DECOIT

D·A·CH Security 2008

Trusted Network Connect

sicherer Zugang ins Unternehmensnetz

Dr.-Ing. Kai-Oliver Detken
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Inhalt

- State-of-the-Art
- Anforderungen an mobile Endgeräte
- Anwendungsfälle
- Umsetzung im SIMOIT-Projekt
- Fazit und Ausblick

State-of-the-Art (1)

- Zunehmende Vernetzung und verteilte Systeme
- Stark zunehmende Gefahr durch Malware (insbesondere Trojaner, Viren und Rootkit-Werkzeuge)
- Die Absicherung von Netzwerkzugriffen erfolgt meist nur über eine reine Benutzerauthentifizierung
- Es findet keine Integritätsprüfung der verwendeten Rechnersysteme statt und damit keine Unterscheidung zwischen vertrauenswürdigen/nicht vertrauenswürdigen Rechnersystemen
- Immer mehr mobile Endgeräte werden im normalen Unternehmensalltag ungeschützt verwendet

State-of-the-Art (2)

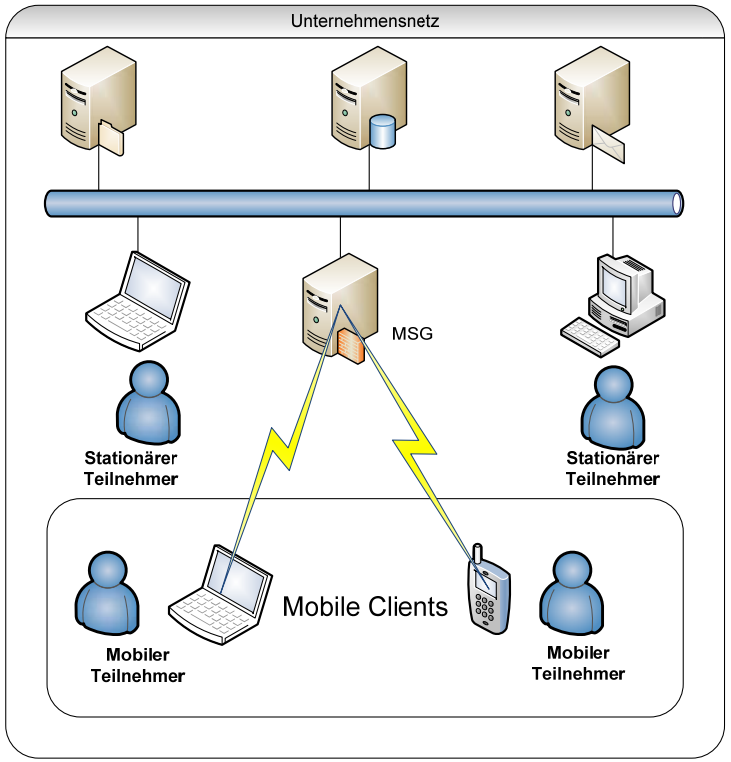
- Fazit:
  - Das Netzwerk ist durch Malware und Eindringlinge gefährdet
  - Netze besitzen keine Vertrauenswürdigkeit
  - Es ist kein ausreichend vertrauenswürdiger Datenaustausch möglich

Anforderungen an mobile Endgeräte

- **Remote Installation:** hierzu ist Serverseitig eine Softwareverteilungslösung erforderlich, die in diesem Fall die Software auch über die Unternehmensgrenzen hinweg transportieren muss. Ein Problem stellt allerdings die Datenmenge bzw. die benötige Downloadzeit bei einer schmalbandigen Verbindung des Endgerätes dar.
- **Patchlevel:** Damit sich ein mobiles Endgerät erfolgreich am Hauptsitz anmelden und auch die Berechtigung besitzt, das interne Netz zu nutzen, muss ein bestimmter Patchlevel der verschiedenen Anwendungen vorhanden sein. Das Bereitstellen von Patches kann von einer Softwareverteilungslösung, analog zur Remote Installation vorgenommen werden. Je nach Strenge der Security Policys kann normal gearbeitet werden, oder man befindet sich in einer Quarantänezone.
- **Quarantänezone:** Eine Quarantänezone ist ein vom Unternehmensnetz abgeschlossener Bereich in dem sich eine Softwareverteilungslösung befindet. Die Softwareverteilung hält alle aktuellen Patches von Anwendungen und sicherheitsrelevanten Diensten wie Anti-Viren- und Anti-Spyware-Definitionen. Endgeräte die sich bei der Anmeldung ans Netz in einem sicherheitskritischen Zustand befinden, bekommen nur Zugang zur Quarantänezone

