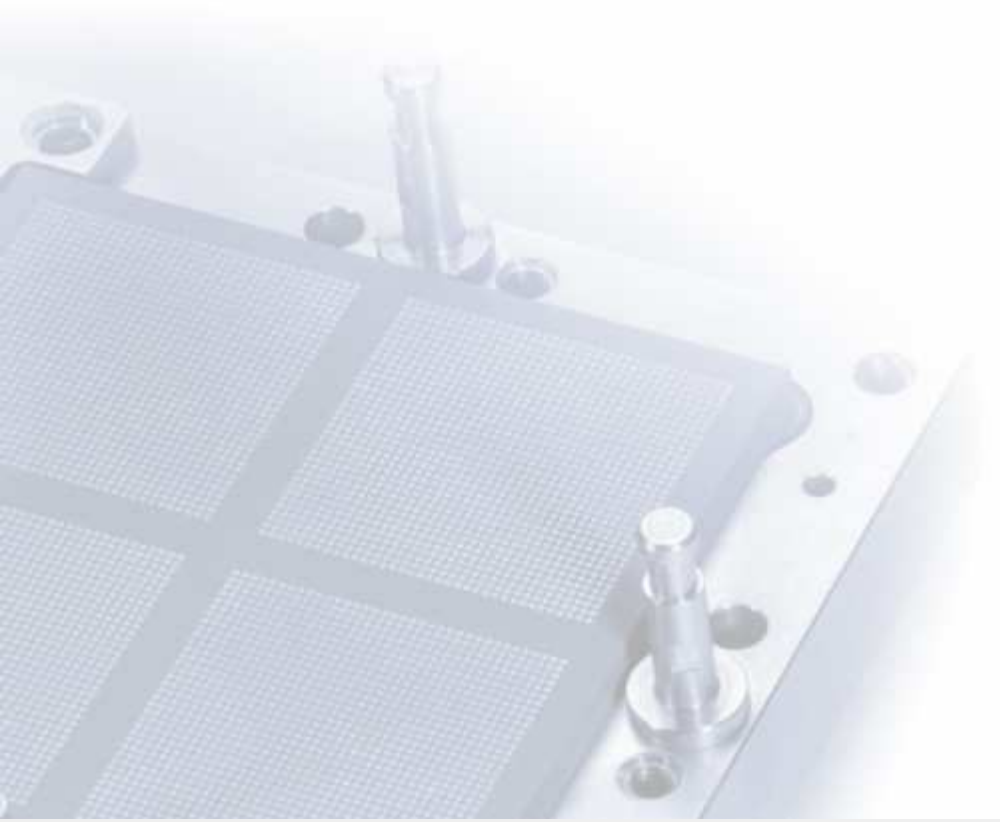
Leibniz Universität Hannover

Zur Sicherheitslage

Hergen Harnisch
harnisch@luis.uni-hannover.de



„Die Digitalisierung prägen drei zentrale Charakteristika, aus denen sich die Herausforderungen für die Informations- und Cyber-Sicherheit ergeben.

1. **Technologische Durchdringung und Vernetzung:**
   Alle physischen Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden.
2. **Komplexität:**
   Die Komplexität der IT nimmt durch vertikale und horizontale Integration in die Wertschöpfungsprozesse erheblich zu.
3. **Allgegenwärtigkeit:**
   Jedes System ist praktisch zu jeder Zeit und von jedem Ort über das Internet erreichbar."

(aus: BSI-Lagebericht 2014)

Programm

Dienstag 17.11.15

09:15-10:45 Sicherheitslage
10:45-11:15 *Pause*
11:15-12:45 TLS/SSL Verschlüsselung & Authentifizierung

Mittwoch 18.11.15

09:15-10:30 Kerberos
11:00-11:30 *Pause*
11:15-12:45 NFS – v4 mit Kerberos

Angriffsmotive & -typen

"Traditionelles":

Mobile IT

Sicherheitsvorfälle

Amplification-Attacks:

- NTP
- DNS

DNS:

- Hintergrund
- Veränderungen LUH
- Windows

Advanced Persistent Threat

...Raketentechnik hat viele Interessenten...

Big Brother

„Three Letter Agencies“

Kriminelle Angriffe

Erpressung
Betrug
SPAM
...

