

Hochsicherheits-Duo SBC und Thin Clients

Roger Klose, rklose@ernw.de

Vorstellung

- ERNW GmbH
- Firmensitz: Heidelberg (kleines Büro in Lissabon)
- wissensorientiert, unabhängig, international tätiger IT-Security Dienstleister
- Aktuell 12 hochspezialisierte Mitarbeiter

- Schwerpunkte:
 - Definition: Policies, IT-Sicherheitshandbücher, Sec-Management*
 - Umsetzung: Implementierung von Sicherheitsmaßnahmen*
 - Kontrolle: Überprüfung von Sicherheitsmaßnahmen (z.B. Pen-Tests / Audits)*
Security-Research

- Typische Kunden:
Banken, Versicherungen, Gesundheitswesen, öffentliche Hand, Konzerne,
Mittelständler mit marktbeherrschender Stellung

Agenda

- Ein „(un)gewöhnlicher“ Angriff auf einen Fat-Client
- Allgemeine Security Prinzipien
- Allgemeine Security Prinzipien bei Thin-Client und SBC im Vergleich zu Fat-Clients
- Compliance bei Thin-Client und SBC im Vergleich zu Fat-Clients
- Thin-Clients mit SBC und PKI – Ein Erfahrungsbericht

Ein (un)gewöhnlicher Angriff?

- Im Wandel der Zeit: Demonstration eines Angriffs mit einem präparierten USB-Stick



Voraussetzungen für das Gelingen des Angriffs...

...sind wie immer – siehe später -;) – eine Kombination von Fehlern:

- Technische Fehler (XP):
 - (per Default aktiviertes) Autoplay
 - Angemeldet als Admin (im privaten Bereich ebenfalls Default)
- Organisatorische Fehler:
 - Mangelnde Security-Awareness
- Fehler im Design:
 - des Betriebssystems (=> anders z. B. bei Windows Vista)



...und ein wichtiger weiterer Faktor:

- ...i. d. Regel sogar eine Voraussetzung für das Gelingen des Angriffs:

Der angegriffene Rechner ist ein **FAT-Client** -;(
)

Mögliche Maßnahmen zur Verhinderung

- **Technisch:**
 - Definition in der GPO
 - Definition der Registry
- **Organisatorisch:**
 - Security-Awareness durchführen
 - Training der Mitarbeiter
- **Design:**
 - Migration auf ein anderes Betriebssystem
 - Migration auf eine andere Plattform

Der kleine (ERNW-) Katechismus von Sicherheitsprinzipien

- Keep it simple
- Patch-Level
- Minimal Machine
- Segregation of Duties
- Least Privilege
- Defense in Depth
- Starke Authentifizierung



Und nun... Gegen welche wurde bei dem Fat-Client verstoßen?

• ...



Vielfältige Einsatzmöglichkeiten von TCs – Klassifizierung:

- **Basic Terminals**

- Sehr sicher, sehr wenig Funktionalität: Locked-down OS im Flash-Speicher, kein lokaler Speicher, kein MS(D)OS, häufig keine Peripherie (z. B. kein USB)
- Einsatz z. B. im Gesundheitswesen

- **Browser Terminals**

- Windows CE inkl. IE, Terminalemulation (etwa ICA-Client), lokaler Speicher meist löscher nach Sitzung /bei Herunterfahren, eingeschränkte /dedizierte Peripherie
- Einsatz z. B. in Call Centern

Vielfältige Einsatzmöglichkeiten von TCs – Klassifizierung:

- **XP Embedded Terminals**

- Volle Win-32-Unterstützung, inkl. IE, JVM, ICA-Client, potentiell sind Windows-Anwendungen lauffähig, meisten umfangreiche Peripherie-Optionen, häufig auch ohne Netzwerkanbindung produktiv als etwas ‚reduziertes‘ Windows
- Einsatz oft als Ersatz für Arbeitsplatz PC mit Office-Anwendungen auf dem TS u. vielfältigen Anschlussmöglichkeiten (Drucker, Scanner, USB-Sticks...-;)

- **Linux Terminals**

- Reduzierter Kernel, Peripherie einbindbar oder nicht einbindbar, ggf. lokale Datenverarbeitung (auch abhängig von TC-Hardware), ggf. auch ohne Netzanbindung produktiv; von reinem Browser-Terminal bis zu dedizierten Applikationen

Zurück zum Demo-Angriff – Security bei Fat- vs. Thin Client

Können die im Vorausgegangenen diskutierten Schwachstelle /Fehler auch bei einem „typischen“ Thin-Client auftauchen?

