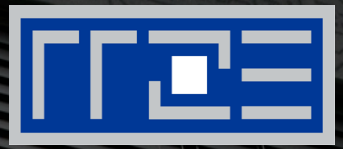
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



# IT-Sicherheit

## Digitales Rüstzeug in der IT-Sicherheit am RRZE

Campustreffen − IT-Dienste des RRZE und der FAU,
17.06.2020, Marcel Ritter, RRZE

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

# AGENDA

1. Bedrohungsszenarien
2. Angriffe
3. Gegenmaßnahmen
4. Reaktion & Analyse
5. Aktuelles

# BEDROHUNGSSZENARIEN

- Zielsetzung der Angreifer
- Verbreitungswege
- Ausprägungen

# Welche Ziele verfolgen die „Einbrecher“?

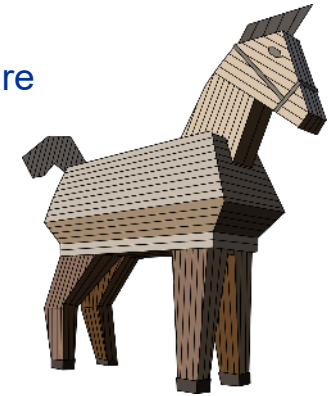
- Zugriff auf
  - Schützenswerte / wertvolle Daten (z.B. Forschungsdaten)
  - Logins / Passwörter (oder Passwort-Hashes), damit Zugriff auf weitere Systeme
- Missbrauch von Ressourcen
  - Spam-Mail
  - (D)DOS-Client, Botnet / Control-Server (Zentral vs. P2P)
  - Rechenleistung (Bitcoin-Mining)
  - Hardware (Drucker, Kamera, …)
  - Scan / Angriff auf weitere Systeme
- Erpressung
  - Datenverschlüsselung! (Ransomware)
  - Aber auch durch Zugriff auf persönliche/vertrauliche Daten

# Auf welchem Weg drohen Gefahren?

- Nicht technisch:
  - Diebstahl
  - Social Engineering
  - Entsorgung von „Datenträgern“ (analog wie digital)
    - › Verkauf gebrauchter Speichermedien, Recycling von SSD-Speicherchips in USB-Sticks
- Technisch:
  - Speichermedien mit Schadsoftware
  - Drive-By (Web) / Mail-Attachments
  - Scans / Aktive Angriffe

# Wie können technische Gefahren aussehen?

- Hardware:
  - USB-Killer-Sticks (Überspannung)
  - Programmierte USB-Sticks („Rubber Duck“)
- Hard- oder Software:
  - Floppy/USB-Stick/SD-Card mit Schadsoftware
  - Keylogger / Screenlogger
  - Backdoors
- Software
  - Viren, Würmer, TrojanerRootkits
  - Adware / Nagware / Ransomware



# OFFENSICHTLICH BIS „UNSICHTBAR“

IT-Sicherheit jenseits vom klassischen Server/PC

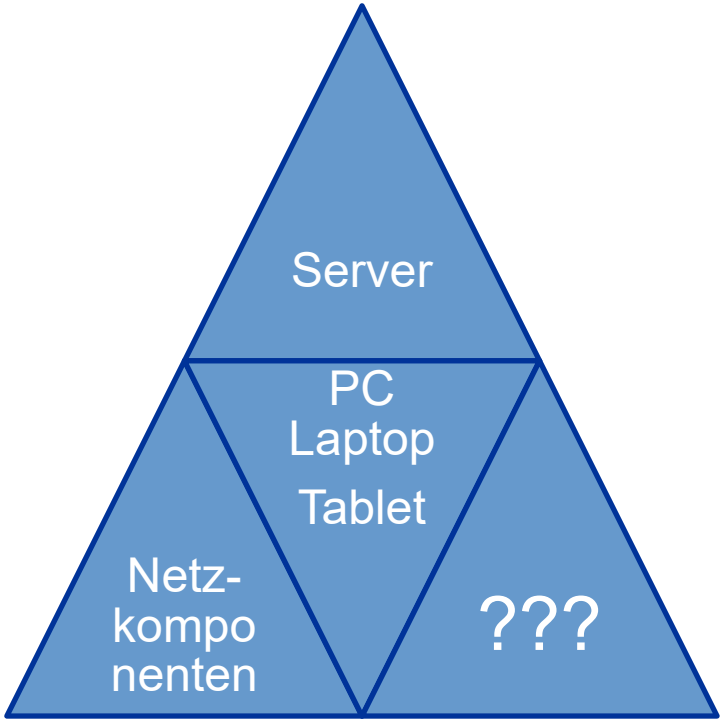
- „unsichtbare“ IT-Geräte (IoT)
- „virtuelle“ IT-Systeme

# Altbekannte Gefahrenquellen

- Server
- Endgeräte
- Netzwerkkomponenten

- Aber:
  - Zunehmend nur

    „die Spitze des Eisbergs“



# Gefahrenquelle: „Intelligente Hardware“ und „Internet of Things“ …

Klassische IT-Komponenten:

- Netzwerkkomponenten: WLAN-AP, IP-Telefon,…
- Drucker/Kopierer

Mobile Geräte

- Handy, Tablet, Smart-Watch

IoT (Internet of Things), Home Automation

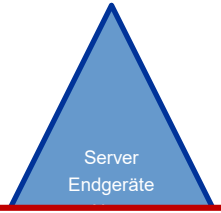
- Heizungsanlage, Auto, Kühlschrank, …

Multimedia-Geräte

- DVD/Blu-ray-Player, Medienstation

Medizingeräte

- Herzschrittmacher, Insulinpumpen, …




Nach einer anfänglichen Hype-Phase gibt es oft **keine Patches** vom Hersteller mehr. Damit werden die Geräte verwundbar!

