Designing Education
Connecting People

Schutzbedarfsanalyse im eigenen Arbeitsplatzbereich durchführen

Lernfeld 04

Das erwartet Sie:

- Angriffsszenarien

Die Themen

Hacking

Lernziele

Definition, Hackarten

Hackingprozess

Lernziele

Einzelne
Hackingprozesse

Malware

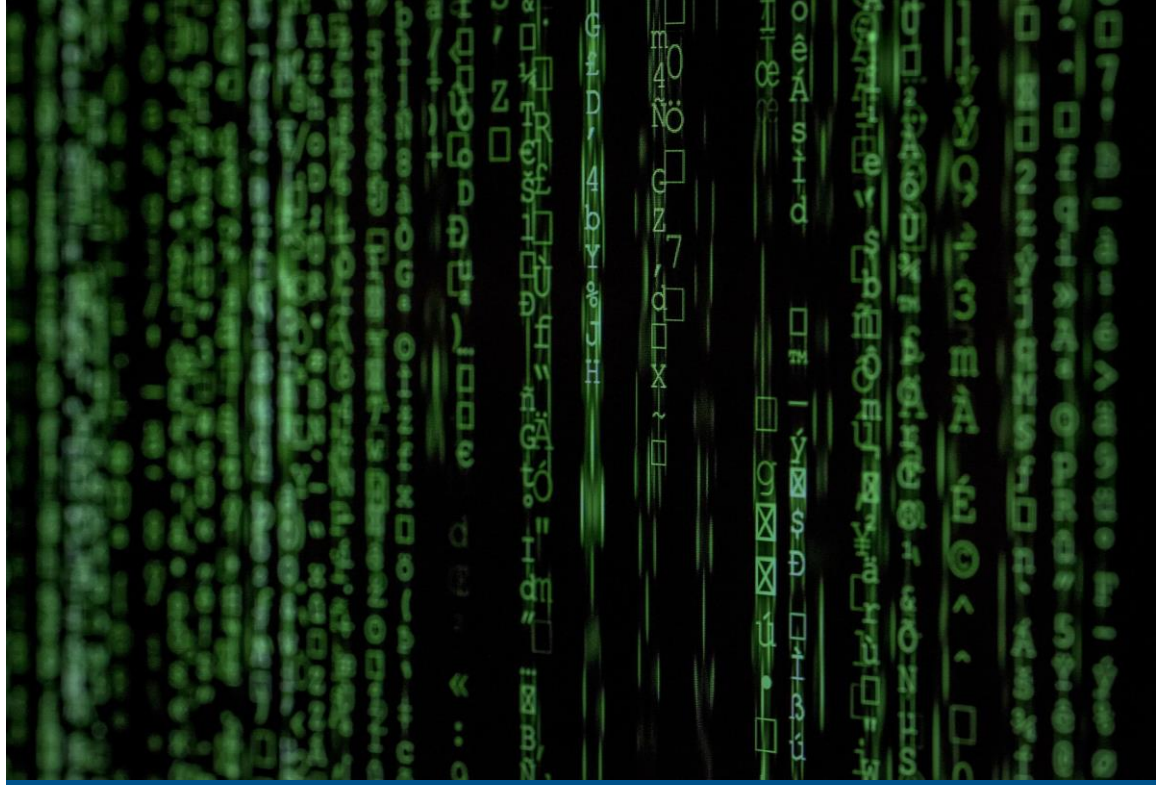
Lernziele

Grundlage Malware
Definition
Auswirkung
Verschiedene Malware

Angriffsarten

Lernziele

Verschiedene
Angriffsmöglichkeiten



Hacking

Lernziele

Was ist Hacking

Hackarten

Hackingprozess

Warum Hacking?

„Wenn du dich und deinen Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.
Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden.
Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.“

- Sun Tzu „Die Kunst des Krieges“

Hacking

Definition:

- Illegales Eingreifen in ein/en Computer(-System)

Hackerparagraph (§202c StGB)

(1) Wer eine Straftat nach § 202a oder 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einen anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit einer Freiheitsstrafe von bis zu 2 Jahren oder mit einer Geldstrafe bestraft

Hackarten

Double Blind

Angreifer + Verteidiger haben beide keine Informationen

Black Box

- Verteidiger beauftragt Hacker
- Hacker hat keine Informationen

White Box

- Verteidiger beauftragt Hacker
- Hacker hat komplette Informationen

Grey Box

- Verteidiger beauftragt Hacker
- Hacker hat teilweise Informationen

Hackingprozess

Informationsbeschaffung	Zugang verschaffen	Zugang etablieren	Spuren verwischen
Footprinting	Password-Hacking	Programme installieren	Logfiles löschen und manipu-lieren
Scanning	Privilegien-Eskalation	Programme und Dateien verstecken	
Enumeration	Malware & Angriffsarten		

©Urheber

Footprinting

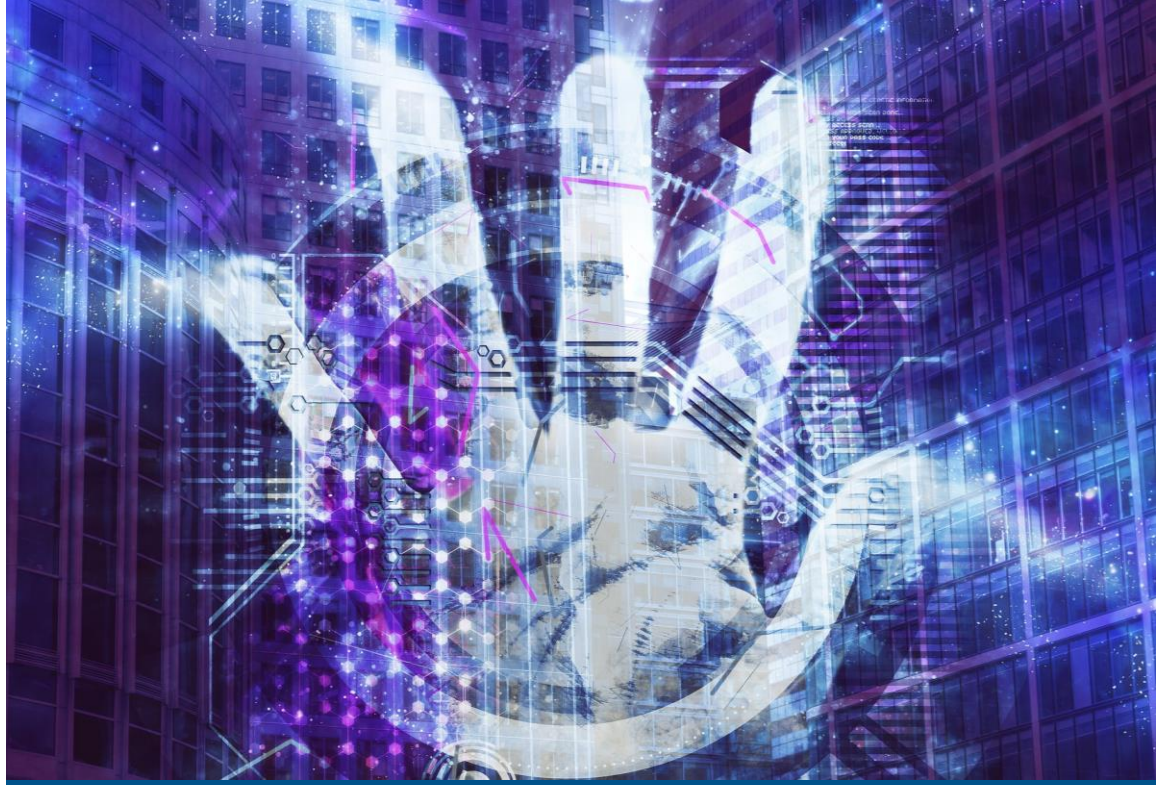
Lernziele

Definition

Methoden

Footprinting

- **Passive**
  - Homepage vom Unternehmen
  - Suchmaschinen
  - Stellenausschrei-bungen
  - Social Media
- **Aktive**
  - Fingerprinting
  - WarChalking
  - WHOIS-Abfragen
  - DNS-Abfragen



©Urheber

Social Engineering

Lernziele

Grundlagen Social Engineering

Prinzipien

Angriffe

Risiken

Maßnahmen

Social Engineering

Definition

- Soziale Manipulation
- Zwischenmenschliche Beeinflussung des Ziels -> Bestimmte Verhaltensweisen hervorrufen

Wie?

- Schwächen von Menschen ausnutzen
  - Unsicherheit, Eitelkeit oder Gier
- Informationen über eine Person erhalten mittels Informationsbeschaffung (Footprinting)