⇒ Least Privilege?

⇒ Nein, wg. ‚Privilegien-Architektur‘ beim SBC (User ist weder auf dem TC noch auf dem TS Administrator)

⇒ AutoPlay?

⇒ Auf dem TC??

⇒ Auf dem TS (falls ja, ist der Benutzer kein Administrator)

⇒ ‚physische Auffälligkeit‘?

⇒ ... nicht zu unterschätzender Faktor

...und die Gretchenfrage: wie halten Sie´s mit der Compliance?

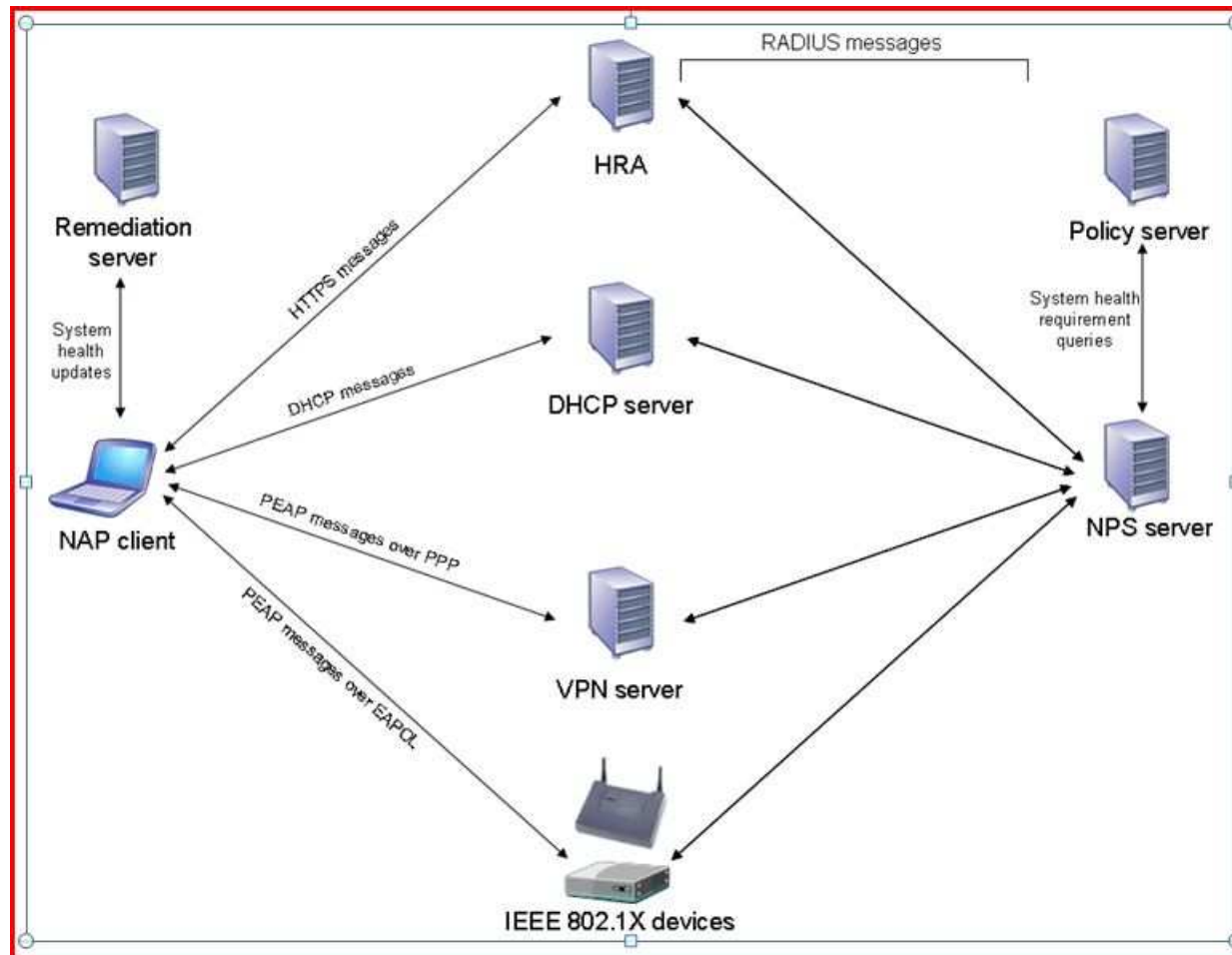
Der Demo-Angriff als ‚Aufhänger‘ für Sicherheit durch Compliance: Wie ließe sich das Sicherheits- oder Compliance-Problem bei Fat-Clients bewerkstelligen?

