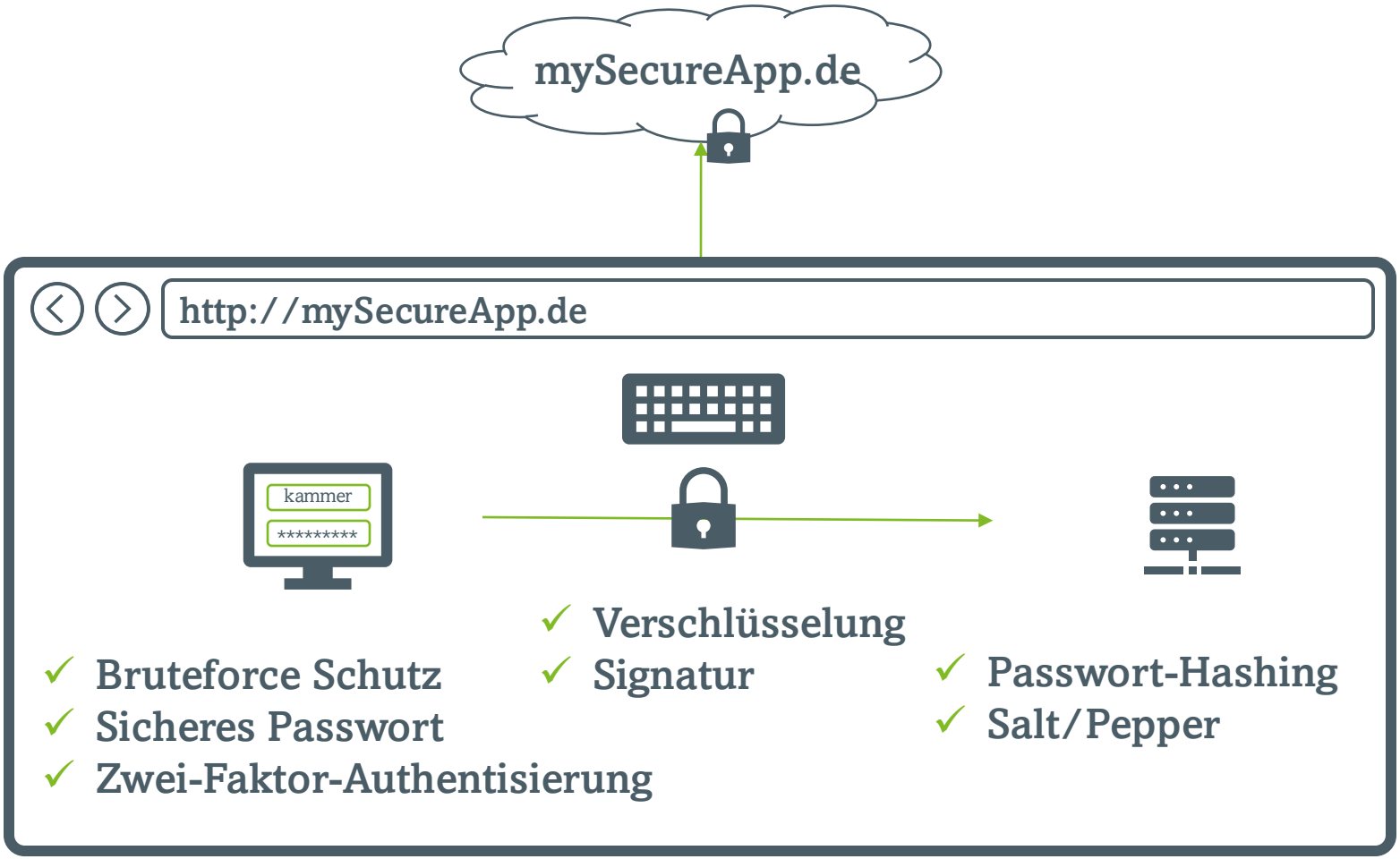
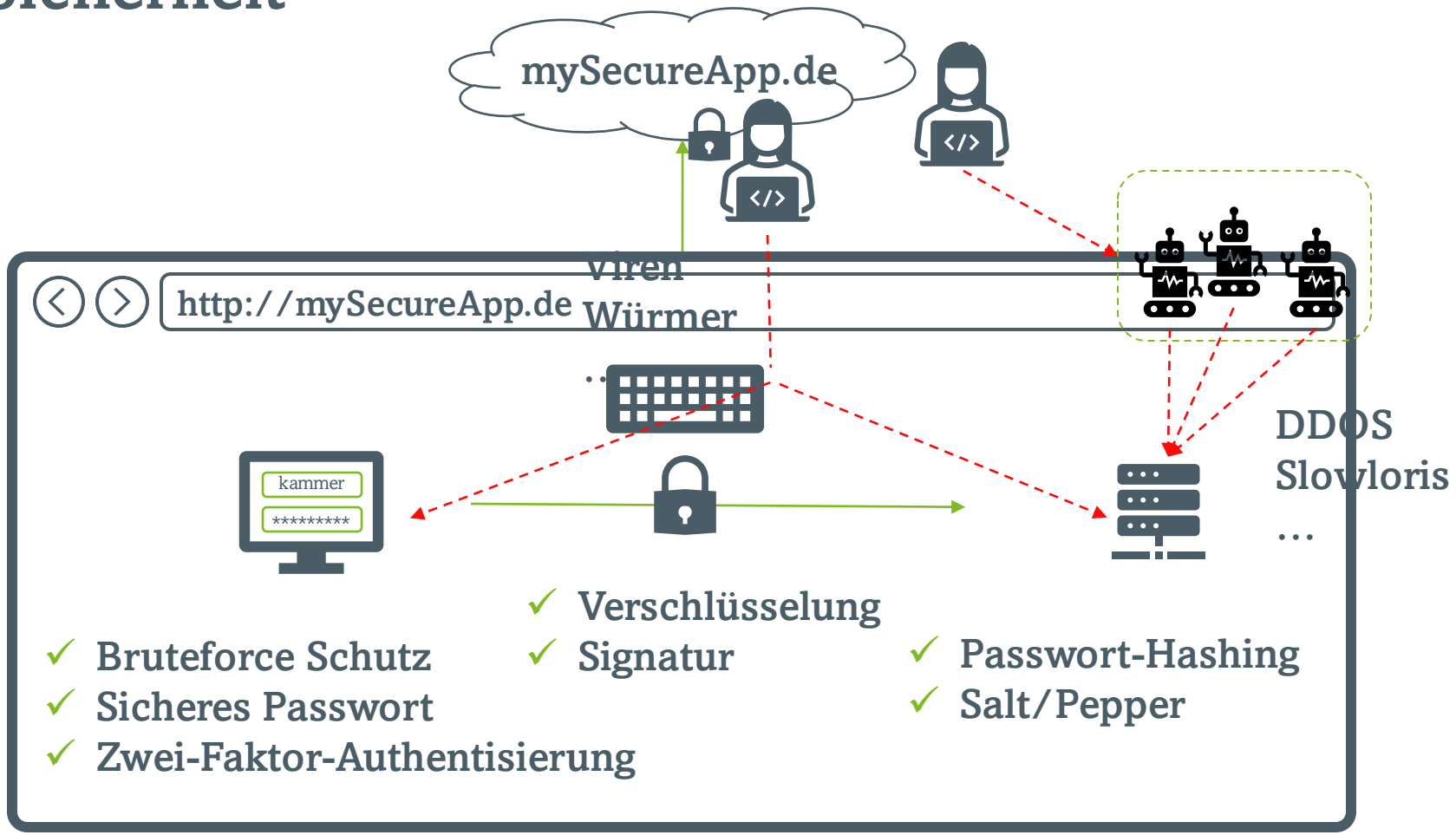
Netzwerk Sicherheit

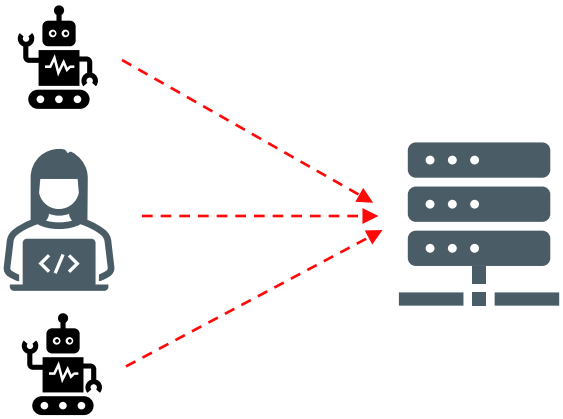
Rückblick


mySecureApp.de
http://mySecureApp.de
kammer
****
✓ Bruteforce Schutz
✓ Sicheres Passwort
✓ Zwei-Faktor-Authentisierung
✓ Verschlüsselung
✓ Signatur
✓ Passwort-Hashing
✓ Salt/Pepper

Netzwerk Sicherheit



Angriffe auf die Infrastruktur

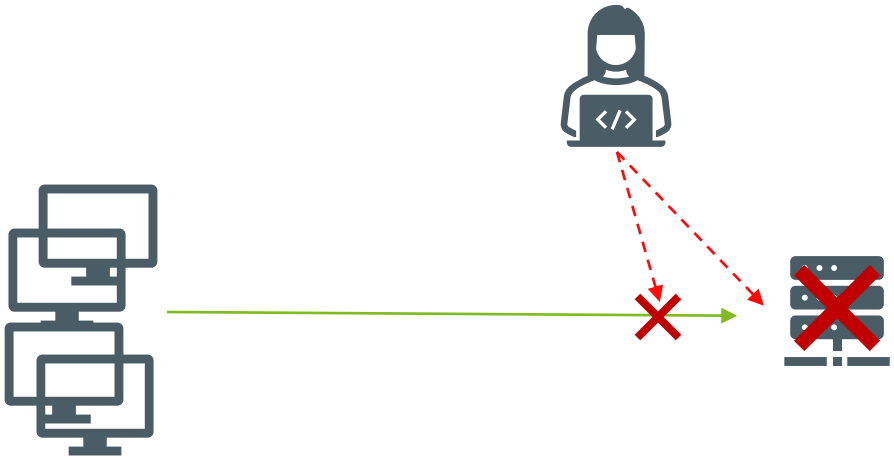


- DDoS
- Slowloris

Angriff

Schutz

Denial of Service (DoS)



Ziel

- Nichtverfügbarkeit des Ziels
- Geschäftsschädigung
- Lösegeld

Distributed Denial of Service (DDoS)

- DoS Angriffe von wenigen Rechnern meist einfach zu Blockieren

DDoS

- Angriff über ein Botnetz aus vielen Rechner
  - Infektion der Rechner meist über Trojaner

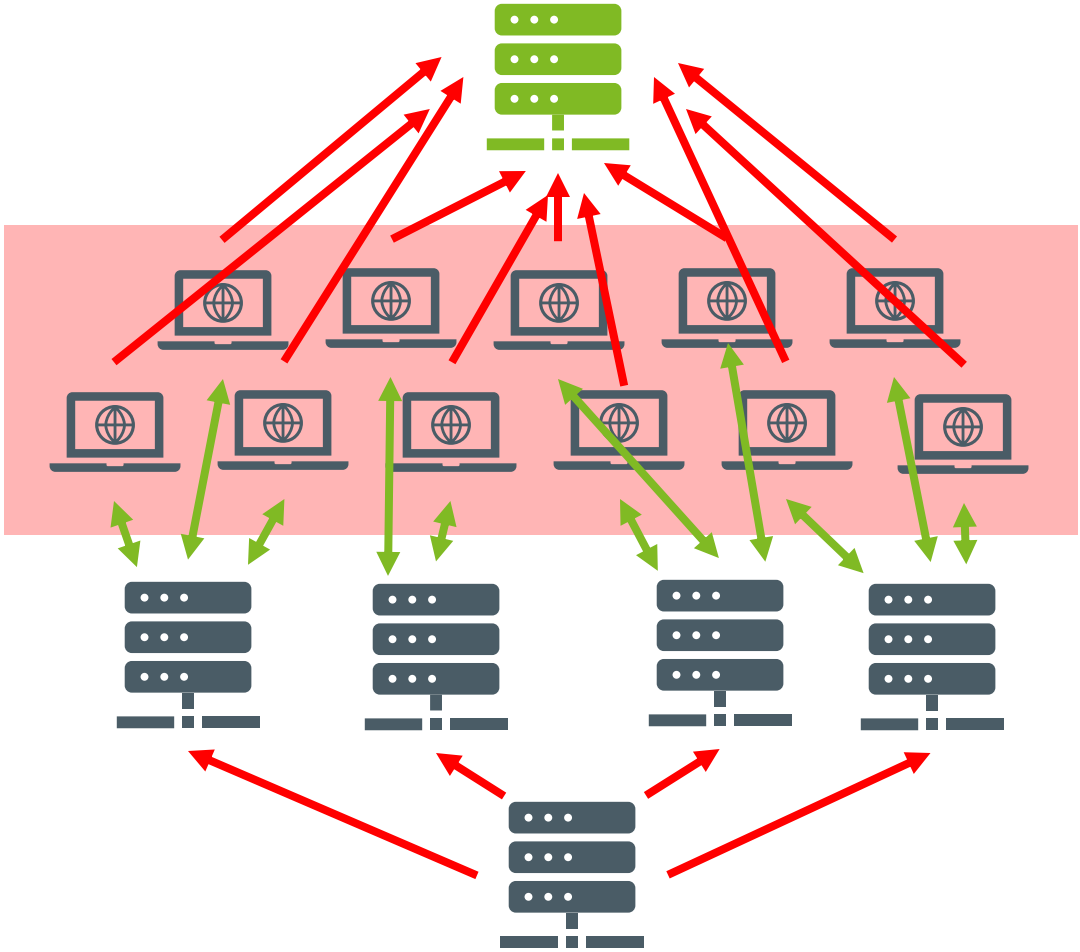
Distributed Denial of Service (DDoS)

