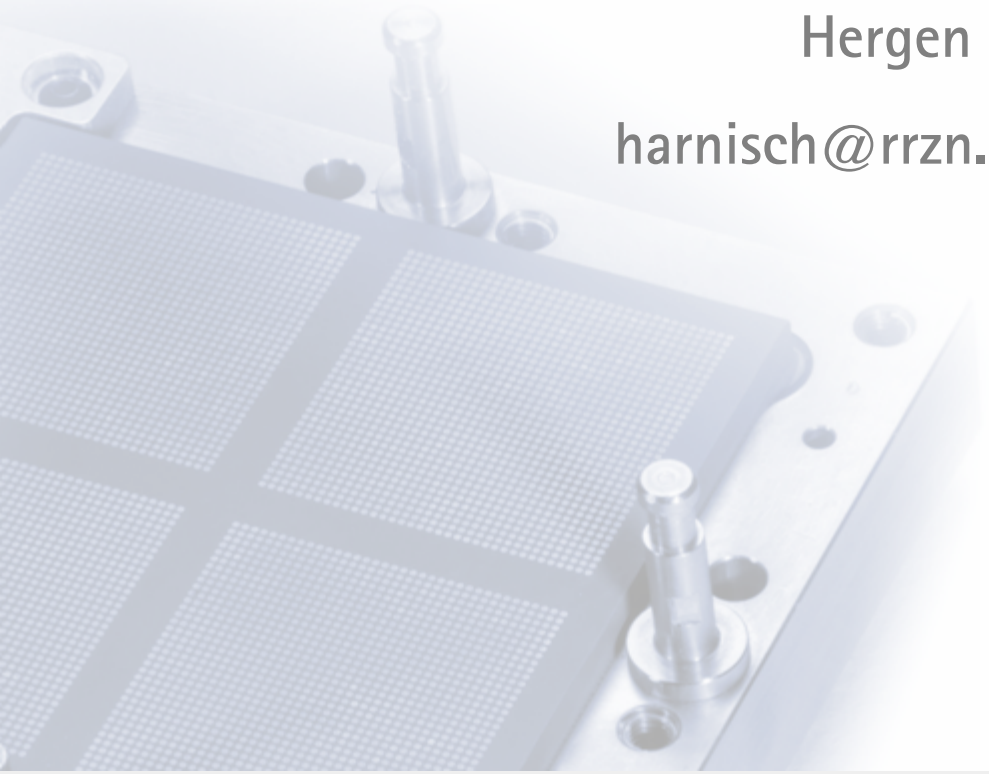
Begrüßung & zur Sicherheitslage



Hergen Harnisch

harnisch@rrzn.uni-hannover.de

Programm

Dienstag 18.11.08

09:15-09:45 Sicherheitslage
09:45-10:45 Shibboleth
10:45-11:15 *Pause*
11:15-12:45 Kerberos

Mittwoch 19.11.08

09:15-10:45 Samba
10:45-11:15 *Pause*
11:15-12:15 Identitätsmanagement
12:15-12:45 Abschlussdiskussion & Fragen

1 Angriffslage

2 Absicherung

3 Wireless-LAN

4 Appliances / embedded devices

R|R|Z|N

Social Engineering

... wie schon mehrfach hier erwähnt:

- kaum noch Würmer, Viren
- stattdessen nachwievor direkte Hacks Websurfer & SSH-Bruteforce
- und vor allem „client-seitig initiierte“ Malware-Hacks

⟶ Clients / Desktops absichern

⟶ Anwender aufklären

aber natürlich weiterhin Firewall, Mailscanning etc.;
„kaum noch“ bedeutet geringerer Zuwachs, weniger neue Varianten!