- **Organisatorisch** durch Policies (z. B. ein Verbot von USB-Sticks)
- **Technisch** teilweise (erst bei Vista vollständig) durch die GPOs, ggf. Dritthersteller-Software
 - Betriebssystem ‚kleiner gleich‘ XP: ggf. durch BIOS
 - Betriebssystem neuer als XP: durch GPO

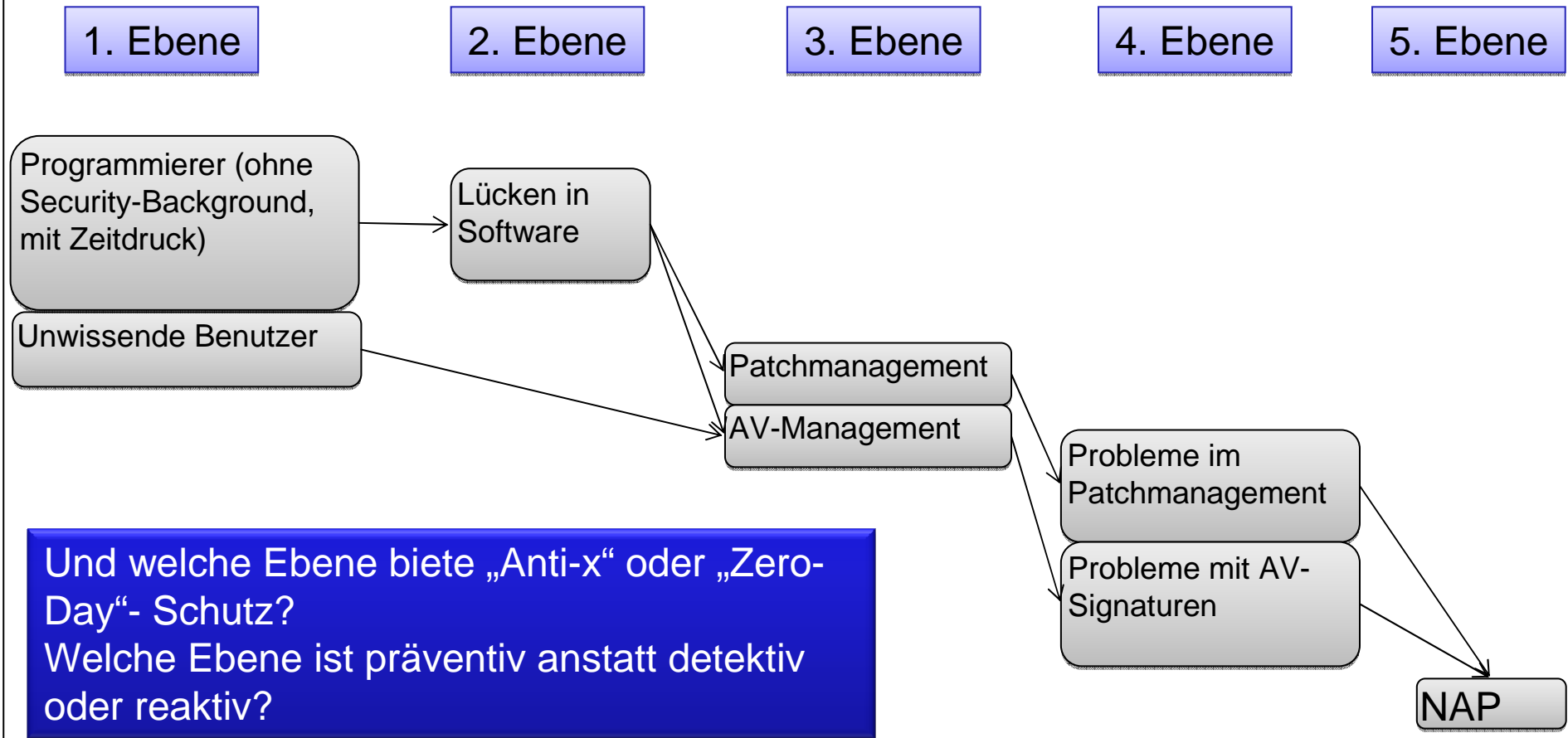
...und die Gretchenfrage: wie halten Sie´s mit der Compliance?