# Besonders „attraktiv“, weil vielseitig:

- Abhören/Mitschneiden von
  - Telefonaten
  - SMS
  - Mails
  - Chats
  - Internetverbindungen
- Medien
  - Bild / Video
  - Ton
  - Position (GPS)
- Und alles: per Fernsteuerung (de-)aktivier- und steuerbar!

# Virtualisierung

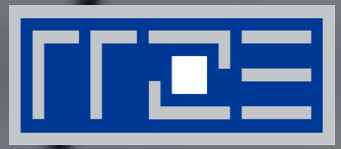
- Vollvirtualisierung
  - Eigentlich wie „echte“ Server
  - Aber: Aufwand/Kosten wesentlich geringer, deswegen
    - Oft hoffnungslos übertriebene Anzahl von VMs, gefolgt von
    - Mangelhafter Betreuung und daraus resultierendem
    - Sicherheitsrisiko

- Container (wie Vollvirtualisierung, aber zusätzlich…)
  - Update-Strategie: Keine – bei Neustart: Reset oder komplett neues Image
  - Keine automatischen Updates
  - Quellen potentiell unsicher / undurchsichtig

# Cloud-Dienste

- Vorteile
  - Oft günstige/kostenlose Angebote
  - Komfortable Nutzung
- Nachteile
  - Verarbeitung von Daten/Dokumenten auf Servern Dritter
  - Unterliegen evtl. anderer Jurisdiktion (Behörden-Zugriff)
  - Kleingedrucktes (Rechte an Bildern, etc.)

# ANGRIFFE



Hauptsächlich technisch …

… aber mit Ausflügen ins Social Engineering

# Hacking 101:
# „Classic Style“: ohne Nutzerinteraktion

**Phase 1:**

- Ausspähen möglicher Ziele

**Phase 2:**

- Zugriff / Ausnutzen entdeckter Schwachstellen

**Phase 3:**

- Ausweiten der Berechtigung

**Phase 4:**

- Verstecken

**Phase 5:**

- Absichern des eigenen Zugriffs

**Phase 6:**

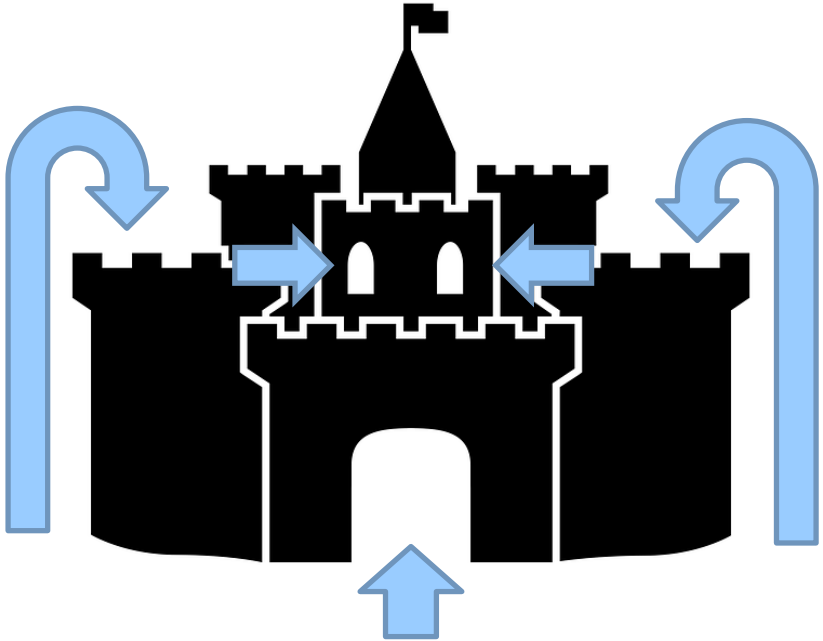
- Schadfunktion nutzen

Social Engineering:

- Erstaunliche Parallelen zur rein technischen Angriffen

# Hacking 101: Ausspähen möglicher Ziele

- Phase 1: Auskundschaften / Scan
  - Welche Systeme sind erreichbar?
    - Evtl. auch OS, Version, usw.
  - Welche Ports (= Dienste) laufen dort?
    - Evtl. auch Hersteller/Produkt, Version usw.
  - Welche Applikation(en) laufen „dahinter“?
    - z.B. bei Webservern: CMS (Wordpress, Typo3, etc.), oder Management-Schnittstellen (phpMyAdmin, usw.)
  - Alternative (ohne Spuren beim Opfer)
    - Nutzung von bereits von Dritten gesammelten Information (Handel, Suchmaschinen)



