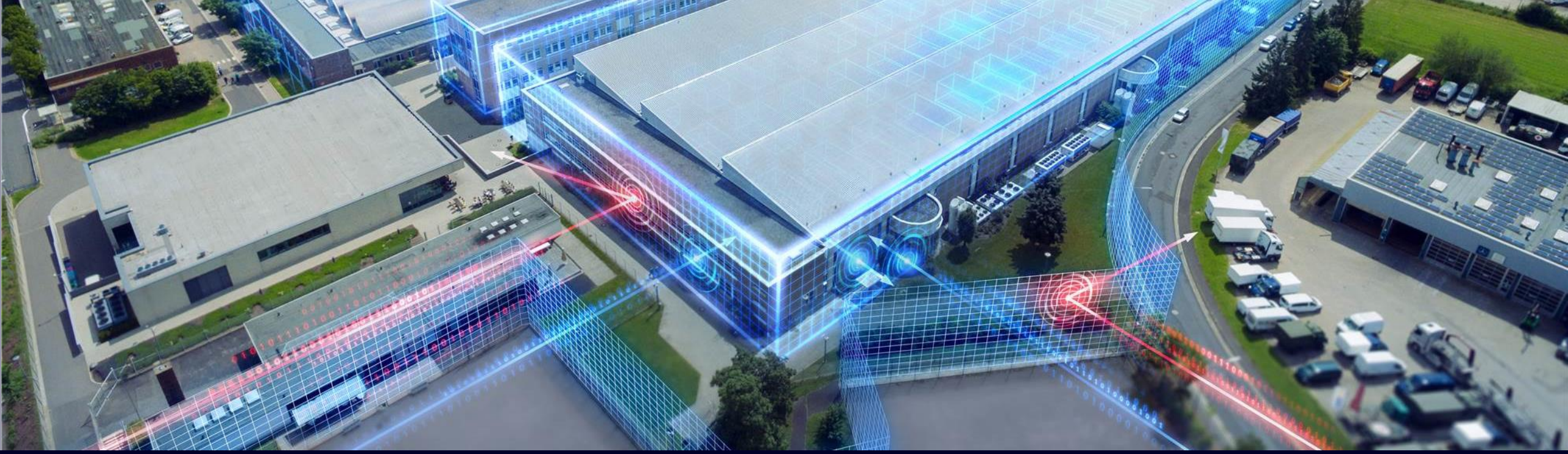


Industrial Security

Produktivität umfassend schützen

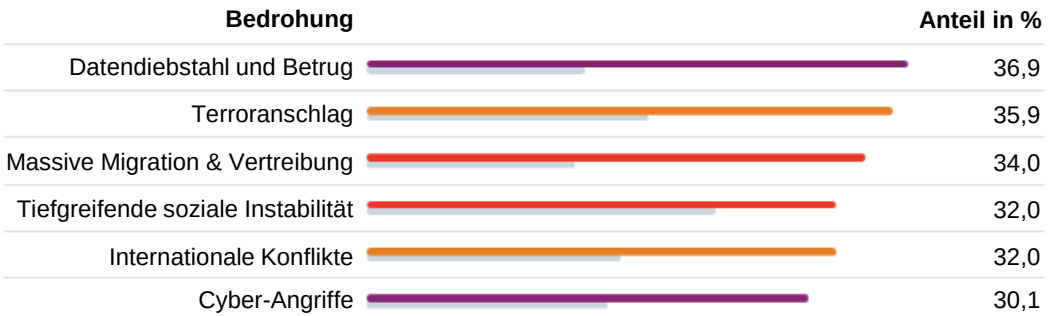
SIEMENS

Trends im Security-Bereich
Ständige Zunahme der weltweiten Vernetzung

Trends mit Auswirkungen auf die Security

- Cloud Computing-Ansätze
- Zunehmender Einsatz von Mobilgeräten
- Drahtlostechnologie
- Verringerter Arbeitskräftebedarf
- Smart Grid
- Weltumspannender Fernzugriff auf Anlagen, Maschinen und mobile Anwendungen
- Das “Internet der Dinge”

Sorgen vor globalen Bedrohungen mit negativem Handelseinflüssen:



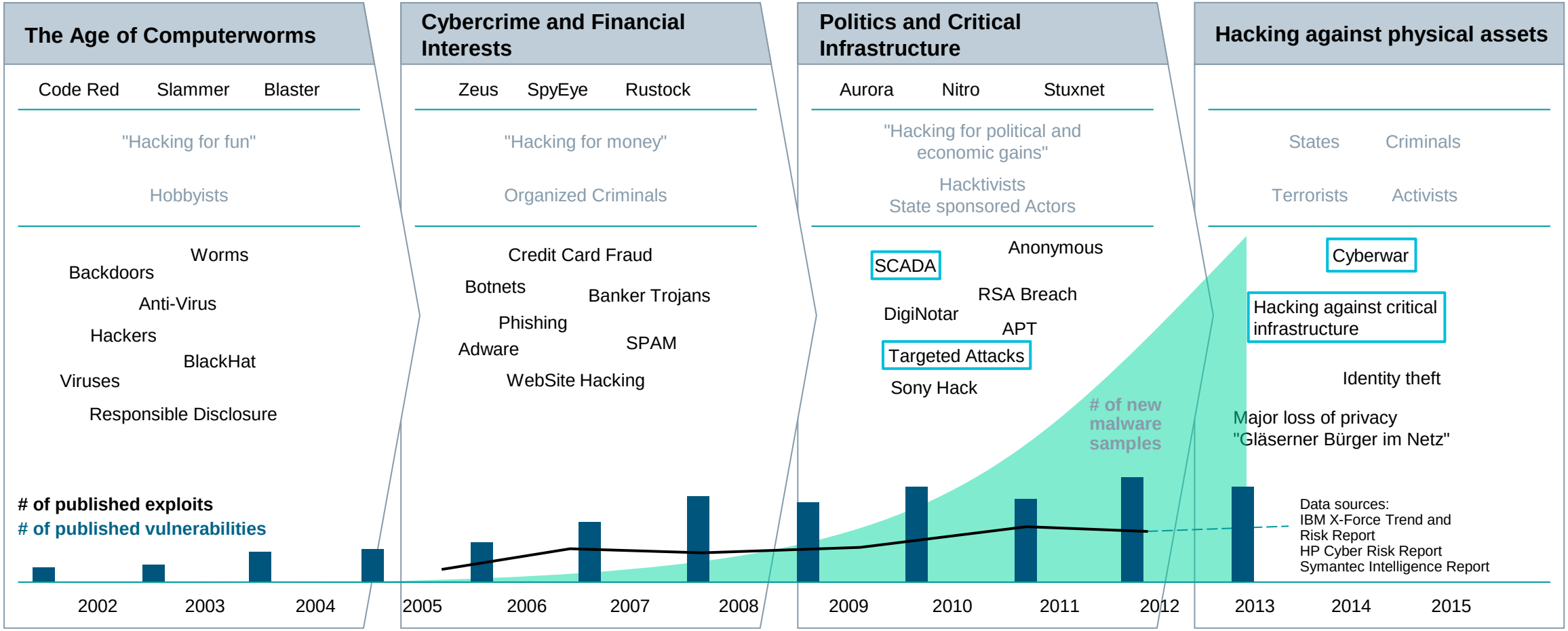
Bedrohung	Anteil in %
Datendiebstahl und Betrug	36,9
Terroranschlag	35,9
Massive Migration & Vertreibung	34,0
Tiefgreifende soziale Instabilität	32,0
Internationale Konflikte	32,0
Cyber-Angriffe	30,1

Quelle: World Economic Forum, Global Risks Report 2017,
Global Risks of Highest Concern for Doing Business – Germany
http://reports.weforum.org/global-risks-2017/

SIEMENS

The threat level is rising –
attackers are targeting critical infrastructures

Evolution of attacker motives, vulnerabilities and exploits



SIEMENS

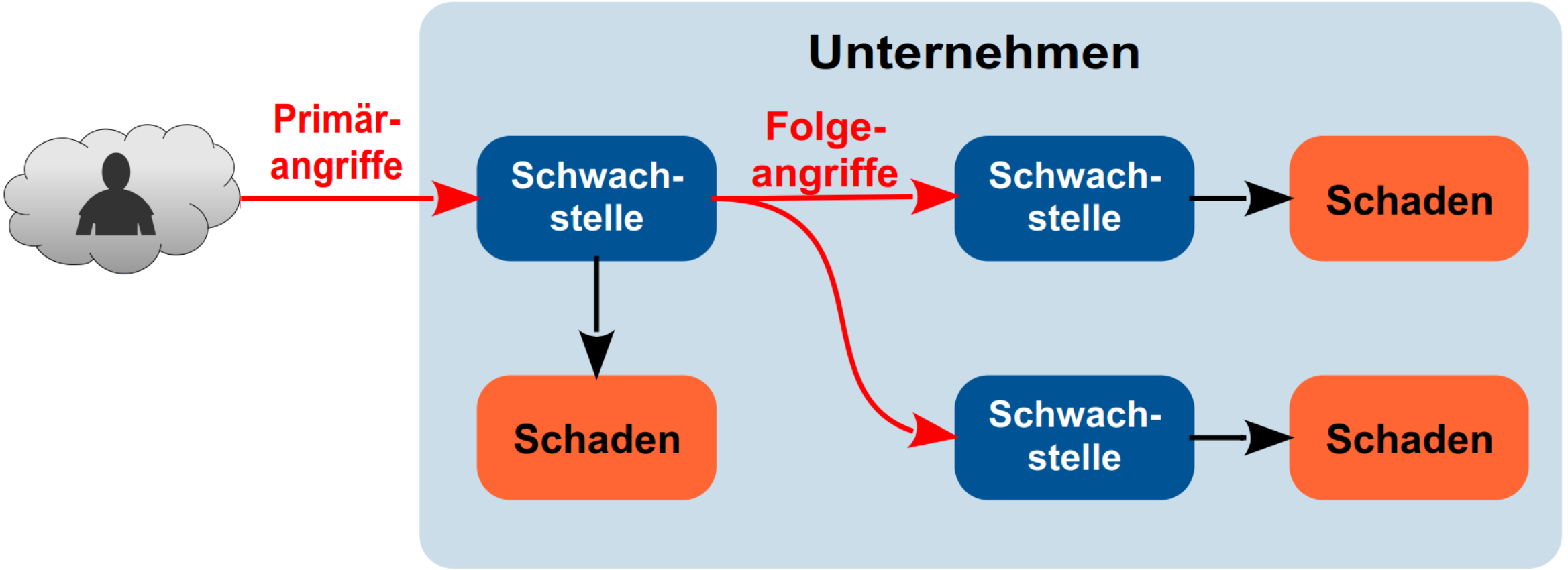
TOP 10 Threats in 2022 (BSI)

Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	
Infektion mit Schadsoftware über Internet und Intranet	
Menschliches Fehlverhalten und Sabotage	
Kompromittierung von Extranet und Cloud-Komponenten	
Social Engineering und Phishing	
(D)DoS Angriffe	

Top 10 Threats	Trend since 2019
Infiltration of malware via removable media and mobile systems	
Infection with malware via Internet and Intranet	
Human error and sabotage	
Compromise of extranet and cloud components	
Social engineering and phishing	
(D)DoS attacks	
Internet-connected control components	
Intrusion via remote maintenance access	
Technical failure and force majeure	
Soft- and hardware vulnerabilities in the supply chain	

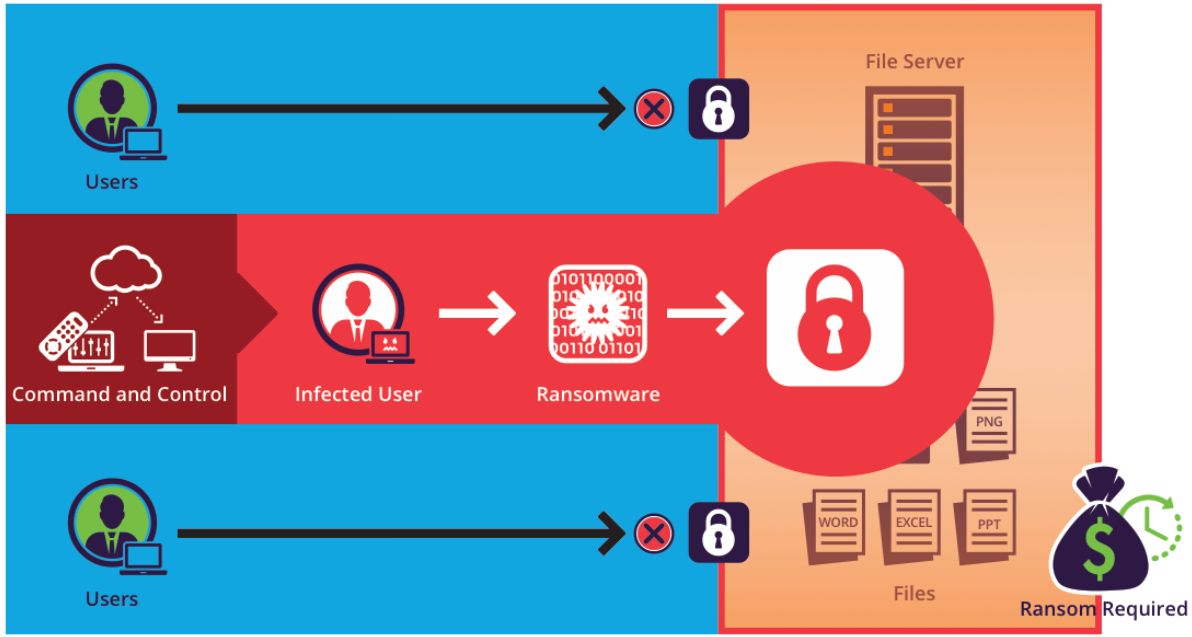
SIEMENS

Vorgehen bei einer Attacke (BSI)