- Mit einem umfassenden Access Control-Framework:
 - NAP (Microsoft)
 - NAC (Cisco)
 - ...
- Aber:
- Darunter leidet die Betreibbarkeit => Verstoß gegen das Gebot von „Keep it simple“
- Oder eine Lösung über ein zur Client-Server-Architektur alternatives **Design**...-
;)
- Aber noch einmal zurück zur Lösungsfindung bei der Client-Server-Architektur... (nächste Folie)

Komplex: (Security-) Compliance für Fat-Clients mit MS NAP



Verwaltung eines Frameworks wie NAP: Where do you want to spend the \$\$\$?



...und wie müssen Sie´s mit dem Patchmanagement halten?

Vulnerabilities in aktuellen Fat- und TC-Versionen von Windows XP:

- Lt. www.securityfocus.com

- XP-Embedded (SP1) = 65 Schwachstellen
- XP-Professional (SP2) = 219 Schwachstellen

- Darüber hinaus:

- schlankes OS = wenige Pakete/Programme
- Per Default ein unprivilegierter Benutzer



Compliance SBC gegenüber den *Sicherheitsprinzipien*?

ERNW Security-Katechismus	SBC
Minimal Machine	+++ (by Design)
Least Privilege	++ (by Design)
Patchen	+/-
Segregation of Duties	+++
Defense in Depth	+
Keep it Simple	+
Starke Authentifizierung	+/-

Hochsicherheits-Duo SBC + Thin Clients mit PKI

Titel eines mit einer Bank durchgeführten Projekts:

„Evaluierung von Roaming-Funktionalitäten zusammen mit Smartcard-Logon (PKI) in einer Active Directory-Umgebung mit Presentation Server, Thin- und Fat Clients“

- Ziele des erfolgreich abgeschlossenen Projekts (das mittlerweile großflächig umgesetzt wird):
- Starke Authentifizierung per Smart Card
→ (Security / Compliance / Revisionsicherheit)
- Single-Sign-On → Usability
- Roamingfähigkeit → Produktivität
- Reduktion der HW Kosten → Wirtschaftlichkeit)

Hochsicherheits-Duo SBC + Thin Clients mit PKI

- Es geht also nicht nur um SBC mit TCs – das ist gewissermaßen schon die Voraussetzung – sondern zusätzlich um Smartcard-Logon und Roaming-Funktionalität (im Projekt sogar zwischen Thin- und Fat-Clients)
- Begriffsklärung: „Smartcard-basiertes Roaming“
- Vereinfacht:
Karte bei Rechner A ziehen (Sitzung wird Unterbrochen)
Karte bei Rechner B einführen (Sitzung läuft weiter)
der Workspace des Users bleibt wie es ist