Anwendungsfälle

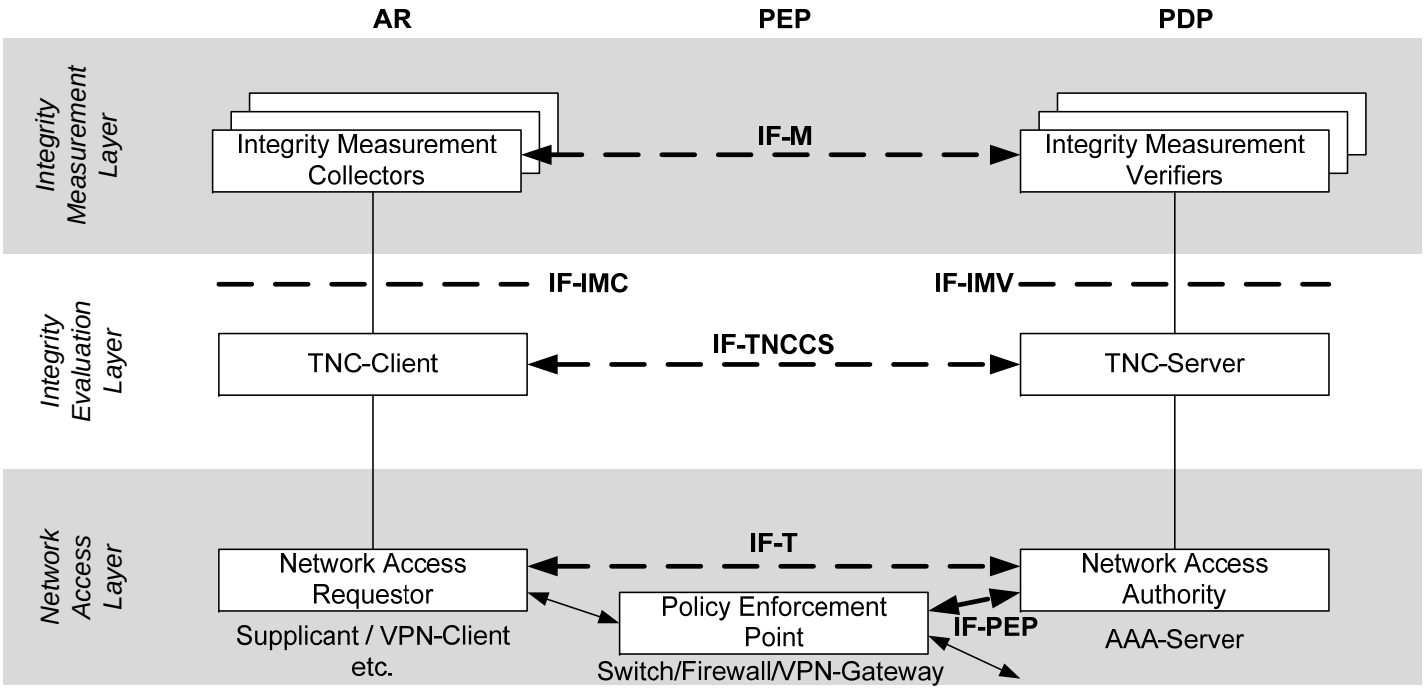
- Nutzung mobiler Endgeräte in der Zentrale
- Remote-Zugriff ins Unternehmensnetz
- Remote-Zugriff auf abgelegene Standorte
- Remote-Zugriff über das Unternehmensnetz auf Kundennetze