Target

Botnetz

C & C Server

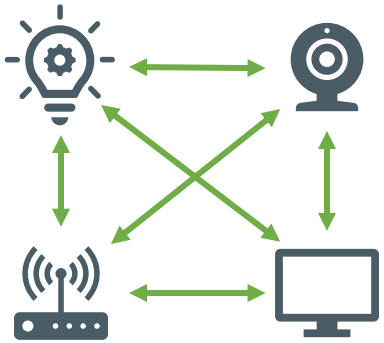
Master-Server



Beispiel

Mirai

- Schadsoftware zum Aufbau von Botnetzen
- Ursprüngliches Netz mit 500.000 kompromittierte IoT-Geräte



Bekannte DDos Angriffe

- Telekommunikationsanbieter OVH
  - Eigentliches Ziel: Minecraft-Server
- DNS Service Anbieter Dyn
  - Eigentliches Ziel: PlayStation Network
- …

Distributed Denial of Service (DDoS)

Schutz

- Angriffsfläche verringern
- Bandbreite
- Blockieren (schwierig)

Distributed Denial of Service (DDoS)

Angriffsfläche verringern

- Content Distribution Networks (CDNs) oder Load Balancer verwenden
- Direkten Internetdatenverkehr begrenzen
- Firewalls oder Access Control Lists (ACLs) verwenden
- Nutzung von VPN oder WAN für interne Dienste

Distributed Denial of Service (DDoS)

Bandbreite

- ausreichend redundante Internetkonnektivität bereitstellt

Distributed Denial of Service (DDoS)

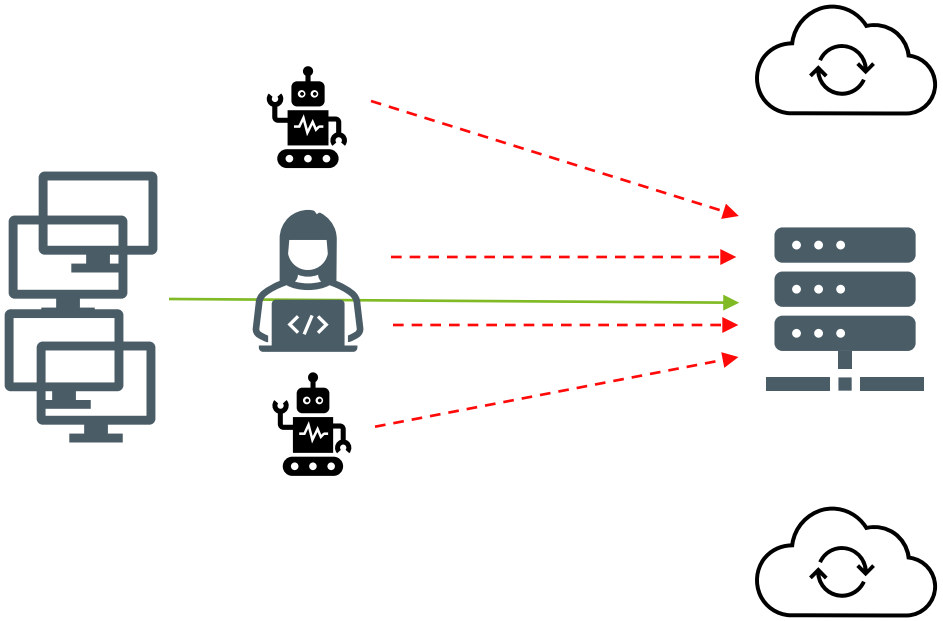
Blockieren

- Blockieren von bestimmten IP-Bereichen (z.B. nur Anfragen aus Deutschland)
- Quotenbegrenzung
- Filtern von böswilligem Datenverkehr

Distributed Denial of Service (DDoS)

Blockieren

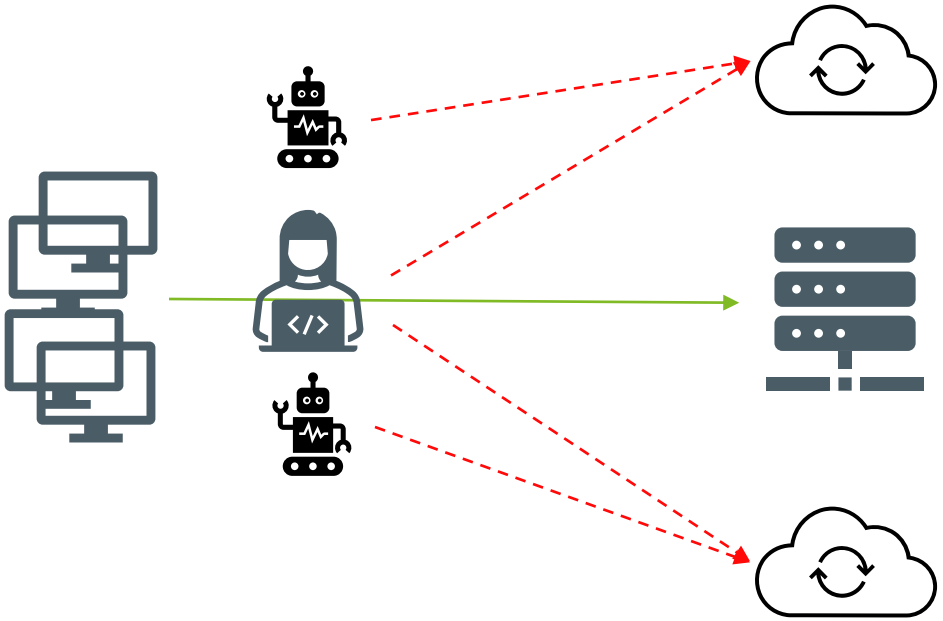
Filtern von böswilligem Datenverkehr



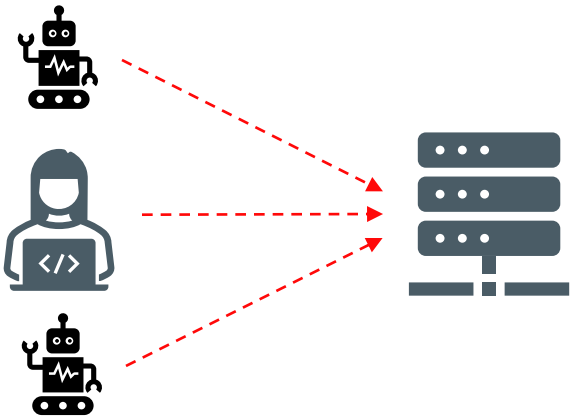
Distributed Denial of Service (DDoS)

Blockieren

Filtern von böswilligen Datenverkehr

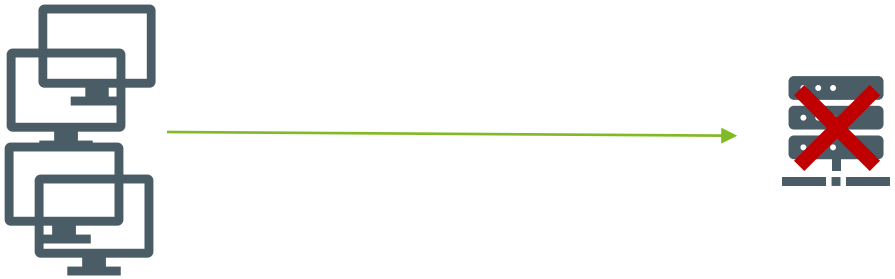


Angriffe auf die Infrastruktur



- DDoS
- Slowloris

Slowloris



Ziel:

Threadpool erschöpfen

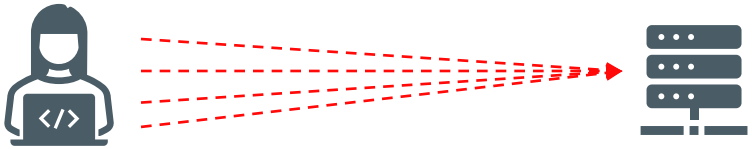
Slowloris

Methode:

- Protokoll Angriff (Layer 7) - greift den Webserver an
- Benötigt wenig Bandbreite
- Nutzt threadbasierte Verbindungen z.B. von Apache aus

„Boring a server to death“

Slowloris



Vorgehen:

- viele Verbindungen zum Zielserver aufzubauen
- Verbindungen so lange wie möglich offen halten

Beispiel

Bekannte Slowloris Angriffe

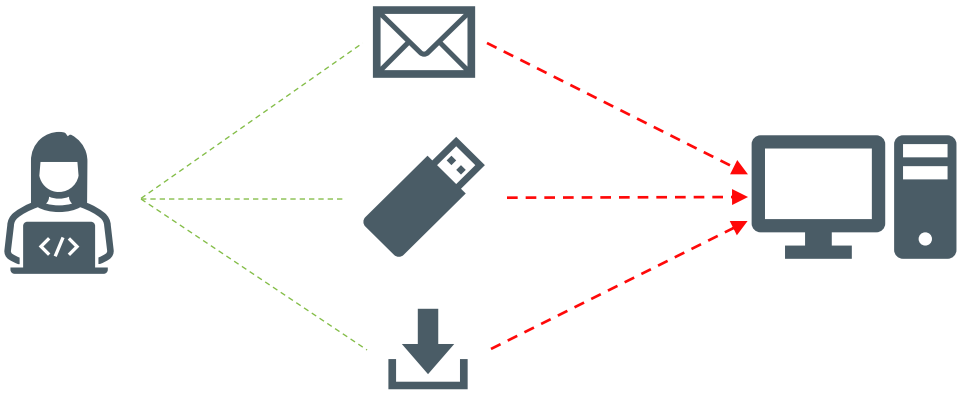
- 2009 Mehrwöchiger Angriff auf die Webseiten der Iranischen Regierung
- 2011 Angriff auf die Website der CIA

Slowloris

Schutz:

- Reverse Proxy
- Firewall
- Apache Module

Angriffe auf das System



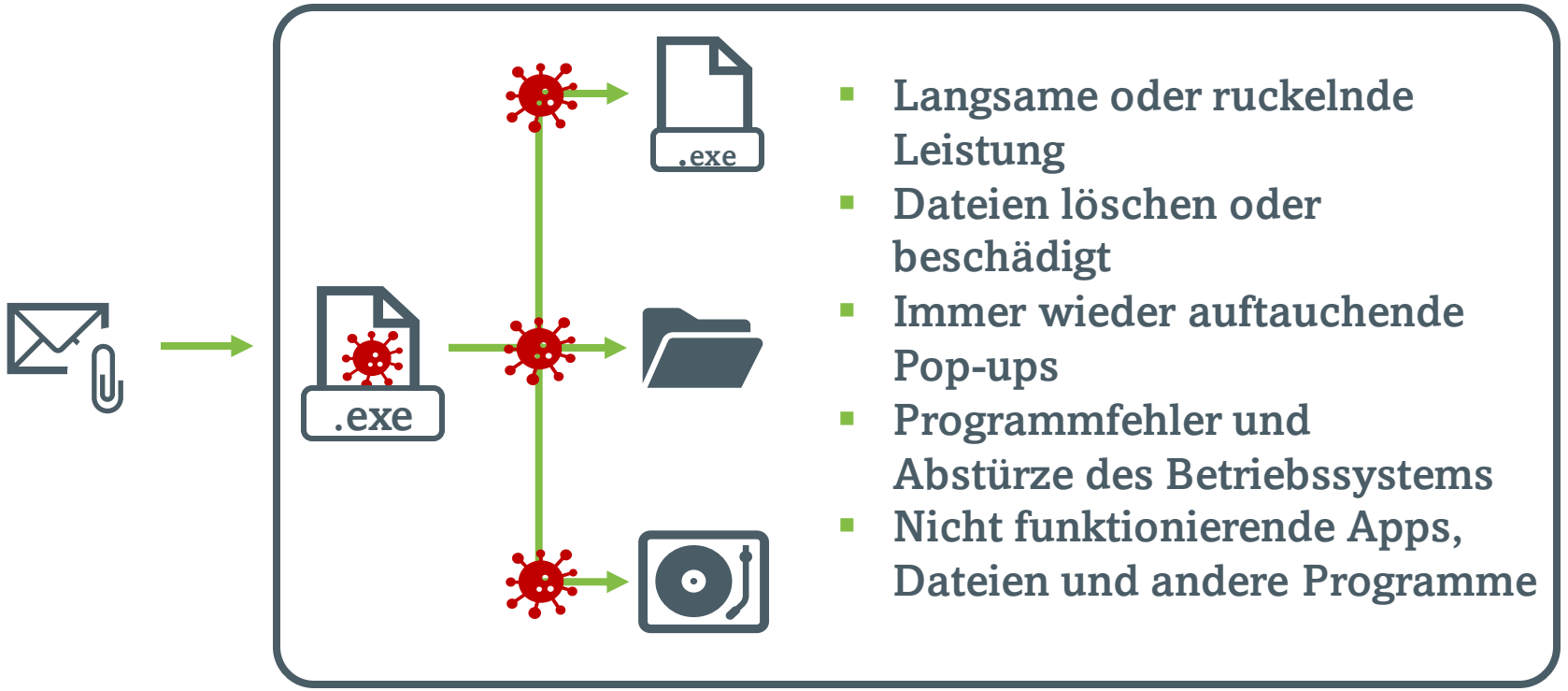
- Viren
- Würmer
- Ransomware
- Wiper

Viren

- Schadprogramm, dass sich selbständig reproduziert
- Wie werden Viren verbreitet?
  - E-Mail-Anhang
  - Infizierte Website
  - Ausführbare Dateien
  - Infizierte Speichermedien
- Ein Virus benötigt eine Benutzeraktion, um sich zu verbreiten.
- Ein Virus kann alles, was ein Computerprogramm auch kann.