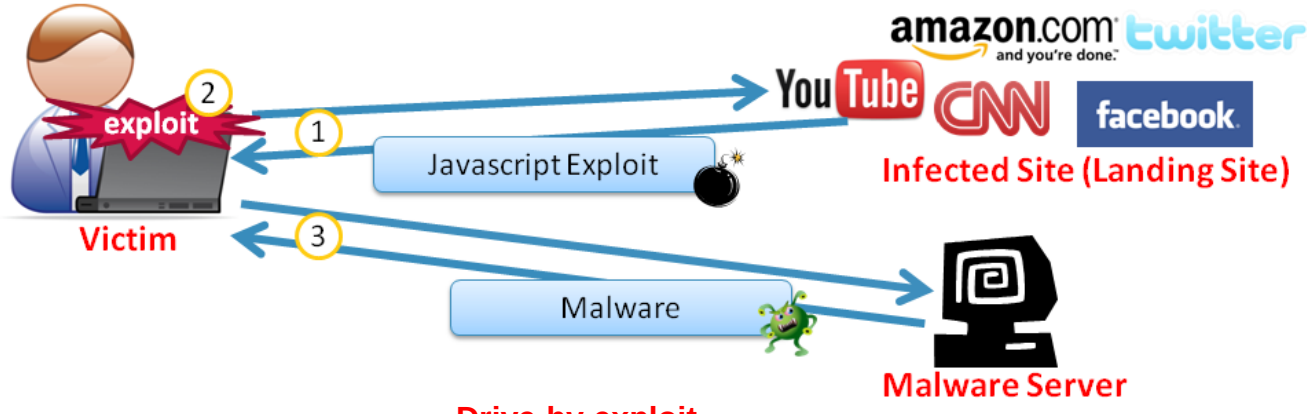


Malware, Ransomware and Drive-by-exploits

Malware



Ransomware



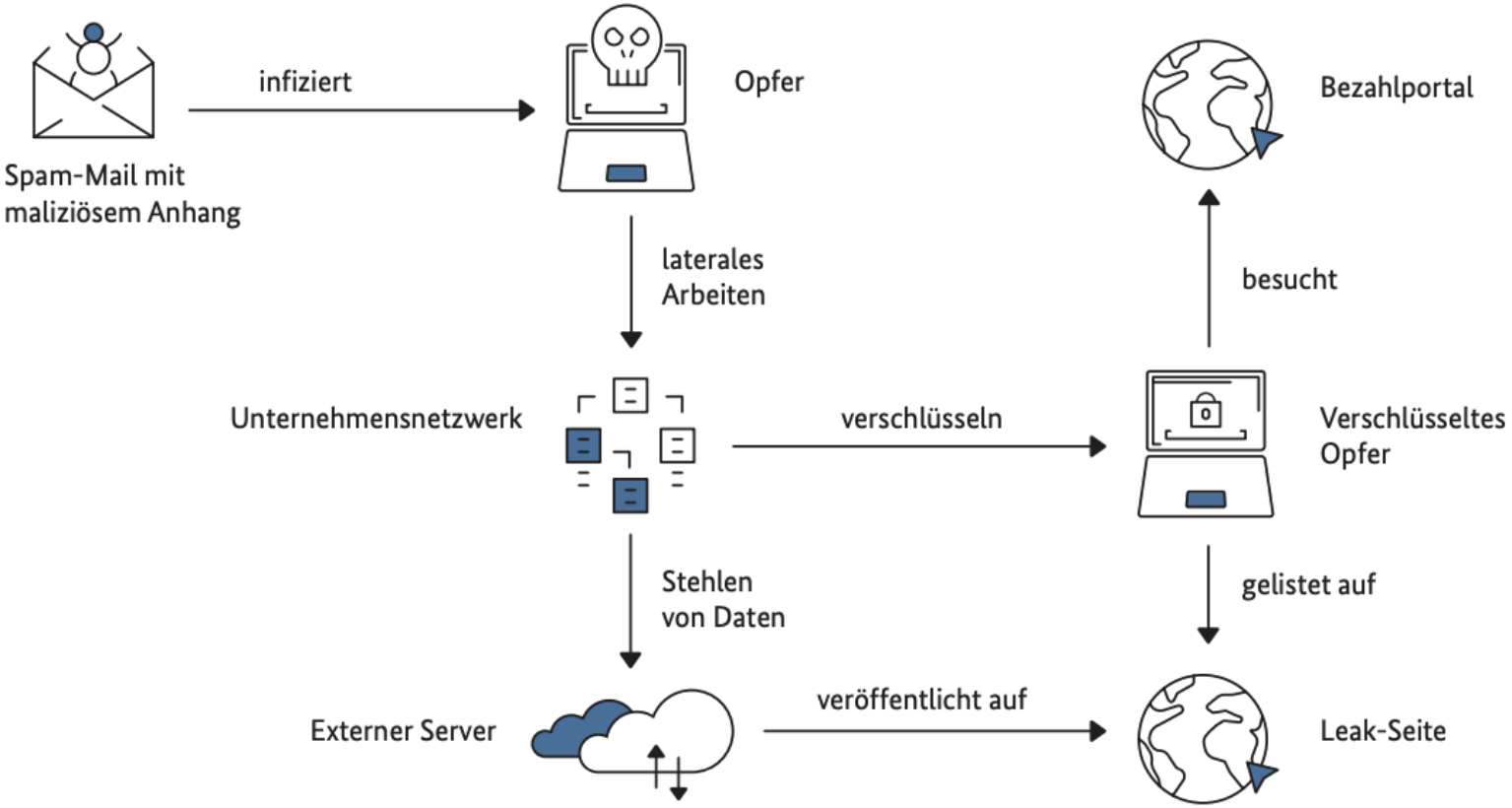
Drive-by-exploit

SIEMENS

Ransomware

