

Selbstverteidigung im Web

Marcel Heisig
Norman Planner
Niklas Reisinger

am 27.10.2011

Inhalt der Veranstaltung

- Live-Vorführung gängiger Angriffsszenarien
- Schutzmaßnahmen
- Diskussion

Vernetzte Welt

- Fast 50 Millionen Deutsche online, davon nutzen 76% das Internet täglich
- 80% der Unternehmen in Deutschland mit eigenem Internetauftritt
- E-Government auf dem Vormarsch (Gesundheitskarte, ELENA, neuer Personalausweis)

Aber

- jährlicher Schaden durch Wirtschaftsspionage in Deutschland: 20 Milliarden Euro
- vier Millionen Deutsche Opfer von Computerkriminalität mit finanziellem Schaden
- Schwachstelle in AusweisApp des neuen Personalausweis entdeckt

Grundgedanken

Nicht:

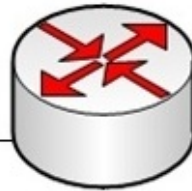
- Anleitung zum Hacken
- Angst verbreiten

Vielmehr:

- Sensibilisieren

→ Vernetzung ohne Sicherheitsvorkehrungen ist ebenso wenig möglich wie der Verzicht auf Teilnahme am globalen Netz

Aufbau der Testumgebung



Apple airport extreme

Desktop Operating System Market Share

September. 2011

Total Market Share



Angriffsszenarien

- Fokus auf PC
- Weites Spektrum an Angriffen
- Aus Angriffsszenarien allgemeingültige Präventionsmaßnahmen ableiten

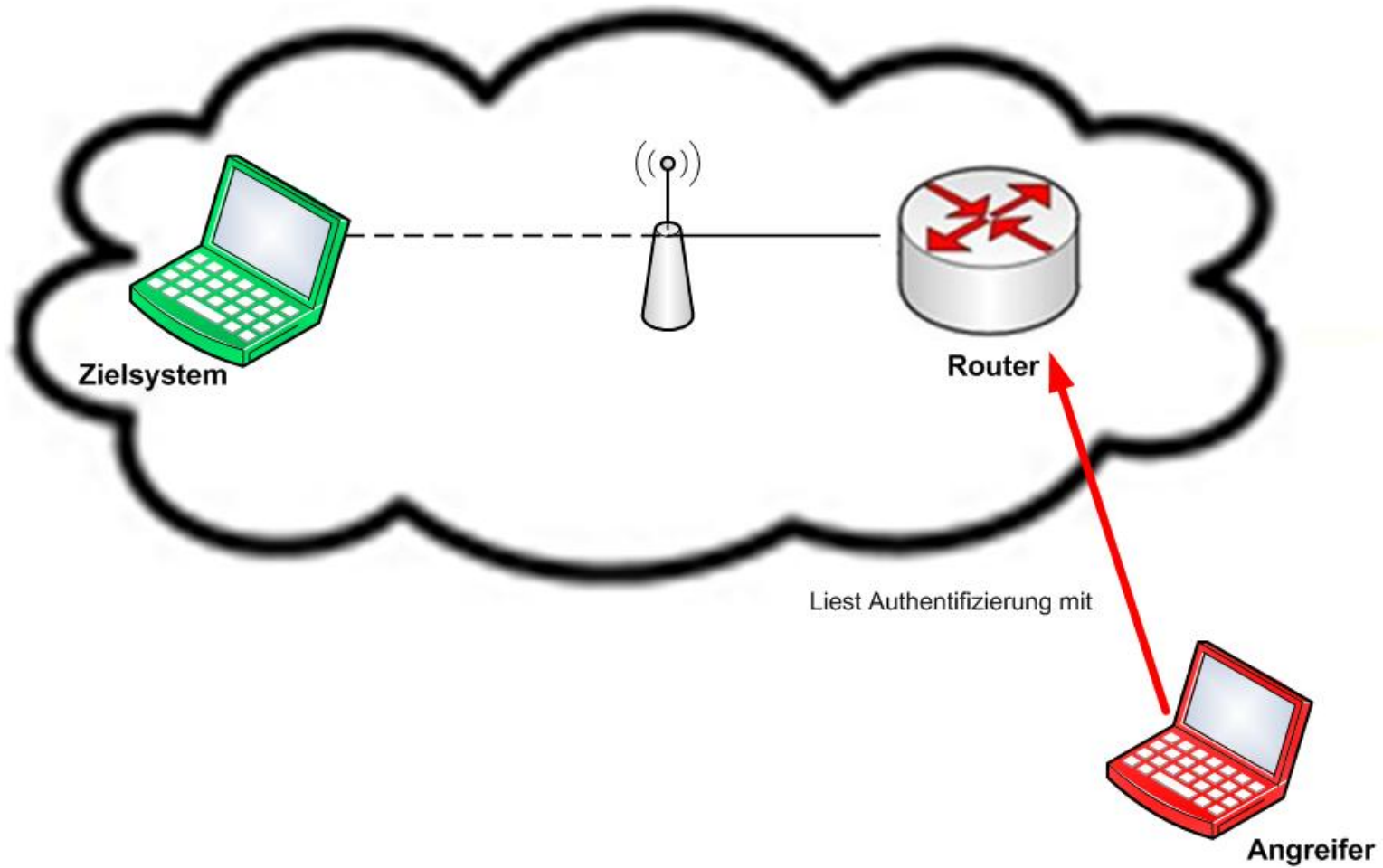
Angriff auf WPA verschlüsseltes Netzwerk via dictionary attack