Viren

Funktionsweise

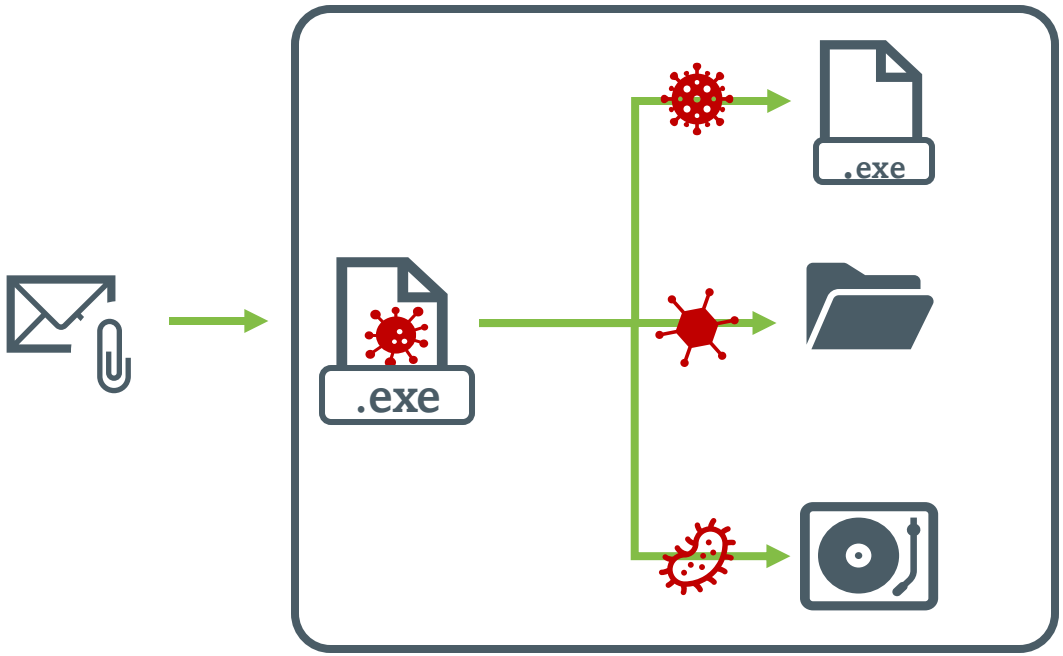


- Langsame oder ruckelnde Leistung
- Dateien löschen oder beschädigt
- Immer wieder auftauchende Pop-ups
- Programmfehler und Abstürze des Betriebssystems
- Nicht funktionierende Apps, Dateien und andere Programme

Viren

Funktionsweise

Mutation: Virus verändert sich beim Kopieren



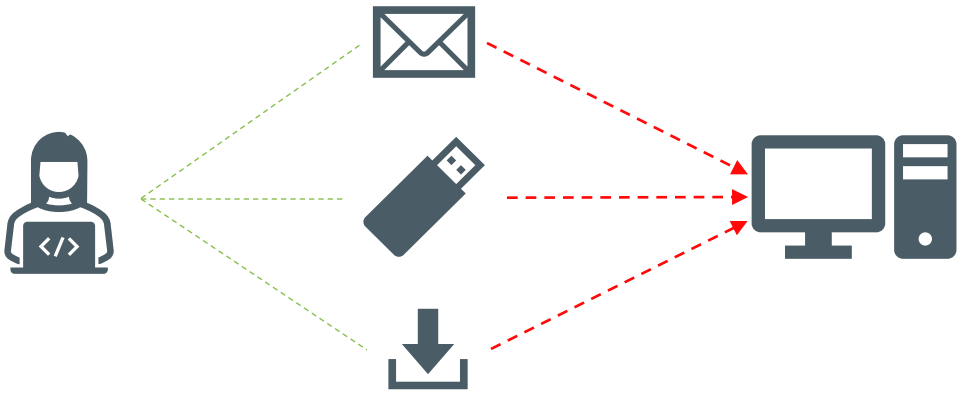
Viren

- **Speicherung von Viren in**
  - Code-Segmenten ausführbarer Programme
  - Betriebssystemen
  - Boot-Sektor des Hintergrundspeichers
- **Bedrohung durch Viren: Integrität, Vertraulichkeit, Systemverfügbarkeit**

Viren

- **Abwehrmaßnahmen:**
  - Integritätsprüfungen (Code-Inspektion)
  - Signierte Software
  - Quarantänestationen für neue Software
  - Sorgfalt der Benutzer
  - gutes Rechte-Management (minimale Rechte)

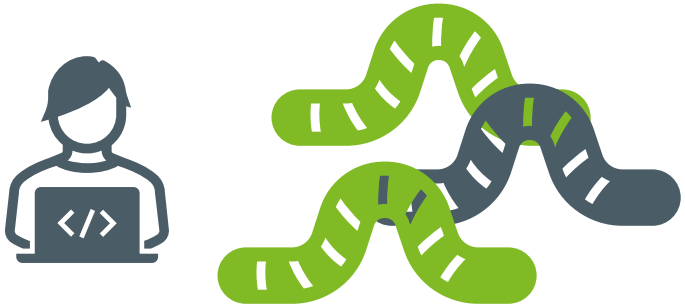
Angriffe auf das System



- Viren
- Würmer
- Ransomware
- Wiper

Würmer

- Haben klassische Viren verdrängt.
- Benötigen keine Benutzeraktion zu Reproduktion.
- Verbreitung vor allem über Internet
- Angriffspunkte häufig Fehler in Betriebssystem oder zentralen Systemprogrammen/Netzwerkschnittstellen
- Ausbreitung oft rasend schnell (bevor Patches verfügbar sind oder flächendeckend installiert sind)



Würmer

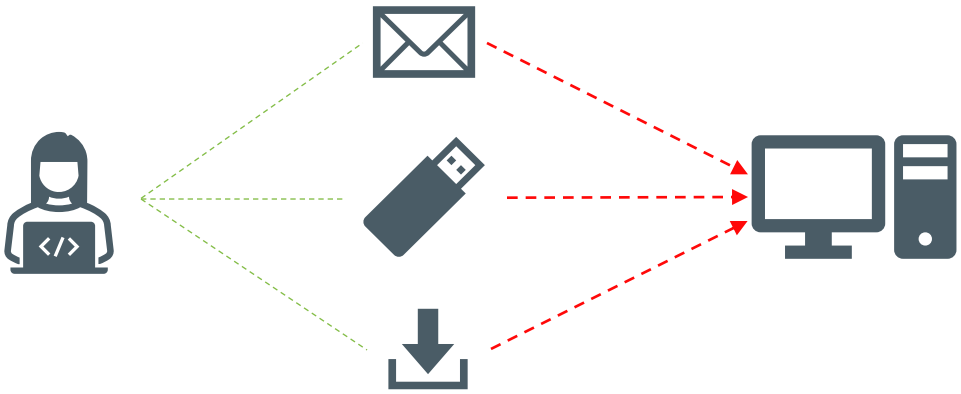
Bedrohungen

- Integrität und Vertraulichkeit von Daten
- vor allem Systemverfügbarkeit
- Schaden alleine durch Systemausfälle oft ~ 10 - 100 Mio. $

Würmer

- **Abwehrmaßnahmen:**
  - Schutz vor Social Engineering
  - Umgang mit E-Mail-Anhängen und anderen Dateien aus externen Quellen
  - Schutz durch Software
    - Virenscanner
    - Firewall
    - gutes Rechte-Management (minimale Rechte)

Angriffe auf das System



- Viren
- Würmer
- Ransomware
- Wiper

Ransomware

Auswirkungen

- **Zugang zu einem System ist gesperrt**
- **Daten sind verschlüsselt**
  - Neben lokalen Laufwerken auch angeschlossene externe Medien (z.B. USB-Sticks) sowie Netzlaufwerke

Ransomware

Häufigste Angriffsarten

- Anhänge von Spam-Emails
- Drive-by-Angriffe: Sicherheitslücken in aktiven Inhalten (JavaScript, ActiveX, Browser-Plug-ins, ...) mithilfe so genannter Drive-by-Exploits ausnutzen.

Wie merkt man, dass man angegriffen wurde?

> **Leider erstmal gar nicht. Irgendwann ...**

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   X86GcZ-7PRNBE-3mNFMp-z88VnG-uF5nhF-4wzxwZ-XdNrr6-FYG89D-xk4rNz-9yPzJS

If you already purchased your key, please enter it below.
Key: _

Ransomware

Gegenmaßnahmen

- Bei einem Ransomware-Befall wenig Möglichkeiten, falls kein Backups oder Sicherheitssoftware vorhanden sind
- Verzeichnisse von Schlüsseln & Entschlüsselungsprogrammen → Mögliche Entschlüsselung ohne Bezahlung

Prävention

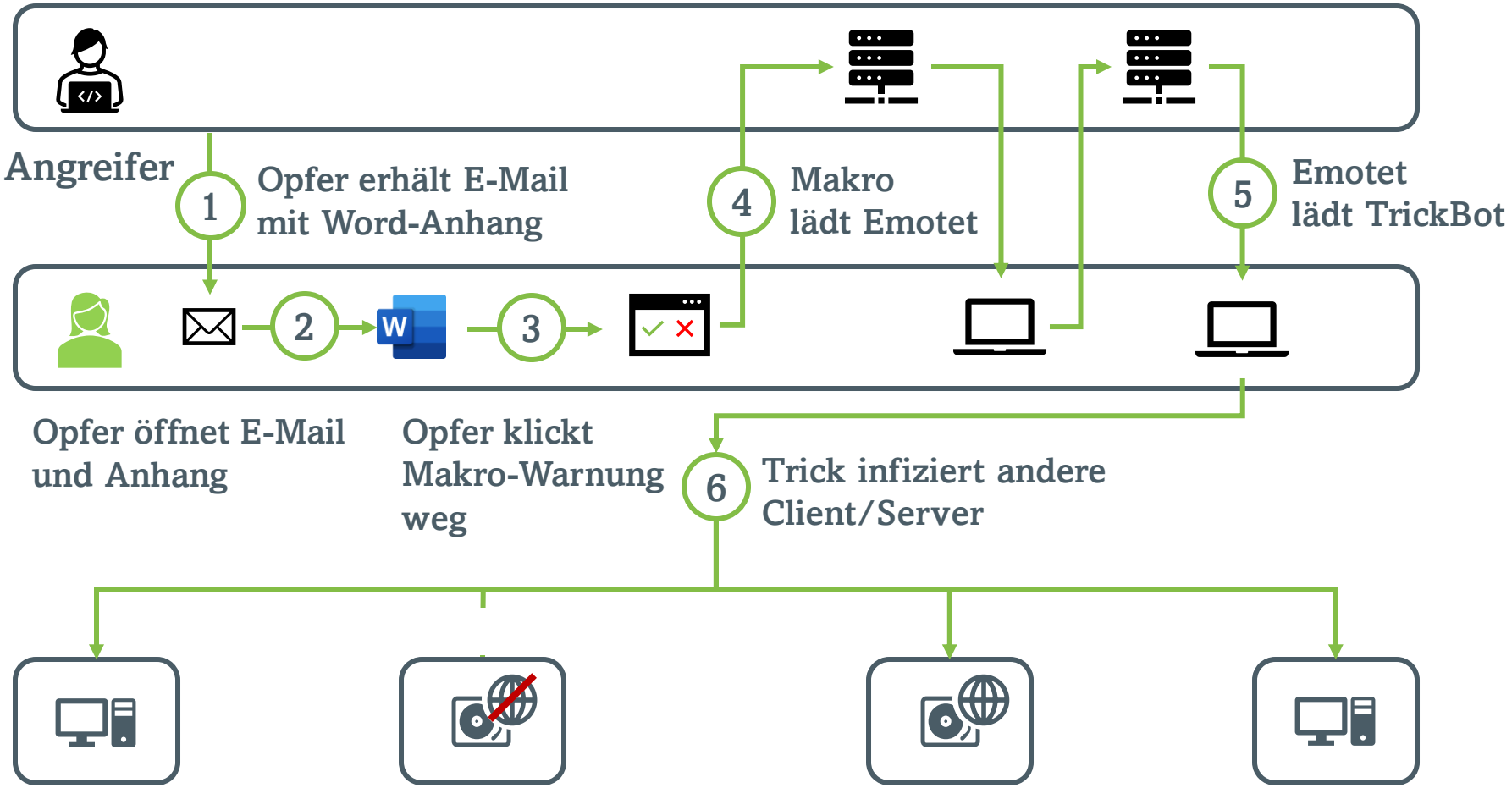
- Befolgen einfacher Sicherheits-Maßnahmen im Internet

