Trusted Network Connect – sicherer Zugang ins Unternehmensnetz

Prof. Dr.-Ing. Kai-Oliver Detken[1], Dipl.-Inf. (FH) Stephan Gitz[2], Dipl.-Inf. Steffen Bartsch[3], Prof. Dr.-Ing. Richard Sethmann[4]

[1]DECOIT GmbH, Fahrenheitstraße 9, D-28359 Bremen
detken@decoit.de

[2 und 4]Institut für Informatik und Automation (IIA) der Hochschule Bremen,
Flughafenallee 10, 28199 Bremen
sethmann@hs-bremen.de, gitz@hs-bremen.de

[3]Technologie-Zentrum Informatik (TZI) der Universität Bremen,
Am Fallturm 1, D-28359 Bremen
sbartsch@tzi.de

Zusammenfassung

Durch den Ansatz Trusted Network Connect (TNC) soll es ermöglicht werden Rechner mit einem Server „vertrauenswürdig“ authentifizieren zu können. Die Trusted Computing Group (TCG) hat diesen Ansatz spezifiziert, mit dem Ziel einen gemeinsamen Standard vorzugeben. Die TCG ist eine internationale Standardisierungsinstitution, die die Arbeiten der ehemaligen Trusted Computing Alliance übernommen hat. Neben der höherwertigen Authentifizierung, die durch Benutzer- und Hardware-Identifizierung ermöglicht wird, ist auch der Mechanismus einer Quarantänezone für unsicheres Equipment eingeführt worden. Der TNC-Ansatz soll durch seine Mechanismen die Veränderung eines Endgerätes ausschließen, welche durch Fehlkonfiguration, Plattformangriffe oder Sicherheitslücken in Applikation und/oder Betriebssystem hervorgerufen werden kann. Dies ist gerade für den Einsatz mobiler Endgeräte wichtig. Die TCG hat mit diesem Ansatz ein Rahmenwerk geschaffen, das den Konfigurationszustand eines Rechners an den Server meldet, damit dieser eine Entscheidung bzgl. der Vertrauenswürdigkeit fällen kann. Das Projekt SIMOIT (www.simoit.de) hat diesen Ansatz, obwohl er noch nicht komplett spezifiziert ist, bereits herstellerneutral in Teilen innerhalb eines Prototyps implementiert. Die Ergebnisse dieser Implementierung werden hier dargestellt.

1 Hintergrund

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 steigenden Funktionalität mobiler Endgeräte wächst auf der anderen Seite auch das Sicherheitsrisiko. 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.

Durch das ständige Wachsen und Erweitern von IT-Infrastrukturen entstehen häufig Teillösungen, die für die schnelle Nutzung geeignet sind, jedoch auch etliche Einschränkungen mit sich bringen. Eine erste Anforderungsanalyse im SIMOIT-Projekt (www.simoit.de) hat ergeben, dass ein großer Bedarf besteht, sowohl den mobilen Mitarbeitern als auch weltweit verteilten Tochterunternehmen einen gesicherten mobilen Zugriff auf die IT-Infrastruktur des Unternehmens so einfach wie möglich zu ermöglichen. Die mobilen Endgeräte sollen sowohl im Unternehmen, bei einem Tochterunternehmen, unterwegs auf Reisen als auch bei einem Kunden einen schnellen, sicheren und problemlosen mobilen Zugriff auf das Unternehmensnetz bekommen.

Ziel des SIMOIT-Projektes ist es, eine universelle, einfach nutzbare Sicherheitsplattform zu entwickeln, die in heterogener Umgebung flexibel und sicher einsetzbar ist. Dabei wurde der Ansatz des Trusted Network Connect (TNC) näher untersucht und für das Projekt soweit das möglich war umgesetzt. Mit Hilfe des Pilotpartners konnte eine Testplattform entwickelt werden, die TNC im Zusammenspiel mit Hersteller-Ansätzen untersuchte und Empfehlungen für eine Integration ermöglichte.

2 Angriffsvektor auf mobile Endgeräte

Der Schutzbedarf von IT-Infrastrukturen steigt ständig, da immer mehr Geschäftsprozesse davon abhängen. Durch die Einführung von mobilen Endgeräten verschärfen sich die Anforderungen zusätzlich. Während früher die Angriffsvektoren auf die erreichbaren Serversysteme gerichtet waren, haben sich diese Vektoren heute auf die Firewall, das VPN-Gateway und zunehmend auch auf die Endgeräte verlagert. Sind die Endgeräte erstmal in der Kontrolle unautorisierter Personen, greifen viele der existierenden Sicherheitsmaßnahmen nicht mehr. Ein VPN verschlüsselt z.B. nur die Kommunikation zwischen Endgerät und Gateway. Sobald der Angreifer jedoch Kontrolle über das Endgerät hat, ist diese Kommunikation für ihn transparent und ein Zugriff auf Unternehmensressourcen möglich, siehe auch Abb. 1. Im Idealfall erhalten Endgeräte deshalb nur Zugriff auf kritische Ressourcen im Unternehmensnetz, wenn ihre Integrität gewährleistet werden kann.