- Mitlesen der Datenpakete und Auslesen der Anmeldeinformationen (verschlüsselt)
- Wörterbuchangriff
- nutzt schwache Passwörter aus
- nur erfolgreich, wenn Passwort in Wörterbuch

Angriff auf WPA verschlüsseltes Netzwerk via dictionary attack

Ausgangssituation

WLAN



Risikopotenzial

- Zunächst nur Teilnehmer im Netzwerk → Basis für weitere Angriffe
- WPA2 als aktueller Standard → nur sicher bei Verwendung von starken Passwörtern
- Wörterbücher legal und offen zugänglich
- sorglose Vergabe schwacher Passwörter

Analyse von Passwörtern

32 Millionen Passwörter ausgewertet

Password Popularity – Top 20

| Rank | Password | Number of Users with Password (absolute) |
|------|-----------|--|
| 1 | 123456 | 290731 |
| 2 | 12345 | 79078 |
| 3 | 123456789 | 76790 |
| 4 | Password | 61958 |
| 5 | iloveyou | 51622 |
| 6 | princess | 35231 |
| 7 | rockyou | 22588 |
| 8 | 1234567 | 21726 |
| 9 | 12345678 | 20553 |
| 10 | abc123 | 17542 |

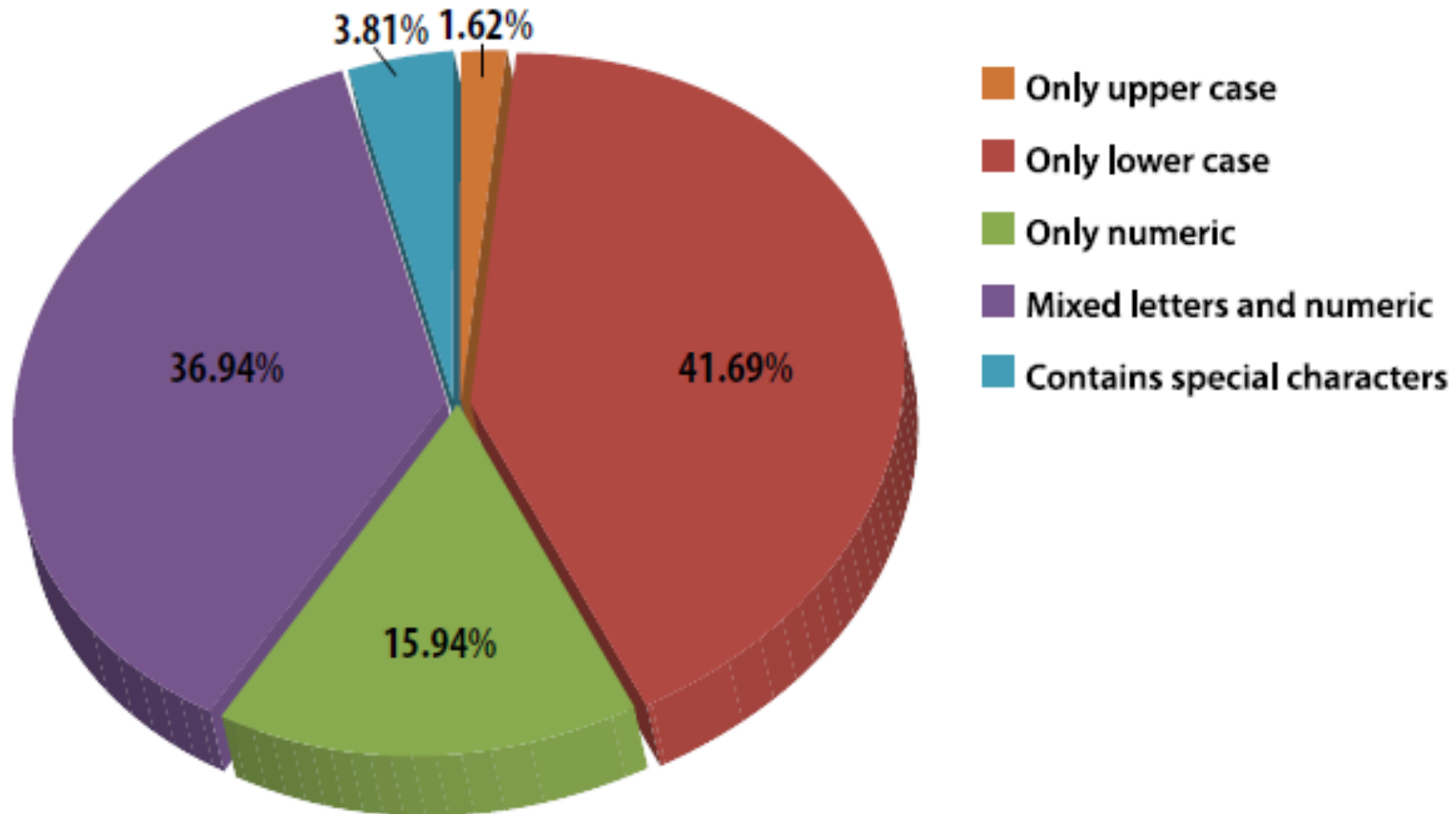
| Rank | Password | Number of Users with Password (absolute) |
|------|----------|--|
| 11 | Nicole | 17168 |
| 12 | Daniel | 16409 |
| 13 | babygirl | 16094 |
| 14 | monkey | 15294 |
| 15 | Jessica | 15162 |
| 16 | Lovely | 14950 |
| 17 | michael | 14898 |
| 18 | Ashley | 14329 |
| 19 | 654321 | 13984 |
| 20 | Qwerty | 13856 |

Quelle: http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Analyse von Passwörtern

- keine Veränderung im Verhalten bei der Passwortvergabe in den letzten 20 Jahren
- 30 % der Passwörter nicht länger als sechs Zeichen
- Allgemein zu schwache Passwörter

Analyse von Passwörtern



Quelle: http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Passwort Recovery mit EWSA