Ziel

- Vertrauliche Informationen
- Sicherheitssysteme umgehen
- Insider Attack

Social Engineering - Prinzipien

Authority

Eine Autoritätsperson

Intimidation

Durch Bedrohung erschrecken

Consensus

Von allgemeinen Gruppenvereinbarung überzeugen

Scarcity

Einen Mangel beschreiben

Familiarity

Eine engere Beziehung

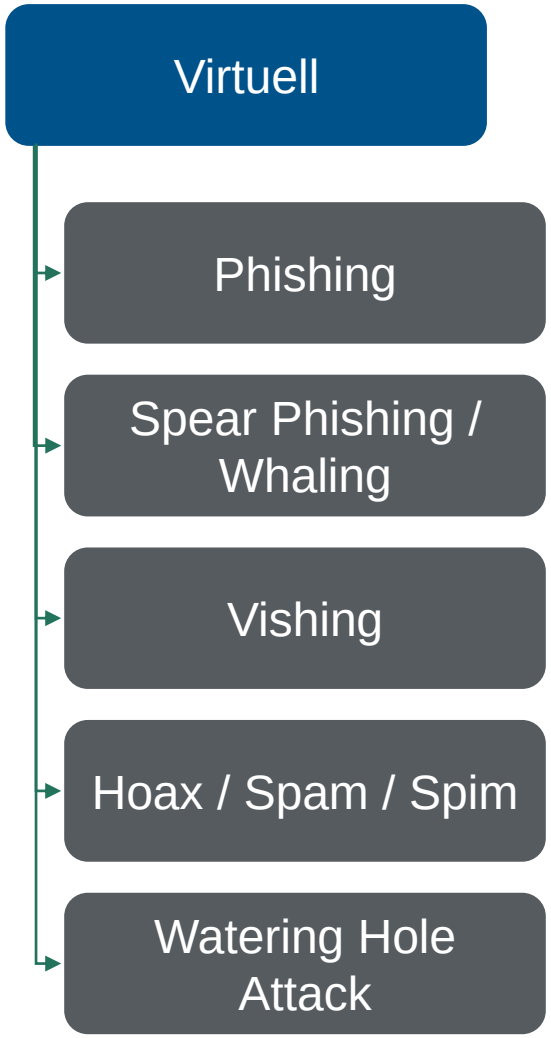
Trust

Vertrauen auf Ehrlichkeit und Integrität

Urgency

Sofortiges Handeln fordern

Social Engineering Angriffe



©Urheber

Scanning

Lernziele

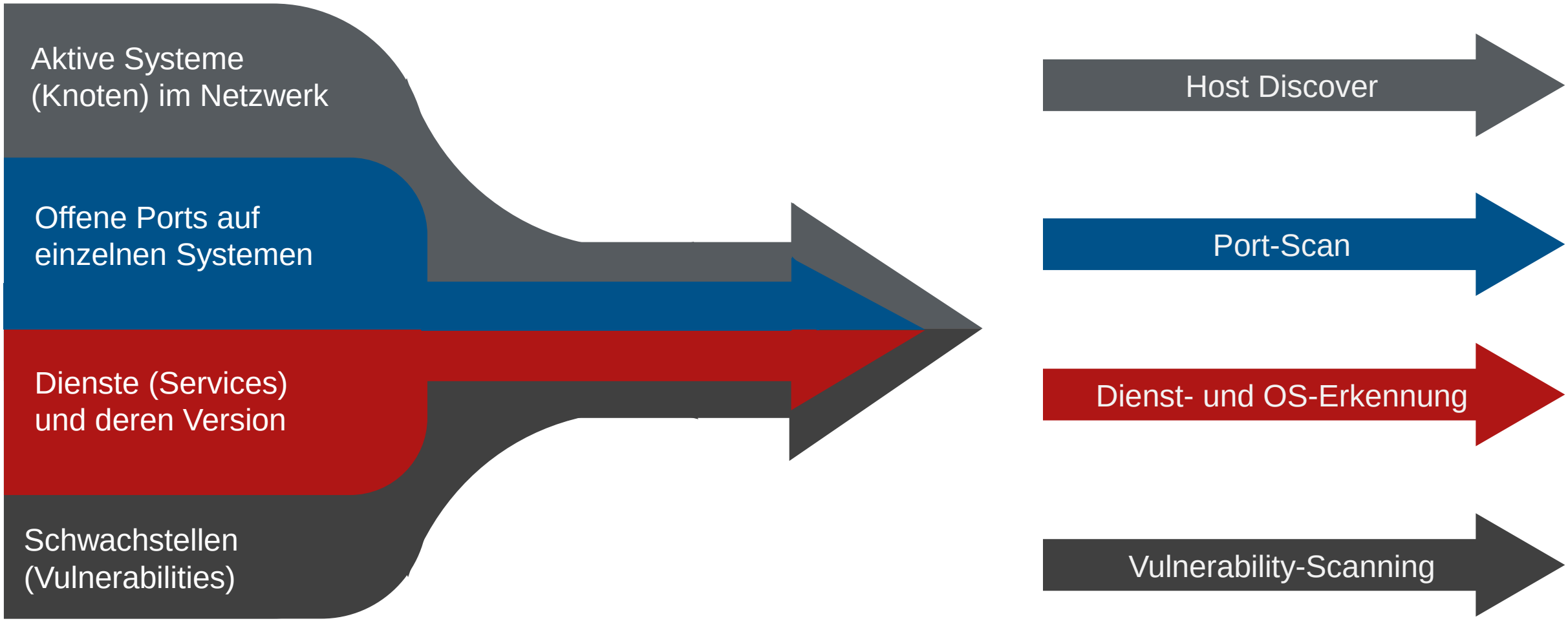
Ziele des Scanning-Prozesses

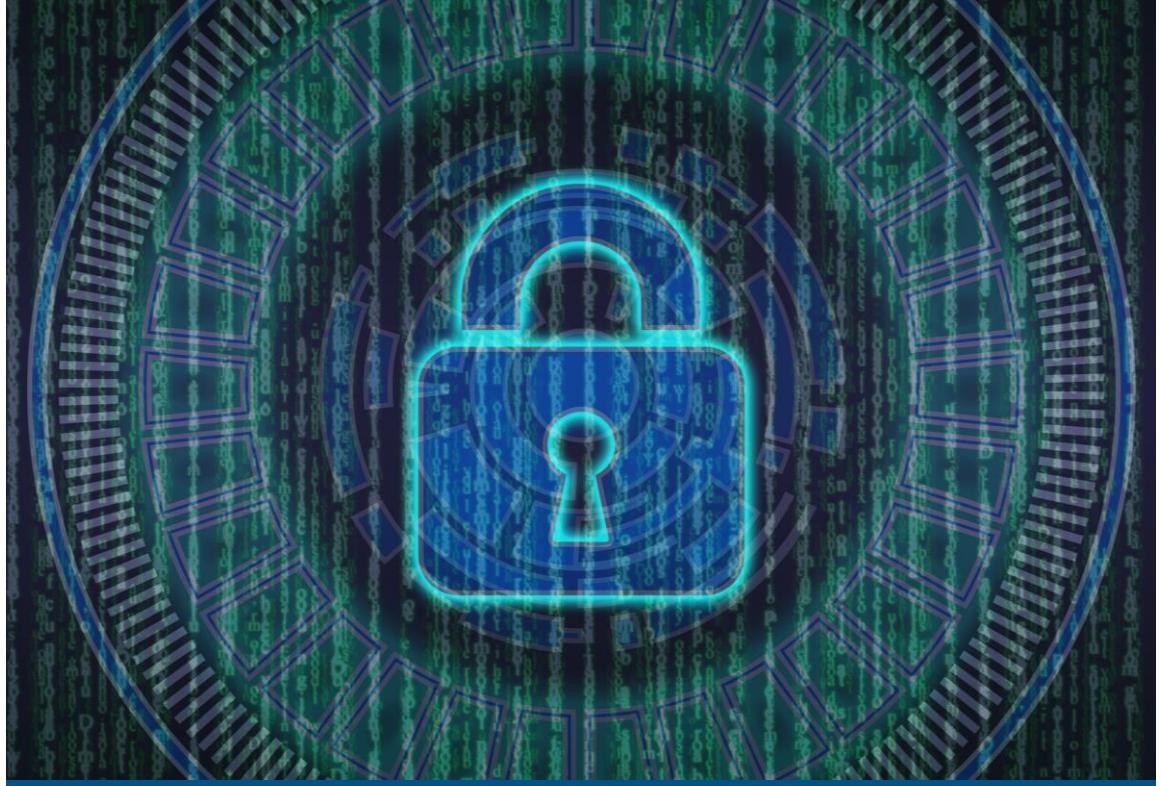
Scanning-Methoden

Scanning

Ziele des Scanning-Prozesses

Scanning-Methoden





©Urheber

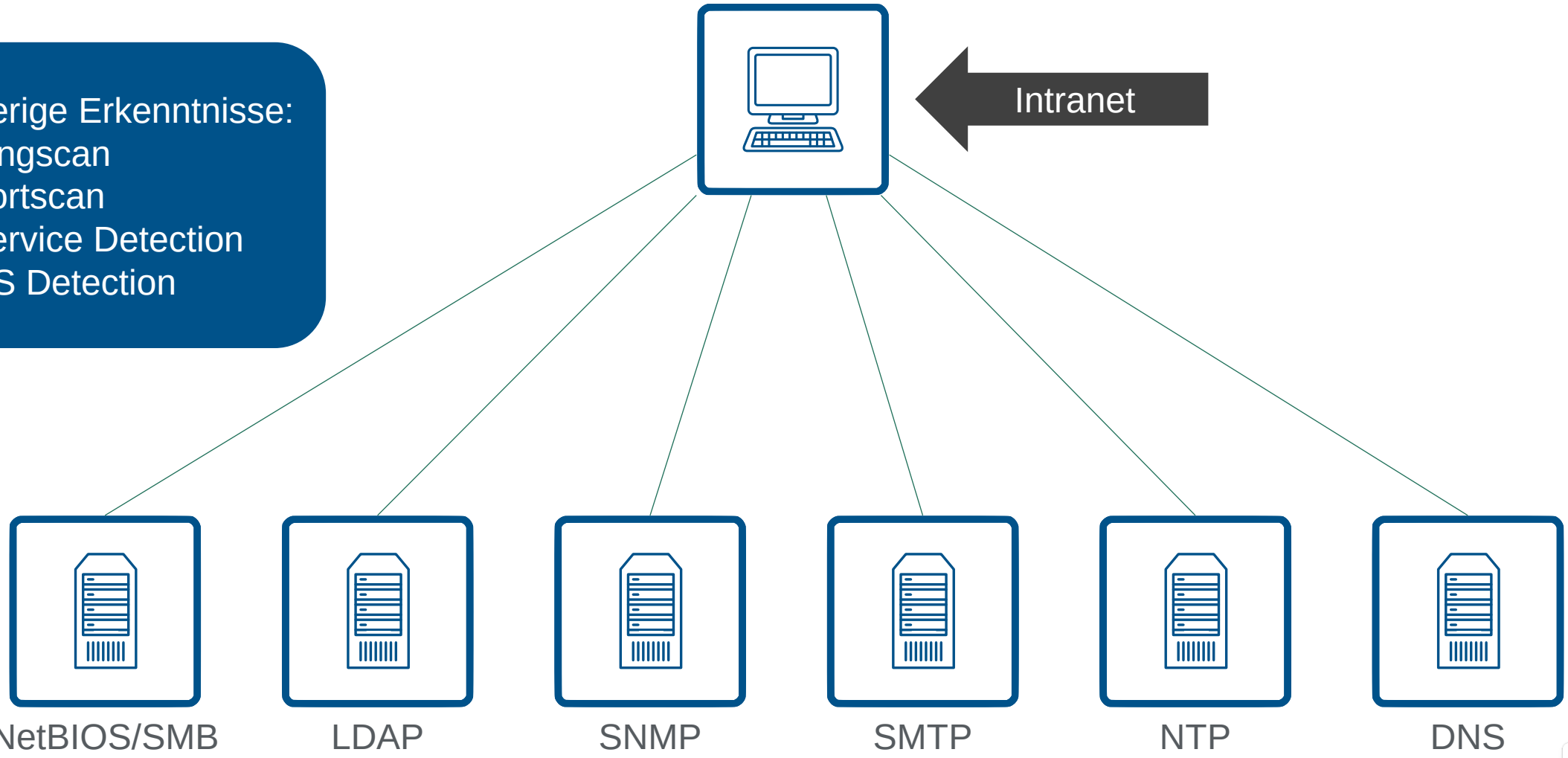
Enumeration

Lernziele

Grundlagen Enumeration

Enumeration

Bisherige Erkenntnisse:
- Pingscan
- Portscan
- Service Detection
- OS Detection