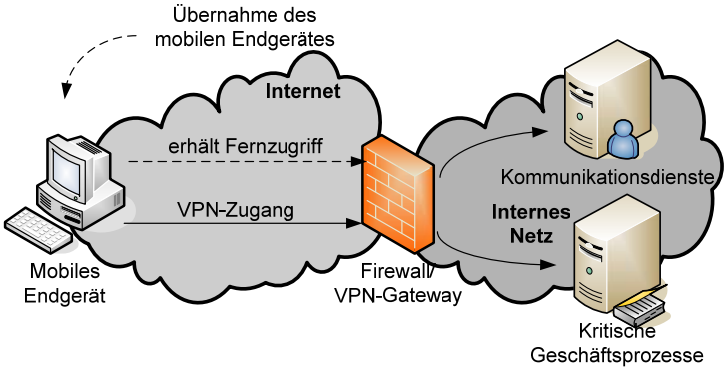

Abb. 1: Angriffsvektor: mobile Endgeräte, dadurch Zugriff des Angreifers aufs Unternehmensnetz

3 State-of-the-Art “Network Access Control”

3.1 Trusted Network Connect (TNC)

Heutige Rechnersysteme können nur mit hohem Aufwand und proprietären Lösungen auf Vertrauenswürdigkeit und Systemintegrität geprüft werden. Aus diesem Grund ist eine vertrauenswürdige Kommunikation zwischen z.B. einem mobilen Mitarbeiter und seinem Unternehmen schwierig. Die Trusted Computing Group (TCG) entwickelte mit der Spezifikation Trusted Network Connect (TNC) einen standardisierten Ansatz zur Realisierung vertrauenswürdiger Verbindungen z.B. über das Internet. Die TNC-Architektur ist die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten. Die Architektur bezieht dabei schon bestehende Sicherheitstechnologien, wie VPN-Technologien, IEEE 802.1x (802.1x), Extensible Authentication Protocol (EAP) und RADIUS mit ein.

Als Besonderheit bietet TNC optionale Hardwareunterstützung mit dem Trusted Platform Module oder dem Mobile Trusted Module an, mit denen die Sicherheit von TNC erhöht werden kann. So macht das TPM es unter anderem möglich, dass nur signierte Software auf einem System aufgeführt werden kann. Während das Trusted Platform Module schon seriemäßig in Hardware (z.B. von IBM) eingebaut wird, existiert jedoch das Mobile Trusted Module bisher nur als Entwurf.

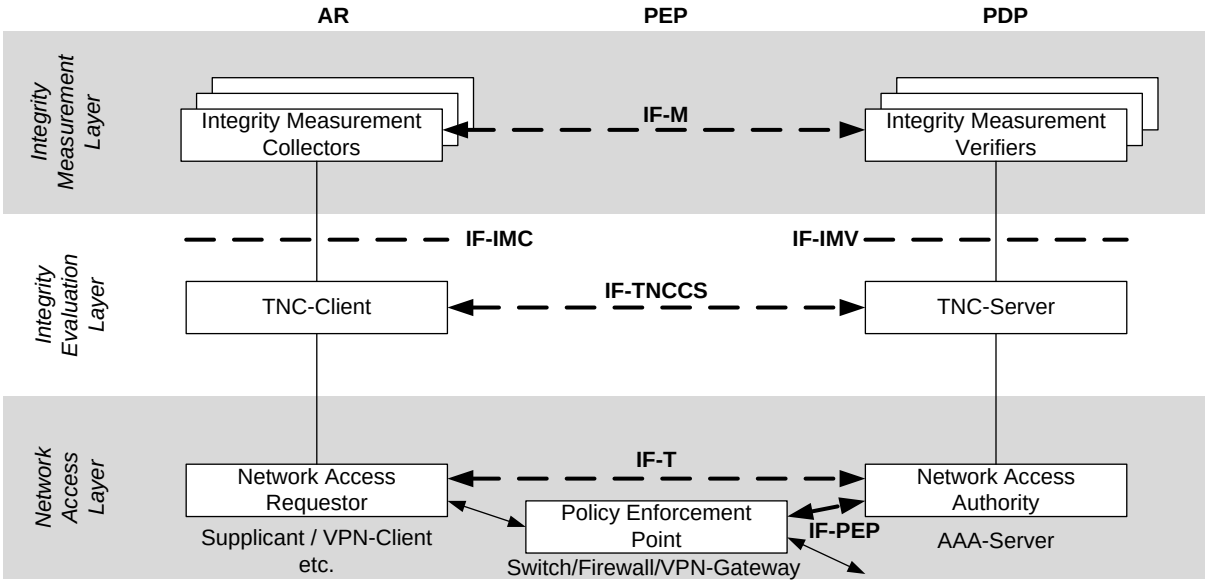

Abb. 2: TNC-Architektur [TNC02]