# Hacking 101: Ausspähen möglicher Ziele

**Oftmals sehr freigiebige Information „frei Haus“:**


```
# ssh -v someserver.somewhere.com
<…>
debug1: Remote protocol version 2.0,
        remote software version OpenSSH_5.9p1 Debian-5ubuntu1.9
```

Social Engineering:

- Fotos oder Meldungen in sozialen Medien von
  - Geburtstagsfeier => Geburtstag/Alter
  - Urlaubsbilder => nicht anwesend
  - … Verwandte, Haustiere

# Scan Results – Operating System

```
# nmap -O someserver.somewhere.com
Starting Nmap 6.40 ( http://nmap.org ) at 2015-07-07 08:42 CEST
Nmap scan report for remotehost (1.2.3.4)
Host is up (0.000022s latency).
rDNS record for 1.2.3.4: remotehost.local
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
79/tcp    open  finger
111/tcp   open  rpcbind
2049/tcp  open  nfs
4045/tcp  open  lockd
6112/tcp  open  dtspc
7100/tcp  open  font-service
Device type: general purpose
Running: Sun Solaris 9|10
OS CPE: cpe:/o:sun:sunos:5.9 cpe:/o:sun:sunos:5.10
OS details: Sun Solaris 9 or 10 (SPARC)
Network Distance: 4 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.60 seconds
```

# Hacking 101:
# Ausnutzen entdeckter Schwachstellen

## Phase 2: Zugriff

- Variante 1: Zugriffsdaten (Login/Passwort) bekannt
- Variante 2: Einbruchsversuch
  - Gezielt Schwachstellen „abklopfen“:
  - Exploits auf Zielsysteme anwenden und „Daumen drücken“
  - Heiß begehrt (nicht nur bei Geheimdiensten):
    - Zero-Day-Exploits (noch kein Patch vorhanden/veröffentlicht!)
  - Informationen über verwundbare Systeme
    - Beispiel Apache: http://httpd.apache.org/security_report.html
    - CVE (Common Vulnerabilities and Exposures)
    - … und in dunkle Quellen gibt‘s die passenden Exploits dazu

Social Engineering:

- Ändern von Zugangsdaten über „Sicherheitsfragen“:
  - Geburtsdatum
  - Name des Haustiers
  - …

# Hacking 101: Ausweiten der Berechtigung

## Phase 3 (optional): Ausweiten der Berechtigung

- Kompromittierter Dienst lief als unprivilegierter Benutzer
- Ziel: Möglichst Admin-Rechte
- z. B.:
  - Auslesen und (Offline-)Cracken von Passwort-Hashes
  - Anwenden weiterer (lokaler) Exploits zum Erreichen privilegierter Admin-Berechtigungen

Social Engineering:

- Nutzung der vorhanden Informationen um Vertrauen zu schaffen und „Zielperson“ für eigene Zwecke „einzuspannen“

# Hacking 101: Verschleiern des Einbruchs

## Phase 4 (optional): Verschleiern des Einbruchs

- Manipulation (z.B. Löschen) von Log-Files / Login-Daten
- Verstecken von Prozessen / Dateien / Netzverbindungen
  - Als nichtprivilegierter Benutzer:
    - Verwendung üblicher Programm- / Datei- / Verzeichnisnamen
    - Verstecken „in der Masse“
    - „Old School“: Verwendung von Leer / Sonderzeichen, „…“
  - Als Administrator / root:
    - Austausch typischer Systemprogramme
    - Kernel-Rootkit
      - potentiell schwer zu finden, da volle Systemkontrolle!

Social Engineering:

- Auftreten z.B. als Vorgesetzter der „Zielperson“
- Agieren im Auftrag Anderer

# Hacking 101:
# Sicherstellen der dauerhaften Nutzbarkeit

## Phase 5 (optional): Dauerhafte Zugriffsmöglichkeit schaffen

- Ursprüngliche Schwachstelle könnte durch Patches behoben werden
- Durch zusätzliche Backdoor
- Einbinden der Ressourcen in ein existierendes Botnetz
  - Ansteuerung über Control-Server
  - Verbindung wird von betroffenen System aufgebaut, d.h.
    - Auch Systeme hinter Firewall/NAT können noch ferngesteuert werden!

Social Engineering:

- Erpressung / Entlohnung der „Zielperson“
- Evtl. Ausweiten auf weitere Personen im Umfeld

# Hacking 101: Schadfunktion nutzen

## Phase 6: Schadfunktion installieren und nutzen

- Bis zur (potentiellen) Entdeckung …

Social Engineering:

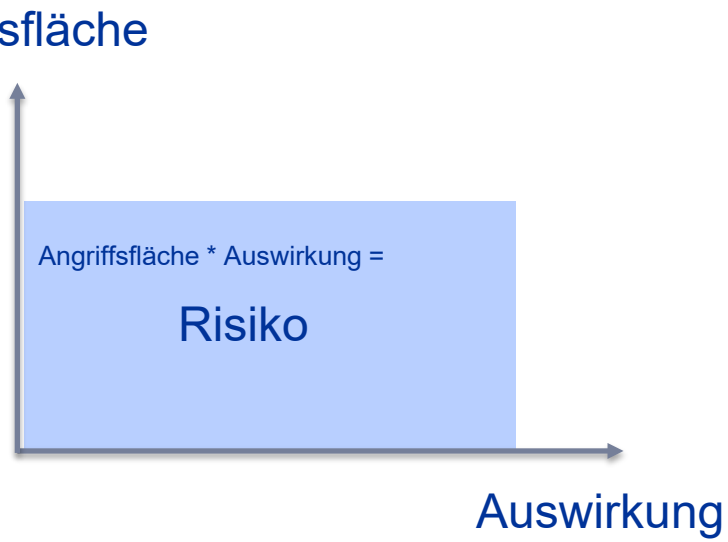
- z. B. Stehlen von Firmengeheimnissen

# GEGENMASSNAHMEN

- Sicherheitsvorfälle verhindern
- Sicherheitsvorfälle erkennen
- Auswirkungen reduzieren