R|R|Z|N

sichere Clients

gelegentlich deaktivieren Nutzer Virenscanner oder Firewall,

häufiger werden Updates nicht eingespielt.

großes Problem

Updatelage mit dem Betriebssystem meist noch akzeptabel,
Viewer (Flash, PDF, Video, ...) stellen großes Problem und Risiko dar:

- individuelle Update-Prozeduren, umständlich, unübersichtlich;
  nicht automatisch, eigentlich Software-Verteilung einzige Lösung
- öffnet Einfallstor in Browser, Mail, Chat etc.
- mangelndes Bewusstsein der Nutzer bzgl. Multimedia-Viewer/-Plugins

R|R|Z|N

(Multimedia-) Viewer

immer wieder und auch in letzter Zeit Sicherheitsupdates für:

- Adobe Flash
- Adobe Reader, andere PDF-Viewer
- VLC, mplayer (auch Windows-Media-Player)
- ...
- Thunderbird und Firefox, Opera (auch IE)
- Java

Viele von diesen sind auch Plugins im Browser:

- Sicherheitslücken sehr schnell von *malicious websites* ausgenutzt
- auch hier hilft z.B. Firefox-Plugin NoScript

Windows-Clients

In letzter Zeit wieder sehr wichtige MS-Patches:

```
                CERT-Bund  --  Warn- und Informationsdienst

          KURZINFORMATION ZU SCHWACHSTELLEN UND SICHERHEITSLUECKEN

             ID: CB-K08/0610
          Titel: Schwachstellen in den Microsoft XML Core Services
                 ermoeglichen Codeausfuehrung
          Datum: 12.11.2008
       Software: Microsoft XML Core Services
        Version: 3.0, 4.0, 5.0 und 6.0
     Plattform: Microsoft Windows
    Auswirkung: Ausfuehren beliebigen Programmcodes
Remoteangriff: Ja
        Risiko: hoch
```

Windows-Clients

In letzter Zeit wieder sehr wichtige MS-Patches:

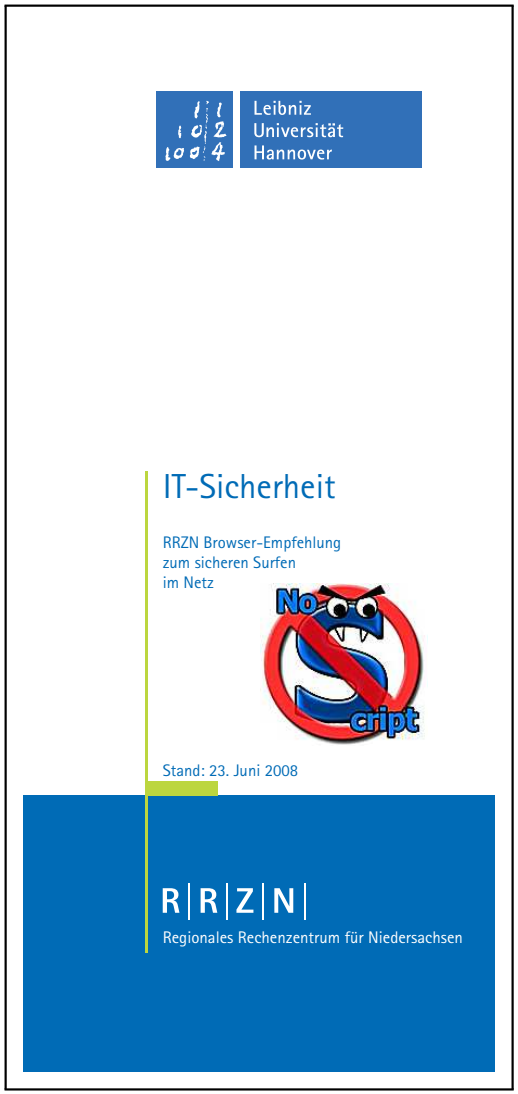
```
Schwachstellen in den Microsoft XML Core Services (MSXML) ermoeglichen
einem entfernten Angreifer die Kompromittierung eines Opfersystems
oder das Ausspaehen sensibler Daten. Dazu versendet der Angreifer in
der Regel eine E-Mail oder eine Instant Messenger-Anfrage mit einem
Link zu einer manipulierten Webseite. Die Ausnutzung der Schwachstelle
erfolgt, sobald das Opfer auf den Link klickt.
```

$\longrightarrow$ typisches Beispiel für *malicious websites*

Absicherung

aufgeklärter Anwender

Websurfen absichern,
Firefox mit NoScript-Extension



Windows-Clients: Netbios

Vulnerability in Server Service Could Allow Remote Code Execution

„The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit."

http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

Betrifft RPC über NetBIOS-Port TCP-139 aber auch Port TCP-445.