Die Architektur des Trusted Network Connects ist von der Trusted Computing Group in der Spezifikation 1.1 (Revision 2) vom 1. Mai 2006 veröffentlicht worden [TNC01]. Wie in Abb. 2 zu sehen ist, besteht die TNC-Architektur aus der Einheit Access Requestor (AR) mit den Komponenten Integrity Measurement Collector (IMC), TNC Client (TNCC) und Network Access Requestor (NAR), der Einheit Policy Enforcement Point (PEP) mit der Komponente Policy Enforcement Point und der Einheit Policy Decision Point (PDP) mit den Komponenten Integrity Measurement Verifier (IMV), TNC Server (TNCS) und Network Access Authority (NAA). Ähnliche Funktionen oder Rollen in der TNC-Architektur sind durch den

Network Access Layer, den Integrity Evaluation Layer und den Integrity Measurement Layer zusammengefasst. Diese drei abstrakten Layer sind waagerecht über die Komponenten der drei Einheiten gelegt worden. Das Zusammenwirken der einzelnen Komponenten wird durch Interfaces realisiert.

Die Einheiten besitzen die folgenden Aufgaben:

- **Access Requestor (AR):** Der Access Requestor stellt die Verbindung in ein geschütztes Netz her. Hier sorgt der Network Access Requestor für den sicheren Kommunikationskanal zum entfernten Netz und dem PDP. Der TNC Client ist für das Sammeln von Informationen zum Zustand des Gerätes zuständig. Diese Informationen werden von Integrity Measurement Collectors an den TNC Client geliefert.
- **Policiy Decision Point (PDP):** Der Policy Decision Point entscheidet für die Anfrage des AR, wie die Zugriffsrechte für die Verbindung aussehen. Die Network Access Authority ist dabei für die Kommunikation zum anfragenden Gerät und das Setzen der entsprechenden Policy im PEP zuständig. Die Basis für die Policy bildet die Empfehlung des TNC Servers, der dazu mit dem TNC Client kommuniziert und Daten vom TNC Client an die Integrity Measurement Verifiers zur Entscheidungsfindung weiterleitet.
- **Policy Enforcement Point (PEP):** Der Policy Enforcement Point bildet die vom PDP erhaltene Zugriffsberechtigung des AR ab.

Alle Einheiten und Komponenten in der Architektur sind logische und nicht physikalische Einheiten oder Komponenten. Die Realisierung der Komponenten oder Einheiten kann daher in unterschiedlicher Art und Weise erfolgen.

3.2 Vergleichbare Realisierungen zu TNC

Vergleichbare Realisierungen kommen u.a. von Cisco Systems und Microsoft. Die Network Access Protection (NAP) Architektur [NAP01] ist die Implementierung von Network Access Control durch das Unternehmen Microsoft. Die Architektur von NAP ist mit der des TNC zu vergleichen, wobei sich aber die Schnittstellen und die Bezeichnungen der einzelnen Einheiten unterscheiden [NAP02]. Der Integrity Measurement Collector des TNC hat unter NAP den Namen System Health Agent. Der TNC Client nennt sich in der NAP-Architektur NAP Agent und der Network Access Requestor wird Enforcement Client genannt.

Die Funktion der Network Access Authority wird bei NAP vom Network Policy Server übernommen und der TNC Server wird bei NAP Quarantäne Server genannt. Durch die Freigabe des „Statement of Health“- Protokoll im Mai 2007 [TNC01] existiert eine Interoperabilität zwischen TNC und NAP. Und durch einen Lizenzaustausch zwischen Cisco und Microsoft können die NAP-Clients sowohl mit dem „Statement of Health“-Protokoll als auch mit dem Protokoll des Cisco Trust Agent kommunizieren. Bisher existiert ein NAP-Client nur in Windows Vista und in der Betaversion des Windows Server 2008. Eine zukünftige Unterstützung für XP ist jedoch geplant. Zu Windows Mobile waren keine Aussagen zu finden.

Die „Network Admission Control“-Architektur (NAC) [NAC01] ist eine Umsetzung von TNC durch das Unternehmen Cisco. Die Architektur von NAC ist mit der von TNC und NAP zu vergleichen, wobei sich die Bezeichnungen, Schnittstellen und Protokolle unterscheiden. Der Einsatz von NAC erfordert bisher eine vollständige Cisco-Hardware-Infrastruktur und Cisco-Software-Komponenten. Dank einem Lizenzaustauschabkommen zwischen Cisco und Microsoft, wird der NAP-Client von Microsoft jedoch in Zukunft auch das Protokoll des Cis-

co Trust Agent unterstützen. In Hardwarekomponenten wird NAC dagegen in absehbarer Zeit nur von Cisco angeboten werden.