Messwerte von 2009 und 2011

| | CPU | CPU + SSE2 | GPU |
|------|-----|------------|--------|
| 2009 | 350 | 680 | 12 500 |
| 2011 | 500 | 1600 | 35 000 |

Quelle: Michael Hamm; Passwortsicherheit, S.103

Präventionsmaßnahmen

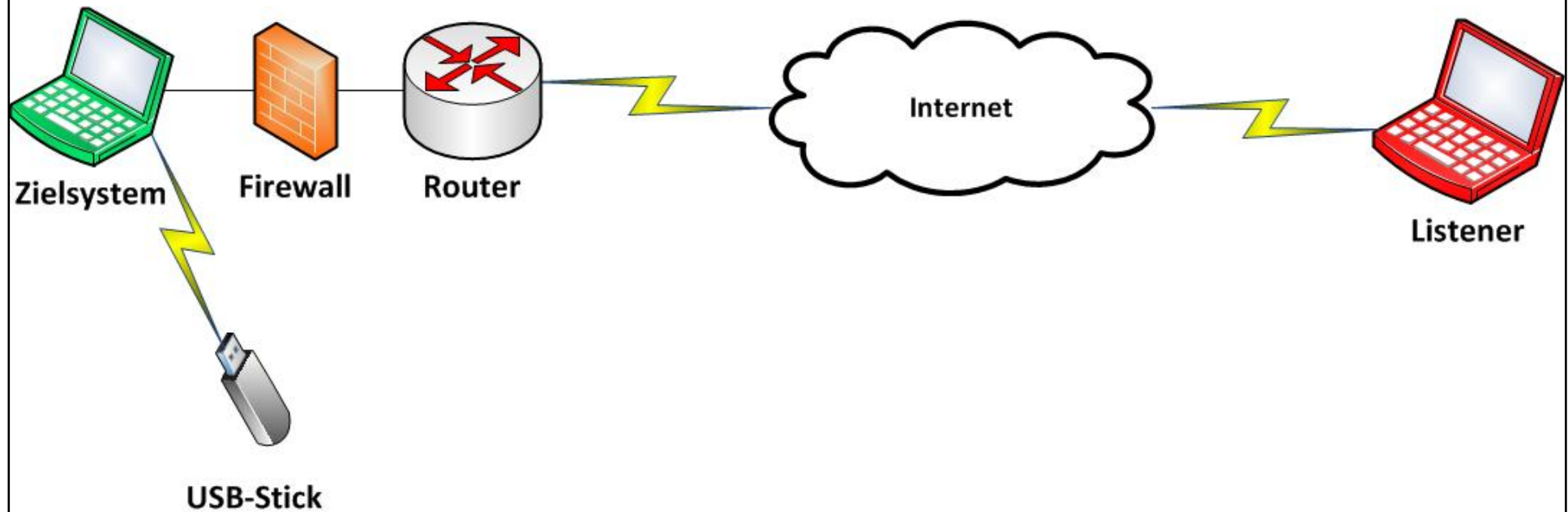
- Starkes Passwort
- Neuester Standard
- In Unternehmen:
 - Ticketsystem zur Autorisierung von Gästen
 - ermöglicht temporären Zugang für Externe

Microsoft Windows Shell LNK Code Execution via USB-Stick

- Schwachstelle bei der Verarbeitung von Short-Cut-Dateien (Exploit)
- Angriff sowohl auf einer manipulierten Webseite als auch von einem Wechselträger möglich
- Betroffene Systeme: Alle Windows Betriebssysteme einschließlich Windows 7, die nicht gepatched sind

Für Windows XP SP2 kein Patch!