Hacktivism

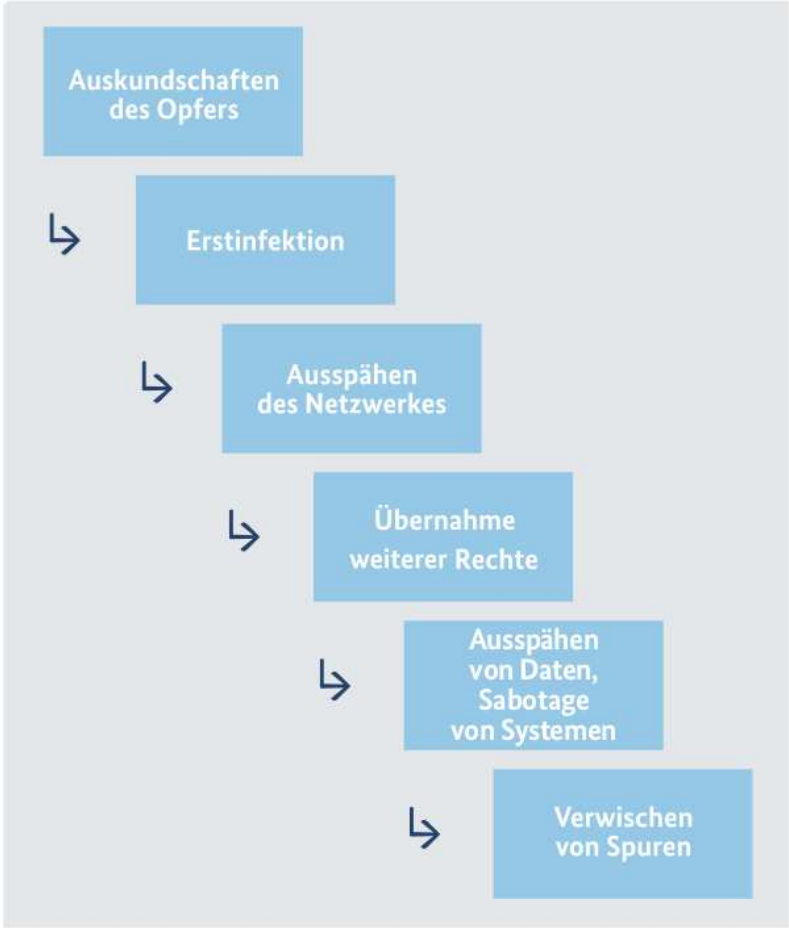
Politisch Motivierte Angriffe

Quelle: Vortrag Ralf Gröper auf DFN-BT in 10/2015

Angriffsmotive & -typen

Advanced Persistent Threat

Zielgerichtete Angriffe zum Zwecke der Wirtschafts- & Wissenschaftsspionage



BSI-Lagebericht 2014

Angriffsmotive & -typen

Advanced Persistent Threat

„Im Fokus von APT-Angriffen stehen vorrangig die Rüstungsindustrie, Hochtechnologiebranchen wie Automobilbau, Schiffsbau und Raumfahrt, Forschungseinrichtungen sowie die öffentliche Verwaltung." (BSI-Lagebericht 2014)

- „sehr hohen Ressourceneinsatz, erhebliche technische Fähigkeiten"
- schwer zu verhindern
- schwer festzustellen
- Dauer von mehreren Monaten bis Jahre
- nicht jeder im Fokus aber auch indirekte Wege, unklare Fallzahl

Wer greift wie an?