Es gab von offizieller Seite kurzzeitig die Aussage, dass der Cisco Trust Agent unter einer Open Source Lizenz gestellt werden sollte, doch diese wurde wieder revidiert. Stattdessen engagiert sich Cisco in der Network Endpoint Assessment – Initiative (NEA) [NAC02] des IETF, welche sich vorgenommen hat, einen IETF-Standard für NAC-Protokolle zu entwickeln, um die Interoperabilität zwischen NAC-Implementierungen unterschiedlicher Hersteller zu gewährleisten.

4 Anforderungen an mobile Endgeräte

An mobile Endgeräte werden spezielle Forderungen gestellt, im Gegensatz zu den fest installierten Endgeräten, die Ihren Ort normalerweise nicht wechseln. Die Mobilität macht die Endgeräte leichter angreifbar und auch die Nutzung unterschiedlicher Netzzugänge lassen PDAs, Laptops etc. nicht einfach handhaben. Die wesentlichen Anforderungen an mobile Endgeräte zur besseren Absicherung sind:

1. **Remote Installation:** Die Remote Installation ist erforderlich, wenn auf dem mobilen Endgerät ein Minimal-Betriebssystem lauffähig ist, in welchem auch die nötigen Treiber für die Konnektivität vorhanden sein müssen. Sind diese Anforderungen erfüllt, kann das Endgerät eine Verbindung zum Hauptsitz aufnehmen und so die benötigten Programme installieren lassen. 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.
2. **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.
3. **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. In der Quarantänezone kann das Endgerät nachträglich einen Zustand erlangen, der den Sicherheitsanforderungen des Unternehmens genügt um daraufhin vollen Zugriff auf die Unternehmensressourcen zu erlangen.

Die Authentifizierung der mobilen Mitarbeiter kann auf Benutzer- sowie auf Hardwareebene erfolgen. Zum einen wird überprüft, ob das Gerät im Firmennetz erlaubt ist und als zweite Stufe wird der anzumeldende Benutzer überprüft. Heutige Authentifizierungsarten beinhalten die wissensbasierte Authentifizierung (Passwort, PIN), die besitzorientierte Authentifizierung (Hardware-Token), die biometrische Authentifizierung (Fingerabdruck, Iris-Scan) und die Multifaktor-Authentifizierung (Kombination verschiedener Authentifizierungsarten).

5 Anwendungsfälle

Nachfolgend werden die wichtigsten Anwendungsfälle, die für ein Unternehmen relevant sind und im SIMOIT-Projekt untersucht wurden, aufgelistet:

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

Ein mobiles Endgerät, wie z.B. das Notebook soll ebenso wie stationäre Clients, Zugriff auf die Unternehmensressourcen wie File-, Datenbank- und Mail-Server bekommen. Der Zugriff erfolgt hier über ein Wireless oder ein kabelgebundenes LAN. Bei diesem Anwendungsfall werden die Clients ähnlich der stationären Clients authentisiert. Abb. 3 zeigt den Zugriff des mobilen Endgerätes über das Mobile Security Gateway (MSG)[1] auf das Unternehmensnetz.