Der TNC-Ansatz

- Mit der Trusted Network Connect-Spezifikation (TNC) entwickelt die Trusted Computing Group (TCG) einen eigenen NAC-Ansatz
- Die Entwicklung findet durch die Trusted Network Connect-Subgroup mit über 75 vertretenen Firmen statt und liegt aktuell (Mai 2007) in der Version 1.2 vor
- Ziel ist die Entwicklung einer offenen, herstellerunabhängigen Spezifikation zur Überprüfung der Endpunkt-Integrität
- TNC baut auf vorhandene Technologien auf, wodurch eine einfachere Integration in bestehende Infrastrukturen möglich ist
  - Netzwerkzugriff: 802.1x, VPN, PPP
  - Nachrichtentransport: EAP, TLS & HTTPS
  - Authentifizierung: Radius Server, Diameter

TNC-Architektur



TNC-Basisfunktionalität

- Überprüfung der Vertrauenswürdigkeit:
  - Richtlinien-abhängige Zugriffssteuerung für Netzwerke
  - Integritätsprüfung: Messen des Systemzustands (Konfiguration der Endgeräte) und Überprüfung dieser Zustände gemäß Richtlinien (Assessment-Phase)
  - Isolation von potentiell gefährlichen Rechnersystemen bei Nichterfüllung der Richtlinien (Isolation-Phase)
  - Wiedereingliederung nach Wiederherstellung der Integrität (Remediation-Phase)
  - Erweiterter Integritätscheck möglich (z.B. Binden von Zugangsdaten an ein bestimmtes Rechnersystem, Signierung von Messwerten)

TNC-Alternativen

- Microsoft NAP (proprietär und Softwareabhängig): ab 2008 verfügbar
- Cisco NAC (proprietär und Hardware-/Softwareabhängig): verfügbar. Benötigt die Hardware von Cisco.
- Checkpoint Interspect-Appliance (proprietär und Softwareabhängig): verfügbar. Benötigt Checkpoint-NG-Software.
- Weitere Ansätze (proprietär): teilweise verfügbar (u.a. von McAfee, F-Secure)

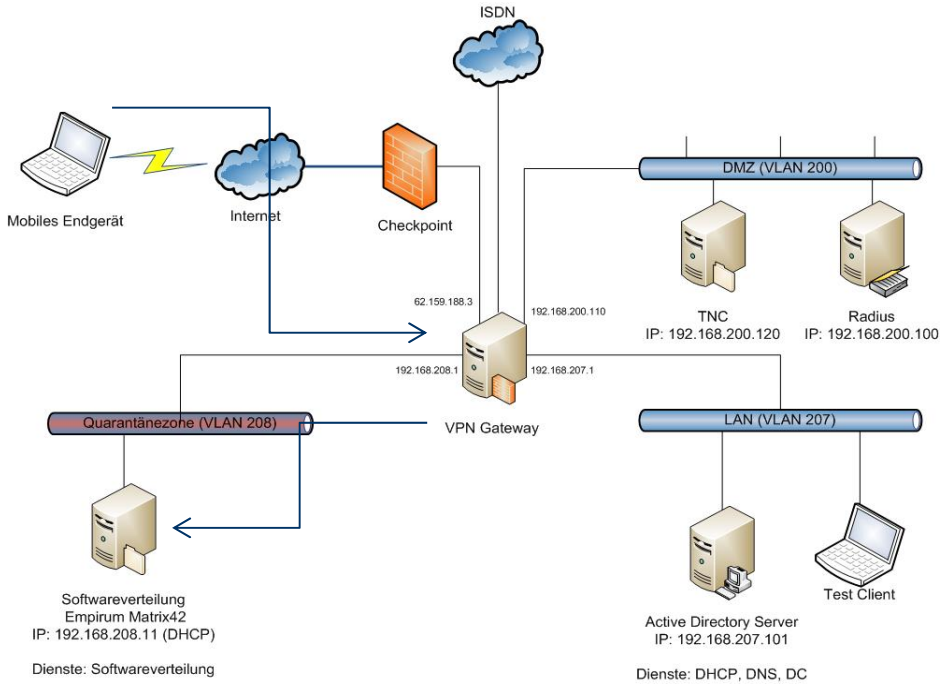
Zielsetzung des Projekts (w

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- SIMOIT = SIcherer Zugriff von MObilen Mitarbeitern auf die IT-Infrastruktur von mittelständisch geprägten Unternehmen
  - Es sollen Konzepte und auch technische Lösungen entwickelt werden, um die neu entstehenden mobilen Anwendungen und mobilen IT-Infrastrukturen von mittelständisch geprägten Unternehmen auf jetzige und zukünftige IT-Sicherheitsanforderungen vorzubereiten
  - Ziel war es, eine auf Standards basierende mobile IT-Sicherheitslösung herstellerneutral für den Bereich hochmobiler Mitarbeiter zu entwickeln