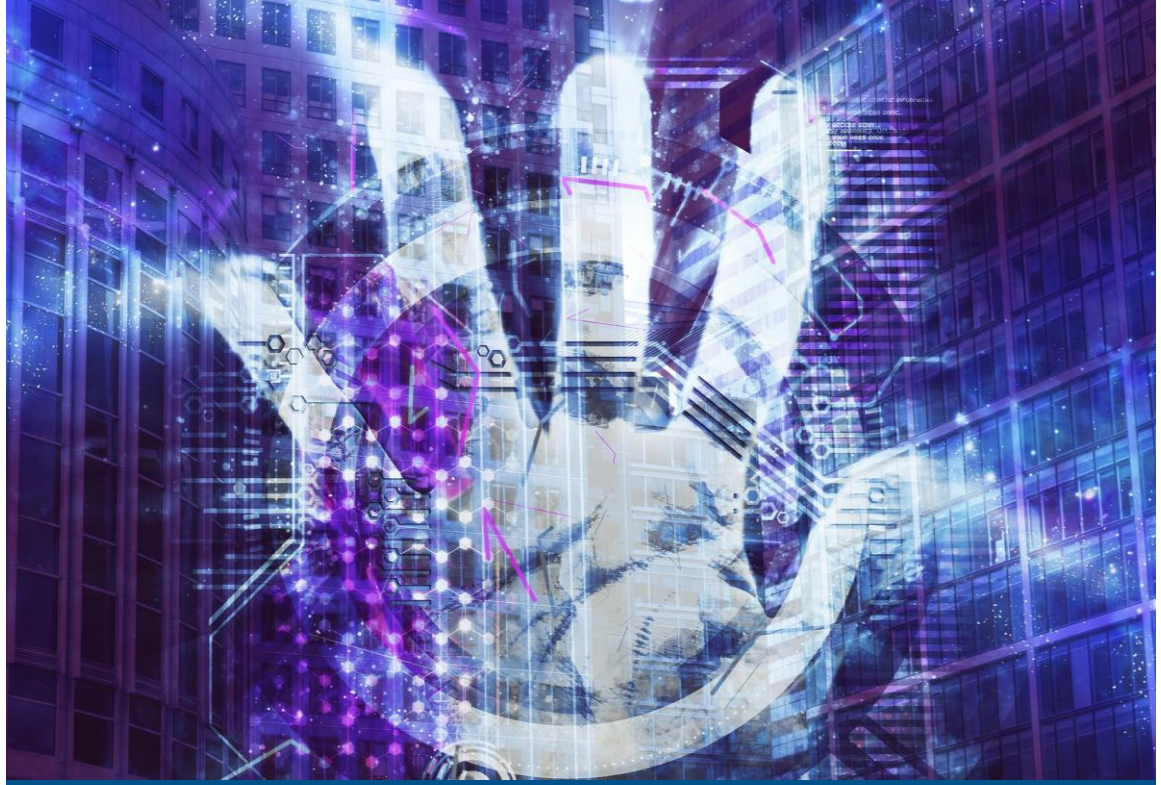
Passwortangriffe

Lernziele

Verschiedene Passwortangriffe

Passwortangriffe

Nicht-elektronische Angriffe	Aktive Online-Angriffe	Passive Online-Angriffe	Offline-Angriffe
Social Engineering	Password Guessing	Sniffing	Dictionary-Angriffe
Shoulder Surfing	Dictionary-Angriffe	Man-in-the-Middle (MITM)	Brute-Force-Angriffe
Dumpster Diving	Brute-Force-Angriffe	Replay-Angriff	Rainbow-Table-Angriffe
	Hash-Injection		Distributed-Network-Attack (DNA)
	Keylogger, Spyware, Trojaner		
	Phishing und Pharming		



Privilegien-Eskalation

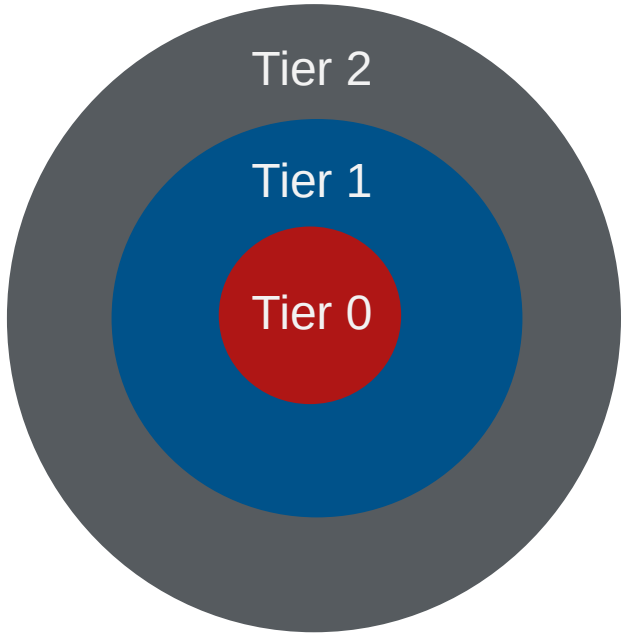
Lernziele

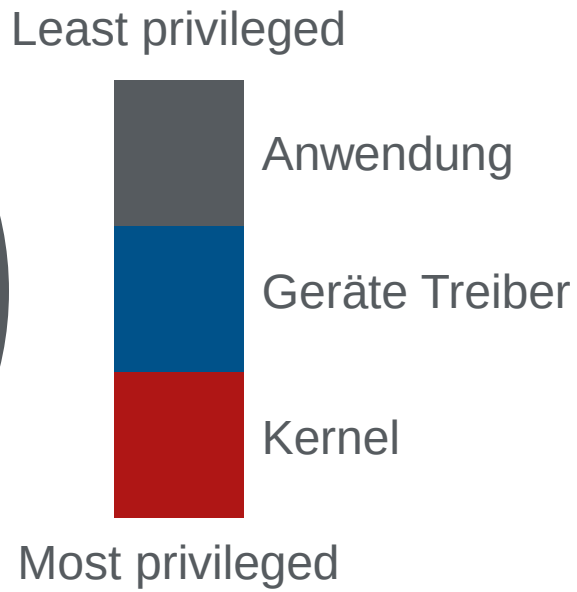
Allgemeines zur Rechteerweiterung

Privilegien-Eskalation

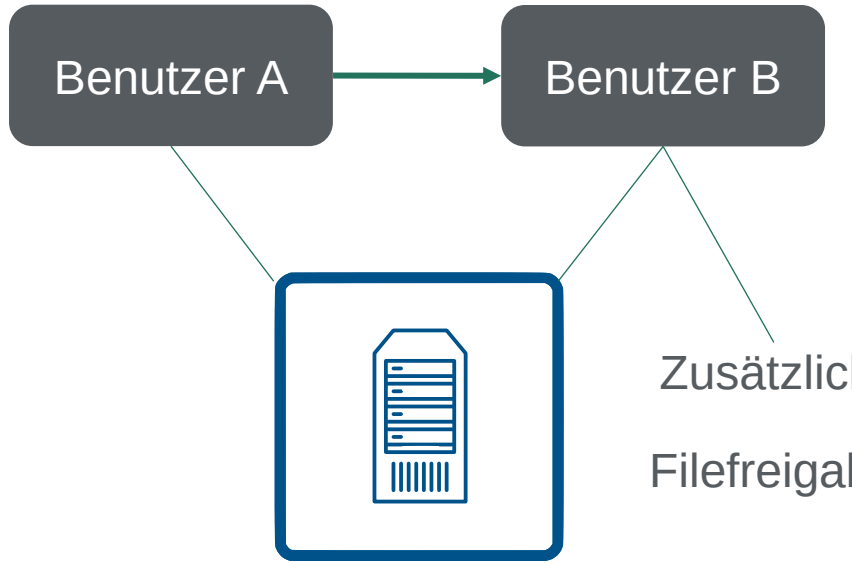
Definition: Ausnutzung eines Computerbugs bzw. eines Konstruktions- oder Konfigurationsfehlers, um erhöhte Rechte zu erhalten