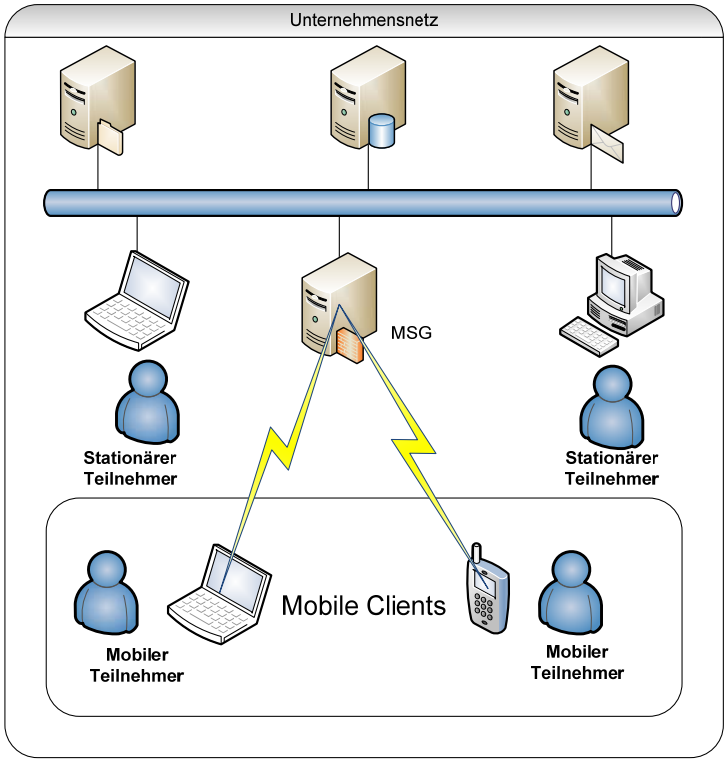

Abb. 3: Nutzung mobiler Endgeräte in der Zentrale

Der Remotezugriff ins Unternehmensnetz in Abb. 4 wird von Außendienstmitarbeitern genutzt, um E-Mails abzufragen oder um im internen Unternehmensnetz zu arbeiten. Der mobile Mitarbeiter wählt sich über ein VPN-Gateway in das Unternehmensnetz ein, authentisiert sich als Benutzer und kann danach auf alle ihm berechtigten Ressourcen zugreifen. Je nach Art der Verbindung des Clients muss das MSG diverse Zugangsmöglichkeiten offenhalten, z.B. WLAN, GPRS, GSM, VPN.

[1] Das Mobile Security Gateway (MSG) ist eine Bezeichnung aus dem SIMOIT-Projekt und bezieht sich auf den TNC-basierten Prototypen

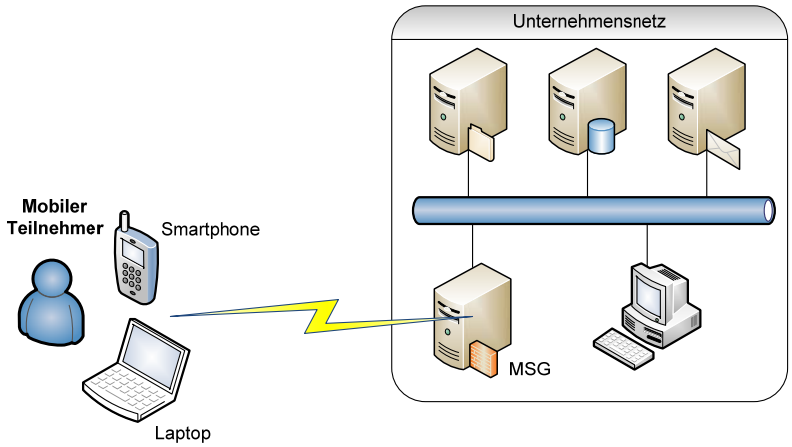

Abb. 4: Remote-Zugriff ins Unternehmensnetz

Ein Remote-Zugriff auf abgelegene Standorte, siehe Abb. 5, ist zum Beispiel die Administration eines Servers oder Clients auf einen Außenstandort. Andererseits kann diese Verbindung auch zur Datenreplikation zur Zentrale benutzt werden. Hierbei ist es jedoch erforderlich das entsprechende Zugänge in der Firewall geschaffen werden.

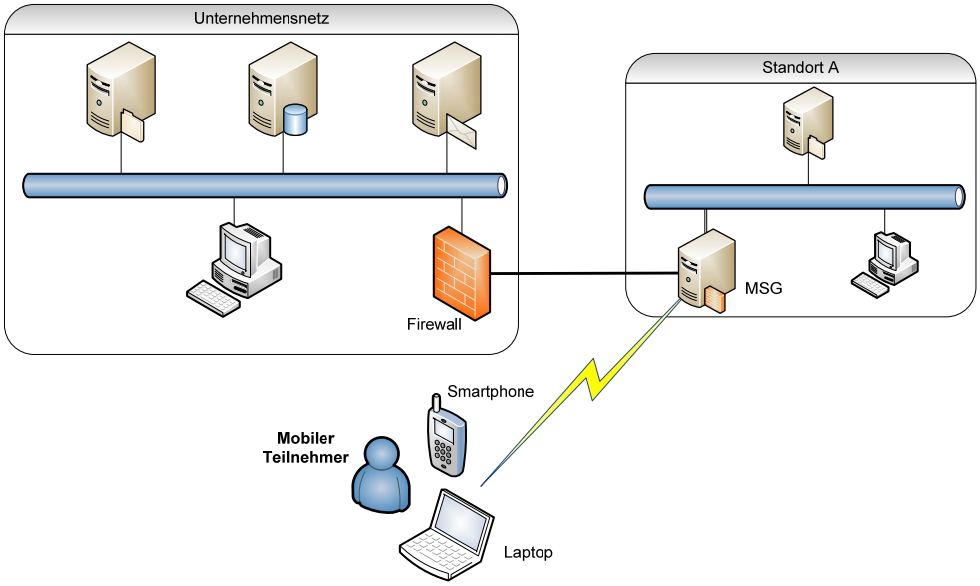

Abb. 5: Remote-Zugriff auf abgelegene Standorte

Ein weiterer Anwendungsfall ist, dass sich ein Außendienstmitarbeiter von Remote sich in die Zentrale verbindet, siehe Abb. 6, und anschließend eine Verbindung zu einem Kundennetz aufbaut. Dies ist erforderlich wenn man keinen direkten Remote-Zugang zum Kundennetz hat bzw. die Security Policys dieses nicht zulassen.