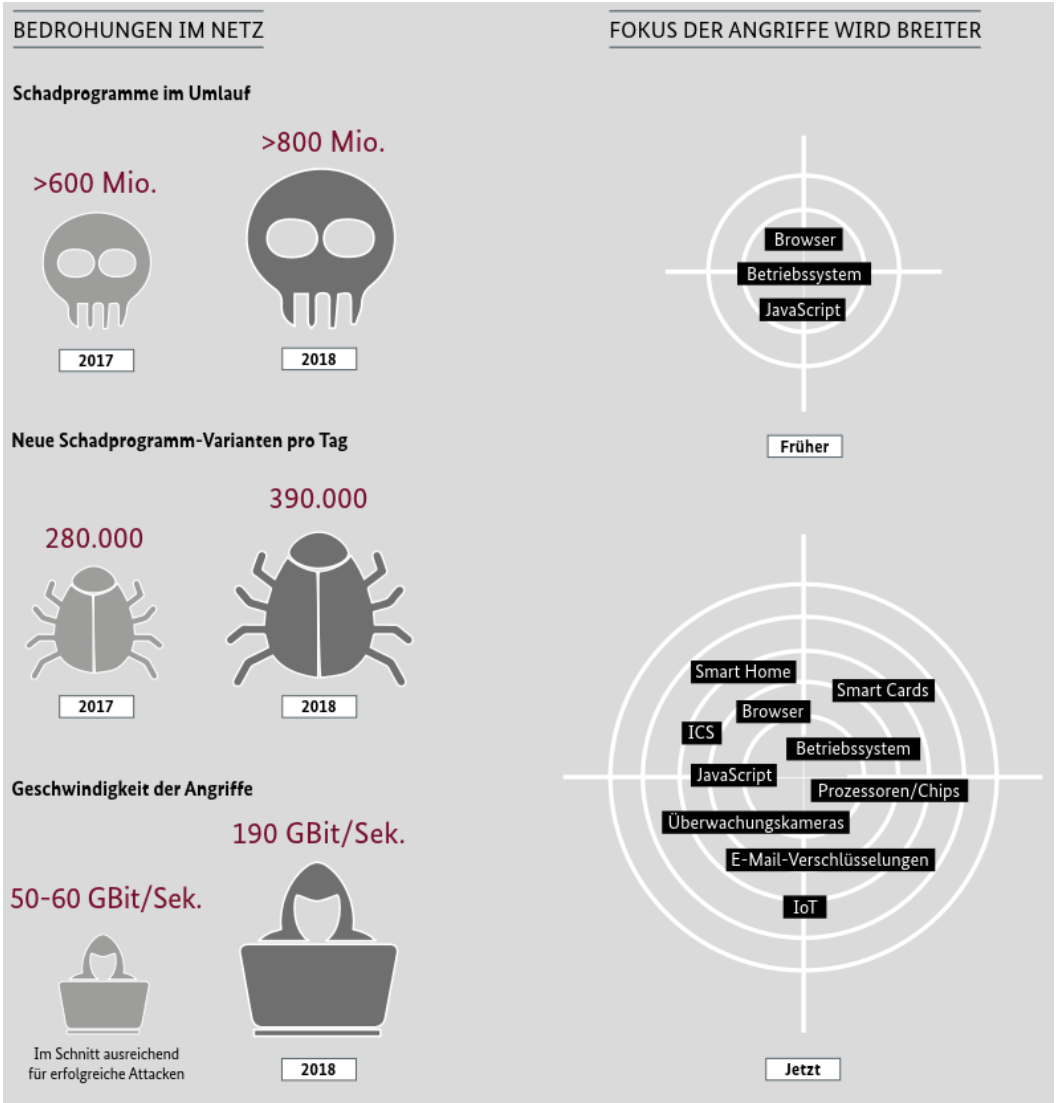
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld- und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



SIEMENS

Ein paar Zahlen (BSI Lagebericht 2018)