Microsoft Windows Shell LNK Code Execution via USB-Stick



Risikopotenzial

- Beliebtes Angriffsszenario unter Hackern
- Allein 2009 185 Millionen Datenträger verkauft
- Laut BSI sichern 45,5% der Unternehmen USB-Schnittstellen nicht ab

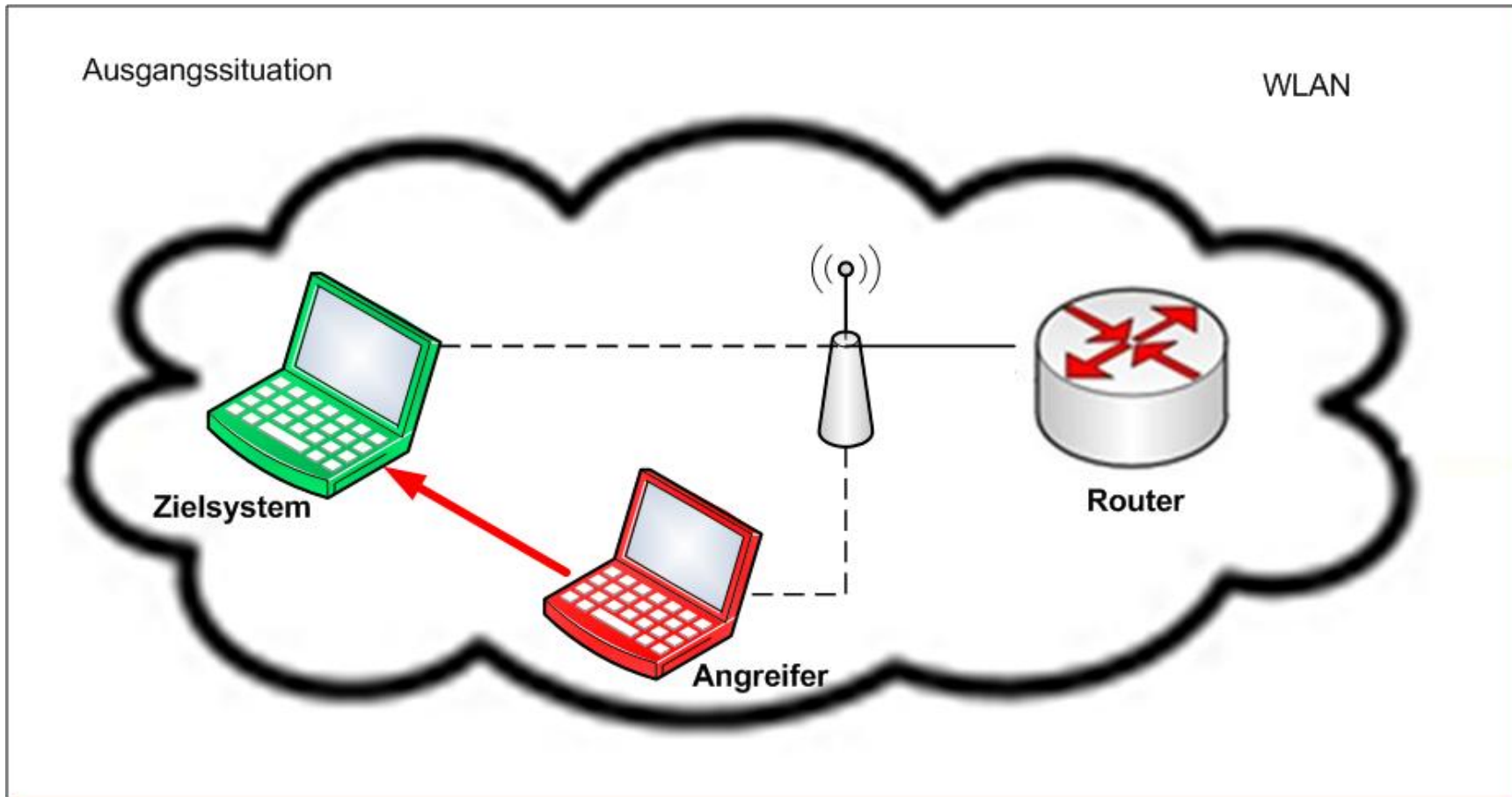
Präventionsmaßnahmen

- Physische oder softwaregesteuerte Kontrollmechanismen
- Sensibilisierung der Mitarbeiter im Umgang mit Wechseldatenträgern
- Vorherige Autorisierung durch IT-Sicherheitspersonal