Beispiel

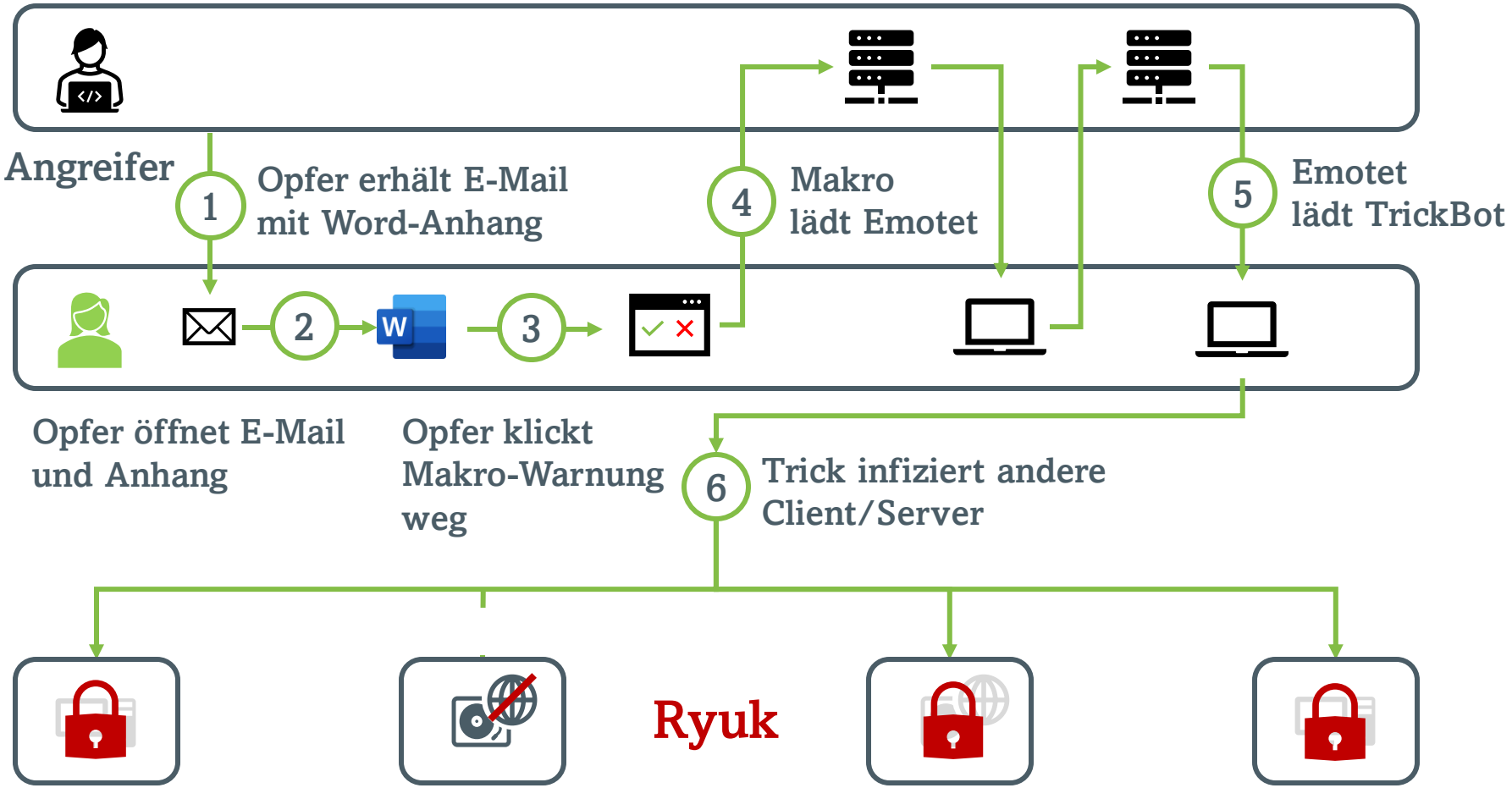
JLUoffline

- Entdeckt am 8. Dezember 2019
- Ca. 5 Wochen alle Systeme offline
  - Monate zur Wiederherstellung aller Systeme
- 1,7 Millionen Euro Schaden
- Infektion über „Emotet“ und der Ransomware „Ryuk“
- Insgesamt wurden 38.000 Passwörter zurückgesetzt.

Beispiel


Angreifer
1
Opfer erhält E-Mail mit Word-Anhang
2
3
4
Makro lädt Emotet
5
Emotet lädt TrickBot
Opfer öffnet E-Mail und Anhang
Opfer klickt Makro-Warnung weg
6
Trick infiziert andere Client/Server

Beispiel

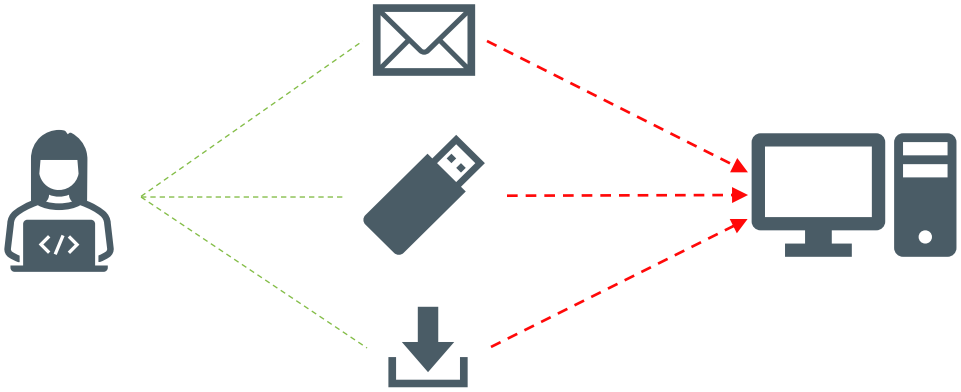

Angreifer
1
Opfer erhält E-Mail mit Word-Anhang
2
3
4
Makro lädt Emotet
5
Emotet lädt TrickBot
Opfer öffnet E-Mail und Anhang
Opfer klickt Makro-Warnung weg
6
Trick infiziert andere Client/Server
Ryuk

Beispiel

c't-Sicherheitstool Desinfec‘t

- Tool zur Überprüfung von Viren, Trojaner, Rootkits usw. auf Windows-Systemen
- Ausführung via Live-USB Stick
- Bietet auch Tools zur Reinigung des Systems

Angriffe auf das System



- Viren
- Würmer
- Ransomware
- Wiper

Angriff

Schutz

Wiper

- Erstmal nicht von Ransomware zu unterscheiden
- Gleiche Angriffsarten (Spam-Emails, Drive-by-Angriffe)
- Oft verschlüsselte Daten und Frage nach Geld
- Analyse der Wiper-Programmcodes offenbart:
  - Eine Datenrettung ist nicht vorgesehen.
  - **Ziel:** Zerstörung (von Infrastruktur)
  - Teil der Cyper-Kriegsführung.

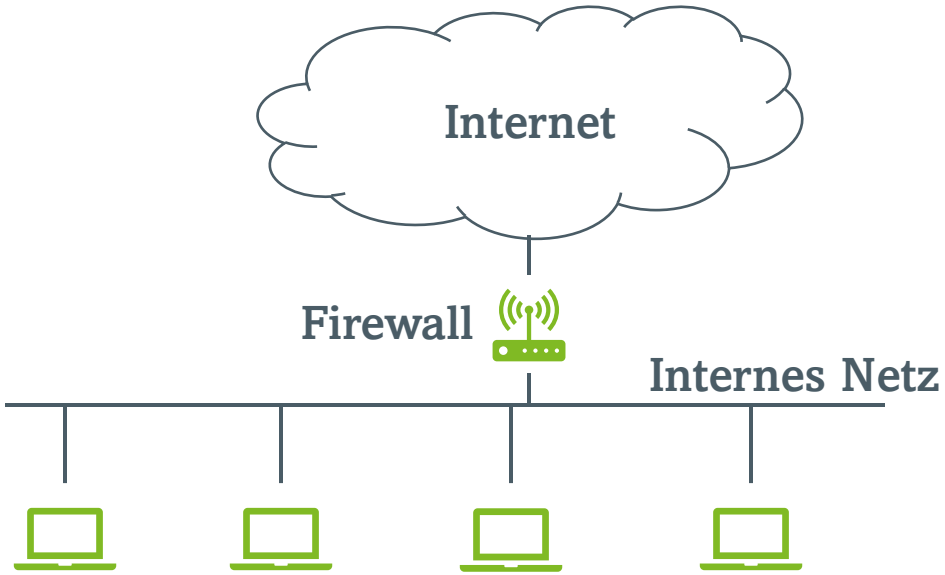
Technologien

- Firewall
  - Iptables
- WAN/VPN
- Proxy

Firewall

- Eine Firewall ist ein Vermittlungsrechner zwischen zwei Netzen, üblicherweise dem Internet und einem geschützten Bereich.
- Die Firewall beschränkt den Datenverkehr zwischen den Netzen.

Firewall

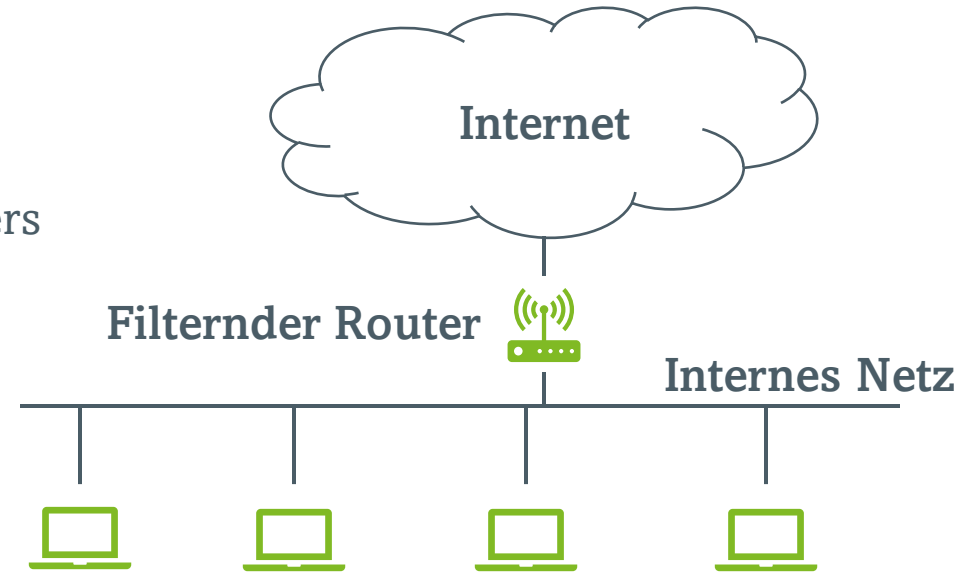


Firewall

- Eine Firewall ist ein Vermittlungsrechner zwischen zwei Netzen, üblicherweise dem Internet und einem geschützten Bereich.
- Die Firewall beschränkt den Datenverkehr zwischen den Netzen.
- Zwei Arten von Firewall gibt es
  - Paketfilter
  - Proxys
- Firewalls arbeiten richtungsabhängig
  - Für eingehenden Verkehr
  - Für ausgehenden Verkehr
- Oft mehrere Firewalls für verschachtelte geschützte Bereiche

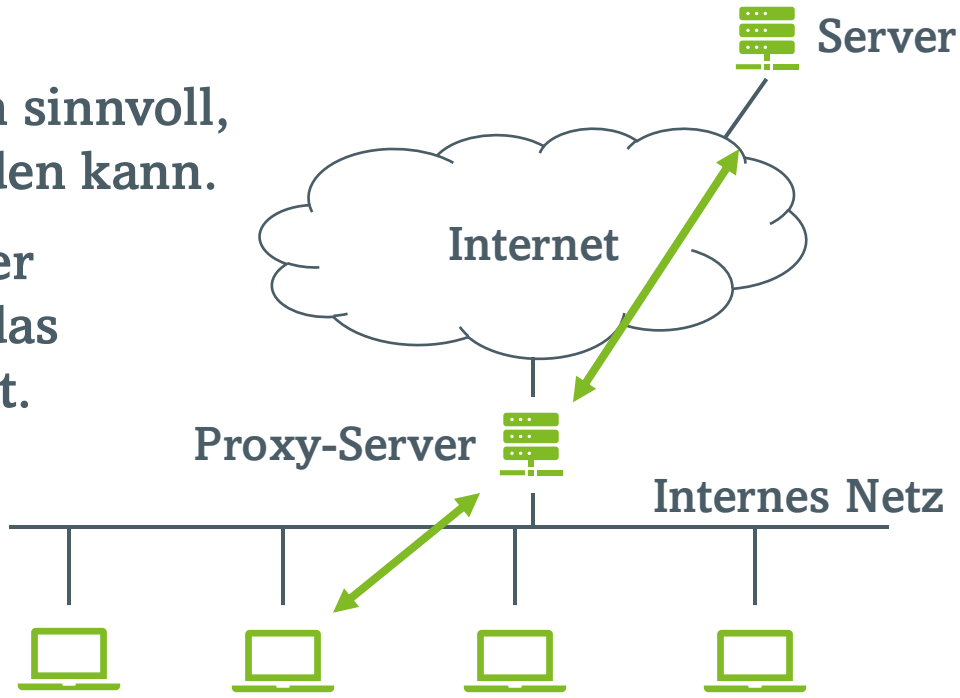
Paketfilter

- **Die Aufgabe des Paketfilterns wird meist von einem Router übernommen, der eingehende und ausgehende Pakete filtert.**
- **Er verwirft Pakete abhängig von**
  - IP Adresse des Senders
  - IP-Adresse des Empfängers
  - Protokoll (TCP, UDP, ICMP)
  - TCP/UDP Port des Senders
  - TCP/UDP Port des Empfängers
  - ICMP-Typ
  - Eingangsnetzwerkkarte
  - Ausgangsnetzwerkkarte
  - UserId



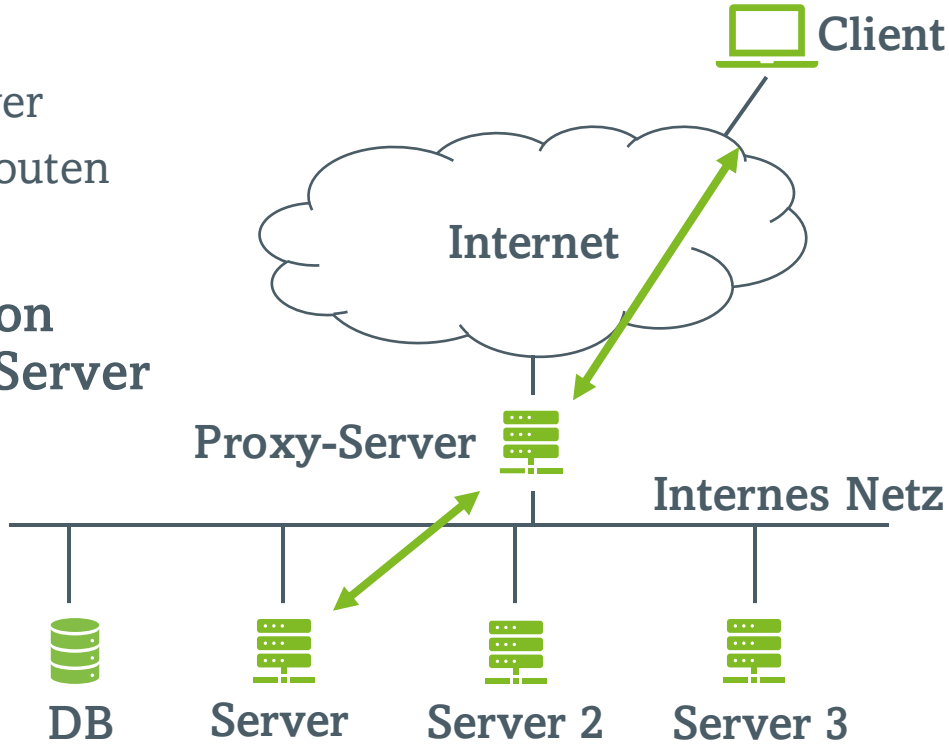
Proxy (Forward-Proxy)