SIEMENS

Botnetze und DDos Angriffe

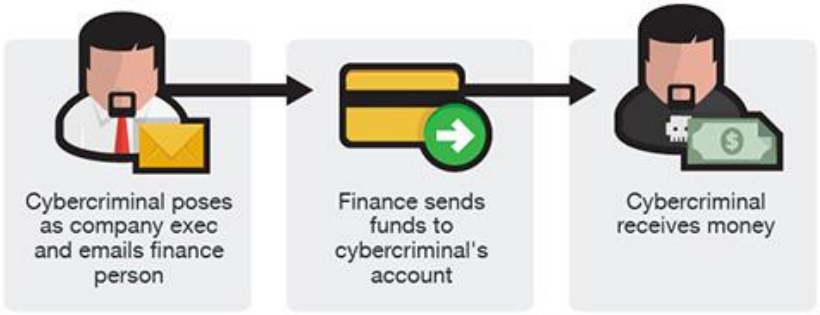
Botnetz

```
The network: client(s)-->handler(s)-->agent(s)-->victim(s)
-----------------------------------------------------------

The stacheldraht network is made up of one or more handler programs
("mserv.c") and a large set of agents ("leaf/td.c").  The attacker uses
an encrypting "telnet alike" program to connect to and communicate
with the handlers ("telnetc/client.c").  A stacheldraht network would
look like this:

                  +--------+            +--------+
                  | client |            | client |
                  +--------+            +--------+
                      |                     |
      . . . --+------+---------------+-----+----------------+-- . . .
              |                      |                      |
              |                      |                      |
        +-----------+          +-----------+          +-----------+
        |  handler  |          |  handler  |          |  handler  |
        +-----------+          +-----------+          +-----------+
              |                      |                      |
              |                      |                      |
. . . ---+----+-----+-----+----------+---+--------+----------+-+-- . . .
         |          |     |              |        |            |
         |          |     |              |        |            |
     +-------+  +-------+ +-------+  +-------+  +-------+
     | agent |  | agent | | agent |  | agent |  | agent |
     +-------+  +-------+ +-------+  +-------+  +-------+

The attacker(s) control one or more handlers using encrypting clients.
Each handler can control many agents.  (There is an internal limit in
the "mserv.c" code to 1000 agents. This is most likely to ensure the
number of open file handles, commonly 1024, is not exceeded by the
program.  Thanks to Adam C. Greenfield <adam@mrniceguy.net> for pointing
this out.  Besides, the code says that "1000 sockets are leet0.")  The
agents are all instructed to coordinate a packet based attack against
one or more victim systems by the handler (referred to as an "mserver"
or "master server" in the code.)
```

„stacheldraht“
Botnetz und DDos Tool

SIEMENS

Sozial Engineering and Identity Theft



Social Engineering
CEO - Betrug

```
        The one stop shop for all of your SE needs.

   Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product o

           Visit: https://www.trustedsec.co

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 2
```

```
  7) Full Screen Attack Method

 99) Return to Main Menu

set:webattack>2

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import
```