# Gegenmaßnahmen - Zielsetzung

- Verminderung „Angriffsfläche“
  - Gepatchte Software (Updates)
  - Nur benötigte Dienste
  - Beschränkung der Zugriffsmöglichkeiten
    - Login/Passwort, lokal (z.B. Subnetz), temporär (z.B. 10/s)
  - Keine Klartext-Authentifizierung (FTP, telnet, rsh, …)
- Verminderung der Auswirkungen
  - Dienste als nichtprivilegierter Benutzer ausführen
  - Ausführung in gesicherter Umgebung (chroot, separate VM)
  - Ressourcenbeschränkung (DOS-Attacken)
  - Role Based Access Control (AppArmor, SELINUX)



# Gegenmaßnahmen - physische Sicherheit

- Bei direkten, physischem Zugriff auf Geräte viele Angriffsszenarien einfach möglich, deswegen:

- Beschränkung des direkten Zugriffs
  - Gesicherter Rechnerraum
  - Abgeschlossene Büroräume / Schränke
  - Leicht transportable Geräte sichern (z.B. Kensington-Lock)
  - Absicherung von Netzwerk-Verkabelung

  - Schwieriger bei mobilen Geräten (Laptop, Handy), weil physischer Zugriff leicht möglich
    - Daten-Verschlüsselung
    - PIN-Code / Fingerabdruckscan etc.

# Gegenmaßnahmen – technische Sicherheit

## Lokaler Rechner

- Updates / Aktuelle OS-Versionen (z.B. Windows 7 nur mit ESU!!!)
- Zugriffsmöglichkeiten/Dienste einschränken
- Virenscanner / Malware-Detection
- Lokale Firewall
- Backup (!)