- Wird zwischen Client und Server eingefügt und arbeitet als Server und als Client. Er ist
  - Protokollspezifisch
  - Oft transparent
- Sicherheitstechnisch nur dann sinnvoll, wenn er nicht umgangen werden kann.
- Für jeden Dienst ist ein eigener Proxy erforderlich, der dann das passende Protokoll unterstützt.
  - z.B. HTTP, SMTP, NNTP



Proxy (Reverse-Proxy)

- **Dient zum Schutz eines (Web-) Servers**
  - Blockieren von bekannten Angriffen
  - Bruteforceschutz
  - DDoS Schutz
  - Zugriff nur auf bestimmte Server
  - Autorisierung für bestimmte Routen
  - Bietet weniger Angriffspunkte
- **Ermöglicht die Verwendung von mehreren Domains auf einen Server**
- **Vereinfacht die Einrichtung von SSL**



Proxy (Reverse-Proxy)

Bekannte Reverse-Proxy Server

- nginx https://www.nginx.com
- caddy https://caddyserver.com/
- traefik https://traefik.io/traefik/

traefik

```yaml
version: "3.3"

services:

  traefik:
    image: "traefik:v2.10"
    container_name: "traefik"
    command:
      - "--api.insecure=true"
      - "--providers.docker=true"
      - "--providers.docker.exposedbydefault=false"
      - "--entrypoints.web.address=:80"
    ports:
      - "80:80"
      - "8080:8080"
    volumes:
      - "/var/run/docker.sock:/var/run/docker.sock:ro"
```

traefik

```yaml
whoami:
  image: "traefik/whoami"
  container_name: "simple-service"
  labels:
    - "traefik.enable=true"
    - "traefik.http.routers.whoami.rule=Host(`whoami.localhost`)"
    - "traefik.http.routers.whoami.entrypoints=web"
```

https://doc.traefik.io/traefik/user-guides/docker-compose/basic-example/

traefik (https)

```
traefik:
  …
  command:
    …
    - "--entrypoints.websecure.address=:443"
    - "--certificatesresolvers.myresolver.acme.tlschallenge=true"
    - "--certificatesresolvers.myresolver.acme.email=<email>"
    - "--certificatesresolvers.myresolver.acme.storage=<path>"
whoami:
  image: "traefik/whoami"
  container_name: "simple-service"
  labels:
    …
    - "traefik.http.routers.whoami.entrypoints=websecure"
```

https://doc.traefik.io/traefik/user-guides/docker-compose/acme-tls/

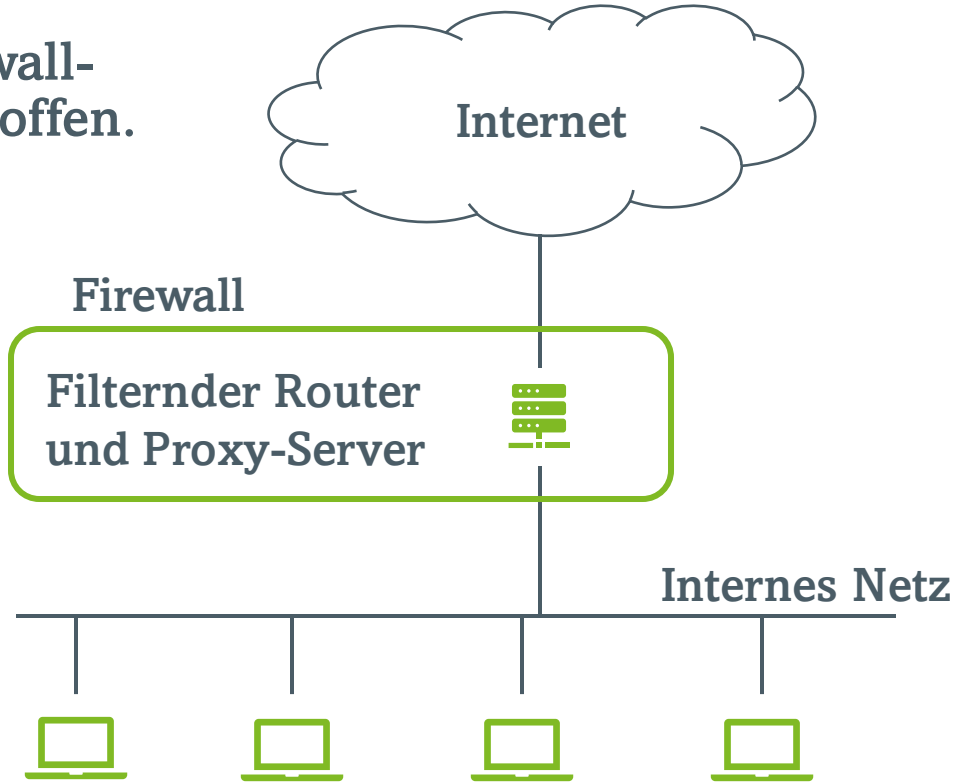
traefik (Ratelimt)

```
whoami:
  image: "traefik/whoami"
  container_name: "simple-service"
  labels:
    …
    - "traefik.http.middlewares.test-ratelimit.ratelimit.average=100"
    - "traefik.http.middlewares.test-ratelimit.ratelimit.burst=50"
```

https://doc.traefik.io/traefik/middlewares/http/ratelimit/

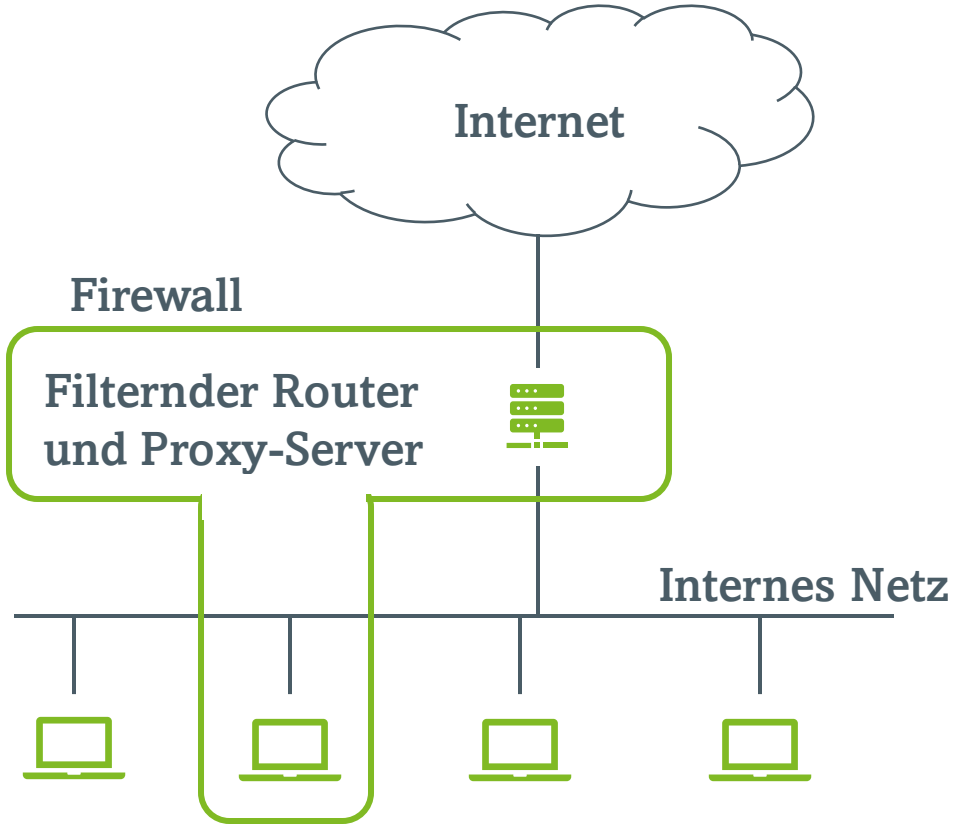
Entwurf 1: Firewall im Router

- Sparversion – nicht sehr sicher.
- Nach Einbruch in Firewall-Rechner sind alle Tore offen.



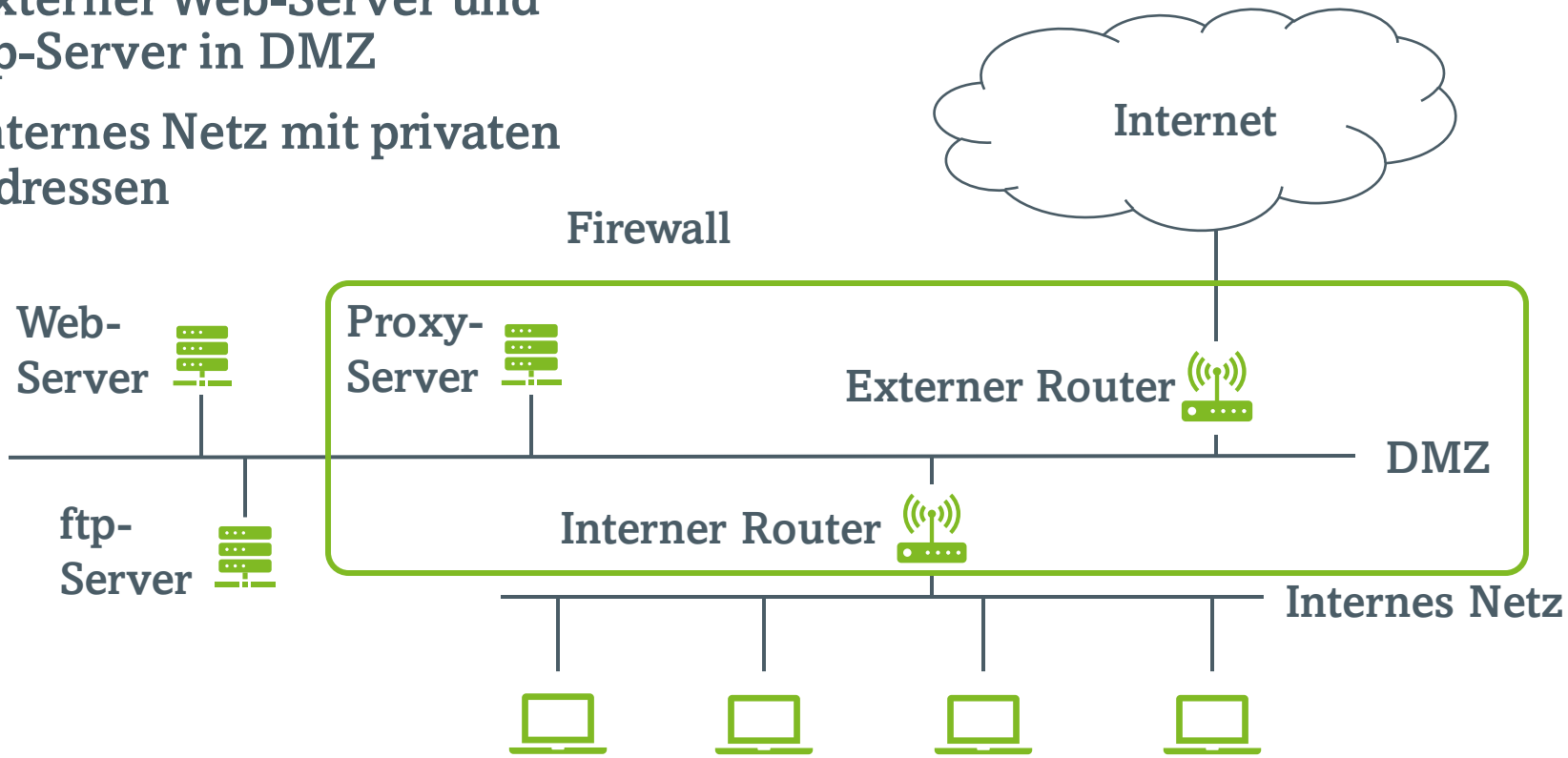
Entwurf 2: Extra geschützter Rechner

- Sparversion 2.