Microsoft Windows SMB Relay Code Execution

- Remote-Exploit
- Schwachstelle des Microsoft LAN Managers
- dieser beruht größtenteils auf dem Server-Message-Block-Protokoll (SMB)
- SMB ist standardmäßig aktiviert und der Nutzer besitzt typischerweise auch Administratorenrechte

Microsoft Windows SMB Relay Code Execution



Risikopotenzial

- Kaspersky identifizierte 2010 8,5 Millionen unterschiedliche Exploits
- Ziel: Erlangen der lokalen Benutzerrechten (Privatanwender und Kleinunternehmen besonders gefährdet)
- Sicherheitslücke erst nach sieben Jahren geschlossen!

Präventionsmaßnahmen

- unternehmensübergreifendes reaktives Update- und Patchmanagement (Betriebssysteme, Hard- und Software)
- eingeschränkte Benutzerrechte
- Windows 7 standardmäßig mit eingeschränkten Nutzerrechten (Benutzerkontensteuerung)

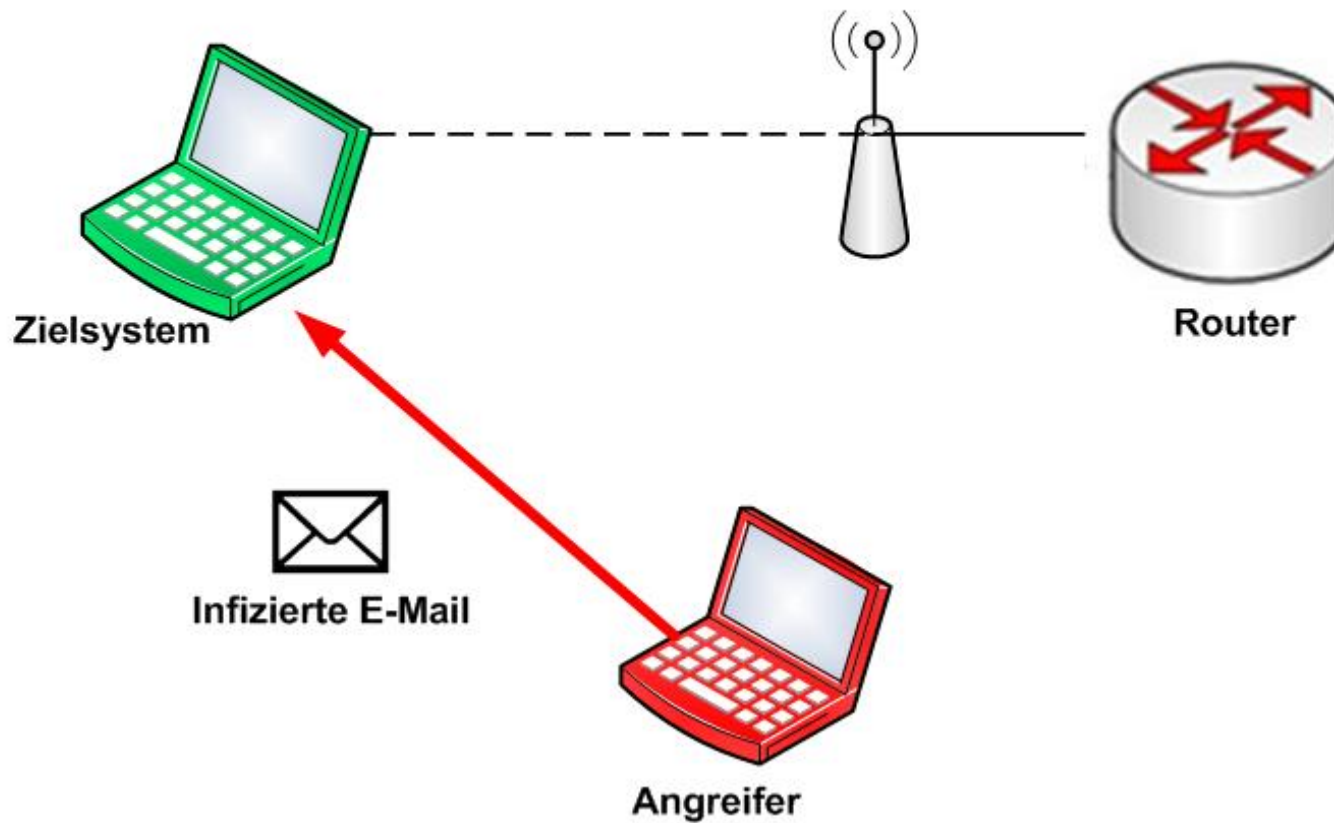
VideoLAN VLC ModPlug

- Local-Exploit
- Generiert eine manipulierte Datei
- Versand der manipulierten Datei per E-Mail
- Nutzt Schwachstelle des VLC Media Players
(Version von April 2011)

VideoLAN VLC ModPlug

Ausgangssituation

WLAN



Risikopotenzial

- Im Jahr 2010 107 Billionen verschickte E-Mails
→ 294 Milliarden pro Tag
- 89,1% aller E-Mails Spam
→ 262 Milliarden pro Tag
- VLC Media Player ca. 500 Millionen mal
runtergeladen

Quellen: <http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/>
<http://www.videolan.org/vlc/stats/downloads.php>

Präventionsmaßnahmen

- Gesunder Menschenverstand
- Aktuelle Antivirensoftware + aktuelle Software (z.B.: VLC Media Player)