Aufbau des Nutzertests - Phase 1

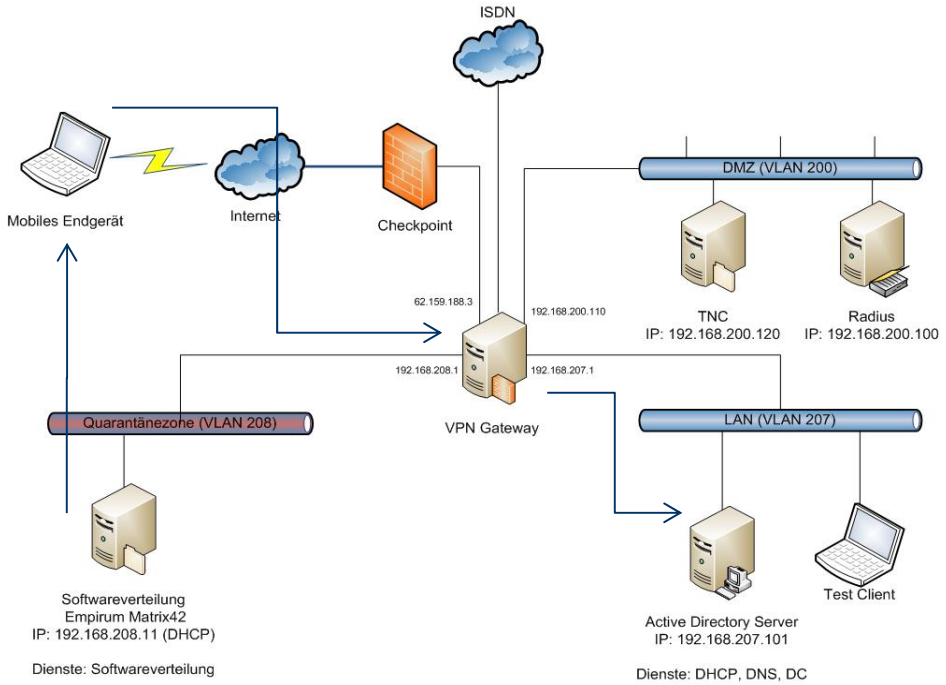
- Szenario: Mobiler Mitarbeiter wählt sich mit **veraltetem System** ein
- Die Benutzerauthentisierung ist erfolgreich
- Auf Basis von Daten der Softwareverteilung wird das System in allerdings in die **Quarantäne** verschoben
- Der Mitarbeiter hat nur Zugriff auf Software-Updates



SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

Aufbau des Nutzertests - Phase 2

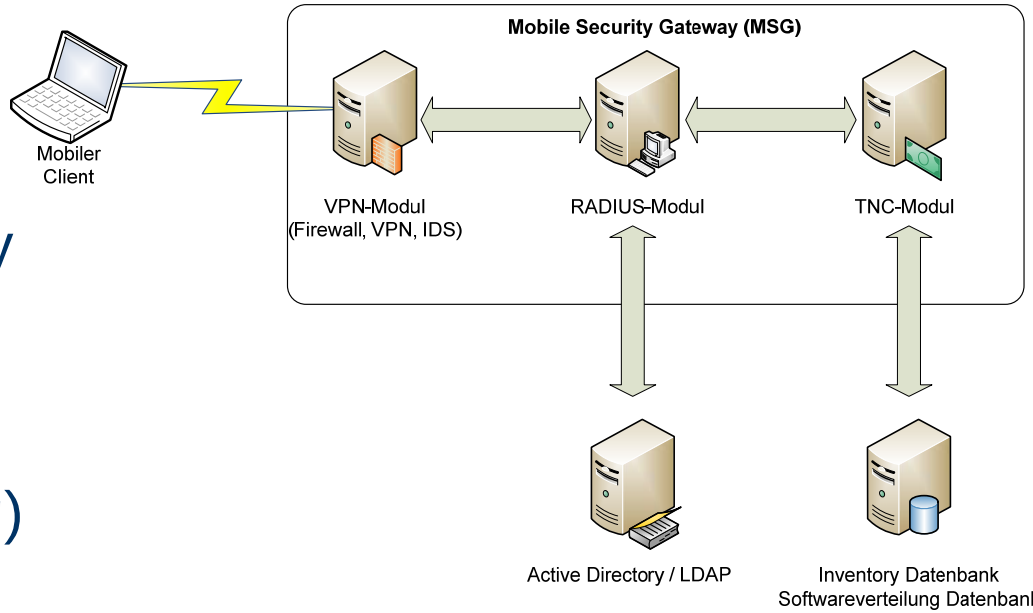
- Installation von kritischen Softwarepaketen
- Abbau des IPsec-Tunnels
- Wiedereinwahl mit aktuellem System
- Der Mitarbeiter erhält **vollen Zugriff**



SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

SIMOIT-Implementierung (1)

- VPN-Modul
- Radius-Modul mit TNC-Modul
- MS Active Directory (AD)
- Inventory-Datenbank (Softwareverteilung)



SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

SIMOIT-Implementierung (2)

- VPN
  - OpenSWAN
  - xl2tpd
  - pppd
  - radiusclient
- Firewall
  - iptables
- IDS
  - Snort
  - ACIDBASE
- freeRADIUS
  - LDAP-Autorisierung
  - Authentisierung (Samba / Winbind): User und Passwort werden gegen AD geprüft
- freeRADIUS-Module
  - LDAP
  - MS-Chap
  - TNC

SIMOIT-Implementierung (3)

- Policy-Decision-Point (TNC-Server)
  - TNC-Server implementiert als freeRADIUS-Modul
  - Verwendetes TNC-Framework: libtnc
  - Inventory-Koppelung: TNC-Integrity-Measurement-Validator
    - Modul, das sich über TNC-IF-IMV in TNC-Server integriert
    - Definierte Schnittstelle (HTTPS) zum Inventory-Modul

Erreichte Ziele von SIMOIT

- Sichere Authentifizierung des Benutzers und der vorhandenen mobilen Hardware
- Quarantäneschutzbereich für nicht konforme Endgeräte zum Aktualisieren der Software
- Serverseitige Entwicklung, wodurch mobile Endgeräte unterschiedlicher Art eingebunden werden können
- Modulare Entwicklung (VPN, Firewall, IDS, RADIUS/802.1x, TNC, LDAP, VoIP), wodurch auch andere Hersteller einbezogen werden können
- Unterstützung diverser Standards und Schnittstellen
- VoIP-Nutzung der vorhandenen sicheren Verbindung
- Auswahl unterschiedlicher Sicherheitsprofile
- Netzüberwachungswerkzeuge überwachen kontinuierlich den Netzverkehr

Ausblick und Fazit (1)

- Administration
  - Erhöhter Aufwand bei Verwendung unterschiedlicher Hard- und Softwarelösungen (heterogenes Netz)
  - Jede einzelne Konfiguration muss durch Richtlinien abgedeckt werden
  - Gefahr zu restriktiver Richtlinien
  - Mitarbeit der Hardware-/Softwarehersteller nötig
- Sicherheit
  - Bei Agenten-basierten Systemen (Client/Server) besteht die Gefahr gezielter Angriffe zur Veränderung von Messwerten
  - TNC bietet durch offene Standards eine mögliche Integration in andere Plattformen

Ausblick und Fazit (2)

- Standardisierung
  - Alle bisherigen Lösungen sind inkompatibel zueinander
  - Erste Bestrebungen der Standardisierung durch die IETF
    - Network Endpoint Assessment (NEA) Working Group
    - Bis jetzt sind nur Drafts vorhanden
    - Mitglieder sind u.a. Cisco und Intel
  - Eine (offene) Standardisierung ermöglicht auch eine einfachere Portierung auf neue Plattformen (z.B. Sicherheitsplattformen)
  - „Trusted Computing“ bietet aus Sicht der Bundesregierung einen wesentlichen Schritt zur Erreichung der IT-Sicherheitsziele, wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität

Danke für Ihre Aufmerksamkeit

SIMOIT URL:
http://www.simoit.de

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies