Workshop: Mobile Sicherheit

SIMOIT: *Sichere Zugriff von Mobilen Mitarbeitern auf die IT-Infrastruktur von mittelständisch geprägten Unternehmen*

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

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

Consultancy & Internet Technologies

Portfolio der DECOIT GmbH

- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Entwicklung von Internet-Projekten
- Schaffung innovativer eigener **Produkte**
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen

Agenda

- Netzwerksicherheit: Stand heute
- Ziel und Aufgabe des SIMOIT-Projekts
- RADIUS und 802.1X
- Der TNC-Ansatz – die Quarantänezone
- Marktbetrachtung
- Ausblick und Fazit
- Zusammenfassung

Netzwerksicherheit: Stand heute (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

Netzwerksicherheit: Stand heute (2)

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

Sicherheitsbeispiel

- VPN-Verbindung zwischen einem Außenstandort und einer Firmenzentrale
  - *Kein* Schutz vor Angriffen von einem mit Malware infiziertem Rechner, weil keine Integritätsprüfung der Geräte ermöglicht wird
  - *Kein* Schutz vor gestohlenen Zugangsdaten des VPN-Clients, weil keine Identität des Geräts festgestellt werden kann

Das SIMOIT-Projekt

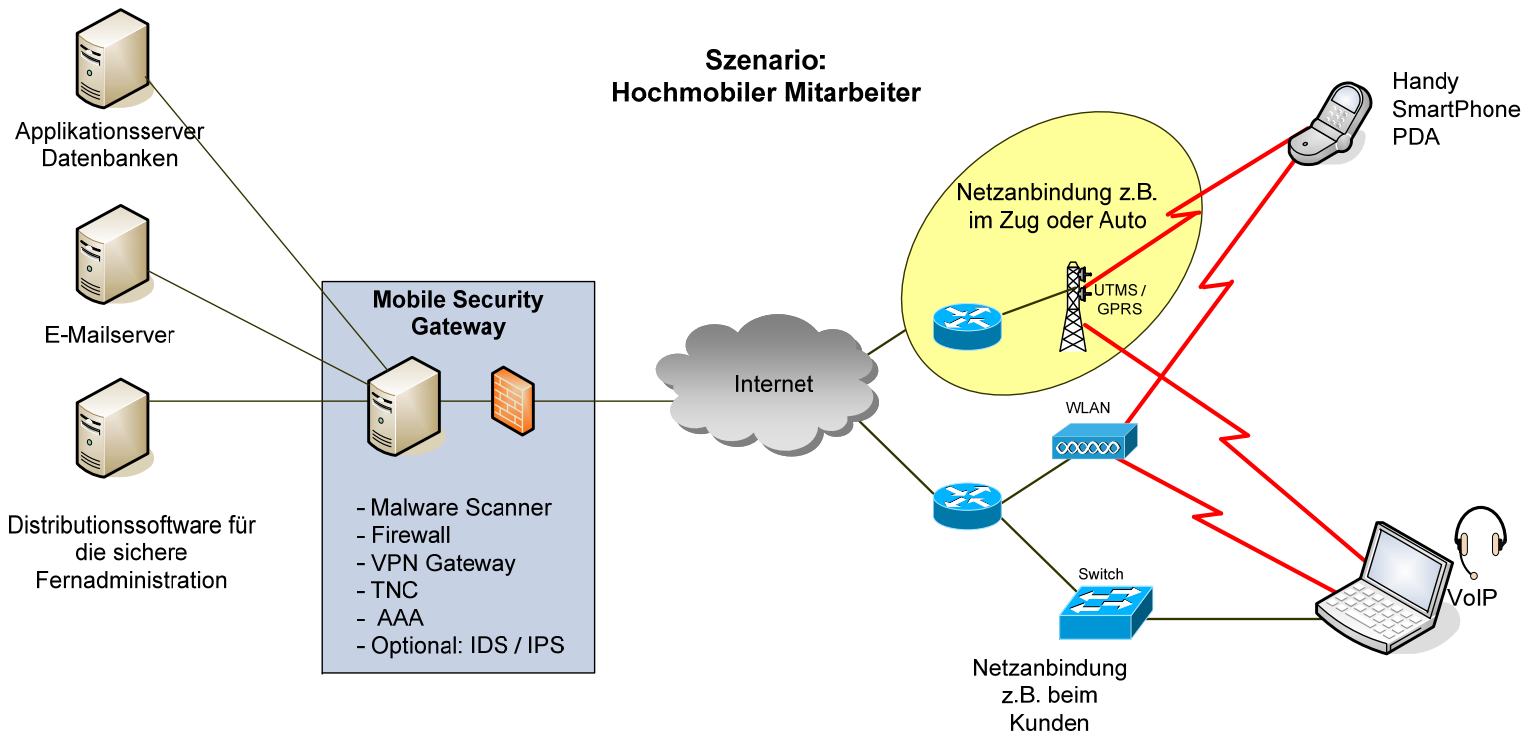
SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- 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 ist es, eine auf Standards basierende mobile IT-Sicherheitslösung herstellerunabhängig für den Bereich hochmobiler Mitarbeiter zu entwickeln

Eigene Webseite: www.simoit.de

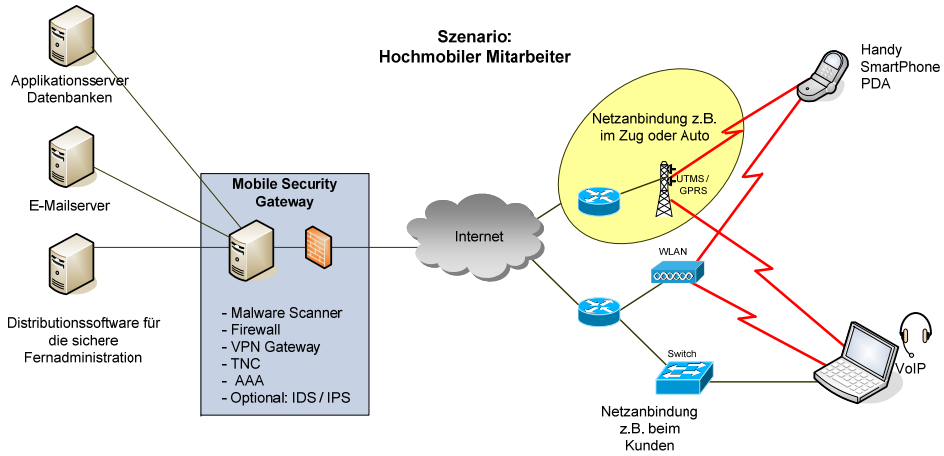
- Programm: InnoVision2010 von Bremen
- Partner:
  - TZI – Uni Bremen
  - IIA – HS Bremen
  - DECOIT GmbH
  - ThyssenKrupp Krause GmbH (Pilot)
  - Pan Dacom Networking AG (Kooperation)
- Laufzeit: 12 Monate
- Aktuellen Termine und Arbeiten werden veröffentlicht: www.simoit.de

Anwendungsszenario eines mobilen Mitarbeiters



Aspekte der mobilen Sicherheit

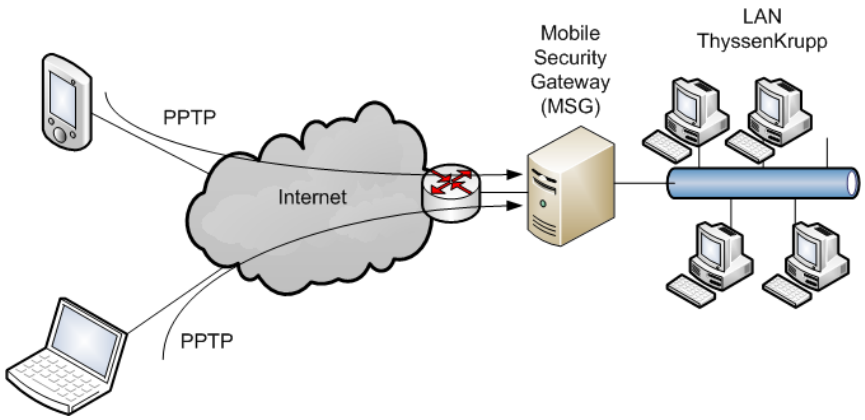
- Zentrale Fernadministration von Netzen mobiler Endgeräte
- Identität durch starke Authentisierungsmethoden
- Absicherung der mobilen Kommunikation durch starke Verschlüsselung
- Absicherung des entfernten (remote) Zugriffs auf mobile Endgeräte
- Datenverschlüsselung
- Firewall-, Viren- und allgemein Malwareschutz-Funktionalität
- Trusted Network Connect (TNC) Funktionalität
- Herstellerunabhängigkeit und modularer Aufbau