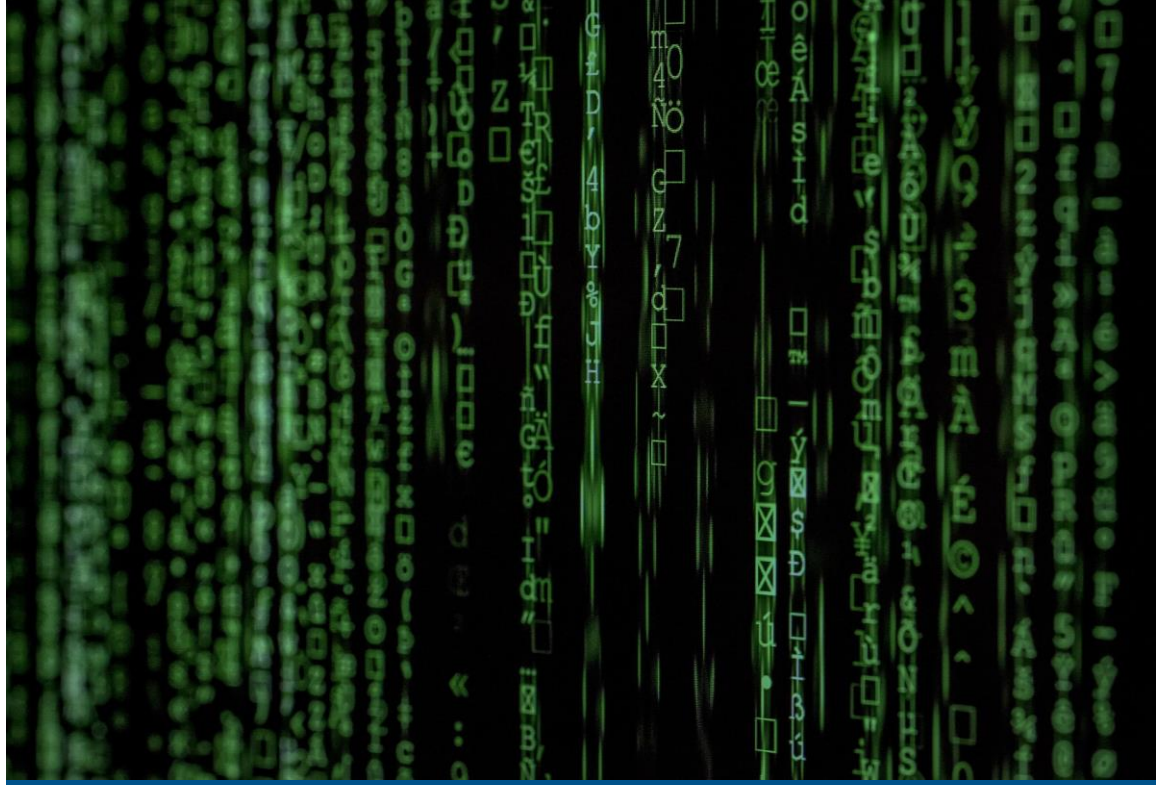
Vertikale





Horizontale



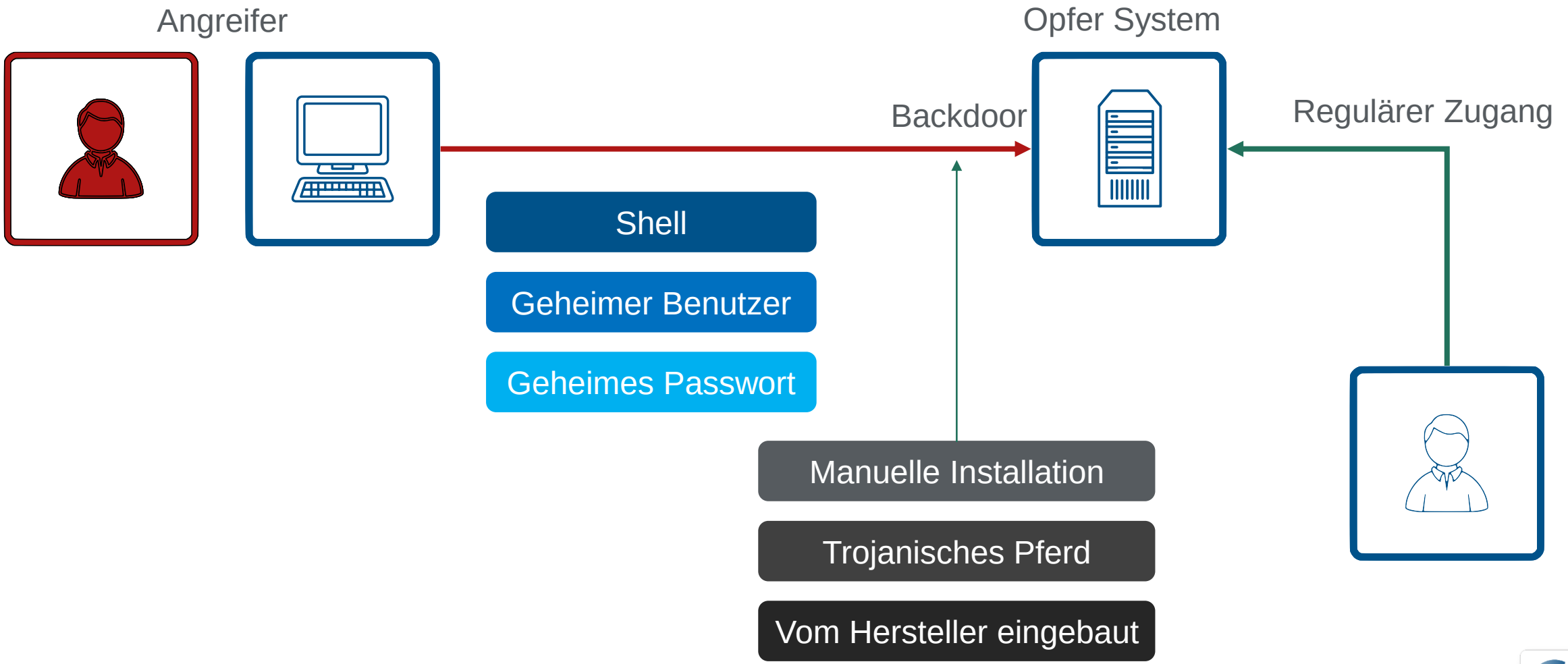


Zugang etablieren

Lernziele

Möglichkeiten Zugänge zu etablieren

Backdoor


Angreifer
Opfer System
Backdoor
Regulärer Zugang
Shell
Geheimer Benutzer
Geheimes Passwort
Manuelle Installation
Trojanisches Pferd
Vom Hersteller eingebaut

Malware

Lernziele

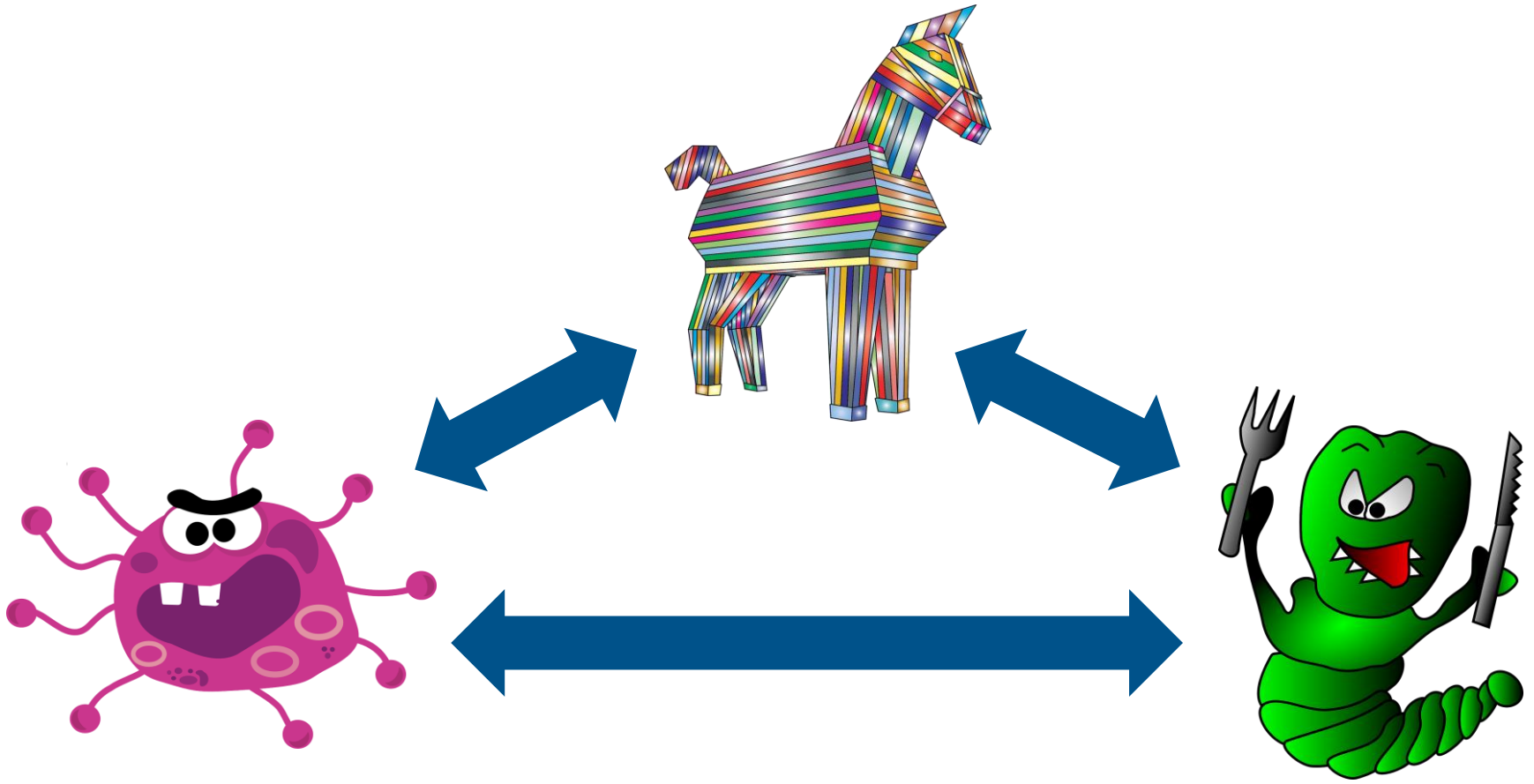
Grundlagen Malware

Definition

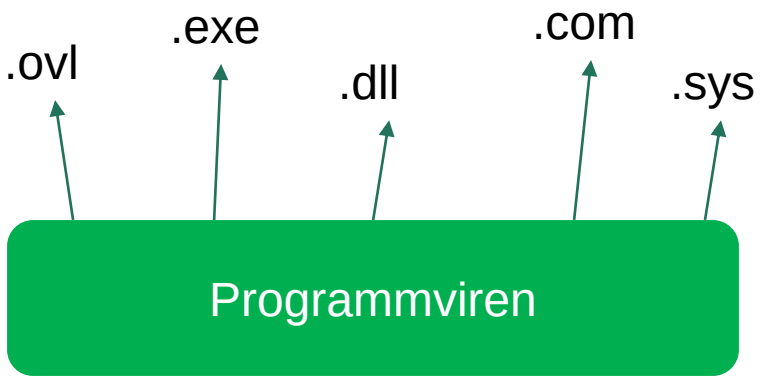
Auswirkung

Verschiedene Malware

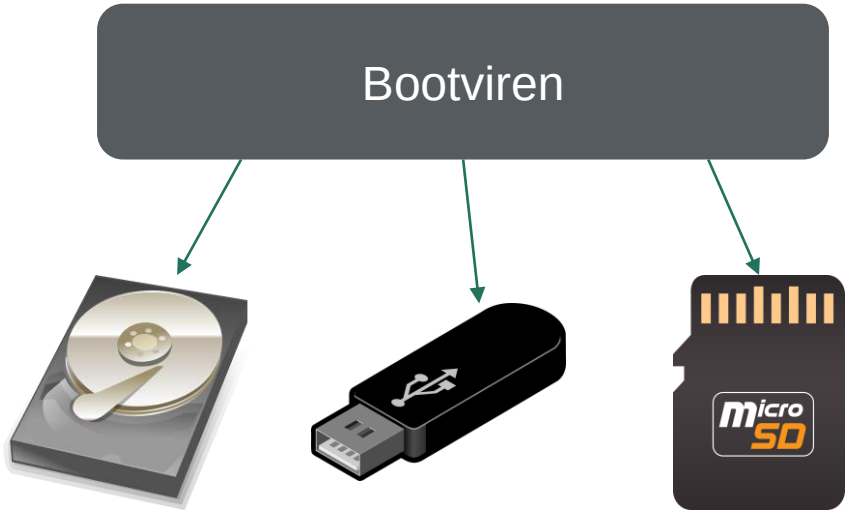
Hauptmalware – Viren / Würmer / Trojaner

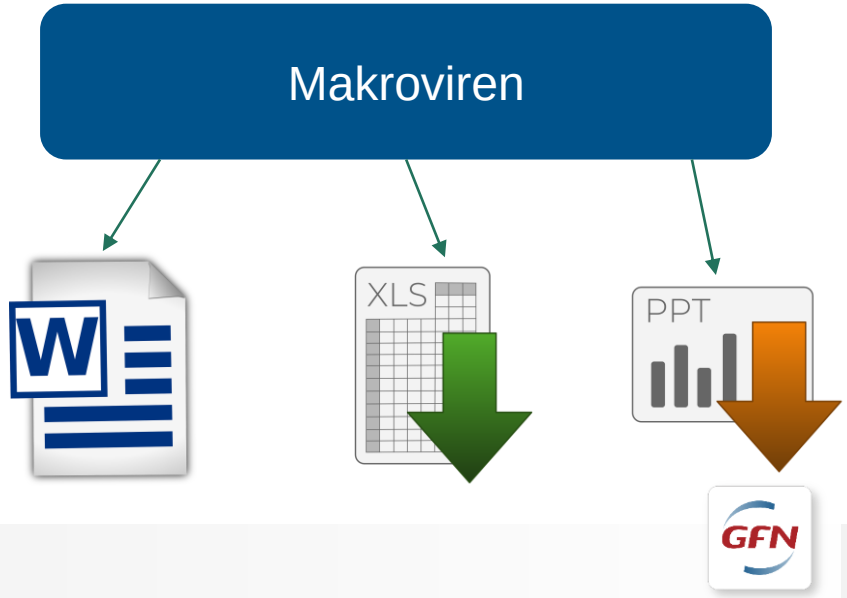


Virenarten


.ovl
.exe
.dll
.com
.sys
Programmviren


JavaScript
Scriptviren


Bootviren
micro SD


Makroviren
XLS
PPT
GFN

Malwarearten

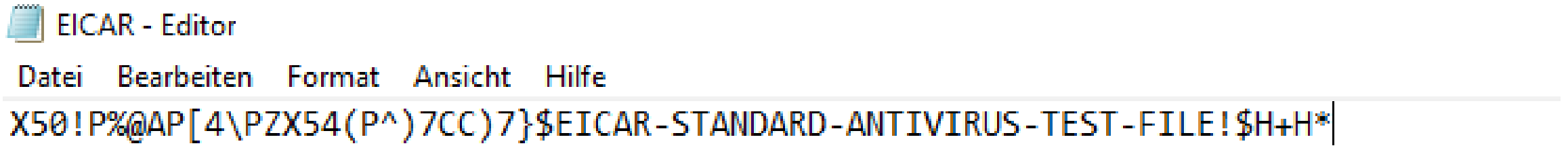
Backdoor	Exploit	Payload	Dropper
RAT	Adware	Toolbar	Bloatware
Scareware	Logic Bomb	Crypto Mining	Ransomware
Rootkit	Spyware	Keylogger	Riskware
Rogueware	Crapware	Eicar	Dialer

Eicar

European Institute for Computer Antivirus Research

Keine Malware - > The Anti-Virus oder Anti-Malware Test File

- Dient zur Prüfung, ob Antivirensoftware korrekt laufen



Exploit und Payload

Exploit

Ziele:

Remote-Shell
Denial of Service (DoS)
Zugriff auf Daten/Informationen
Manipulieren von Komponenten
Man in the Middle
usw.

