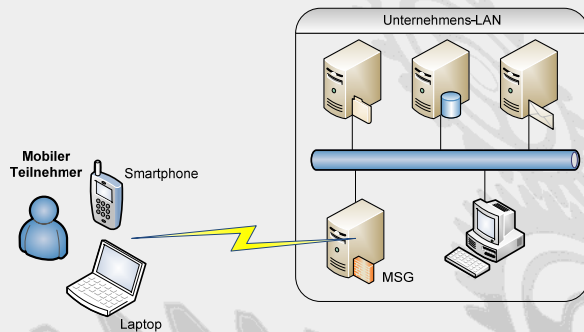


Mobile Endgeräte (Smartphones, Handys, PDAs) finden eine immer weitere Verbreitung. Zunehmend werden auch sicherheitskritische Geschäftsprozesse über mobile Endgeräte (mBusiness, mCommerce) abgewickelt und sensible Daten auf den Endgeräten verwaltet. Mobile Endgeräte werden zudem verstärkt in Unternehmensnetze integriert. Mit der steigender Funktionalität mobiler Endgeräte wächst auf der anderen Seite auch das Risiko von Sicherheitsproblemen. Es gibt zwar verschiedene Sicherheitslösungen im Bereich mobiler Anwendungen und Netze; viele dieser Lösungen sind aber proprietär und behandeln häufig nur einen bestimmten Sicherheitsaspekt (Verschlüsselungssoftware, Virenschutz, mobiles VPN). Oftmals fehlen auch Mechanismen, um eine zentrale und sichere Distribution von Anwendungen und Sicherheitsrichtlinien in Netzen mobiler Endgeräte zu ermöglichen.



Um diese Problematik zu entschärfen, wurde das Projekt SIMOIT (www.simoit.de) von den Firmen Technologie-Zentrum Informatik (TZI) an der Universität Bremen, Institut für Informatik und Automation (IIA) der Hochschule Bremen und DECOIT GmbH ins Leben gerufen. Als Pilotpartner fungiert die ThyssenKrupp Krause GmbH. Ziel des SIMOIT-Projektes ist es, eine universelle, einfach nutzbare Sicherheitsplattform zu entwickeln, die in heterogener Umgebung flexibel und sicher einsetzbar ist. Dazu wurde der Ansatz des Trusted Network Connect (TNC) einbezogen und konsequent umgesetzt. Die TNC-Spezifikation der IETF ist ein herstellernerutraler Standard, der offene und flexible Lösungen ermöglicht, ohne von einem Hersteller abhängig zu sein. Zusätzlich wurde im Projekt SIMOIT eine modulare Plattform geschaffen, die Schnittstellen zu bestehenden Herstellerlösungen beinhaltet. So kann das SIMOIT-Produkt des „Mobile Server Gateways“ (MSG) einfach in bestehende Infrastrukturen eingebettet werden.

Das MSG besitzt folgende Hauptmerkmale:

1. Sichere Authentifizierung des Benutzers und der vorhandenen mobilen Hardware

2. Quarantäneschutzbereich für nicht konforme Endgeräte zum Aktualisieren der Software
3. Serverseitige Entwicklung, wodurch mobile Endgeräte unterschiedlicher Art eingebunden werden können
4. Modulare Entwicklung (VPN, Firewall, IDS, RADIUS/802.1x, TNC, LDAP, VoIP), wodurch auch andere Hersteller einbezogen werden können
5. Unterstützung diverser Standards und Schnittstellen
6. VoIP-Nutzung der vorhandenen sicheren Verbindung
7. Auswahl unterschiedlicher Sicherheitsprofile
8. Netzüberwachungswerkzeuge überwachen kontinuierlich den Netzverkehr

Durch den MSG-Server kann ein Außendienstmitarbeiter einen sicheren Zugang aus dem Hotel, Hotspot oder von unterwegs in das Unternehmensnetz bekommen. Dabei werden sein Login und das genutzte Endgerät untersucht und mit der Sicherheitsrichtlinie des Unternehmens verglichen. Besitzt die Software auf seinem Endgerät nicht mehr die geforderte Aktualität oder wird ein Virus festgestellt, so gelangt der Teilnehmer erst einmal in die sog. Quarantänezone. Hier bekommt er nur Zugriff auf einen Update-Server. Nach erfolgreicher Installation kann dann anschließend wieder der sichere Kontakt mit den internen Serverdiensten hergestellt werden. So gelangen weniger Viren in das Unternehmensnetz und die mobilen Endgeräte sind komplett mit in das Sicherheitskonzept eines Unternehmens integriert.

Die integrierten Schnittstellen können mit vorhandenen Sicherheitslösungen zusammenarbeiten. Das MSG basiert komplett auf Open-Source-Software (OSS), so dass Erweiterungen einfach umgesetzt werden können. Das Betriebssystem ist Linux. Das TNC-Modul ist auch für spätere Spezifikationen ausreichend vorbereitet. Kopplungen mit ADS über LDAP oder Inventory-Datenbanken sind ohne weiteres möglich.

Komponenten:

- Linux-Betriebssystem ab Linux Kernel 2.4
- Module: VPN, Firewall, IDS, RADIUS/802.1x, TNC, LDAP, VoIP
- Schnittstellen: ADS, Softwareverteilung

Systemanforderungen:

- Linux-Betriebssystem
- 2 GHz CPU mit 512 MByte RAM
- 120 GByte SATA Festplatte
- 3 x NIC (intern, Quarantäne, extern)