Globales Szenario

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- Arbeitsschwerpunkte:
  - Softwareverteilung
  - TNC-Anbindung
  - Administrationsoberfläche
- Mobile Security Gateway (MSG)
  - TNC (Trusted Network Connect) Erweiterung
  - Wert auf Herstellerneutralität legen (Offenheit/Modularität)
- Mobile Endgeräte
  - PDAs (Windows Mobile mit .NET Framework, Symbian OS)
  - Laptops (Windows XP, Vista)



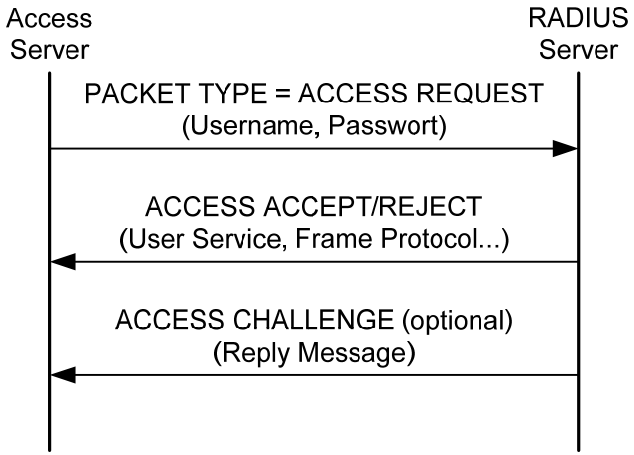
Notwendige Dienste des MSG-Servers

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- Festlegung der SIMOIT-Plattform:
  - Betriebssystem: Debian Linux Plattform, inkl. Samba
  - Verzeichnisdienst: OpenLDAP mit AD-Anbindungsmöglichkeit
  - RADIUS-Dienst zur Authentifizierung: FreeRADIUS
  - Firewall-Funktionalität: iptables
  - VPN-Funktionalität: IPsec/IKE mittels Openswan
  - SSL Root CA und Server/Client-Zertifikate

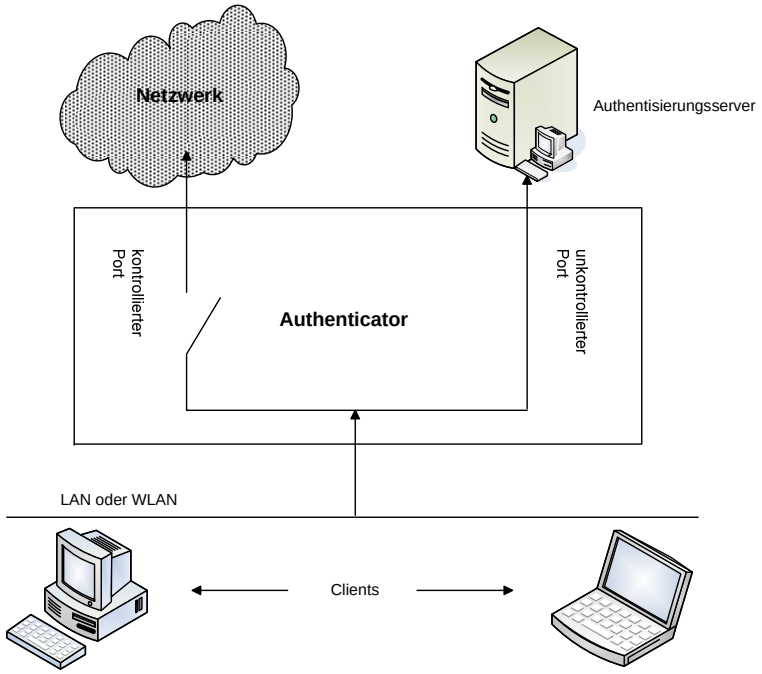
RADIUS-Server

- Authentisierungs- und Autorisierungsprotokoll für Zugangsserver
- Internet-Standard nach RFC-2865
- RADIUS ist ein Client-Server-Protokoll
- RADIUS-Server empfängt alle Verbindungsanforderungen, authentisiert die Benutzer und sendet die notwendigen Konfigurationsinformationen an den Client
- RADIUS verwaltet folgende Informationen:
  - Benutzerinformationen für die Authentisierung
  - Technische Informationen für die Kommunikation zwischen Router und Client (Protokolle, IP-Adressen, Telefonnummern, Time-outs, Routen)
- Es werden diverse Authentisierungsprotokolle unterstützt: PAP, CHAP, MS-CHAP, EAP-MD5, EAP-GTC, EAP-TLS, EAP-TTLS, PEAPv0, LEAP, EAP-SIM, Digest



802.1X

- 802.1X ist eine Port-basierte Zugangssteuerungsmethode, die Authentisierung auf höheren Ebenen erlaubt, um direkt zwischen Client und Authentisierungsserver zu wirken
- 802.1X besteht aus:
  - Der **Supplicant** ist eine Software-Komponente im Client-System, welche einem Netzwerkzugang anfordert.
  - Der **Authenticator** ist das Gerät, welches den Netzwerkzugang sperrt oder freigibt und eine Schnittstelle für die Authentifizierung anbietet. Normalerweise wird die Rolle des Authenticators von einem Access Point oder Access Switch übernommen.
  - Der **Authentication Server** ist das Gerät, welches den eigentlichen Authentifizierungsdienst bereitstellt. Der Authentication Server ist typischerweise ein RADIUS-Server.



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

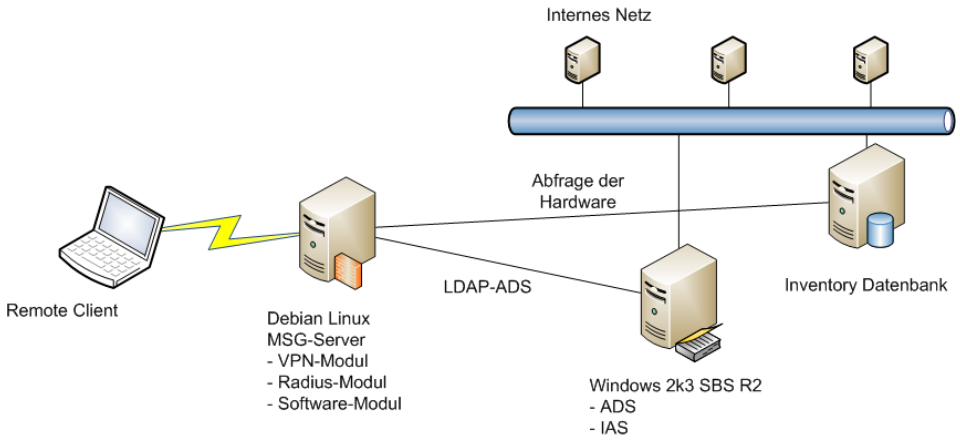
TNC-Basisfunktionalität

- 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)

Prototyp von SIMOIT

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- Mobiler Client baut IPsec-Tunnel zum MSG auf
- MSG fragt Authentifizierungsinfos ab
- Client wird abgewiesen (Quarantänezone) oder zugelassen
- Benutzer-Datenbank und Inventory Infos werden mit MSG synchronisiert
- Weitere RAS-Server können mit einbezogen werden



Marktbetrachtung

- Alternativen
  - Microsoft NAP (proprietär und Softwareabhängig): voraussichtlich Anfang 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): teils verfügbar (u.a. von McAfee, Juniper)

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)

Zusamenfassung

- Vorhandene VPN-Lösungen sind nicht ausreichend für vertrauenswürdige Netzwerkverbindungen
- Mit einer Integritätsprüfung werden vertrauenswürdige Netzwerkverbindungen möglich
- Vorhandene Lösungen sind nicht kompatibel zueinander
- Standardisierungsbedarf ist vorhanden
- Das TNC Framework ist ein offener Lösungsansatz; es fehlt hier aber noch an abschließenden Standards
- SIMOIT-Projekt greift TNC auf und wird die Entwicklung auch weiterhin verfolgen
- Mobile Endgeräte müssen in das Sicherheitskonzept eines Unternehmens einbezogen werden!

Ende

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

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies