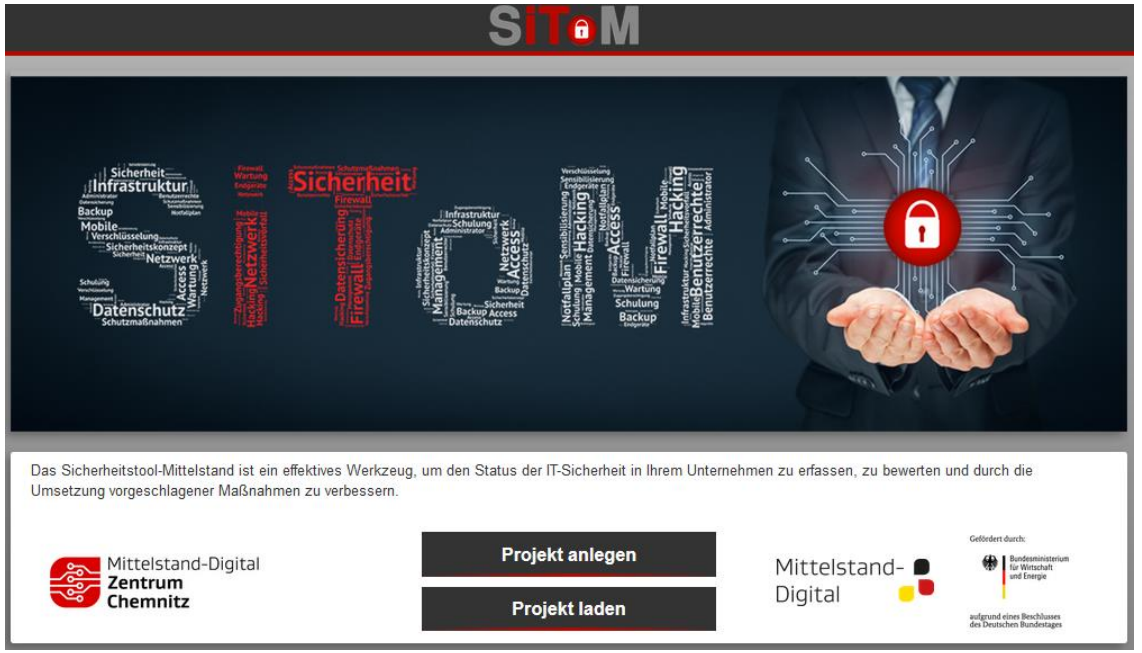
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

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
- Selbstanalyse des IT-Sicherheitsniveaus im Unternehmen
- Empfehlungen geeigneter Maßnahmen zur Steigerung des IT-Sicherheitsniveaus im Unternehmen



Schutzschild Mensch

Weitere Informationen

- https://digitalzentrum-chemnitz.de/wissen/schutzschild-mensch/
- https://it-service.network/blog/2019/03/29/social-engineering-methoden
- https://alarm.wildau.biz
- https://www.bakgame.de
- https://elite-projekt.de
- https://www.its.kompetent.uni-goettingen.de
- https://www.mitnicksecurity.com

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