- Spamfilter aktivieren
- Dateianhänge kontrollieren

Konsequenzen für die Anwender

- Organisatorische Maßnahmen:
 - Sensibilisierung der Mitarbeiter
 - Sicherheitsbeauftragter mit eigenem Budget
 - BSI-Zertifizierung
 - Frühzeitige Einbindung der IT-Sicherheit in Projekte
 - Balance zwischen Flexibilität und Sicherheit finden

Konsequenzen für die Anwender

- Technische Maßnahmen:
 - Update- und Patchmanagement
 - Monitoring (z.B. IDS)
 - Logging
 - Firewall
 - Virens Scanner
 - Verwendung aktueller Technologien (WPA2, https)

Personal Firewall vs. Netzwerk-Firewall

- Personal Firewall: Programme oder Programmpakete, die das Betriebssystem ergänzen oder erweitern, um den Rechner zu schützen (z. B. Windows Firewall)
- Netzwerk-Firewall: eigenständiges System/ Gerät mit mindestens zwei LAN-Schnittstellen, das die Aufgabe hat, ein gesamtes Netzwerk zu schützen (z. B. Router)

Personal Firewall + Netzwerk-Firewall?

Pro:

- Bei Sicherheitsfehlern in Netzwerkdiensten kann eine Personal Firewall den Fernzugriff auf den Netzwerkdienst einschränken
- Meldungen der Personal Firewall helfen beim Erkennen möglicher Schadsoftware

→ Empfehlung des BSI

Personal Firewall + Netzwerk-Firewall?

Contra:

- Auch Firewallsoftware bietet Hackern Angriffsfläche
- Negative Beeinflussung der gesamten Netzwerkperformance (intern & extern)
- Schwieriges Gleichgewicht zwischen Sicherheit und Komfort (Meldungen etc.)

→ Einsatz unter Experten umstritten

Vielen Dank für Ihre
Aufmerksamkeit!