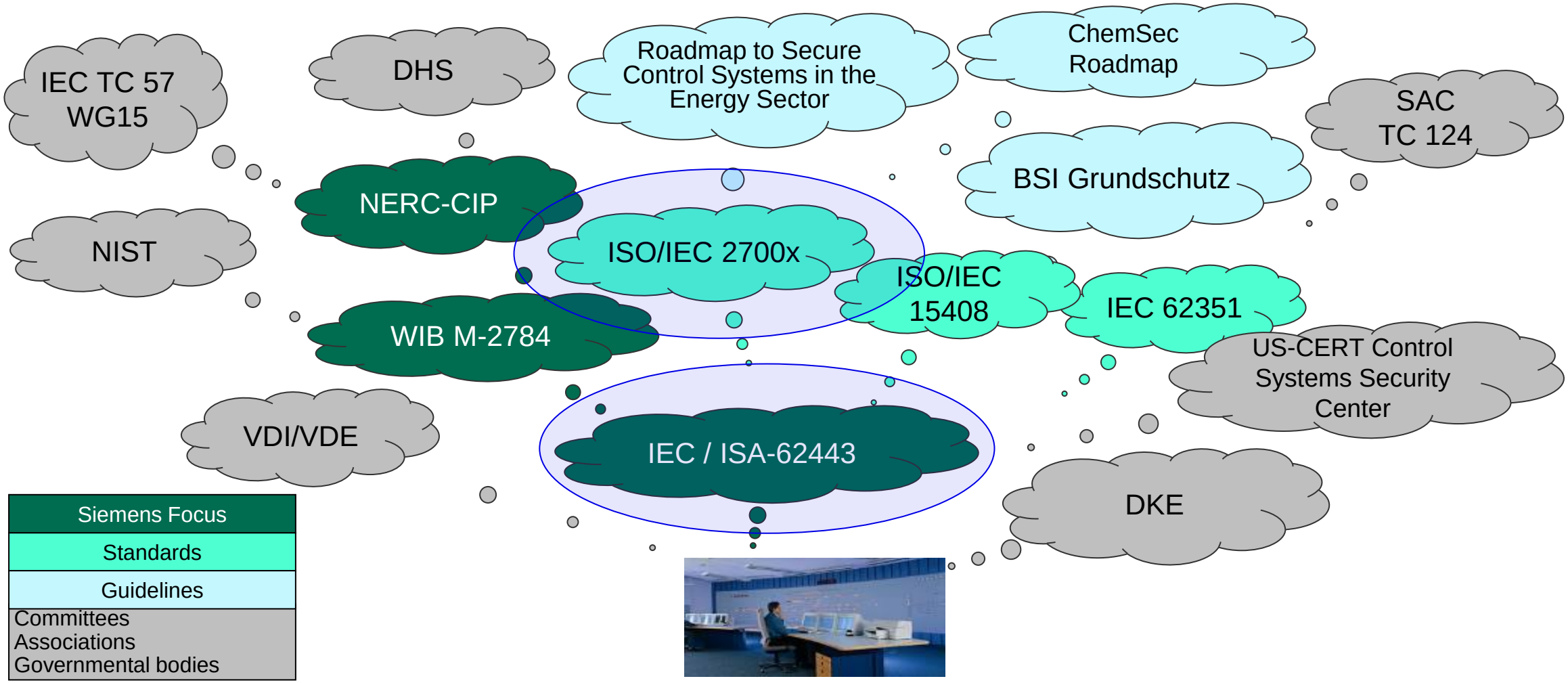
Social Engineering Toolkit
Identitätsdiebstahl

```
192.168.199.132 - - [12/Apr/2013 07:13:11] "GET /index_files/276449379149296_1535348985.png HTTP/1.1"
192.168.199.132 - - [12/Apr/2013 07:13:11] "GET /index_files/276449379149296_1538611903.png HTTP/1.1"
192.168.199.132 - - [12/Apr/2013 07:13:12] "GET /index_files/276449379149296_367648155.png HTTP/1.1"
192.168.199.132 - - [12/Apr/2013 07:13:12] "GET /index_files/276449379149296_646761364.png HTTP/1.1"
192.168.199.132 - - [12/Apr/2013 07:13:12] "GET /index_files/GsNJNwuI-UM.gif HTTP/1.1" 200 -
192.168.199.132 - - [12/Apr/2013 07:13:12] "GET /index_files/safe_image.png HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVoNYZud
POSSIBLE USERNAME FIELD FOUND: email=naivevictim@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=password1234
PARAM: default_persistent=0
PARAM: timezone=600
PARAM: lgnrnd=100252_kBRX
PARAM: lgnjs=1365768159
PARAM: locale=en_US
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

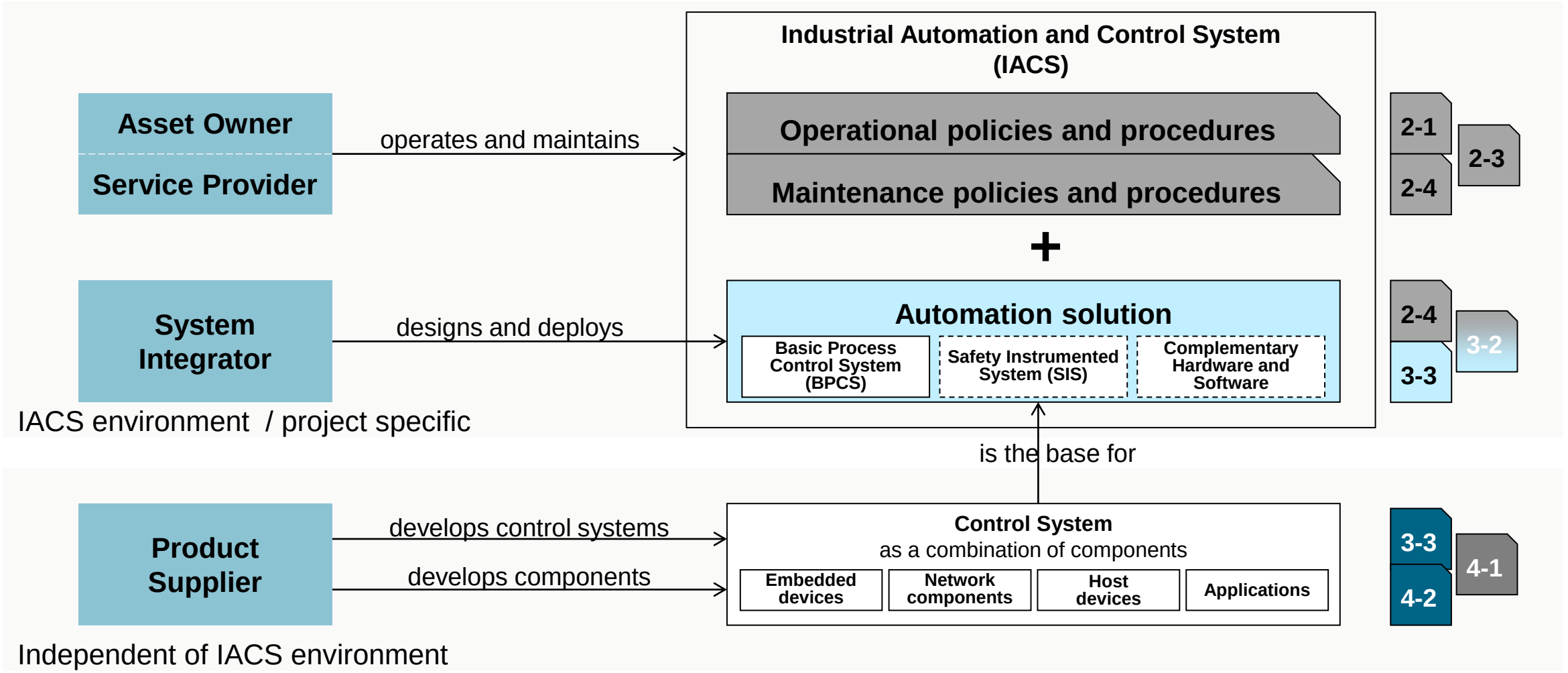
APT und Spam Angriffe

SIEMENS

Selected IT Security Standards, Guidelines and Committees



IEC 62443 Überblick
IACS, automation solution, control system



SIEMENS

IEC / ISA-62443
covers all aspects of industrial security

IEC / ISA-62443

General

- Terminology
- Concepts
- Models
- Compliance metrics
- Security Levels (SL)

Policies and procedures

- Organization
- Training / awareness
- Continuity plan
- Policies, procedures:
  - Architecture (NW, Firewall, etc.)
  - Personnel security
  - Physical security
  - Network segmentation
  - Account administration
  - Authentication
  - Authorization
  - Remote access
  - Portable/Wireless devices & sensors
  - *Cloud usage*

- Risk management and implementation
- Solution development and maintenance
- Incident planning and response

System

- System architecture, network segmentation
- Zones and conduits
- SL for systems

- FR 1 – Identification and authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

Component

- Product development process

- PLCs

- HMI devices
- PC stations

- Firewalls
- Gateways
- Switches

- Functions
- Applications
- Data

SIEMENS

Industrial Security

Grundlage und Maßnahmen für den sicheren Betrieb in einem digitalen Unternehmen

Geschützt

Kommunikation

- Verschlüsselung und Überwachung der Kommunikation

Geschützt

Zugriff

- Zugriffssteuerung für industrielle Komponenten und Netzwerke

Geschützt

Integrität

- Schutz der Übertragung und Speicherung von Daten

Identifikation

- Authentifizierung von Geräten und Benutzern

Grundlage für kontinuierlichen, zuverlässigen Betrieb in einem digitalen Unternehmen

- **Robuste Produkte mit Sicherheitsmerkmalen und Sicherheitsdiensten**
- **Konzepte wie Defense in Depth und ganzheitliches Sicherheitskonzept**
- **Sicherheitsphilosophie wie “Notwendigkeit zur Verbindung” (need2connect)**

SIEMENS

Siemens Product Cert and ICS Cert

Siemens ProductCERT and Siemens CERT

The central expert teams for immediate response to security threats and issues affecting Siemens products, solutions, services, or infrastructure.

Siemens ProductCERT is a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks. The team acts as the central contact point for security researchers, industry groups, government organizations, and vendors to report potential Siemens product security vulnerabilities. This team will coordinate and maintain communication with all involved parties, internal and

https://new.siemens.com/global/en/products/services/cert.html

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: ICS-CERT Advisories by Vendor | ICS-CERT Advisories by Vendor - sorted by Last Revised Date

Items per page 25 Apply

ICSA-22-326-01 : AVEVA Edge
ICSA-22-326-02 : Digital Alert Systems DASDEC
ICSA-22-326-03 : Phoenix Contact Automation Worx
ICSA-22-326-04 : GE CIMPLICITY
ICSA-22-326-05 : Moxa Multiple ARM-Based Computers
ICSA-21-049-02 : Mitsubishi Electric FA Engineering Software Products (Update G)

https://www.cisa.gov/uscert/ics/advisories

SIEMENS

Kontakt

Herausgeber: Siemens AG Österreich

Dr. Lukas Gerhold
Leitung SIMATIC Application Center & Support
RC-AT DI FA
Siemensstraße 90
1210 Wien
Österreich

Mobil +43 664 80117 83833

E-Mail lukas.gerhold@siemens.com

SIEMENS

Disclaimer

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

SIEMENS