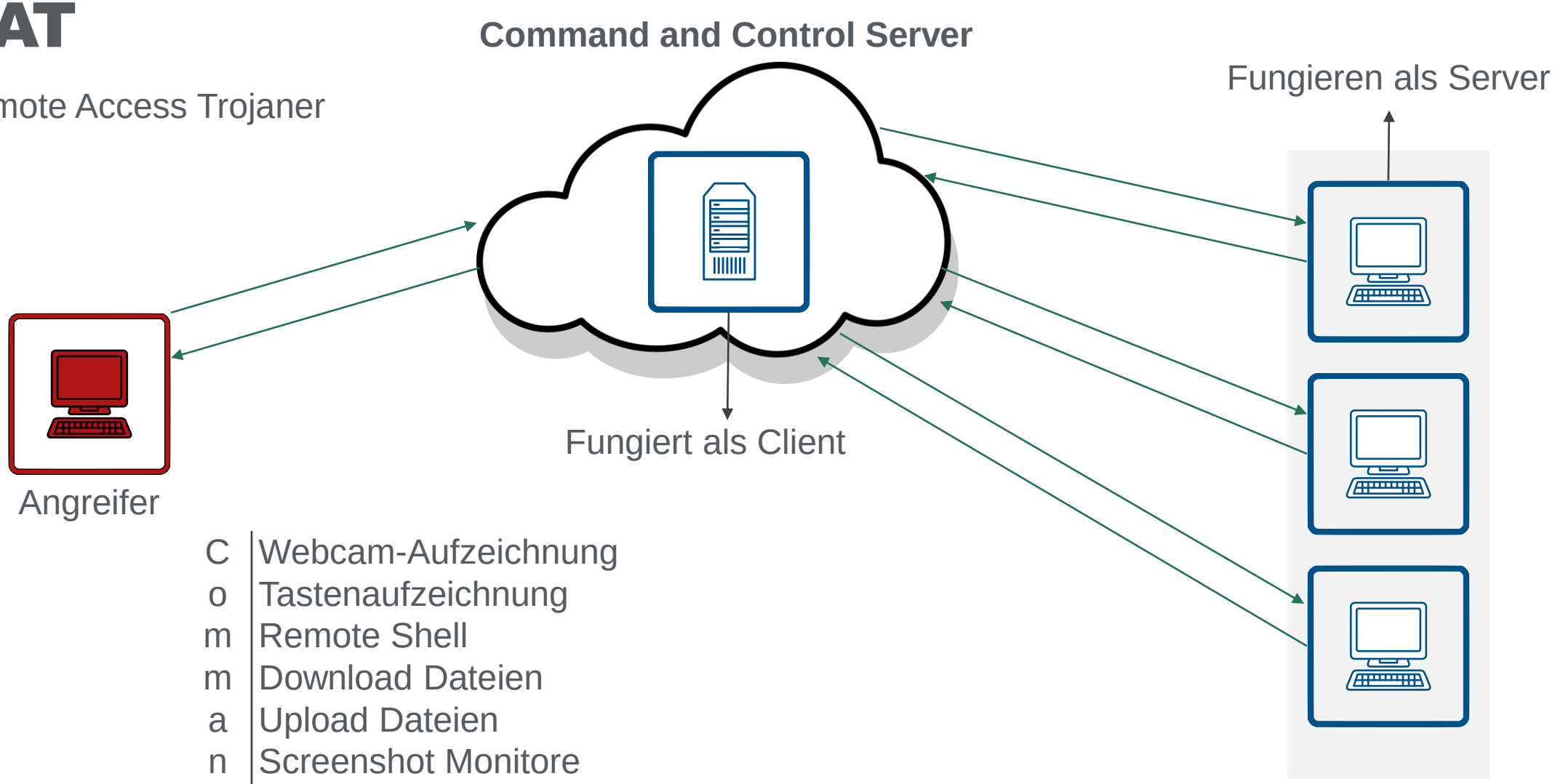
Payload

Anweisung in einer Batchdatei
Skript (Python, Ruby, Perl, Shell)
Assamblercode (Shellcode)
Verpackt in Viren/Würmern/Trojanern

- Unstaged
- Staged

RAT

Remote Access Trojaner



C	Webcam-Aufzeichnung
o	Tastenaufzeichnung
m	Remote Shell
m	Download Dateien
a	Upload Dateien
n	Screenshot Monitore
d	Zwischenstation für andere PC im Netzwerk

Ransomware


Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Rootkit

- Eigentlich ein nützliches Tool (netstat, passwd und ps)
- Abänderung in eine Malware, um sich unbeschränkten Zugriff auf das System zu verschaffen

Zusammensetzung

root	**kit**
Systemadministrator	Werkzeugkasten

Allgemein:

- Ein Programm für bestimmte Elemente (Dateien, Prozesse, Windows-Registrierungsschlüssel, Arbeitsspeicheradressen, Netzwerkverbindungen usw.) das sich vor anderen Programmen oder OS verbirgt
- Heißt: Allein betrachtet keine schädliche Auswirkung

Rootkit

Enthalten Schadcode

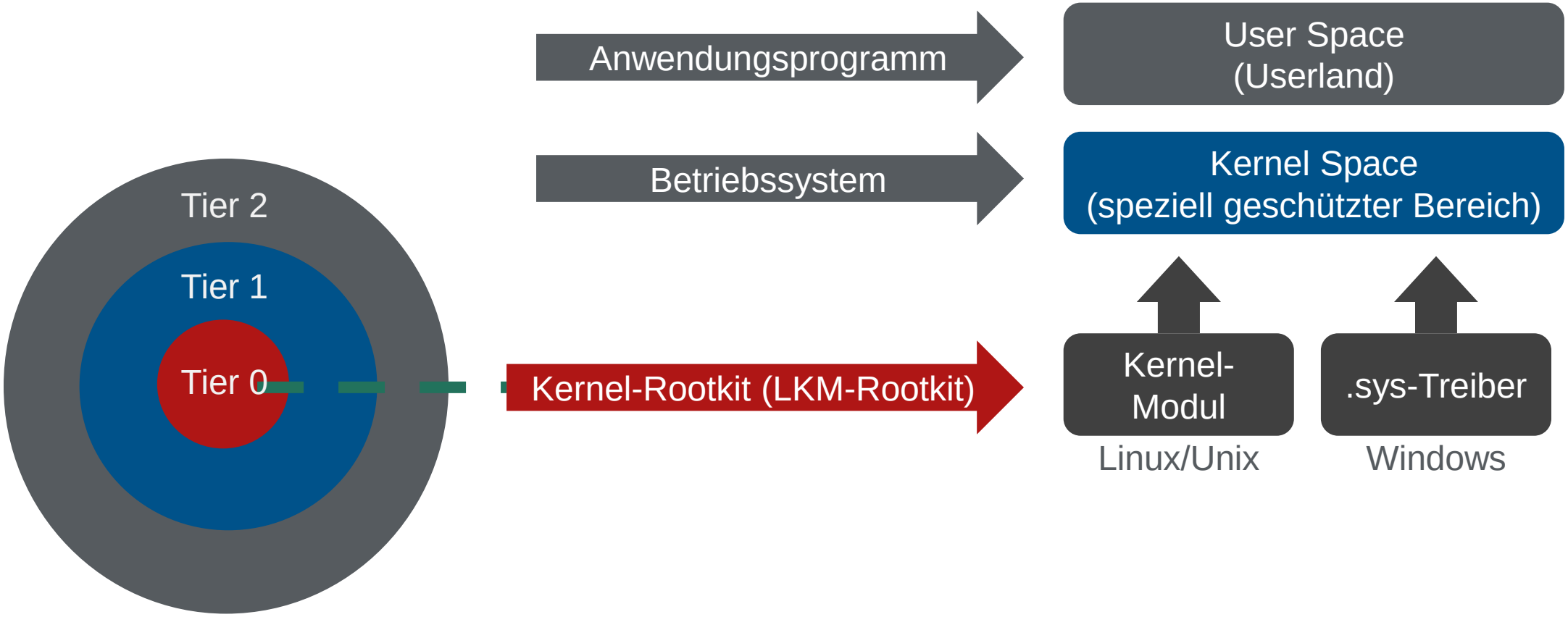
- Backdoor
- Downloader
- Packet Sniffer
- Keylogger / Spyware
- Bot für IRC, Spam oder DDOS-Anwendungen
- Etc.

Verstecken Schadcode

- Abfangen und Manipulieren von Systemaufrufen
- Listings, um versteckte Komponenten bereinigt (Prozesse, Verzeichnis-inhalte, Logfile)
- Deaktivieren des AV-Programms
- Etc.

Rootkit

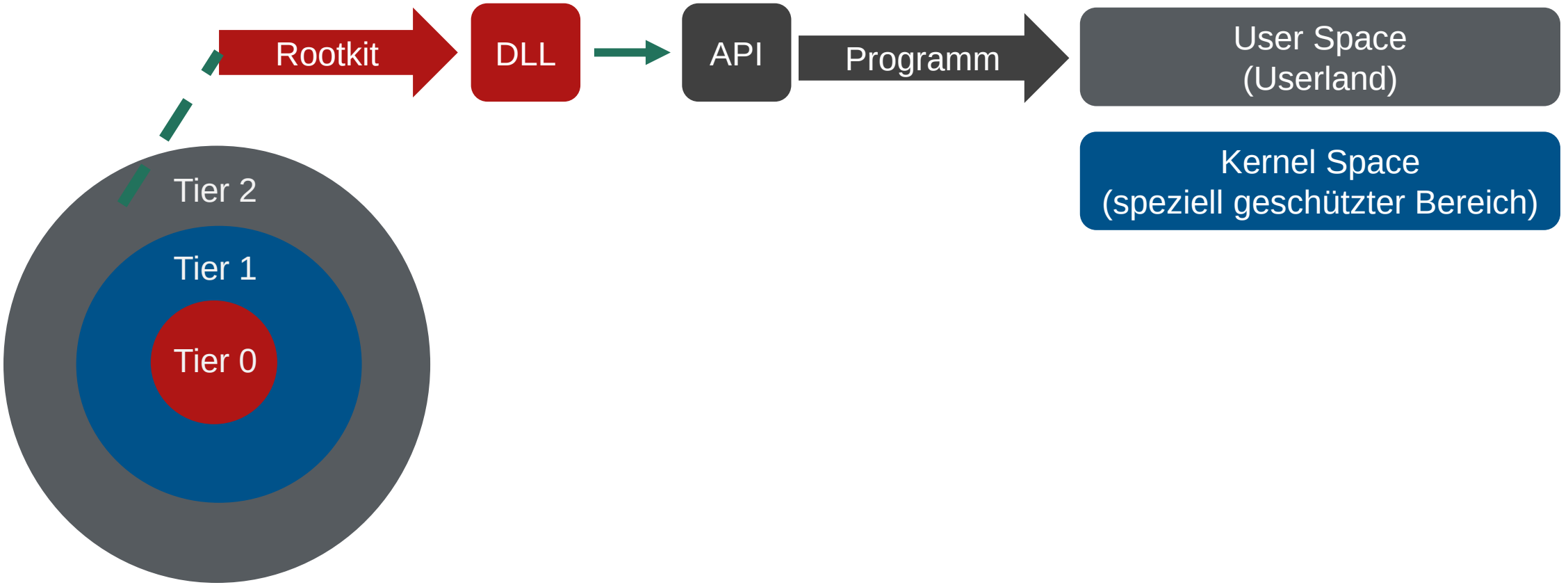
Kernel-Rootkits



Rootkit

Userland-Rootkits

Userland-Rootkits meist unter Windows verbreitet



Rootkit-Beispiele

XCP

- Stammt von Sony
- Digital Rights Management (DRM)
- Installiert in Windows ein Rootkit zum Schutz vor Entdeckung des Kopier-schutzes