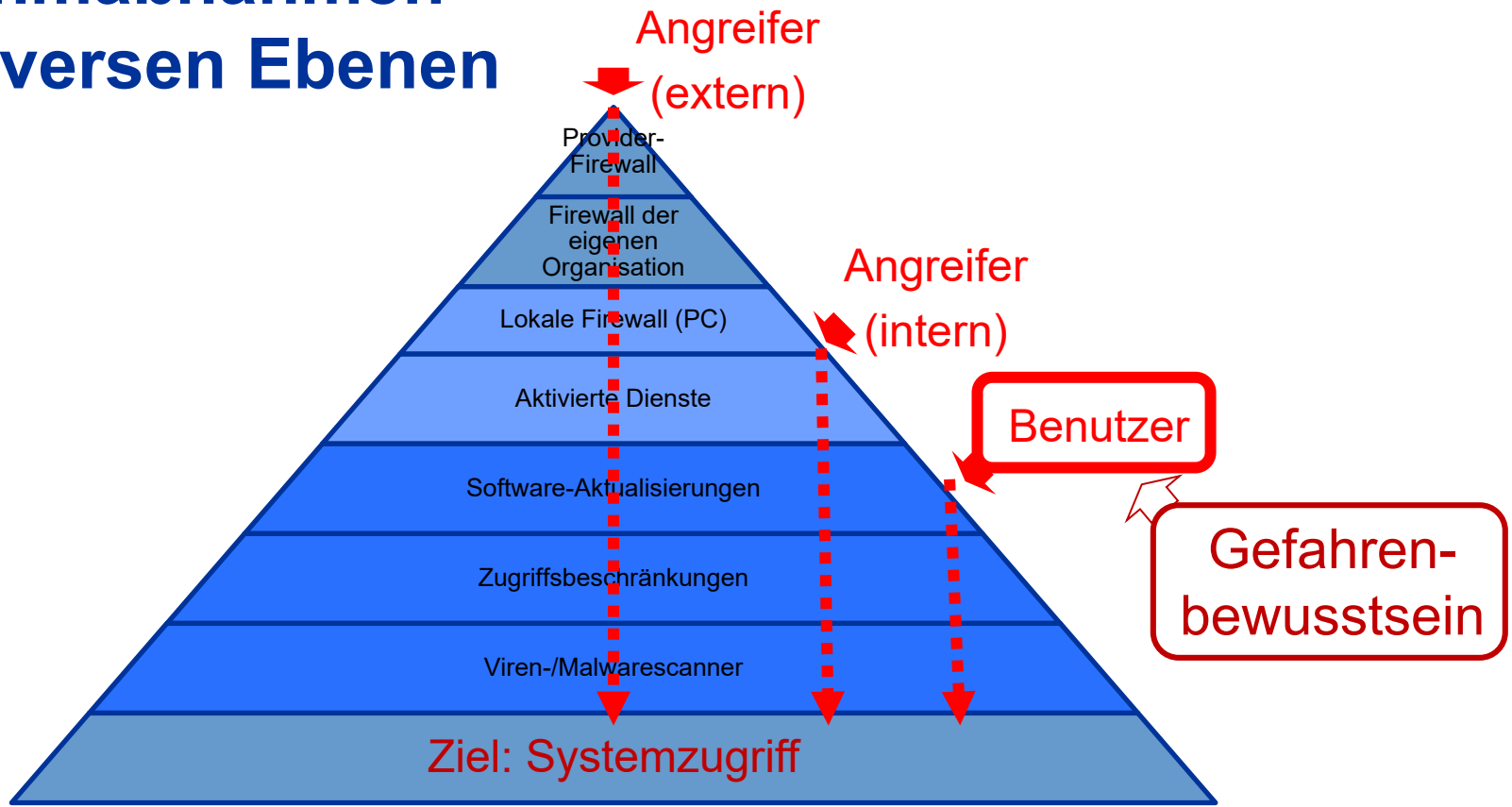
## Netzwerk

- Firewall
- Priv. Subnetze (mit Proxy / NAT (Source+Destination) (SSL!))
- Intrusion-Detection/-Prevention (SSL!)

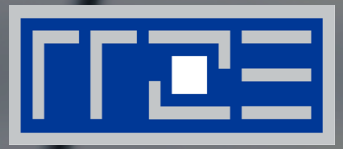
## Proaktive Analyse eigener Systeme

- Nessus / OpenVAS (http://sectools.org/vuln-scanners/)

# Gegenmaßnahmen auf diversen Ebenen



# ANALYSE VON VORFÄLLEN



- Erkennen & erste Schritte
- Analysieren
- Beheben & Vorbeugen

# Erkennung von Vorfällen

- Netz-seitig:
  - Verdächtige Netzverbindungen
    - Hohe Anzahl (SPAM)
    - Unbekannte Kommunikationspartner
  - Meldung von außen
- Host-seitig:
  - HIDS (Host Intrusion Detection System)
    - Überwachung von Dateien:
      - Änderungen (Checksummen, Zeitstempel)
      - Ungewöhnliche Dateien (core – oft Nebenprodukt!)
    - Überwachung von Prozessen
    - Überwachung von Netzverbindungen

# Erste Schritte bei Vorfall

- Mögliche Reaktionen
  - Stromstecker ziehen
  - Netzwerkstecker ziehen
  - Laufen lassen und weiteres Verhalten beobachten
- Andere Systeme durch Vorfall potentiell gefährdet oder Hilfe gewünscht?
  - Meldung an abuse@fau.de
  - Gerne auch Meldung zur reinen Information
- Ermittlungsbehörden involviert?
  - Angeforderte Daten sichern, Herausgabe aber
  - Nach Prüfung der Anfrage durch Datenschutzbeauftragten
  - Durch den Datenschutzbeauftragten
  - Rechtliche Absicherung!

# Analyse von Vorfällen

- Prinzipiell gilt:
  - Analyse einfacher, je vollständiger die Informationen
- Sicherung der zur Verfügung stehenden Daten
  - Log-Files (z.B. Protokoll der Zugriffe / Logins)
  - Sicherung des Dateisystems (oder Teilen davon)
  - Sicherung der Datenträger (Unterschied zu Dateisystem?)
  - Speicher-Dump
    - › Prozessliste, geöffnete Dateien, aktive Netzverbindungen
- Bei Analyse am laufenden System: **VORSICHT!**
  - … erfordert Login (Passwort!)
  - … benötigt entsprechende Tools

# Analyse von Vorfällen

- Alles gesichert, aber trotzdem gehackt? Welche Fragen sollte ich stellen?
  - Auf welchem Weg wurde ich gehackt?
  - Warum war der Angriff erfolgreich?
  - Welche Auswirkungen hat der Vorfall für das übrige IT-Umfeld?
- Welche Schlüsse kann ich ziehen? Wie kann ich dem zukünftig vorbeugen?
  - Welche Gegenmaßnahmen sind möglich (und verhältnismäßig)?

# AKTUELLES

- Entwicklungen und Beispiele

# Phishing – gut gemacht: Bewerbung (12/2016)

Do 08.12.2016 02:23

Andreas M <a.m@s.com>

**Bewerbung** als Studentische Hilfskraft

An Ritter, Marcel (RRZE)

Nachricht | Bewerbung von Drescher.xls (2 MB) | Bewerbung von Drescher.pdf (135 KB)