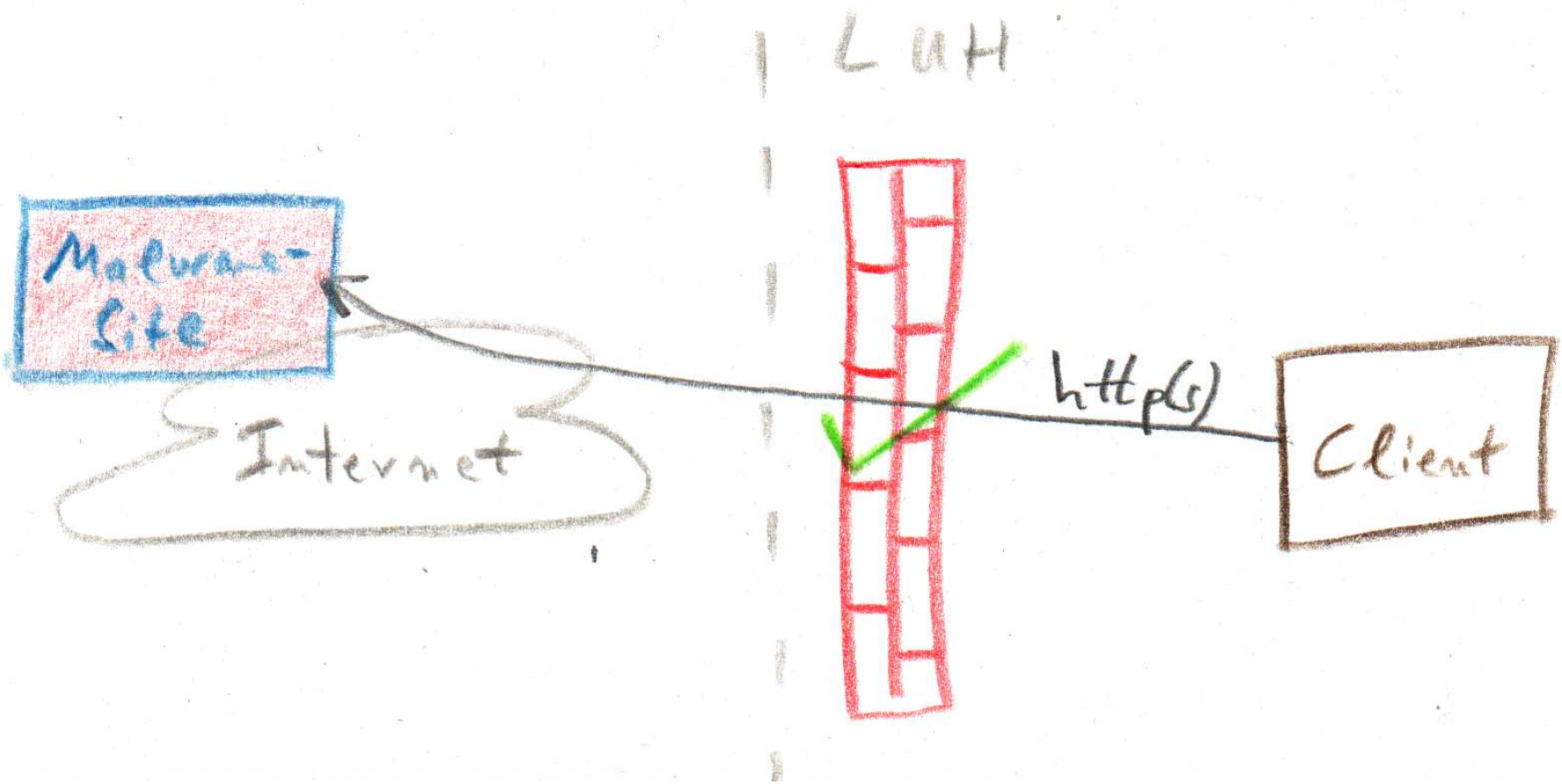
DFN Deutsches Forschungsnetz

	APT	Big Brother	Kriminell	Hacktivism	Unbekannt
Malware	x		x		x
Abhöhren	x	x			
Defacement			x	x	x
Phishing	x		x		
DDoS			x	x	x

Quelle: Vortrag Ralf Gröper auf DFN-BT in 10/2015

"Traditionelles":

Desktops/Notebooks: Drive-By-Downloads



"Traditionelles":
Desktops/Notebooks

eigentlich keine wirklich neue Entwicklung (vgl. SiTa 11/2012)

- Drive-By-Downloads dominieren
- Spam wird zunehmend malicous
- direkte Angriffe kaum noch
- Malware installiert Rootkit, PC wird zum Bot
- Updates von OS *und* Applikationen wichtig

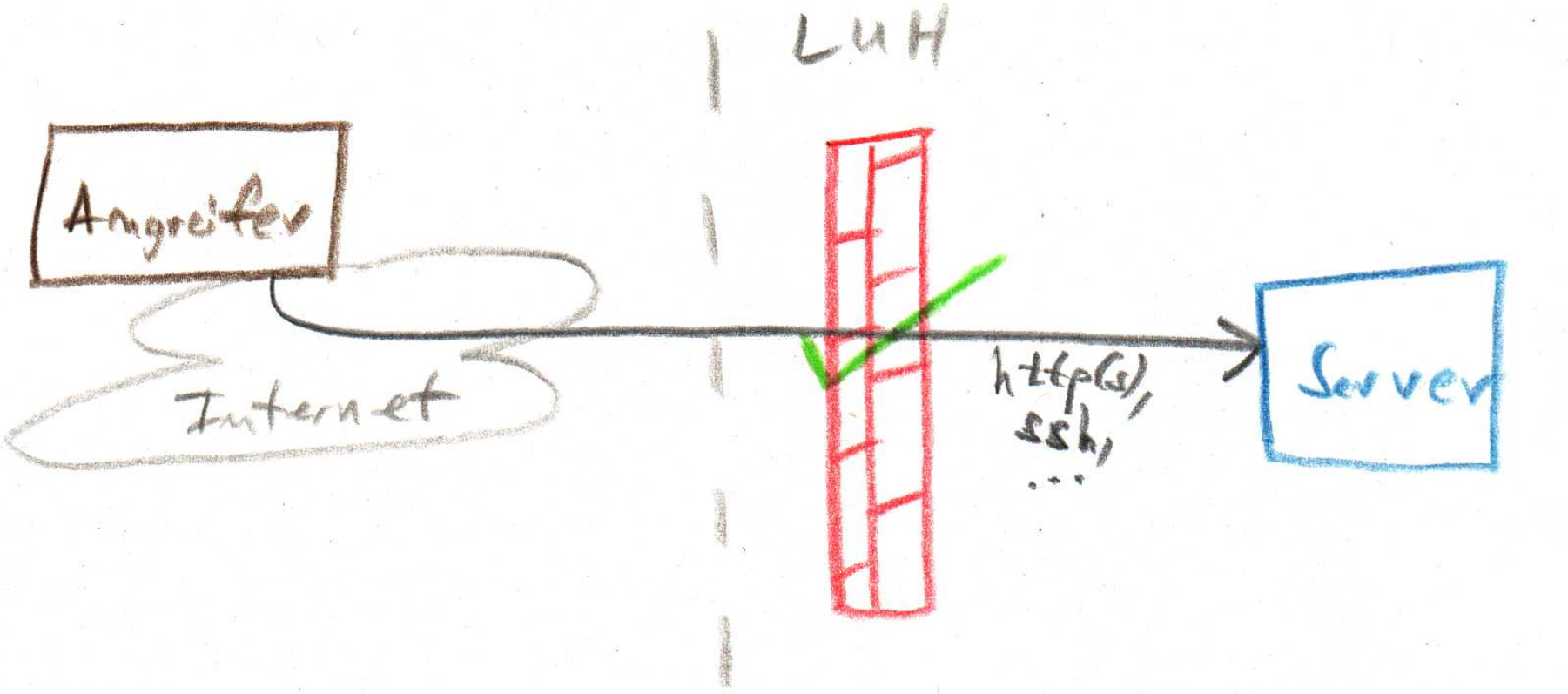
Trends & Veränderungen 2012:

- Zweck ist weniger Bot, mehr Abgriff von Passwörtern / IDs
- rausgehenden Traffic an Firewall zu filtern & loggen ist wichtig
- mehr Filterung auf Applikationsebene (z.B. Proxy)

neuer: deutlich mehr Zeit zwischen Infektion und Auffälligkeit

"Traditionelles":

Server: Angriff auf Serverdienste



"Traditionelles":

Server

Angriffe erfolgen über

- die angebotenen Applikationen (insbesondere Web-Server)
- Remote-Zugänge (z.B. ssh-Bruteforce)
- Server-Management-Zugänge (KVM over IP, IPMI)

Gegenmaßnahmen:

- Applikation absichern …
- Zugriff auf Applikation einschränken
- Teile der Applikation (z.B. Konfig-Seite) im Zugriff einschränken
- Abschotten der Managementzugänge

"Traditionelles":
Social Engenieering

- häufig „malicous spam“:
  Virus ist nicht in Mail sondern in verlinkter Webseite
- Phishing-Attacken auf LUH-Nutzer: einige wenige antworten
- schwierig: malicous Bewerbung an Personalabteilung
- inzwischen auch per Telefon,
  beachte: Anrufer-Nummer nicht verlässlich
- Auslegen eines USB-Sticks (typischer Pentest)

⟶ vielfältigster und erfolgreichster Angriffsvektor

⟶ am schwierigsten zu verhindern

⟶ bei zielgerichteten APT-Angriffen besonders häufig

"Traditionelles":

Social Engenieering: Bsp. Watering-Hole-Angriff

Eigenarten und Interesse des Opfers werden bewusst eingesetzt:

- Opfer liest häufiger Webseite seines Tennis-Clubs
- Angreifer hackt Tennis-Club-Seite
  (häufig eher Hobby-Seite, leichter hackbar)
- Tennis-Club-Seite wird malicious (evt. nur für Opfer)
- Angreifer wartet auf nächsten Besuch …

Für zielgerichtete APT-Angriffe beliebt.

Mobile IT

Hat mehrere Aspekte:

- zunehmende Komplexität auf „embedded Devices“
- Nutzung von Cloud-Diensten sowie Apps
- häufig private Endgeräte
- zunehmend Notebooks statt Desktops

hier betrachtet: Smartphones & Tablets

Mobile IT

Angreifbarkeit

- private (Mit-) Nutzung, selten Profiltrennung
- native Apps statt Webseiten
- teilweise Apps mit fragwürdiger Qualität
- enthaltene Cloud-Nutzung
- Rooting teilweise durch Hacks
- reduzierte Software: auch bzgl. Sicherheits-Tools
- vorallem aber: veraltete Software
  - Bugs auf alten Versionen nicht gefixt
  - kein Update oder Upgrade durch Handy-Hersteller

Besondere Gefahren:

mobil- & WLAN-Netze, PC-Anschluss, persönliche Infos, PWs & TANs

Mobile IT

veraltete Mobil-Software

iOS

noch relativ gute Unterstützung älterer Geräte

Android

sehr heterogen durch Trennung OS- und Geräte-Hersteller

- z.B. Webkit-Probleme in Android ≤ 4.3
- Altgeräte noch im Verkauf
  - Android 2.3 auf eBook-Reader Tolino Shine (bis 10/2015)
  - Abverkauf älterer Geräte mit veraltetem OS als Angebote

$\Longrightarrow$ schützenswere Daten nur bei sehr reduziertem Einsatz …

Sicherheitsvorfälle

xcodeghost

Infektion über Bande mit Multiplikator:

- malicious Xcode-Entwicklungsumgebung für iOS:
  erstellte Apps enthalten Schadcode
- Download lokaler Xcode-Kopien durch Entwickler
- Einstellen infizierter Apps in App-Store
- Installation auf iOS-Geräte aus „vertrauenswürdiger" Quelle

⟶ Löschen oder Aktualisieren betroffener Apps notwendig

⟶ App-Signatur, vertrauenswürdige Quelle, Trusted-Computing ??

⟶ WLAN-Sperrung nicht hilfreich, da Mobilfunk:
Quarantäne-WLAN wäre gut

Sicherheitsvorfälle

Remote-Root-Login

Auffälligkeit erfolgreicher Remote-Root-Login aus Russland

Probleme

- gleiches Root-PW auf allen Systemen, lange nicht geändert
- NFSv3 für Home-Verzeichnisse, kein Kerberos
- Cross-Mounts auch mit Programm-Dateien
- Vermischung von Server-Funktionen (teils über Shares)
- Webserver mit User-Content (Skripte)
- durch Cloning gleiche Host-Keys

Ursache „nur “ Fehlkonfiguration in PAM-Modulen

Folge Statt kompletter Neuinstallation Neuaufsetzen betroffener Arbeitsplätze, sukzessive Problembehebung

Sicherheitsvorfälle

Remote RDP-Login

Auffälligkeit selbst festgestellte Remote-Logins

Probleme keines ursächlich:

- keine Firewall, Irrtum darüber
- keine Admin-Vertretung, Admin abwesend
- Vermischung Labor- und Büro-PCs
- Vertrauensstellung des AD mit Nachbarinstituten

Ursache unklar, evt. APT

Folge Komplette Neuinstallation der Instituts-IT

- Prüfung der Datendateien
- PC-Installation mittels PXE & Softwareverteilung recht zügig
- neues AD, neuer DC

Sicherheitsvorfälle

Webserver

Auffälligkeit von extern gemeldete malicious Website

Ursache veraltetes CMS in einem vhost mit

1. bel. PHP-Code auf Webserver ausführbar
2. bel. Programme als User www-data
3. Rechteausweitung auf root ist erfahrungsgemäß zu unterstellen

Probleme neben veralteter Software

- „Multiserver“: Web, Mail, SSH, DNS
- mangelnde Einsicht & unzureichende Security-Response

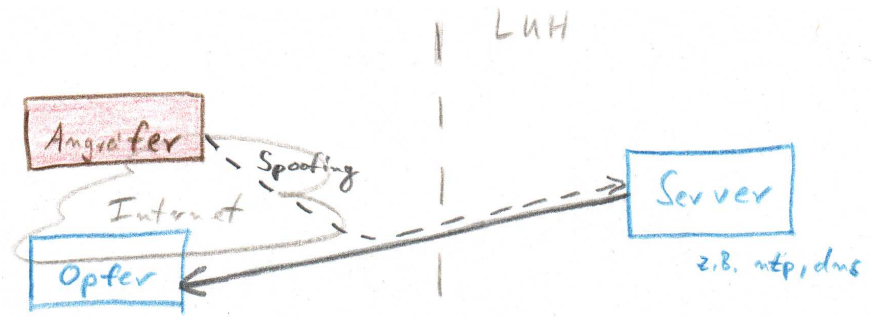
Folge Probleme nur unzureichend behoben, unnötige Sicherheitsrisiken bleiben

Amplification-Attacks:

Reflection

1. Angreifer befragt (UDP-) Dienst mit gefälschter Absender-IP
2. Dienst antwortet an falsche Absender-IP

⟶ „Angriff“ unbekannten Ursprungs



Amplification

Kleine Anfrage erzeugt große Antwort:

⟶ Verstärkungseffekt ⇝ dDoS-Angriff

Amplification-Attacks: NTP

Leibniz Universität Hannover

NTP: Protokoll für die Zeit-Synchronisation vom Zeitserver

Amplification-Attack über monlist-Abfrage:

- monlist: Liste der letzten 600 Anfragenden
- Verstärkung um bis zu $\times$ 200:
  1 Paket mit 234 Bytes $\rightsquigarrow$ 100 Pakete mit $\geq$ 48 kBytes

Maßnahmen

Neben Sperrung eingehender NTP-Anfragen noch je Gerät:

- keine unnötigen Anfragen zulassen
  - Standard-NTP-Daemon schwierig zu konfigurieren
  - Openntpd einfachere Alternative
- dezentrale NTP-Server sind überflüssig
- Clients sollten selbst NTP-Dienst nicht anbieten

Amplification-Attacks: DNS

Leibniz Universität Hannover

Über offene Resolver sind verschiedene Angriffe möglich:

- Last auf angegriffenem DNS-Server durch reguläre Anfrage
- Amplification durch große Antwort-Pakete (z.B. DNSSEC)
  z.B. 60 Bytes-Anfragepaket $\rightsquigarrow$ 4k-Antwort ($\times$ 70)

Maßnahmen

- Verlagerung dezentrale autoritativer Daten auf zentrale Server
- Sperrung eingehender DNS-Anfragen bis auf zentrale DNS-Server
- Absicherung von Windows-DNS-Server (Teil eines DC)

DNS: Hintergrund

autoritativer DNS-Server

Stellt Informationen über bestimmte Domains fürs Internet bereit, z.B.

- unter `uni-hannover.de`

  ```
  www.uni-hannover.de. IN A 130.75.2.151
  ```

- oder zu IPs in `130.75.*.*`

  ```
  151.2.75.130.in-addr.arpa. IN PTR
                                  cmsv023.rrzn.uni-hannover.de.
  ```

Delegiert ggf. auf andere autoritative DNS-Server, z.B.