R|R|Z|N

Windows-Clients: Netbios

Bedingter Schutz durch Windows-Firewall

- teilweise Windows-Ports im LAN doch offen
- Verbindungen, die vom Client initiiert werden, könnten z.B. bei gehacktem Server problematisch sein

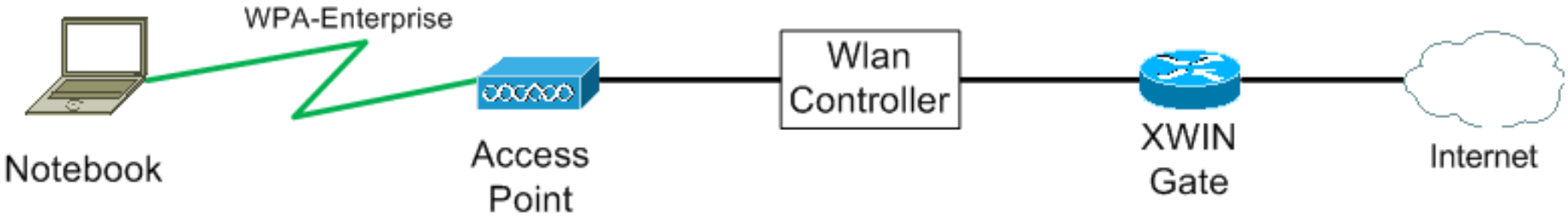
RRZN sperrt Windows-Ports an Gateways auch innerhalb der Universität.

Besser zusätzlich Dienste minimieren

- TCP-139 gehört zu NetBIOS, heutzutage unnötig (vgl. morgen zu Samba)
- NetBIOS deaktivieren: unter Netzwerkeigenschaften, TCP/IP, Erweitert
- auf reinen Clients zusätzlich den gesamten Dienst „Datei- und Druckerfreigabe“ entfernen oder deaktivieren

LUHWPA

- auf Luftschnittstelle auch gegen andere Teilnehmer verschlüsselt
- ab Access-Point keine Verschlüsselung auf (LUH-) Kabelweg



- Verschlüsselung auf Applikationsebene ratsam (z.B. TLS bei imap)
- erste Hacks gegen WPA-RC4/TKIP bekannt, derzeit keine Gefahr

→ besser jetzt auf WPA2 mit AES/CCMP umsteigen & -konfigurieren
aber: WLAN-Client-Hardware muss WPA2 unterstützen

Appliances / embedded devices

R|R|Z|N

gemeint sind Geräte mit Netzwerkanschluss, z.B.

- Drucker
- Scanner, Kopierer
- Beamer, Info-Displays
- Video-Konferenzsysteme
- Kameras / Web-Cams
- Diebstahlsicherungen und Alarmsysteme
- Laborgeräte, Sensoren
- Netzkomponenten

Enthalten abgespecktes Betriebssystem mit Server-Diensten,
z.B. Windows-CE oder Linux mit Web-Server

R|R|Z|N

Probleme

viele wie bei anderen Servern auch:

- Fehler im Netzwerk-/IP-Stack
- Fehler in den Server-Daemons
- Fehlkonfigurationen:
  - unnötige Dienste (z.B. SNMP, Appletalk)
  - ungeänderte Default-Passwörter
- fehlende Einstellungsmöglichkeiten
- unzureichende Absicherung im Gerät selbst (z.B. Firewall)
- fehlende Überwachung / Logging

… leider häufig *falsche* Ansicht, Appliances seien sicher.

R|R|Z|N

Maßnahmen

Installation

- Passwörter setzen
- zugelassene IP-Bereiche konfigurieren oder
  kein Gateway bei geeigneter Netzmaske setzen
- Überflüssiges deaktivieren
- Gerät im Netzschutz sperren lassen

Wartung

- regelmäßige Aktualisierung der Firmware