Sehr geehrte Damen und Herren,

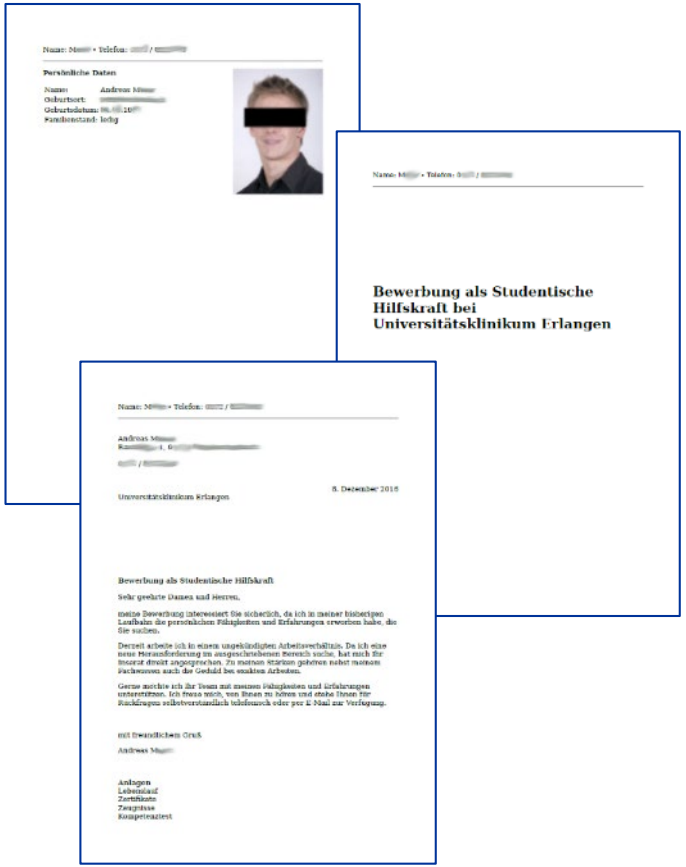
hiermit bewerbe ich mich bei Ihnen für die die Stelle als Studentische Hilfskraft. Meine vollständigen Bewerbungsunterlagen können Sie dem Anhang entnehmen.

Ich freue mich auf Ihre Rückmeldung und stehe Ihnen bei Rückfragen jederzeit gerne zur Verfügung.

Mit freundlichem Gruß

Andreas M

Anlagen
Lebenslauf
Zertifikate
Zeugnisse
Kompetenztest



# Social Engineering – auf hohem Niveau

## Bewerbung per Mail

- Saubere Sprache
- Korrekte Ansprache der Personalstelle
- Korrekte Referenz auf tatsächlich ausgeschriebene Stelle
- Angehängter Lebenslauf (PDF)
- Angehängtes **Excel** (?) mit Bewerbung

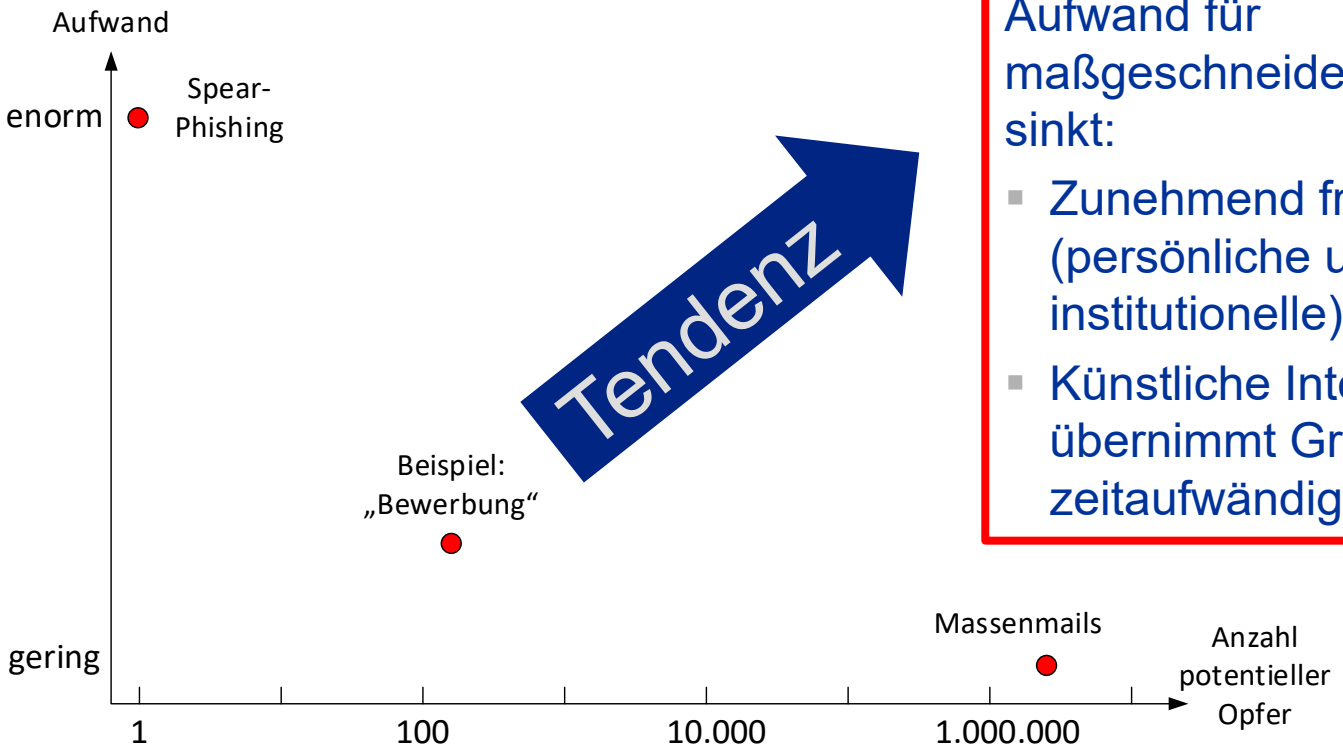
## Schadfunktion

- Crypto-Trojaner
- Aktiviert durch Excel-Makro

## Quelle der Daten

- Datenbank von Arbeitsvermittlern

# Aufwand / Nutzen




Aufwand für maßgeschneiderte Angriffe sinkt:

- Zunehmend frei verfügbare (persönliche und institutionelle) Informationen
- Künstliche Intelligenz übernimmt Großteil der zeitaufwändigen Arbeit

# Dateilose Infektion

**Vorgehen:**

- Code wird direkt in bereits laufende Prozesse injiziert
- keine Dateien, die verräterischen Code enthalten
- keine Spuren bei Offline-Check / nach Reboot

**Problem:**

- Schutzmechanismen / Virenscanner scannen Dateien

**Nachteil für den Hacker:**

- Gehacktes System muss evtl. neu infiziert werden

**Vorteil:**

- Analyse deutlich erschwert
- „Wertvoller“ Schadcode länger geheim (und damit nutzbar)

# Aktuelles 2019 – Emotet
# BSI-Chef: „König der Schadsoftware“

- XX.05.2019 Heise Redaktion
- 02.10.2019 Berliner Kammergericht – weitgehend offline
- 09.11.2019 Humbold-Universität – Teilbefall
- 10.12.2019 Universität Gießen **offline**
- 17.12.2019 Katholische Hochschule Freiburg **offline**
- 19.12.2019 Stadt Frankfurt teilweise offline
- 19.12.2019 Stadtverwaltung Bad Homburg **offline**

# Emotet - Infektionsweg

- Infektion über Office-Dokumente (Makros)
  - VBA-Code startet über WMI (Windows Management Instrumentation) PowerShell
  - PowerShell lädt .exe nach (oft von ebenfalls kompromittierten Wordpress-Seiten) und führt ihn aus
  - .exe wiederum kontaktiert C&C-Server für weiteren Schadcode
  - Integration in Autostart und „Verstecken“ hinter OS-Prozessen

# Emotet – Schadfunktionen (Auszug)

- Optional Einrichtung von Netzfreigaben per UPNP
- Übernahme weiterer Systeme im Netz
- Abschöpfen von Zugangsdaten (mimikatz, Admin-PW bei Hilfe!)
- Auslesen von Mail-Threads und Missbrauch durch gezielte Antworten (inkl. infizierten Office-Dateien)
- Trickbot: Angriffe auf ActiveDirectory
- Deaktivierung von Backups
- Verschlüsselung und Lösegeldforderung

# Emotet - Entdeckungsverhinderung

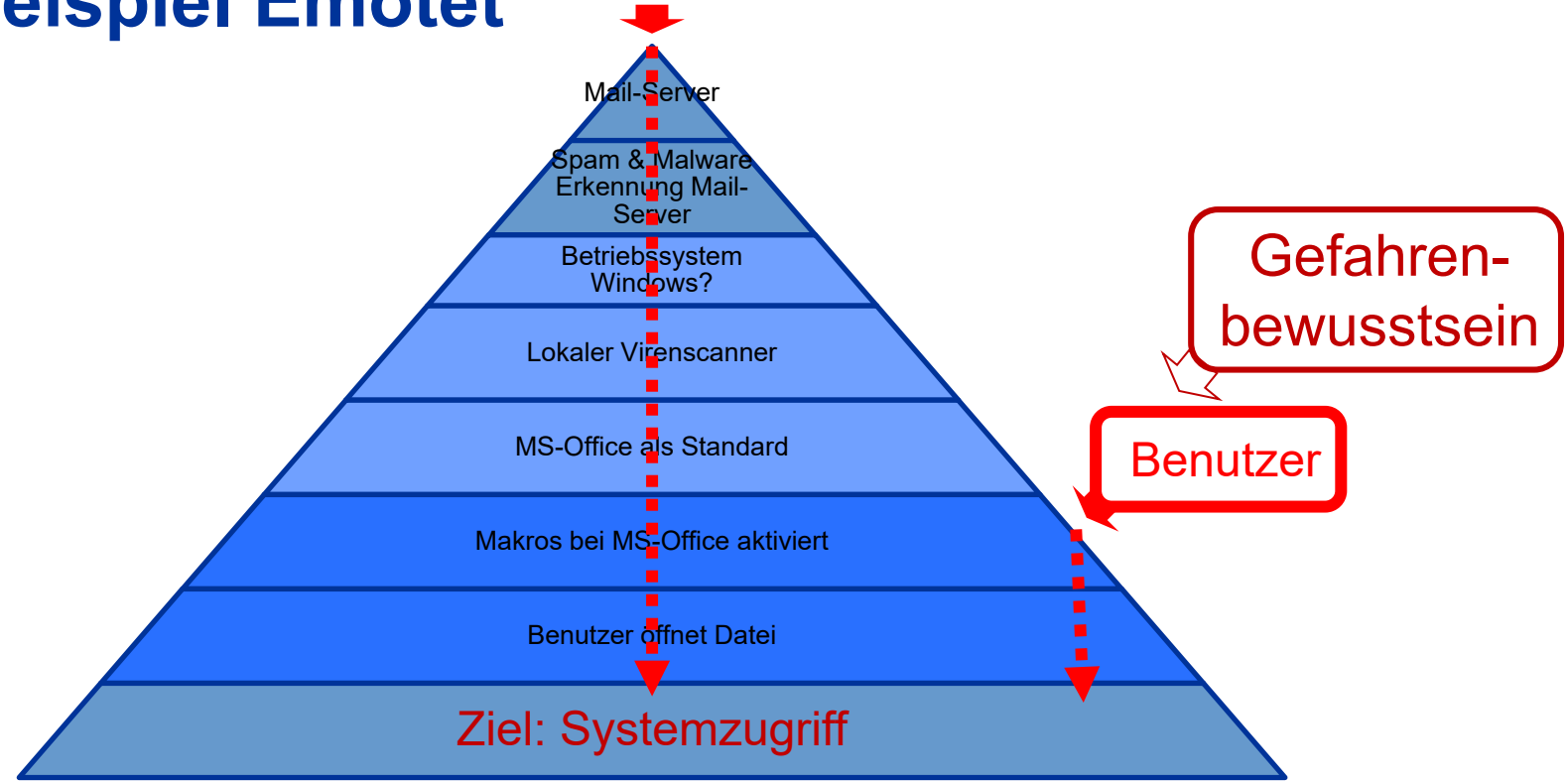
- VBA und PowerShell Skripte verschleiert
- Schadcode für jede Infektionswelle „neu“

  => keine Signaturen für Virenscanner
- Schadcode wird teilweise verschlüsselt nachgeladen

  => für Virenscanner nicht prüfbar
- Download von Schadcode nur in den Arbeitsspeicher

  => keine Spuren auf Platte

# Gegenmaßnahmen auf diversen Ebenen: Am Beispiel Emotet



# Aktuelles 2020

- Verschlüsselungstrojaner
  - Angeblicher Entschlüsselungshelfer verschlüsselt Daten
- Großer Hack von HPC-Systemen
  - Angriffsvektor unklar
  - Schadfunktion unklar (Bitcoin-Miner?)

# Aktuelles 2020 – Gefahren durch Covid-19

- Änderung der IT-Nutzung:
  - Deutlicher Anstieg der Remote-Nutzung
    - Größeres Angriffspotential durch
      - Ermöglichung weltweiter Zugriffe
      - Benutzung privater (und damit unkontrollierbarer) Endgeräte
      - „Offline-Nutzung“ schützenswerter Daten auf ungesicherten Geräten
  - „Neue“ Kommunikationswege (Video-Konferenzen, etc.)
    - Cloud-Basierte Lösungen: Skalierbarkeit contra Datenschutz
    - Sicherheitsprobleme bei eingesetzten Produkten

# Was wäre wenn…

- … während des Corona-Online-Semesters einem massiven Trojaner-Befall ausgesetzt wäre?

# ORGANISATORISCHES

- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge und Anregungen

# Systemausbildung: weitere Vorträge im SoSe 2020

Immer mittwochs (ab 14 c.t.) virtuell (statt in Raum 2.049 am RRZE)

06.05.2020 – Unixoide Betriebssysteme
13.05.2020 – Windows-Betriebssysteme
20.05.2020 – Systemüberwachung/Monitoring
27.05.2020 – Storage & Filesysteme
17.06.2020 – IT-Sicherheit
24.06.2020 –Backup/Archiv
01.07.2020 – Virtualisierung
08.07.2020 – High Performance Computing
15.07.2020 – Benutzerverwaltung MS Active Directory
22.07.2020 – LDAP und Kerberos

# Andere Vortragsreihen des RRZE

**Systemausbildung „Grundlagen und Aspekte von Betriebssystemen und systemnahen Diensten”**

- immer mittwochs ab 14 Uhr c.t. (in den Sommersemestern)
- Ergänzung zur Netzwerkausbildung “Praxis der Datenkommunikation”
- führt in den grundsätzlichen Aufbau eines Systems sowie eingesetzte Techniken und Komponenten ein
- richtet sich primär an alle Studierenden & Beschäftigten

**Netzwerkausbildung „Praxis der Datenkommunikation“**

- immer mittwochs ab 14 Uhr c.t. (in den Wintersemestern)
- führt in die Grundlagen der Netztechnik ein
- richtet sich primär an alle Studierenden & Netzwerkadmins

# Vortragsfolien und Vortragsaufzeichnung

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:
www.rrze.fau.de/ausbildung-schulung/veranstaltungsreihen/campustreffen/

Die meisten Vorträge des RRZE werden aufgezeichnet und können nach der Veranstaltung vom Videoportal der FAU heruntergeladen werden:
www.fau.tv

# RRZE-Veranstaltungskalender und Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter: www.rrze.fau.de/infocenter/aktuelles/veranstaltungskalender/

- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet.
  - Auch diese Liste kann man abonnieren: https://lists.fau.de/mailman/listinfo/rrze-aktuelles

# Themenvorschläge und Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Campustreffen)

# Vielen Dank für Ihre Aufmerksamkeit!

Regionales Rechenzentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
www.rrze.fau.de