- auf `f.nic.de` für unsere Domain

  ```
  uni-hannover.de. IN NS dns1.uni-hannover.de.
  ```

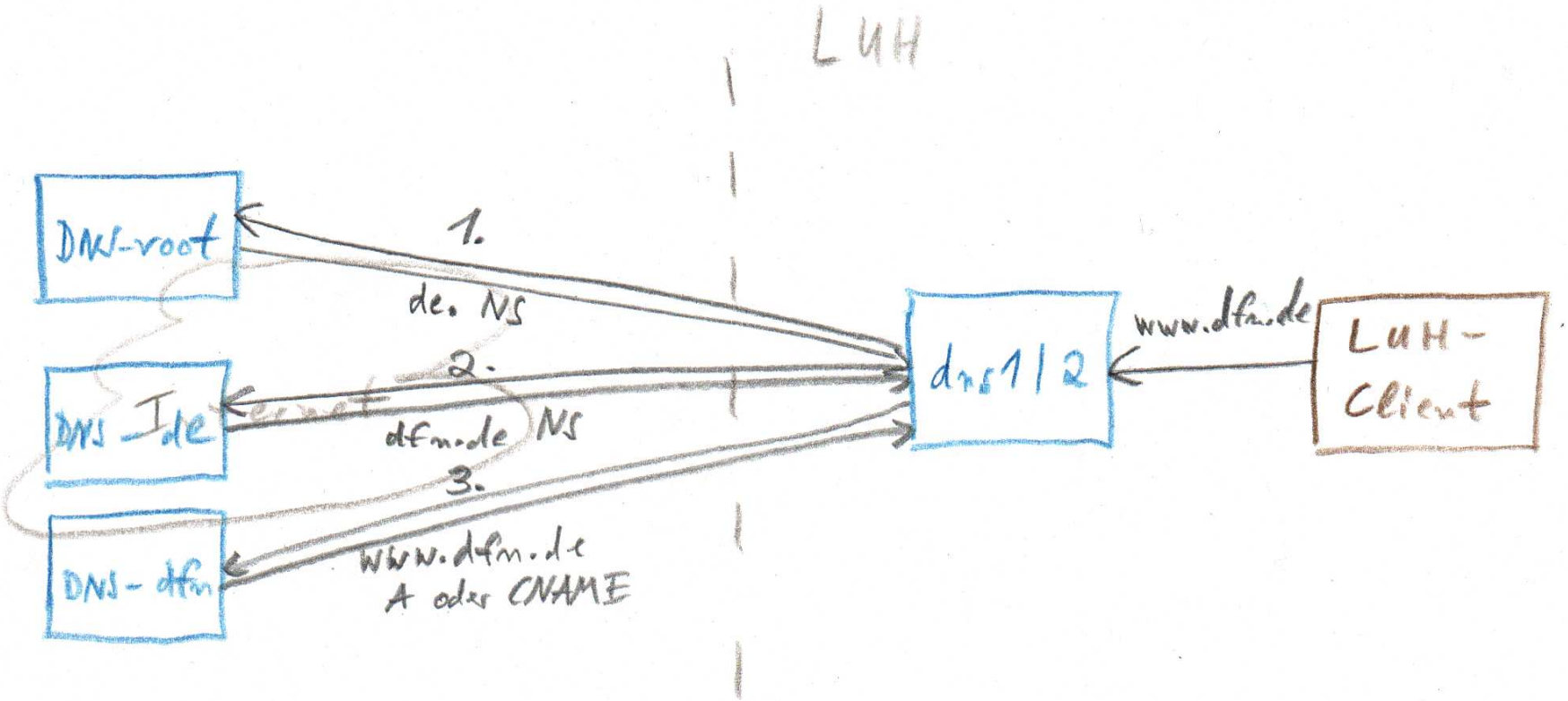
- auf `w.arin.net` für unsere IPs

  ```
  75.130.in-addr.arpa. IN NS dns1.uni-hannover.de.
  ```

DNS: Hintergrund

rekursiver DNS-Server

Löst für Clients durch „Abklappern“ auf und speichert zwischen (Cache):