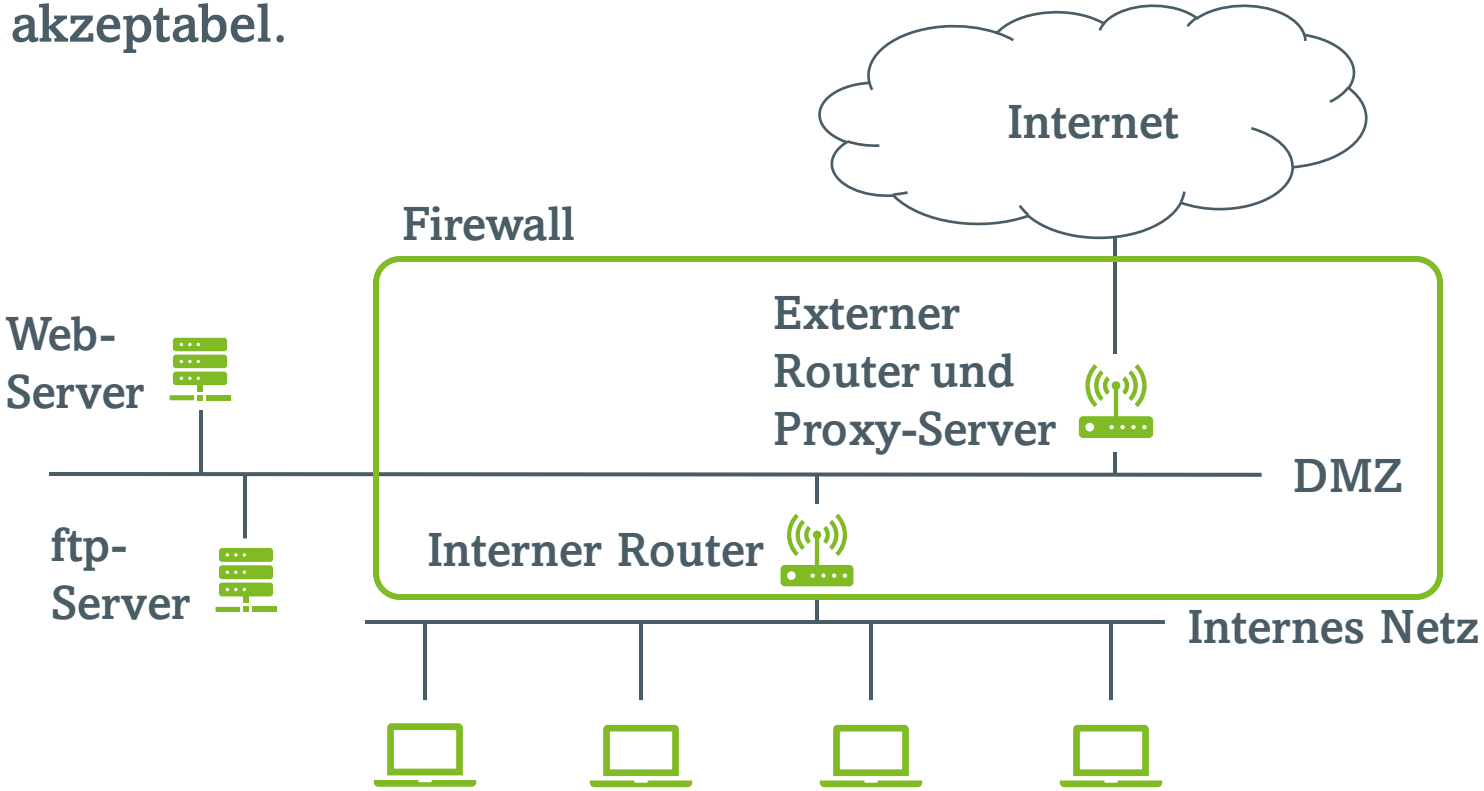
Entwurf 3: Entmilitarisierte Zone (DMZ)

- Standardentwurf
- Externer Web-Server und ftp-Server in DMZ
- Internes Netz mit privaten Adressen



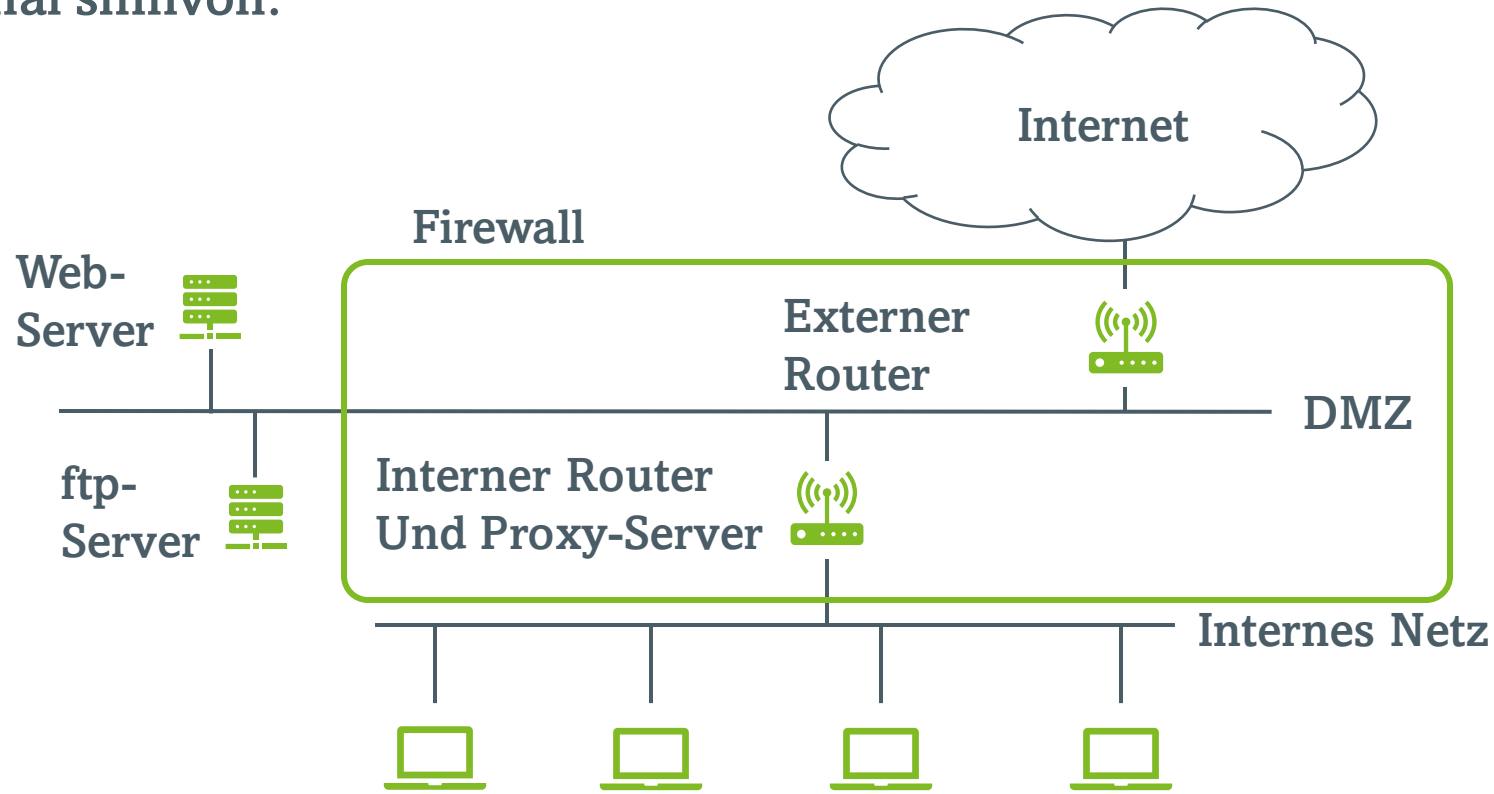
Entwurf 4: Externer Router als Proxy

- Nicht ganz so sicher wie Standardentwurf, aber ziemlich akzeptabel.



Entwurf 5: Interner Router als Proxy

- Ähnlich wie zuvor.
- Manchmal sinnvoll.



Router/Firewall

Wie arbeitet ein Router/ eine Firewall?

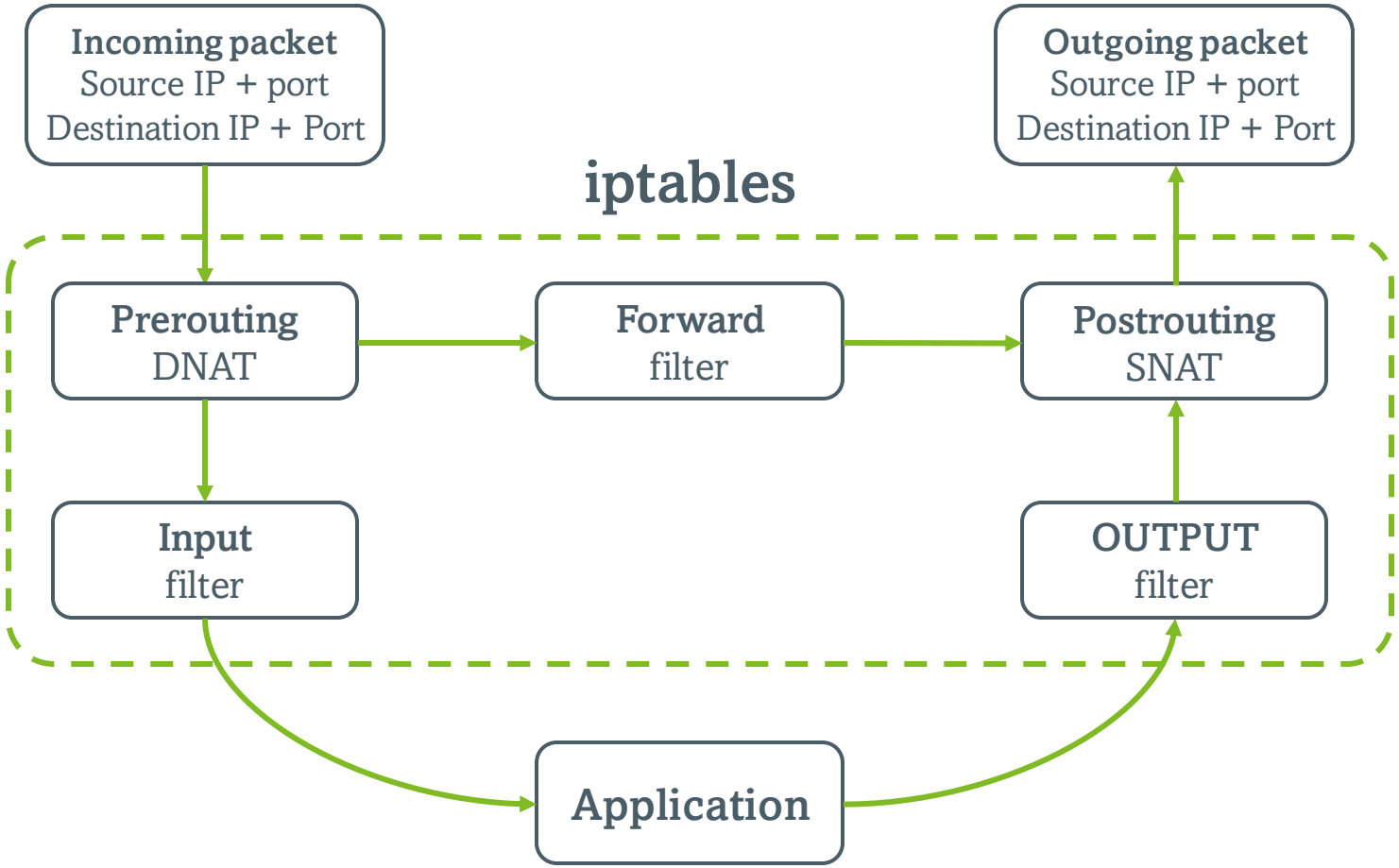
Sie benutzt einen Paketfilter.

Der bekannteste ist iptables.

iptables

- **Teil des Linux Kernels, ab Version 2.3**
- **Ketten-basiertes System zur Definition von Firewallregeln:**
  - Paketempfang (PREROUTING),
  - lokal zugestellt (INPUT),
  - weitergeleitet (FORWARD),
  - lokal ausgegeben (OUTPUT) und
  - Paketversand (POSTROUTING).
- **Bei den Tabellen unterscheidet man noch zwischen**
  - mangle: Eine spezielle Tabelle für Veränderungen an Paketen
  - nat: Eine spezielle Tabelle für NAT (network address translation)
  - filter: Die Standardtabelle mit allgemeinen Filter-Regeln.

iptables


Incoming packet
Source IP + port
Destination IP + Port
Outgoing packet
Source IP + port
Destination IP + Port
iptables
Prerouting
DNAT
Forward
filter
Postrouting
SNAT
Input
filter
OUTPUT
filter
Application

iptables - Kommando

- **Die Defaulteinstellung der Firewall enthält keine Regeln. Alle Pakete werden also ohne Veränderung weitergeleitet.**
- Regeln hinzufügen (Default gilt für Filtertabelle, sonst mit `-t`):

```
iptables -A chain (-t table) options
```

Table kann `nat`,`filter`,`mangle` sein.

`iptables -N mychain`	*erzeugt eine neue Regelkette*
`iptables -L`	*liefert eine Übersicht aller Regelketten.*
`iptables -I chain [Zeile] Regel`	*Einfügen der Regel in die erste / spezifizierte Zeile*
`iptables -A chain Regel`	*Einfügen der Regel in die letzte Zeile*
`iptables –D chain Regel`	*löscht angegebene Regel*
`iptables –F chain`	*löscht alle Regeln der Regelkette*

iptables – Policy

```
> iptables -P chain policy
```

Policy: ACCEPT oder DROP

Man spricht man von einem Blacklist- oder Whitelist-Filterdesign.

Blacklist-Design

- Es ist grundsätzlich alles erlaubt, was nicht explizit verboten wurde.
- Daher ist das Standardziel ACCEPT und die Filterregeln bestimmen, welche Pakete abgelehnt werden sollen.

Whitelist-Design

- Von vorneherein nichts erlaubt. Das Standardziel ist DROP und die Filterregeln bestimmen, welche Pakete durchgelassen werden.
- Inhärent sicherer.

iptables – Ziele

Standardziele:

- ACCEPT: Paket akzeptieren.
- DROP: Paket verwerfen und keine Rückmeldung an en Sender schicken.
- REJECT: Paket verwerfen, aber zusätzlich ein Antwortpaket zurückschicken. Mittels er Option --reject-with Typ wird fest-gelegt, welches Antwortpaket zurückgeschickt wird, standardmäßig wird „Port nicht verfügbar“ (icmp-port-unreachable) verwendet.
- RETURN: Aktuelle Kette verlassen. Wurde die aktuelle Kette von einer anderen Kette aus aufgerufen, dann kehre dahin zurück. Befindet man sich bereits in einer Standardkette (INPUT, ...), dann wende die DEFAULT-Policy der Standardkette an.

Weitere Ziele

- LOG: Informationen zum Paket in das Kernel-Log schreiben. Achtung: Es wird bei der nächsten Regel weitergemacht!

iptables – Beispiele

- Alle Pakete wegwerfen, außer die von einem bestimmten Netz

```
iptables -A INPUT ! -s 212.201.6.0/22 -j DROP
```

- Alle Pakete an eine bestimmte IP wegwerfen

```
iptables -A OUTPUT -o eth0 -d 212.201.6.194 -j DROP
```

- Alle Pakete an TCP-Port 80 zulassen

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

iptables – Beispiele

- Pakete von der lokalen Netzwerkkarte werden immer akzeptiert

```
iptables -A INPUT -i eth0 -j ACCEPT
```

- Pakete zum Verbindungsaufbau an den SSH-Server sind erlaubt

```
iptables -A INPUT -p tcp -m tcp --dport 22 --syn -j ACCEPT
```

- Pakete von aufgebauten Verbindungen werden erlaubt

```
iptables -A INPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Mehr Beispiele:

https://making.pusher.com/per-ip-rate-limiting-with-iptables

iptables – Filtern nach Ländern?

Listen: IP ⟷ Land

z.B. https://github.com/ipverse/rir-ip

Man kann also seine Firewall passend konfigurieren.

- Diese Listen aktualisieren sich jedoch ständig.

  Es muss regelmäßig (per Cronjob) aktualisiert werden.

iptables und tc

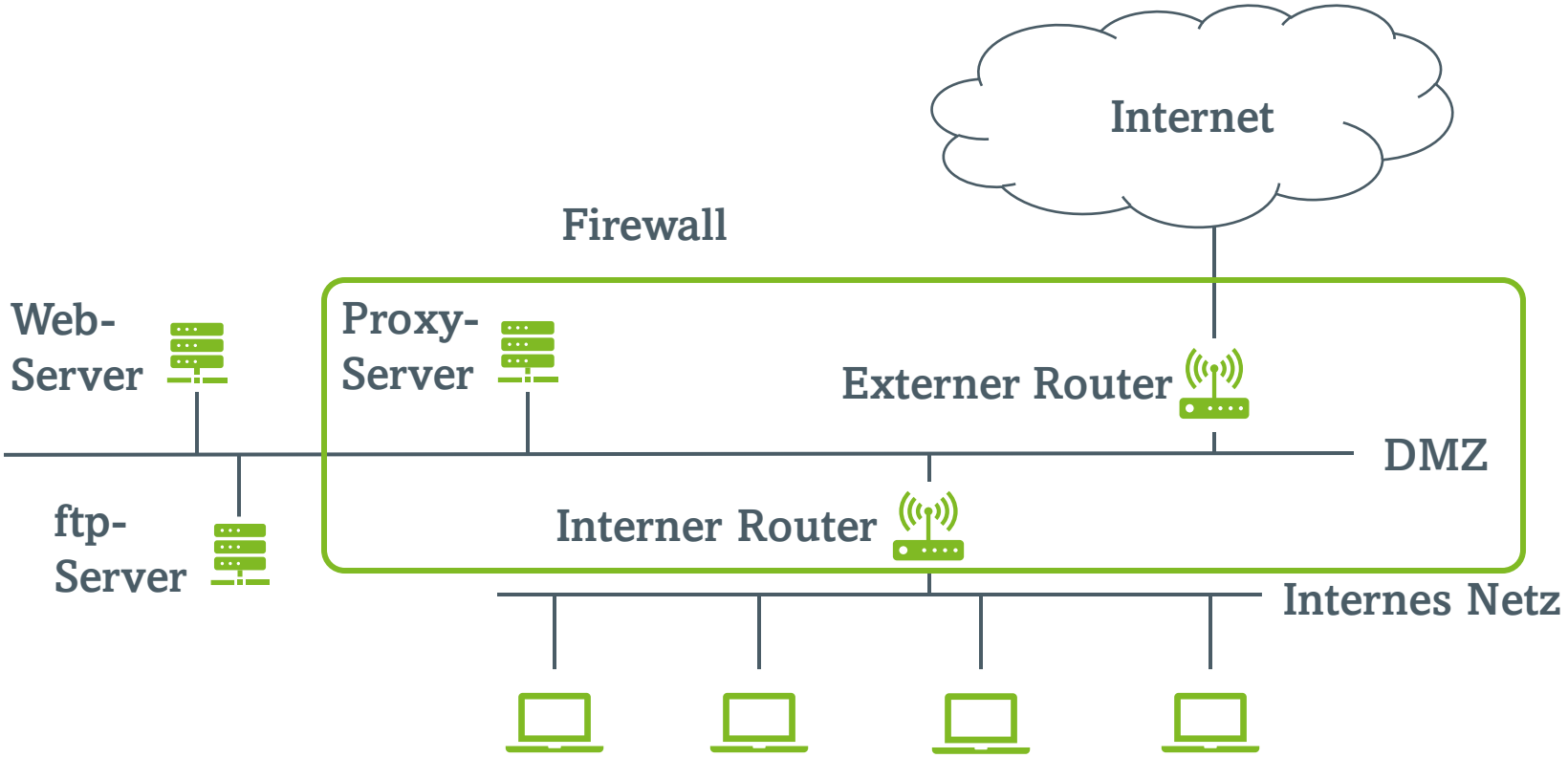
Erweiterte Firewall Einstellungen

- tc (Traffic Control) ermöglicht eine erweiterte Bandbreitenkontrolle in Linux-Systemen. Es unterstützt Traffic Shaping.
- Auf diese Weise können wir den sogenannten Quality of Service unterstützen.

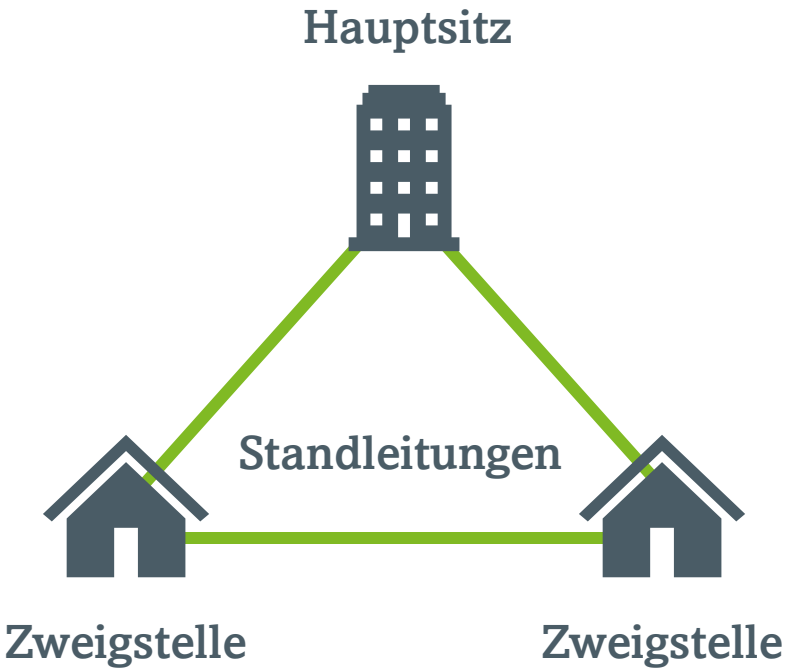
Technische Fakten:

- Warteschlangen steuern, wie Daten gesendet werden.
- TCP/IP steigert die Geschwindigkeit nach und nach, bis Pakete zurückgewiesen werden. Es ist daher möglich zu steuern, mit welcher Geschwindigkeit die Daten ankommen.

Entwurf 3: Entmilitarisierte Zone (DMZ)



WAN



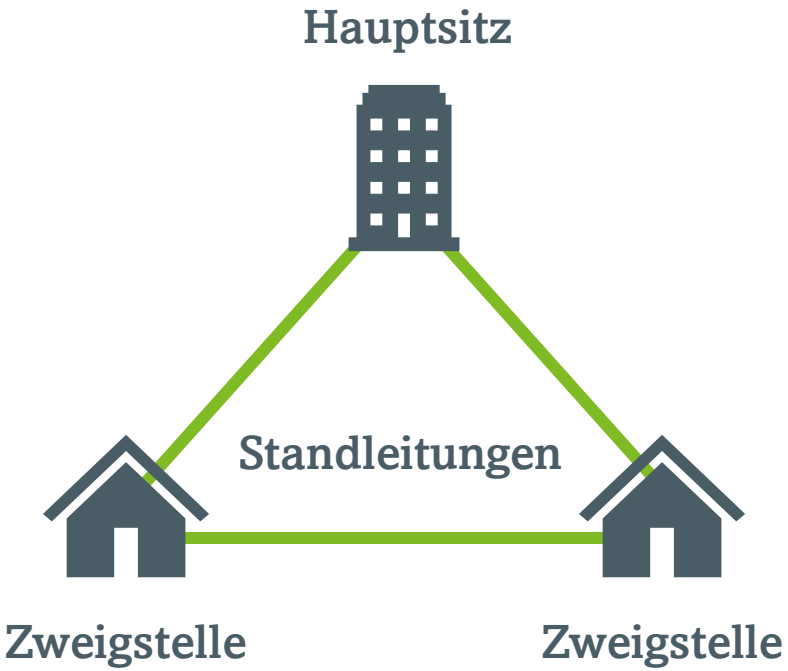
Nachteile:

- Sehr teuer!

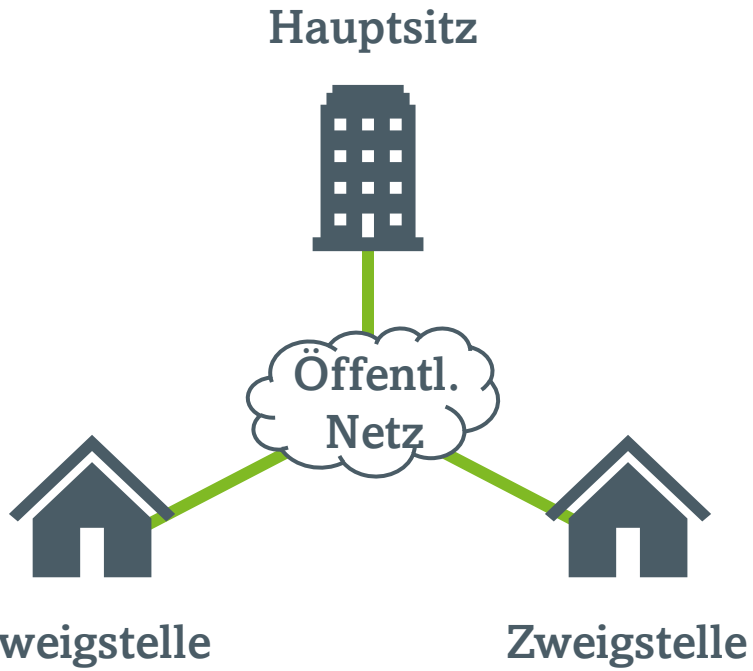
Vorteile:

- Quality of Service

WAN

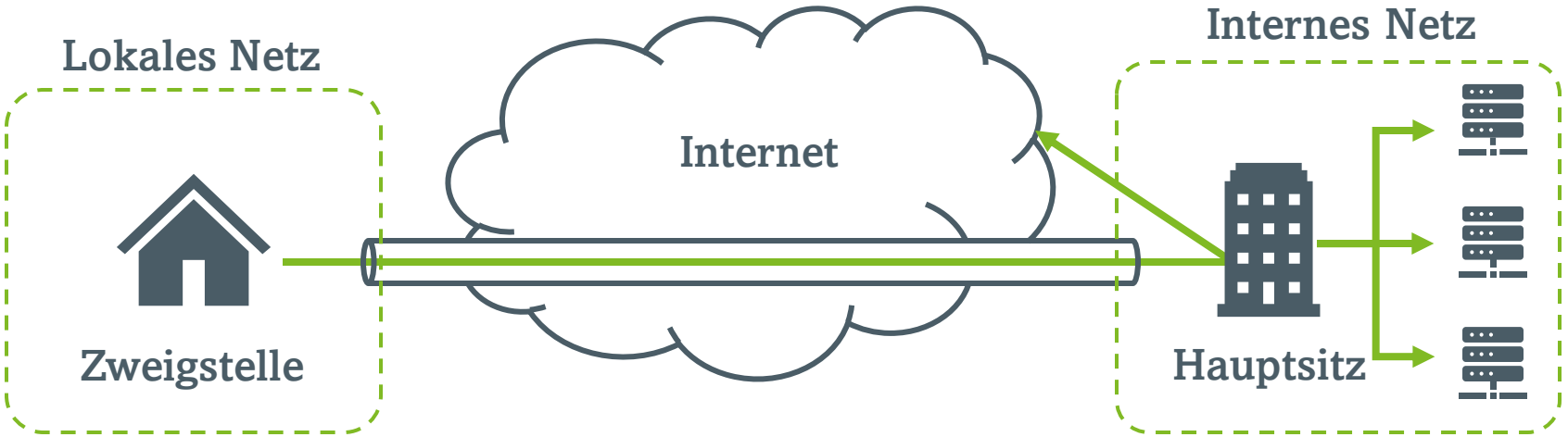

Hauptsitz
Standleitungen
Zweigstelle
Zweigstelle

VPN


Hauptsitz
Öffentl.
Netz
Zweigstelle
Zweigstelle

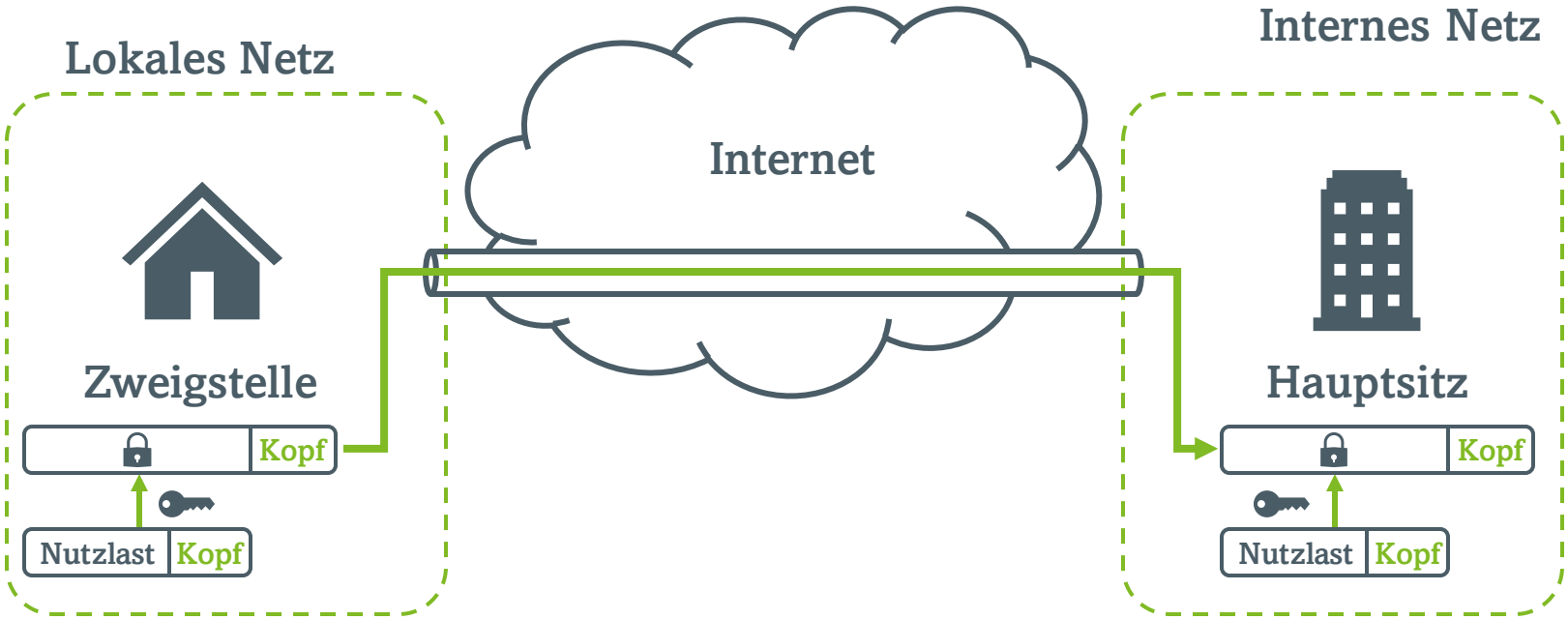
VPN - Realisierung

- Private Adressen werden durch öffentliches Netz getunnelt.



VPN - Realisierung

- Komplettes Paket des privaten Netzes (inklusive Kopf) wird als Nutzlast eines IP-Pakets durch das öffentliche Netz transportiert.



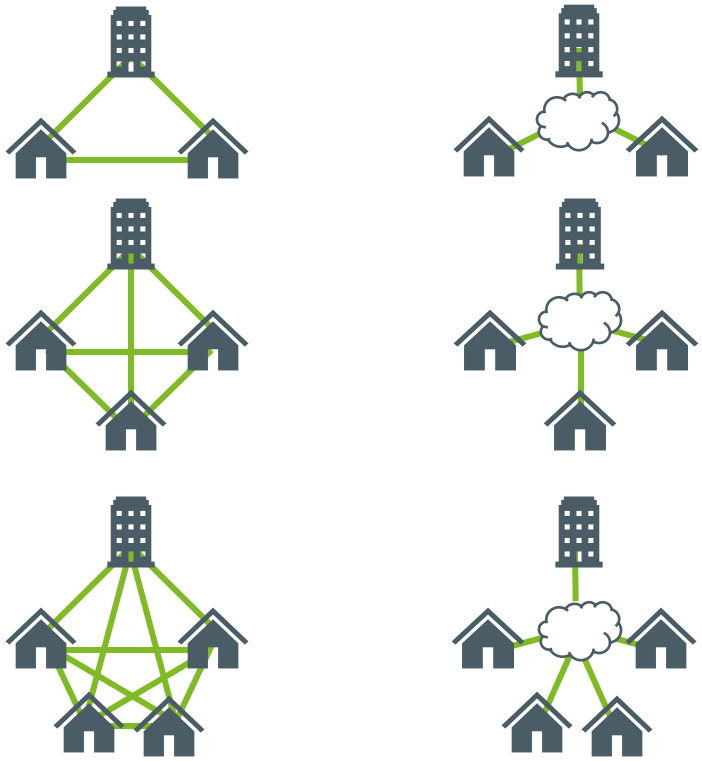
VPN - Realisierung

- Private Adressen werden durch öffentliches Netz getunnelt.
- Komplettes Paket des privaten Netzes (inklusive Kopf) wird als Nutzlast eines IP-Pakets durch das öffentliche Netz transportiert.
- Transport beliebiger privater Netzprotokolle über das Protokoll des öffentlichen Netzes.
- Standard: Verschlüsselung von Nutzlast und privatem Kopf.

VPN vs. WAN

VPN hat zahlreiche potentielle Sicherheitslücken ggü. WAN

- Beobachtung des Datenverkehrs und -menge (Sniffing)
- Abfangen und Filtern von Paketen
- Keine QoS Gewährleistung
- Knacken der Verschlüsselung und somit
  - Datenfälschung
  - Session Hijacking
  - Einbruch ins Intranet



Warum also VPNs nutzen?

- **Kosten**
- **Skalierbarkeit**

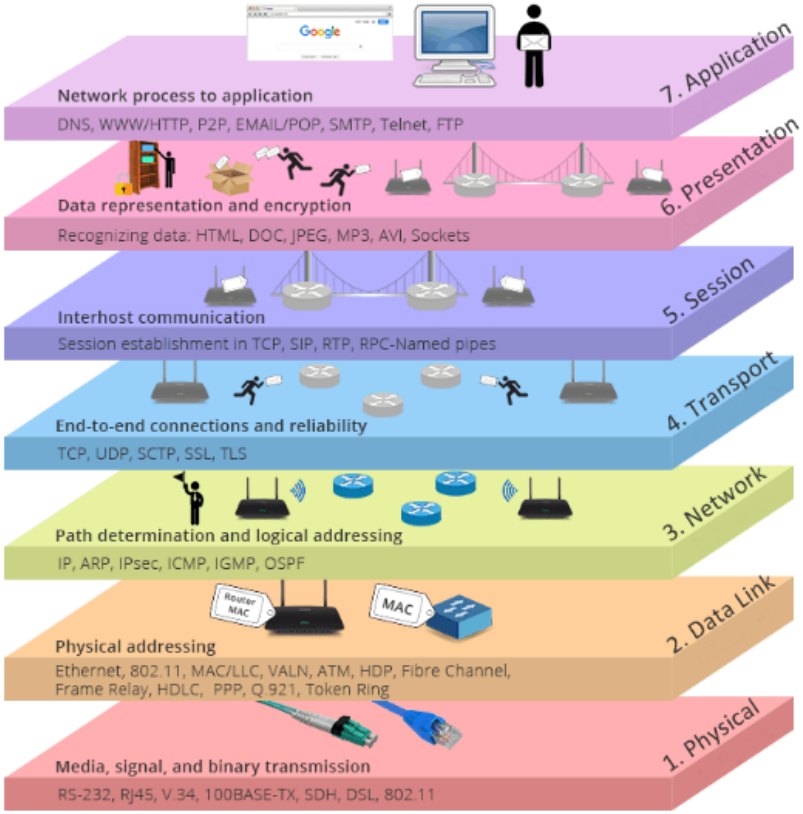
VPN – Protokolle

Paketorientiert

- PPTP (Point-to-Point Tunneling Protocol)
- **L2TP (Layer 2 Tunneling Protocol)**
- AltaVista Tunneling Protocol
- **IPSec (Internet Protocol Security)**

Anwendungsorientiert

- SSH - Secure Shell
- SOCKS
- Sun.NET

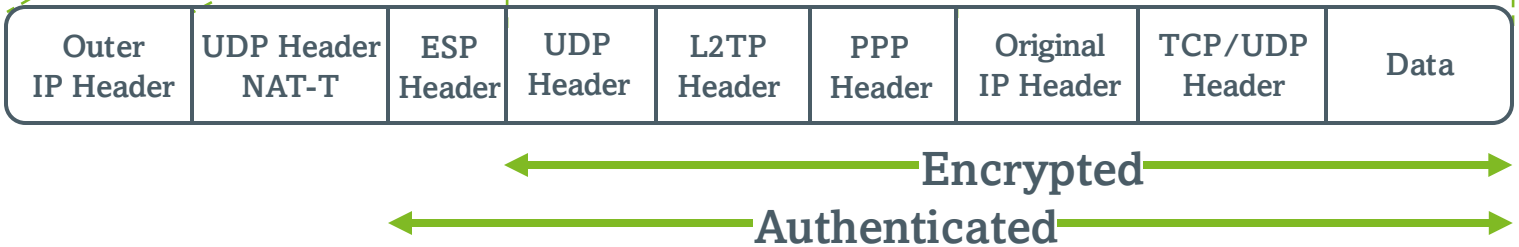


L2TP über IPSec

Vor der Anwendung der L2TP-Kapselung

Nach der Anwendung der L2TP-Kapselung