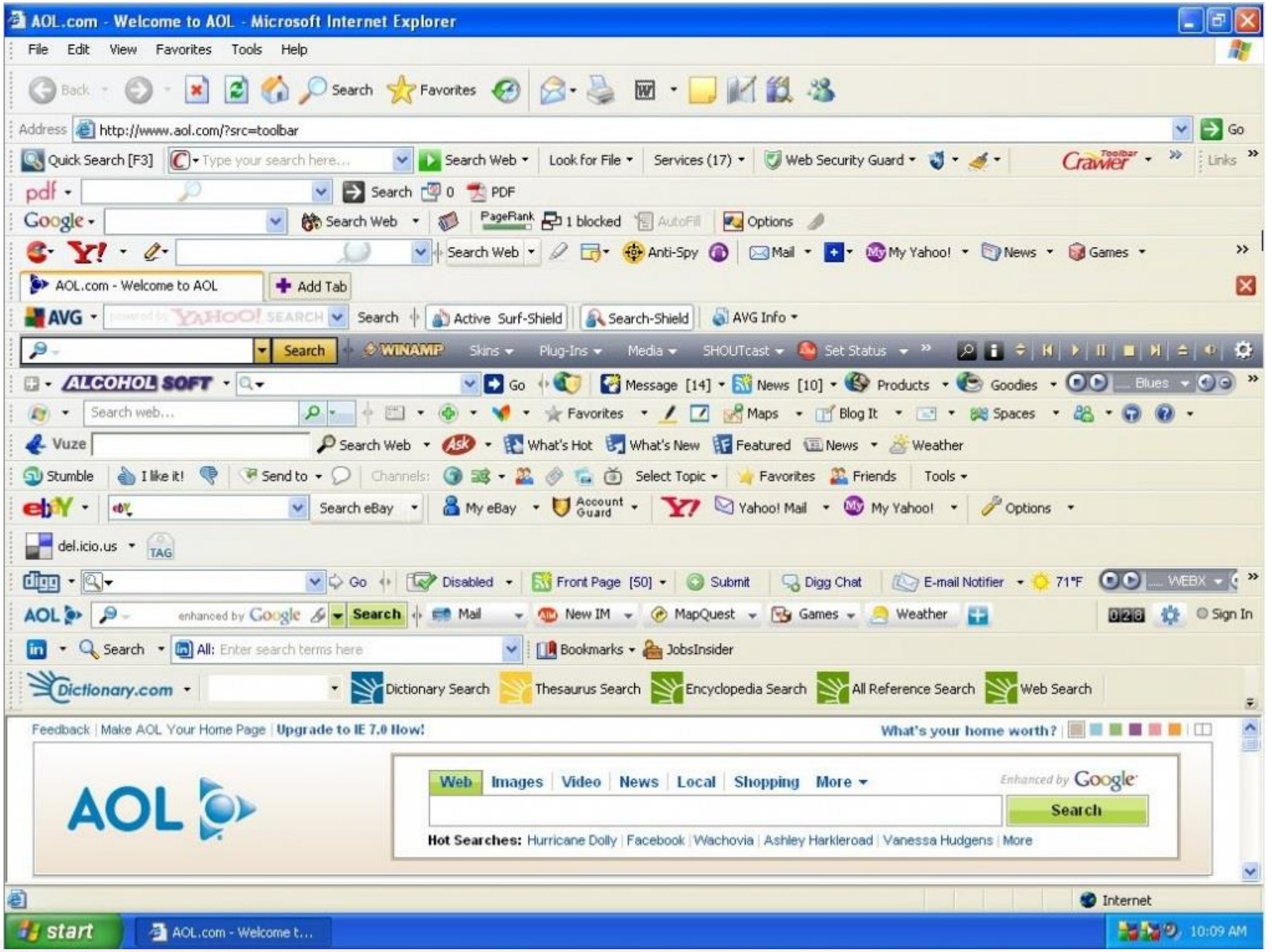
SecuROM

- Stammt auch von Sony
- Ebenfalls DRM
- Wurde in PC-Spielen verwendet (u. a. von EA)
- Nimmt heimlich eine Online-Authentifizierung vor

Botnetz ZeroAccess

- Seit 2011 (Heute nicht mehr aktiv)
- Ehemals bis zu 9 Mio. Computer infiziert
- Infektionswege (Trojaner, Keygen-Tool, Social Engineering, etc.)
- Payload entweder Bitcoin-Mining oder Click Fraud
- Installierte sich in MBR oder als zufälliger Treiber
- Deaktiviert Windows-Firewall + Defender

Toolbar


AOL.com - Welcome to AOL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.aol.com/?src=toolbar
Go
Quick Search [F3]
Type your search here...
Search Web
Look for File
Services (17)
Web Security Guard
Crawler
Links
pdf
Search 0 PDF
Google
Search Web
PageRank
1 blocked
AutoFill
Options
Search Web
Anti-Spy
Mail
My Yahoo!
News
Games
AOL.com - Welcome to AOL
Add Tab
AVG
Search
Active Surf-Shield
Search-Shield
AVG Info
Search
WINAMP
Skins
Plug-Ins
Media
SHOUTcast
Set Status
ALCOHOL SOFT
Go
Message [14]
News [10]
Products
Goodies
Blues
Search web...
Favorites
Maps
Blog It
Spaces
Vuze
Search Web
What's Hot
What's New
Featured
News
Weather
Stumble
I like it!
Send to
Channels:
Select Topic
Favorites
Friends
Tools
Search eBay
My eBay
Account Guard
Yahoo! Mail
My Yahoo!
Options
del.icio.us
TAG
digg
Go
Disabled
Front Page [50]
Submit
Digg Chat
E-mail Notifier
71°F
WEBX
AOL
enhanced by Google
Search
Mail
New IM
MapQuest
Games
Weather
Sign In
Search
All: Enter search terms here
Bookmarks
JobsInsider
Dictionary.com
Dictionary Search
Thesaurus Search
Encyclopedia Search
All Reference Search
Web Search
Feedback | Make AOL Your Home Page | Upgrade to IE 7.0 Now!
What's your home worth?
AOL
Web Images Video News Local Shopping More
Enhanced by Google
Search
Hot Searches: Hurricane Dolly | Facebook | Wachovia | Ashley Harkleroad | Vanessa Hudgens | More
Internet
start
AOL.com - Welcome t...
10:09 AM

Scareware


www.blue
www.blue
www.blue
An error was detected on your computer. Please contact a certified technician at (Toll Free)
OK
VIRUS DETECTED
WARNING!
YOUR COMPUTER MAY BE INFECTED:
System Detected (2) Potentially Malicious Viruses.
Your Personal Financial Information IS NOT SAFE
(24/7 - Toll Free - High Priority Virus Removel Call Line)
To Remove Viruses, Call Tech Support Now:

Malware

Rogueware
- Warnung vor Schadcode auf PC
- Geld bezahlen für gefälschte Tools
- Hintergrund Malware eingeschleust
- Eine Form von Ransomware

Dropper
- Eigenständig ausführbare Programm-Datei
- Kann andere Malware starten

Logic Bomb
- Eintreten bestimmter (logischer) Bedingung zur schädlichen Aktion
- z. B. Erreichen eines Datums oder andere Aktion

Malware

Dialer
- Einwahlprogramm aus früheren Zeiten
- Wählverbindung mit dem Internet
- Missbrauch durch Premium-Rate-Dialer

Spyware/Keylogger
- Ausspionieren von System
- Geben sich oft als Schutz des Unternehmens oder Kinderschutz aus

Cryptomining
- Hardware- und Energieressourcen des Benutzers werden unbemerkt und ohne Zustimmung für rechenintensives Mining verwendet

Malware?

Adware
- Engl. Advertisement und Software
- Werbung, die bei einer Software mit installiert wird

Bloatware
- Software mit Funktionen überladen
- Anwendungen meist unterschiedlicher Arbeitsfelder ohne gemeinsamen Nutzen
- Meist vorinstallierte Software

Crapware
- Unerwünschte Software auf PC und Smartphone
- Software ohne ersichtliche Funktion
- Aus Geschäftsinteresse mitinstallierte Software

Riskware
- Software mit erheblichen Sicherheitsproblemen
- Z. B. Adobe Flash Player

Modernere Malware Architektur

Dropper

Stage 1
Loader

Entschlüsselt & führt nächste Stage aus

Stage 2
Loader

Entschlüsselt & führt nächste Stage aus

Stage 3
Kernel
Framework

Stage 4
User
Framework

Stage 4
Kernel
Module 1

Stage 4
Kernel
Module N

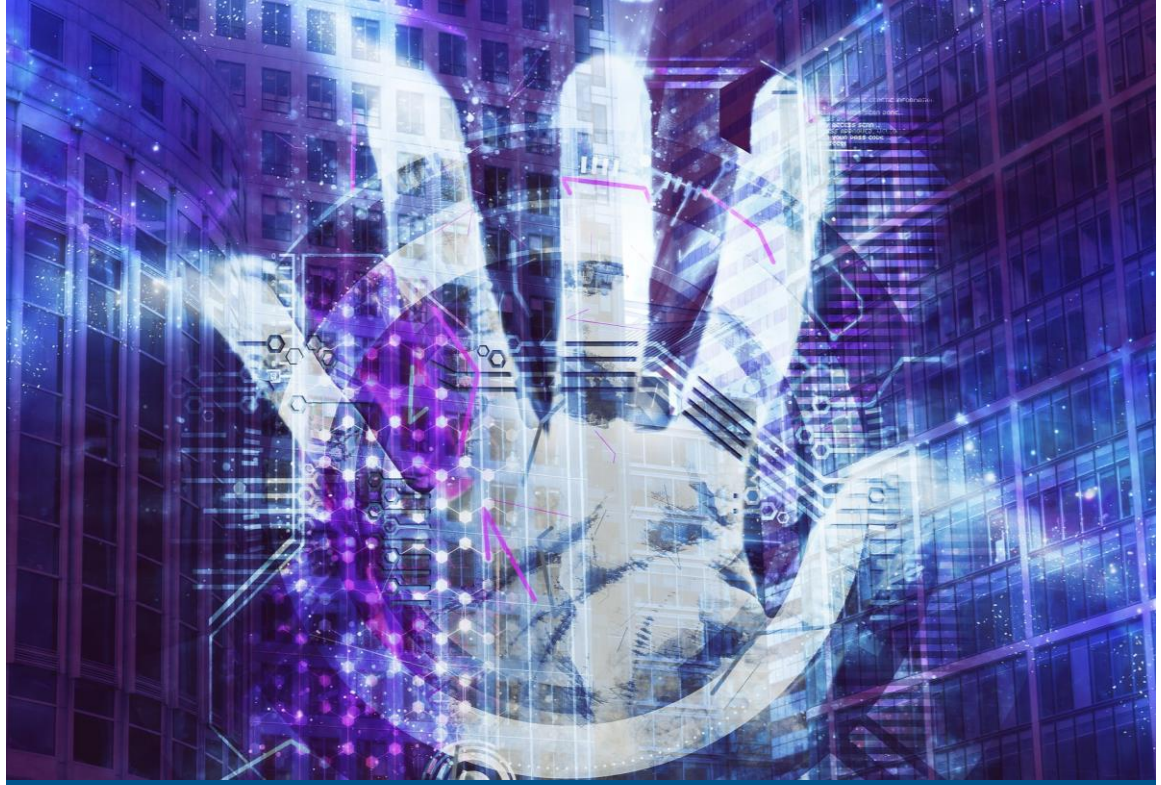
Verschlüsselter Container

Stage 5
Payload
Module 1

Stage 5
Payload
Module 2

Stage 5
Payload
Module N

Verschlüsselter Container



©Urheber

Angriffsarten

Lernziele

Verschiedene Angriffsmöglichkeiten

Angriffsarten

Nicknapping	DOS	DDOS
MitM	Spoofing	Poising
XSS	CSRF (XSRF)	Injection
Jailbreak / Rooting	Zero-Day	Cybersquatting

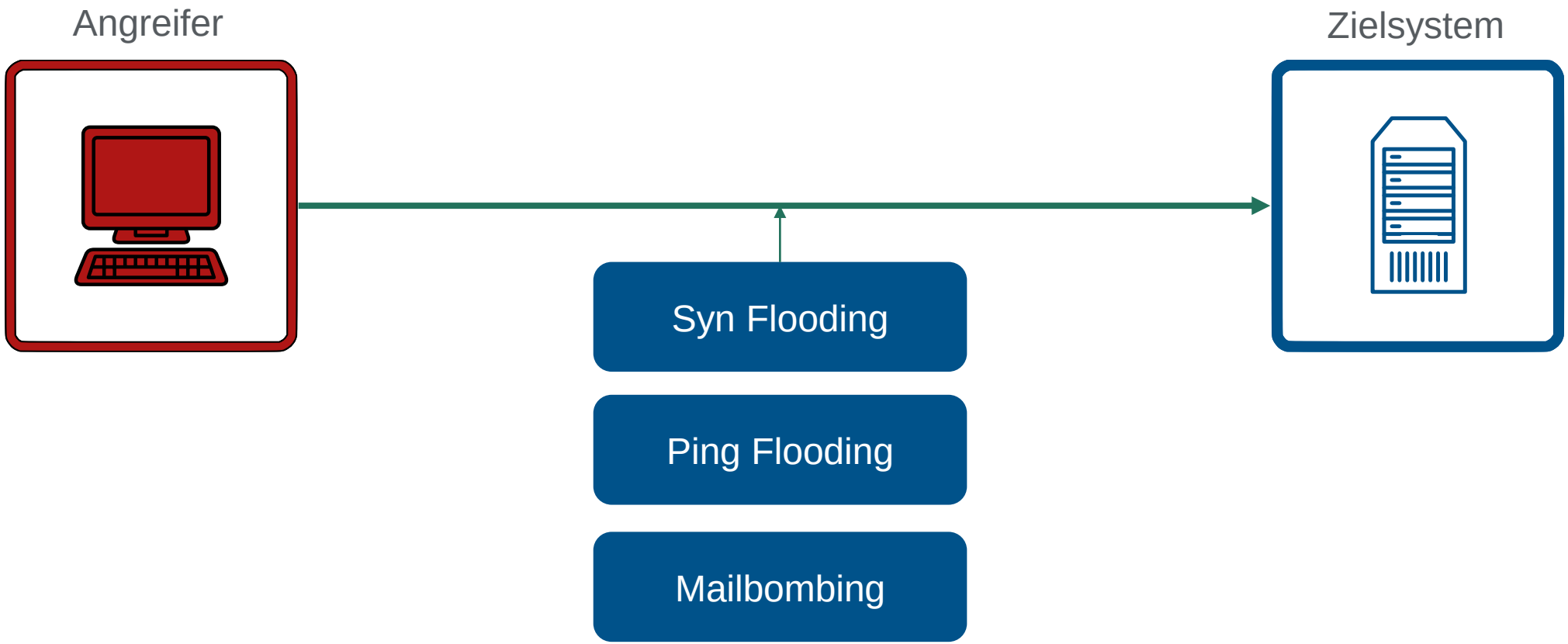
Nicknapping

- Spitzname, Alias-Name oder richtiger Name wird sich widerrechtlich angeeignet, gestohlen und verwendet
- Meist Zusammenhang mit gestohlenen Zugangsdaten und Passwörtern

- Kann auch zum Identitätsdiebstahl führen

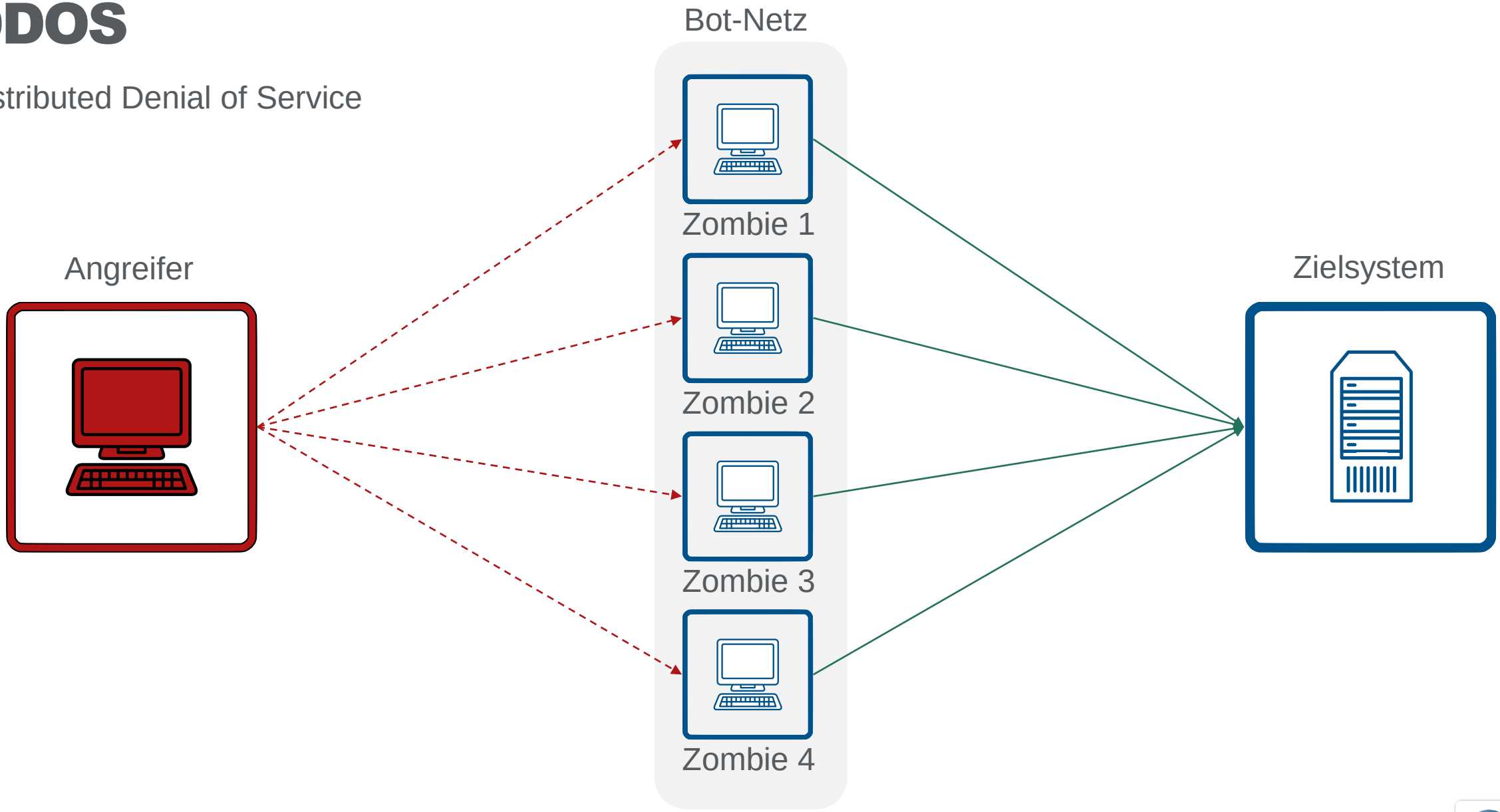
DOS

Denial of Service



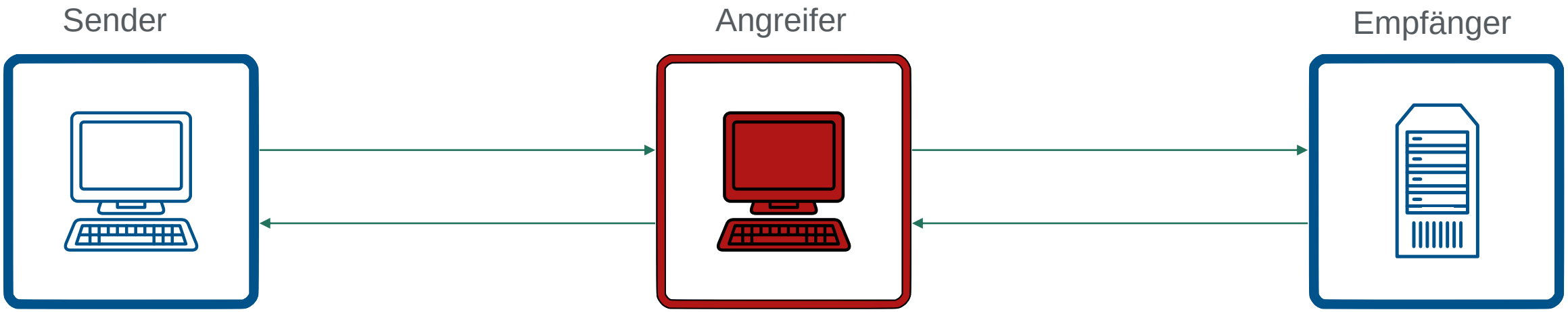
DDOS

Distributed Denial of Service



MitM

Man in the Middle



Spoofing / Poising

Spoofing

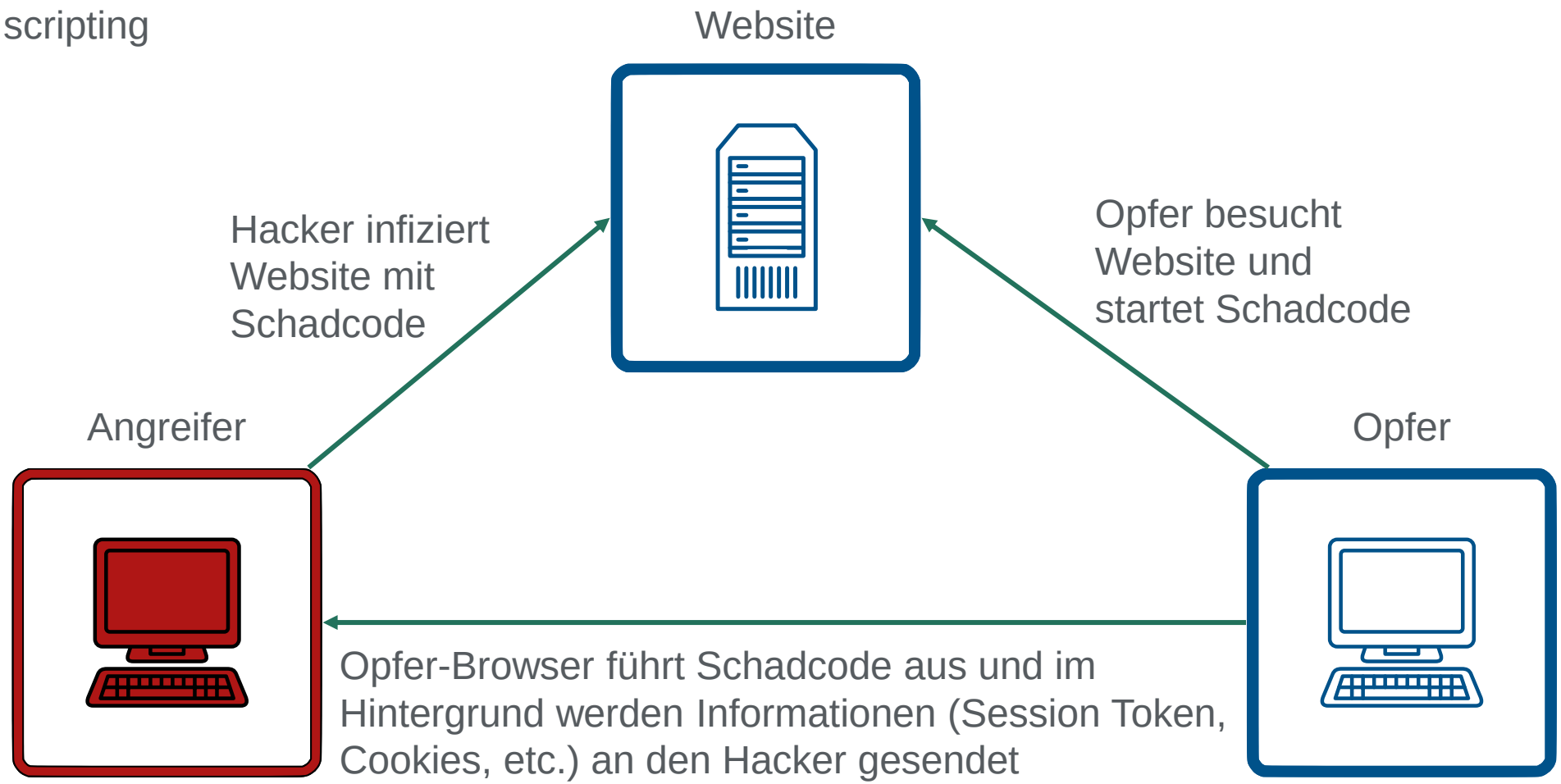
- Verschleiern der eigenen Identität
- Mail-Spoofing
- IP-Spoofing
- DNS-Spoofing
- ARP-Spoofing

Poising

- Manipulieren von Einträgen
- Cache-Poising
- ARP-Poising

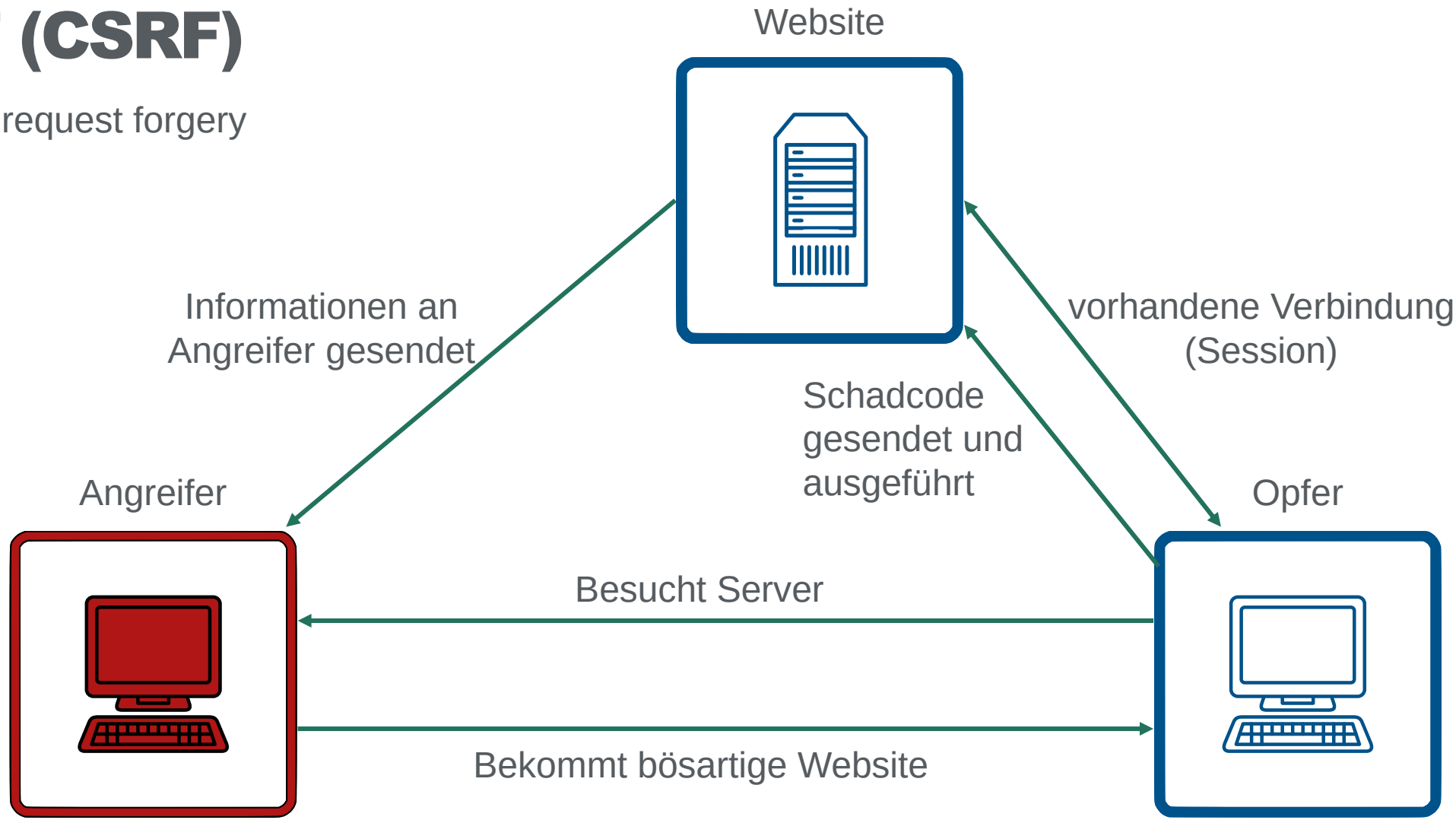
XSS

Cross-Site scripting



XSRF (CSRF)

Cross-Site request forgery



Injection

Code Injection
- Anwendungscode wird eingefügt
- Code wird mit Berechtigung des Users ausgeführt

- Vollständiges System kompromittiert

Cross-Site-Scripting
- Script wird auf Webserver eingefügt, um Opfer anzugreifen

- Identitätswechsel des Kontos

CRLF Injection
- HTTP-Antwortdatei aufteilen und beliebigen Inhalt implementieren

- Cross-Site Scripting möglich

E-Mail-Header Injection
- IMAP/SMTP-Befehle an Mailserver
- Ähnlich wie CRLF-Injection

- Spam-Relay, Offenlegung von Informationen

Injection

Host-Header Injection
- Missbrauch des HTTP-Headers
- Rücksetzen der Kennwörter und Web-Cache-Vergiftung

- Kennwort-Reset-, Cache Poising

SQL Injection (SQLi)
- SQL-Befehle an DB-Server, um Werte zu lesen, ändern oder löschen

- Offenlegung von Informationen, Datenverlust, Verlust Datenintegrität

LDAP Injection
- LDAP-Befehle, um Berechtigungen zu erhalten und Inhalte des LDAP-Baums zu ändern

- Umgehung der Authentifizierung

XPath Injection
- XPath-Abfragen in Daten
- Zugriff auf nicht autorisierte Daten ohne Authentifizierung

- Offenlegung von Informationen

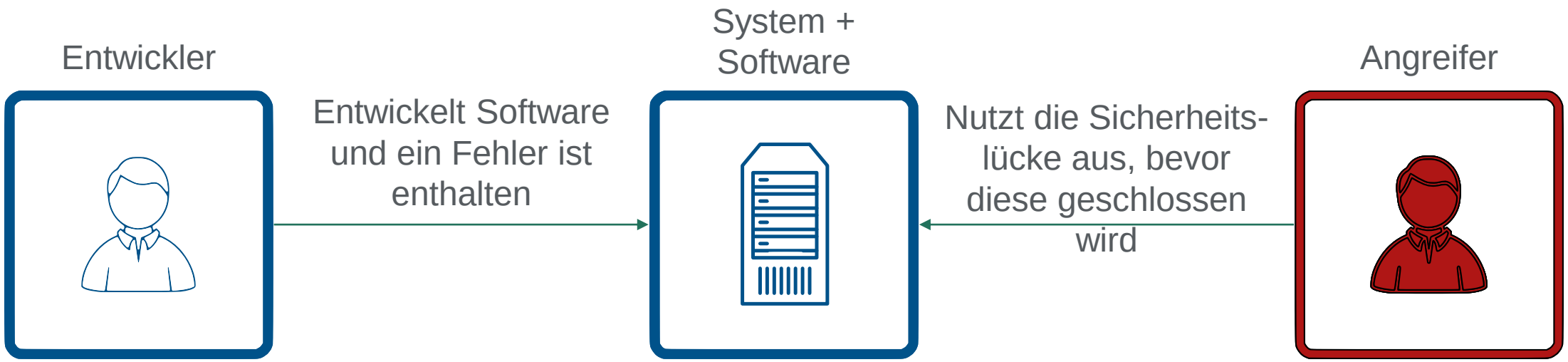
Jailbreak & Rooting

- Nicht autorisiertes Entfernen von Nutzungsbeschränkungen
- Meist zum Entfernen von vorinstallierter Software

- Jailbreak = BSD-Systeme
- Rooting = Unix-Systeme

Zero-Day-Attack

- Ein Fehler in der Software oder Hardware
- Ausnutzung der Schwachstelle, bevor sie entdeckt wird



Cybersquatting

- Domainsquatting genannt
- Aneignen einer Domain, die einem nicht zusteht

Typosquatting

- Tippfehler in der URL
- z. B. www.gfm.de
- statt www.gfn.de

Combosquatting

- Nennung eines bekannten Anbieternamens und diesen mit unübersichtlichen Zusätzen erweitern
- z. B. Für Phishing-Mails