DNS: Veränderungen LUH

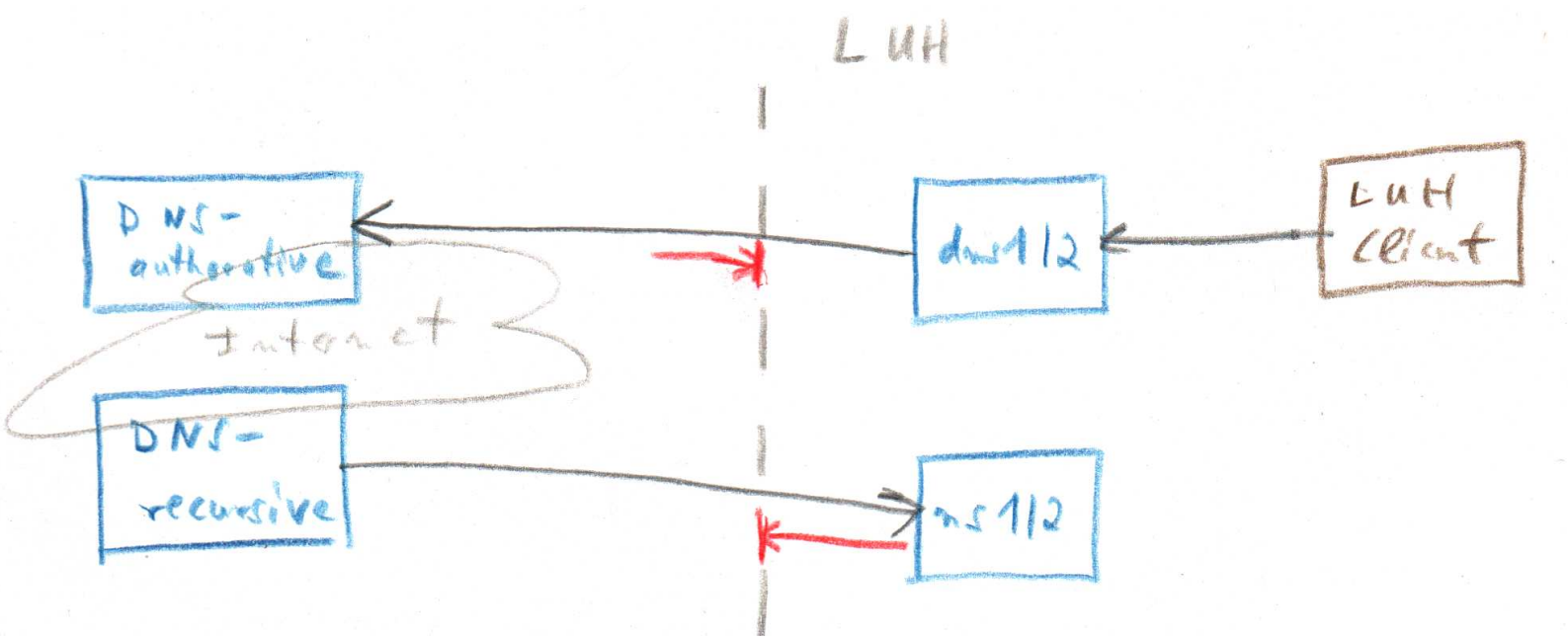
Trennung autoritativ und rekursiv

früher `dns1|2` für beide DNS-Serverarten

zukünftig Trennung (reduziert Angreifbarkeit & Poisoning)

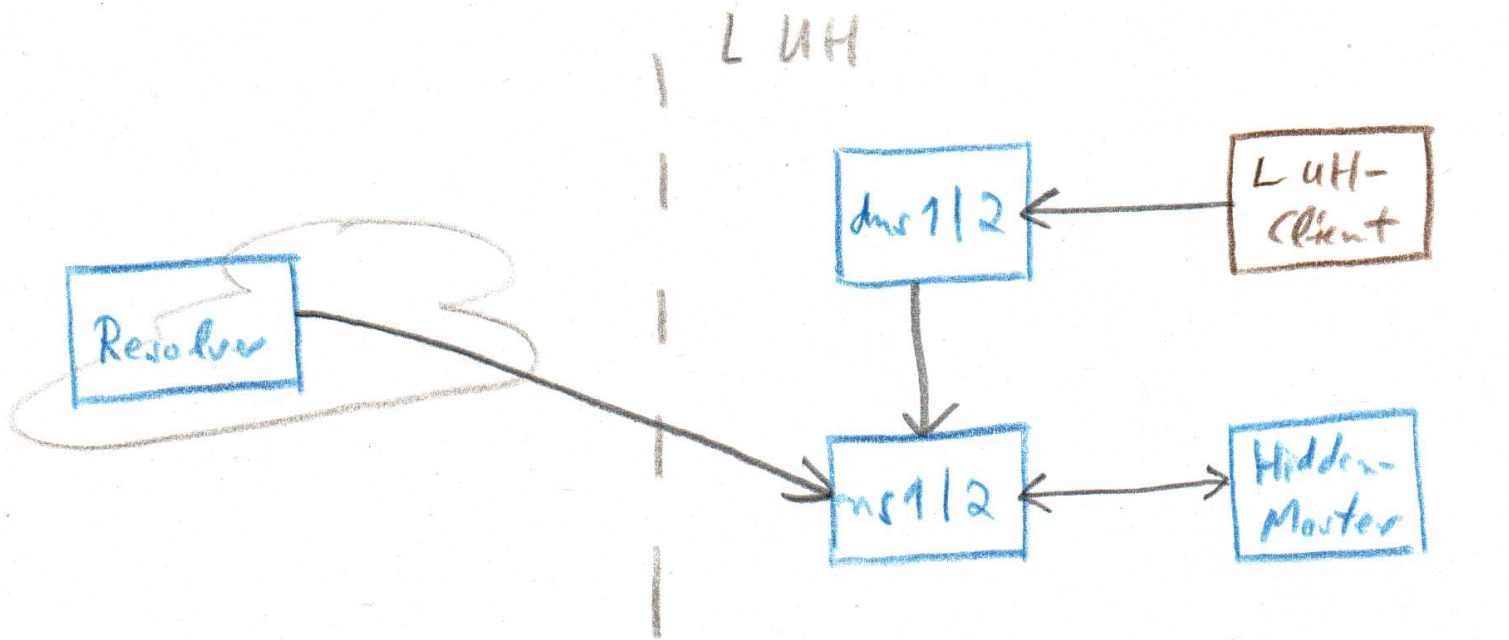
`dns1|2` als rekursive DNS-Server für LUH-Clients

`ns1|2` als autoritative DNS-Server für das Internet



DNS: Veränderungen LUH

Dezentrale autoritative „Sub“-DNS-Server



aber eigentlich unschön

- nach Ablauf von TTL Probleme, sogar für Mail (MX)
- Aufwand, z.B. bzgl. neuer Gateway-Firewall;
  wg. Aufwands keine Unterstützung für DNSSEC & DFN-Secondary

DNS: Veränderungen LUH

Andere Zonen als `uni-hannover.de`

Werden für Forschungsverbünde, Konferenzen etc. besorgt:

- über Rechenzentrum beim DFN
- bei anderem Registrar/Hoster
  - meist dort auch der DNS-Server
  - selten selbst-gehostetes DNS

zentrale Registrierung

- über Rechenzentrum zu günstigen Konditionen (neu)
- Besitz oder Admin-C ist LUH, zentrale DNS-Server der LUH
- möglich: Zertifikate aus der DFN-PKI-Global, Mail-Service

… *aber bitte beachten:* macht Arbeit, Domain-Inflation vermeiden

DNS: Veränderungen LUH

DNSSEC – Vorteile

DNSSEC ist eine Absicherung von DNS-Eintragungen über Public-/Private-Key-Methoden und (signierter) Delegierung

- Signatur von DNS-Einträgen verhindert Spoofing
- Keine Verschlüsselung oder Absicherung gegen falsche Lame-Delegations

Aber auch zusätzlicher Nutzen

- DANE: Prüfung von Schlüsseln/Zertifikaten über DNSSEC, z.B. zwischen Mail-Servern (dabei ohne CA-Trusts)
- Verlässlichkeit
  - von Dienste-Server-Zuordnungen (SRV)
  - von Config-Suchen (Autoconfig-Funktionen)

DNS: Veränderungen LUH

DNSSEC – Umsetzung

rekursiv

Prüfung auf `dns1|2`, eher problemlos

autoritativ

Schwierig: Fehler entspricht in Wirkung vollständigem Serverausfall

- Signatur auf Hidden-Master im Rechenzentrum, Keymanagement/-rollover wichtig
- dezentrale „Schatten“-DNS-Server problematisch:
  - instituts-interne Views $\longrightarrow$ abschalten
  - Windows-AD auf `.uni-hannover.de` $\longrightarrow$ migrieren zu `.intern`, d.h. neuaufsetzen

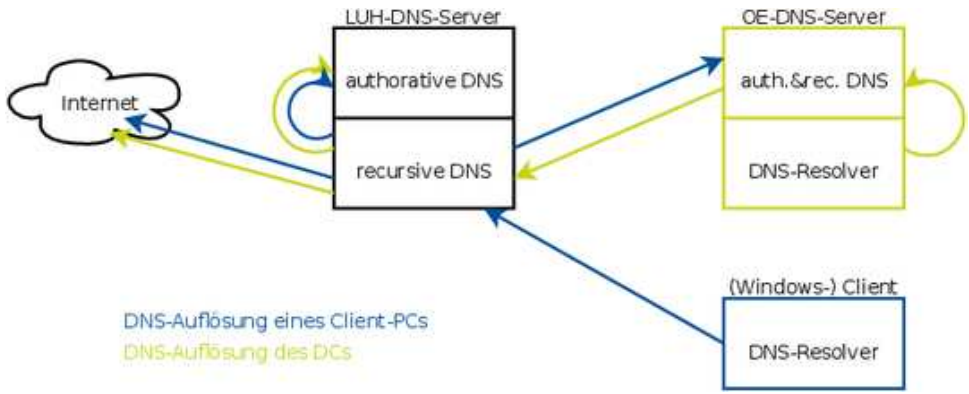
DNS: Windows

DNS in Windows-ADs

Rechenzentrum empfiehlt schon lange `.intern`:

`example.uni-hannover.de.` ⇝ `example.intern.`

- Windows-DNS ist rein intern, unabhängig vom Internet-DNS: keine gleichen Einträge mit unterschiedlicher Auflösung
- kann (und sollte!) auf zentralen DNS-Servern delegiert werden, `dns1|2` und nicht DC als DNS-Server für Clients



DNS: Windows

Host-Benennung DNS vs. Windows

- im DNS hierarchisch, unproblematisch (insb. unter Linux)
- unter Windows mit AD oder flach, Windows-Tools zeigen eher nur Computernamen (z.B. viele `pc1` in Sophos-EC)

Daher Empfehlung (bei PXE-Windowsinstallation automatisch):

DNS `pc1.luis.uni-hannover.de`

Windows Computername=`luis-pc1` `AD=luis.intern`

Algorithmus: left(left(OE_OHNEMINUS,6) + '-' + RDN ,15)

vgl. `http://www.luis.uni-hannover.de/win-dns.html`

Hausaufgaben

- überprüfen Sie administrative Zugänge
  - wer kennt PW, wann zuletzt geändert
  - personalisierte Logins, ggf. vorgeschaltet
  - unterschiedliche PWs je Gerät (auch je PC beim Administrator!)
- NTP-Server abbauen, NTP-Konfigurationen prüfen
- DNS ins Rechenzentrum verlagern, Rekursion abbauen, Windows-Domains unter `.intern` oder `.local` zentral anmelden

- Trennung von Diensten, keine Single-Passwort-Policy, Abgabe von Diensten an uns?
- Patch-Management, kein XP mehr auf Internet-Rechnern
- Aktualisieren der `sec-*@ou.uni-hannover.de`-Verteiler