Nach der Anwendung der ESP/UDP Kapselung



BackUps

Datenrettung

Löschen einer Datei

- **Löschen mit del oder rm: Die Information ist auf einer konventionellen Festplatte erstmal nicht gelöscht.**
- **Sicheres Löschen erreicht man durch Überschreiben der Informationen mit anderen Daten (z.B. Zufallszahlen)**
  - z.B. mit dem Kommando `shred`:
    `-f` wenn nötig Zugriffsrechte ändern, um Schreiben zuzulassen
    `-n N` N-fach überschreiben
    `-u` Datei nach dem Überschreiben abschneiden und entfernen
    `-v` Fortschritt anzeigen

Aufgabe: Finden Sie in einem Festplattenimage die eigentlich gelöschten jpg-oder pdf-Dokumente.

BackUps – Goldene Regeln

1. Backup-System technisch prüfen

Nur durch eine regelmäßige Kontrolle können Sie sicherstellen, dass das System auch ordnungsgemäß funktioniert und die Medien einwandfrei beschrieben werden. Kontrollieren Sie die Logfiles.

2. Wiederherstellung durchführen

Backup und Recovery gehören untrennbar zusammen. Das ausgefeilteste und aktuellste Backup nützt rein gar nichts, wenn Sie im Ernstfall die Daten nicht zurückspielen können. Daher sollten Sie in regelmäßigen Abständen eine Wiederherstellung in einer Testumgebung durchführen.

3. Backup-Kopie auslagern

Mindestens eine Kopie des Backups sollte an einem anderen Standort aufbewahrt werden. Ein Backup muss auch einen Schutz vor Diebstahl und Beschädigung der Anlage darstellen.

BackUps – Goldene Regeln

4. Skalierbare Hardware

Stellen Sie sicher, dass das Backup-System zumindest den Anforderungen der nahen Zukunft (Kapazität, Performance) genügt.

5. Automatisiertes Backup

Die Datensicherung muss vollständig automatisiert ablaufen. Nur so ist sichergestellt, dass die Sicherung regelmäßig mit den identischen Parametern erfolgt.

6. Eindeutige Intervalle festlegen

Sichern Sie Ihre Daten so oft wie möglich und vom Aufwand her tolerierbar in regelmäßigen Abständen.

7. Transparentes Backup

Es muss eindeutig ersichtlich sein, welches Backup-Set welche Daten enthält.

BackUps – Goldene Regeln

8. Alle Rechner / Medien einbeziehen

Daten befinden sich an verschiedensten stellen. Eine Backup-Strategie muss die Sicherung aller dieser Daten beinhalten.

9. Redundante Backup-Lösung

Was für die Backup-Medien gilt, trifft auch auf die Hardware zu. Es muss sichergestellt sein, dass Sie im Schadensfall die Wiederherstellung gegebenfalls auf einer anderen Hardware-Umgebung durchführen können.

10. Backup-Strategie anpassen

Abläufe können sich ändern, eine gute Backup-Strategie muss diesbezüglich immer up to date sein..

Duplicati – Duplicity (Opensource)

- Wenige Klicks, um Wichtiges vor Ransomware zu sichern
- Backup kann flexibel eingerichtet werden, Daten werden standardmäßig mit AES-256 verschlüsselt gespeichert
- Backup-Speicher können USB-Sticks, externe Platten, NAS, Online-Dienste außer Haus schnell eingerichtet
- Duplicati beherrscht FTP, SSH (SCP) oder auch das Speichern in Amazons S3-Cloud, Google Drive, etc.
- Dabei gilt: viel hilft viel! An je mehr Orten die Backups liegen, destogrößer ist die Wahrscheinlichkeit, dass man nach einem Trojanerbefall noch Zugriff auf mindestens eine Kopie hat
- Mit ein paar Kniffen richtet man das Backup-Tool so ein, dass es mit Hilfe der Aufgabenplanung automatisch eine Sicherung startet, sobald ein bestimmter USB-Speicher mit dem Rechner verbunden ist.
- Das Backup-Tool läuft unter Windows, OS X und Linux.

Abschlussprojekt

- **Webanwendung mit bestimmten Vorgaben entwickeln**
  - Abgabetermin: 07.07.2023
  - Präsentationen: 07.07.2023 + 14.07.2023