= User und Workspace können „roamen“

Hochsicherheits-Duo SBC + Thin Clients mit PKI

Von der Bank eingesetzte Hardware und Betriebssysteme

Rechner	Bemerkung	Betriebssystem
IBM M50	Basis VMware	Windows XP Prof SP2
IBM M50	Domain Controller VMware	Windows Server 2003 SP1
IBM M50	Citrix Terminalserver PS 4.0 VMware	Windows Server 2003 SP1
IBM M50	Citrix Metaframe FR3 SP3 VMware	Windows Server 2003 SP1
IBM S52	Windows2000 SP4 Fat Client	Windows 2000 Prof SP4
IBM S52	Windows XP SP2 Fat Client	Windows XP Prof SP2
Igel 3600 XP Compact	Windows XP embedded Thin Client	Windows XPe
Igel 3600 XP Compact	Windows XP embedded Thin Client	Windows XPe
IBM T22	Windows XP SP2 Fat Client Laptop	Windows XP Prof SP2
Igel 3200 CE Compact	Windows CE Thin Client	Windows Mobile 5.0
Igel 3200 LX Compact	Linux Thin Client	Linux

Thin-Client / SBC in der Zukunft?

- Viele Unternehmen und Behörden stellen auf Thin-Clients und SBC um
- Unterstützung durch viele (immer mehr) Hersteller gewährleistet
- Compliance- und Sicherheitsaspekte im Vergleich zu traditionellen Fat-Clients sind „by Design“ implementiert
- Da Compliance- und Sicherheitsaspekte eher zunehmen, ist man für die Zukunft sowohl was die technischen Anforderungen betreffen wird als auch was Manageability und Kosten betrifft sehr gut gerüstet

Fazit

- SBC mit Thin Clients = is good and smart
- Management: bei konsequenter Umstellung vereinfacht (man beachte dabei auch die Mehrheit der Benutzer, die komplexe Fat-Clients weder verstehen können noch wollen)
- Compliance: stark vereinfacht
- Security: bei konsequenter Umsetzung besser (vgl. den ERNW Security-Katechismus)

Fazit

- Die Sicherheit auf den (Terminal-) Servern spielt eine (noch) wichtigere Rolle
- Gruppenrichtlinien müssen in Windows-Umgebungen beherrscht werden
- (Web-) Applikationen auf den Terminal-Servern müssen auf Sicherheitslücken überprüft werden

Fazit

Dennoch:

- Interne Angreifer müssen im Auge behalten werden (siehe den Demo-Angriff)

Und:

- Angriffsmöglichkeiten sollten professionell getestet werden (z. B. durch ERNW -;))



Fragen? Und Antworten...

22. Januar 2008 in München
„Desktop-Virtualisierung und Thin Client Computing“

www.troopers08.org

CONTACT | SPONSORS

TROOPERS 08

SIGN UP

get skilled,
or get owned

HOME | SPEAKERS | AGENDA | VENUE | SIGN UP | DOWNLOAD | SPONSORS

Troopers 08 - get skilled or get owned

Today, information is power - and sharing information is the multiplication of power. We experience an era where connectivity is not a feature anymore - it's just there. Technologically & socially everyone and everything is connected to anything & anyone, anytime.

Given this, the ability to control who may collect, store, process and digest information is one of the key assets of every organisational unit, may it be .gov, .mil, .com, .org or a single private person.

But the benefits of today's technologies also bring a wide range of attack vectors right into the core of our networks. The everchanging attack strategies and methodologies make „traditional“ network-security concepts obsolete.



WHO HOSTS THIS CON AND WHY?

ditis
The Security Company

FAQs

HOSTED BY
ERNW
Living Security

22. Januar 2008 in München
„Desktop-Virtualisierung und Thin Client Computing“

ERNW
Wir leben IT-Security

konradin
EVENTS

27