Im letzten Anwendungsfall (siehe Abb. 7) befindet sich der Mitarbeiter außerhalb der Zentrale in einem Kundennetz. Im Notfall soll der Mitarbeiter nun über das Kundennetz A über die Zentrale auf das Kundennetz B zugreifen können und so beispielsweise administrative Aufgaben übernehmen können.

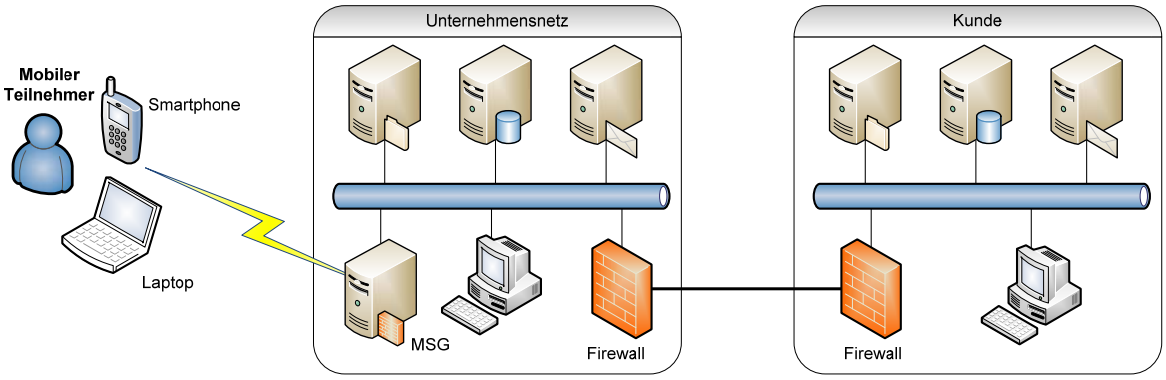

Abb. 6: Remote-Zugriff über das Unternehmensnetz auf Kundennetze

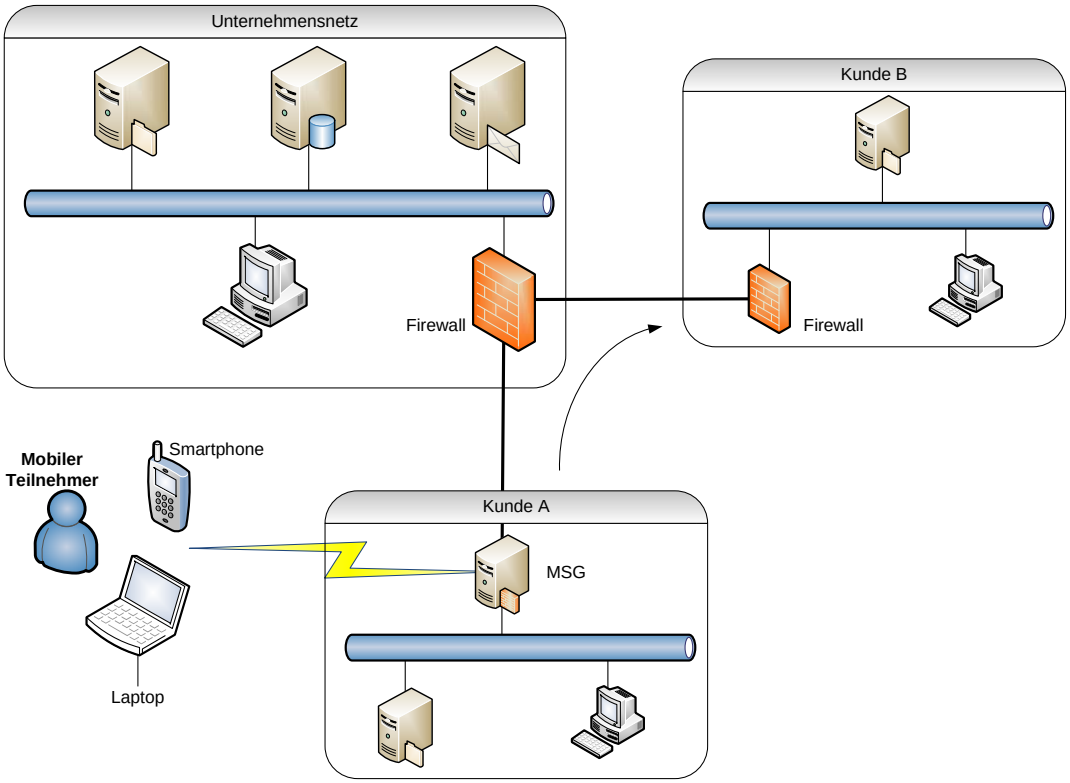

Abb. 7: Remote-Zugriff von Kundennetz A über die Zentrale auf Kundennetz B

Es gilt verschiedene mobile Szenarien zu beachten, um ein sicheres Einloggen über ein mobiles Endgerät zu ermöglichen. Im Vordergrund steht dabei die Authentisierung des Benutzers, damit überprüft werden kann, welche Person bestimmte Dienste innerhalb des Unternehmensnetzes nutzt. Auch würden hierdurch die bisherigen Zugriffsrichtlinien des Unternehmensnetzes weiter zum tragen kommen. Nach der Authentisierung muss der Datenkanal sicher verschlüsselt werden. Ebenso sollte der unerlaubte Zugriff auf das mobile Endgerät von außen dann nicht mehr möglich sein. Diese Anforderungen müssen für alle Szenarien gleichermaßen umgesetzt werden.

6 Umsetzung im SIMOIT-Projekt

6.1 TNC-Lösung im SIMOIT-Projekt

Im SIMOIT-Projekt wurde anhand der Anforderungen an mobile Endgeräte und der Anwendungsfälle beim Pilotkunden eine Entwicklungs- und Testplattform aufgesetzt, die den TNC-Ansatz praktisch evaluieren soll. Aufgrund der hohen Anforderungen an die organisatorische Sicherheit der Unternehmen bei der Einführung einer vollständigen TNC-Architektur, wurde dabei eine Lösung entwickelt, die eine schrittweise Migration auf TNC ermöglicht. Die Hauptplattform stellt dabei das Mobile Security Gateway (MSG) dar, welches aus verschiedenen Modulen (VPN, Firewall, TNC, RADIUS, LDAP) besteht, siehe Abb. 8. Dabei wurden speziell Open-Source-Software (OSS)-Projekte und -Ansätze gewählt, um eine offene, standardkonforme Umsetzung zu ermöglichen. Gleichzeitig ist die Flexibilität gewahrt geblieben, so dass bestehende Komponenten wie z.B. Firewall-Systeme eingebunden werden können. In diesem Fall würde das jeweilige SIMOIT-Modul nicht verwendet, sondern nur eine Schnittstelle zur Verfügung gestellt werden. Beim Pilotkunden war zusätzlich die Anbindung an einen internen Active Directory Server (ADS) notwendig, weshalb über LDAP [Serm06] auch hier eine Schnittstelle zur Verfügung gestellt wurde. Darüber werden sämtliche internen Benutzerprofile abgefragt, die für die Authentisierung wichtig sind, und an den MSG weitergeleitet. Beide Systeme gleichen sich gegeneinander mehrmals am Tag ab, da der ADS innerhalb des Unternehmensnetzes zu finden ist und unabhängig vom MSG arbeitet.

Während vollständige TNC-Architekturen Softwareagenten und Integrity Measurement Collectoren auf der Client-Seite voraussetzen, arbeitet die SIMOIT-Plattform auch mit unveränderten Clients zusammen, welche nur über eine Standardinstallation verfügen. In diesem Fall wird zusätzlich zur gewohnten Nutzerauthentisierung, die verwendete Hardware über ein X.509 identifiziert. Der im SIMOIT verwendete FreeRadius-Server (www.freeradius.org) [NeDe07] wurde dafür so erweitert, dass er über standardisierte Schnittstellen mit einem TNC-Server verbunden ist. Der TNC-Server baut auf die Open-Source-Bibliothek „libtnc“ auf und nutzt spezielle Integrity Measurement Verifier zur Integritätsprüfung. Die entwickelten Integrity Measurement Verifier sind an die Softwareverteilung des Pilotkunden angepasst und ermitteln den gewünschten und vorhanden Softwarestand eines Endgerätes, um über diese Informationen den Zugriff auf das Unternehmensnetz zu regeln. Es können allerdings beliebige Softwareverteilungssysteme angebunden werden.

6.2 Kommunikationsablauf

Der Kommunikationsablauf läuft in SIMOIT nun wie in Abbildung 9 dargestellt ab. Beim Einwahlvorgang wird vom mobilen Client eine VPN-Verbindung mit dem Mobile Security Gateway aufgebaut. Vom VPN-Modul wird die ID des X.509 Zertifikat [HPFS02] vom mobilen Client ermittelt und mit dessen Benutzerauthentisierung zum RADIUS-Server übermittelt. Der RADIUS-Server unterstützt mittels Modulen unterschiedliche Authorisierungs- und Authentisierungsmechanismen und nutzt beim Pilotkunden eine Schnittstelle zu einer bestehenden Active Directory Datenbank. Im Autorisierungsprozess des Nutzers werden die auf dem VPN-Gateway einzustellenden Berechtigungen für den VPN-Tunnel ermittelt. Bevor diese jedoch über RADIUS an das VPN-Modul gesendet werden, wird vom TNC-Server überprüft, ob diese Berechtigungen auch wirklich gewährt werden dürfen. Dafür wird die ID des X.509 Zertifikat des Clients vom RADIUS-Server zum TNC-Server übertragen und der Software-

stand des jeweiligen Clients über einen Integrity Measurement Verifier bestimmt. Sollte sich der Client in einem unerwünschten Zustand befinden, ändert der TNC-Server die dem Nutzer zugeordneten Berechtigungen, so dass nur noch der Zugriff auf die Quarantänezone gewährt wird. Nachdem der TNC-Server mit seinen Überprüfungen fertig ist, sendet der RADIUS-Server die ermittelten Berechtigungen des Clients zum VPN-Modul, welches diese dann für den Client aktiviert. Das RADIUS-Modul sendet die notwendigen Firewall-Einstellungen an das VPN-Modul zurück welches dann die ermittelten Berechtigungen durchsetzt.

Es gibt also zwei mögliche Autorisierungsvarianten:

- In der Variante 1 versucht sich ein Mitarbeiter mit einem veralteten Softwarestand eines mobilen Systems in das Unternehmensnetz einzuwählen. Dabei wird zuerst eine Benutzer- und Hardwareauthentisierung vorgenommen, die er erfolgreich besteht. Auf Basis von Daten in der Softwareverteilung wird das mobile System allerdings in die Quarantänezone verschoben. Der Mitarbeiter hat nun ausschließlich nur Zugriff auf Software-Updates, kann aber keinen internen Server erreichen.
- In der Variante 2 versucht sich ein Mitarbeiter mit einem aktuellen Softwarestand seines mobilen Systems in das Unternehmensnetz einzuwählen. Dabei wird zuerst eine Benutzer- und Hardwareauthentisierung vorgenommen, die er erfolgreich besteht. Die Softwareverteilung meldet, dass das Gerät sich auf dem aktuellen Stand befindet und der Mitarbeiter erhält den vollen Zugriff auf das Unternehmensnetz.

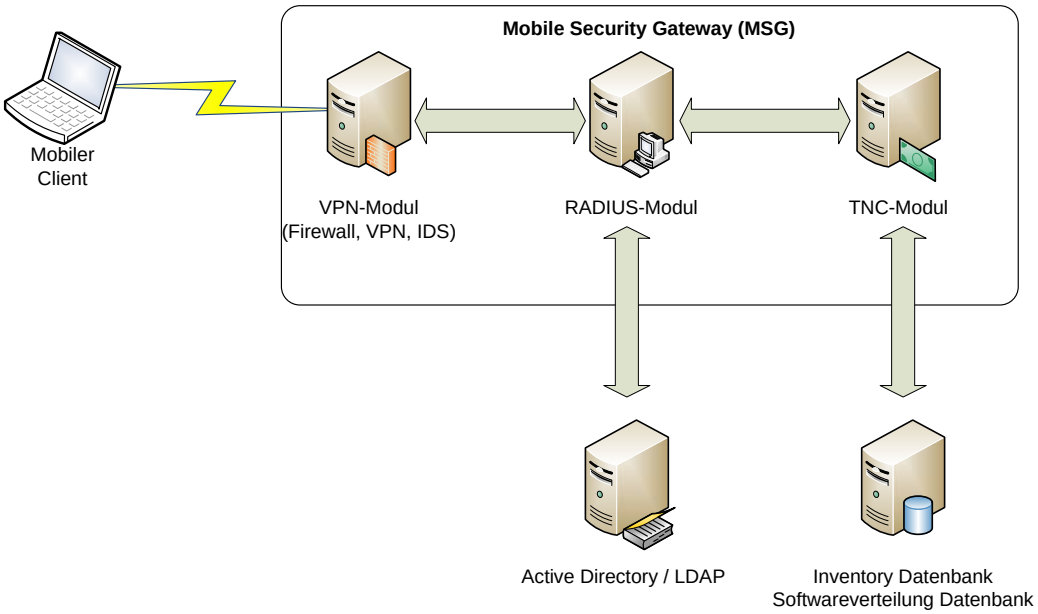

Abb. 8: Übersicht der SIMOIT-Module

Durch das beschriebene Erzwingen von notwendigen Gerätezuständen beim Netzzugang, kann die Endgerätesicherheit und damit die Sicherheit der Unternehmensressourcen entscheidend erhöht werden. Durch Nutzen der Datenstände von Softwareverteilungen zur Integritätsprüfung des Clients wird die Komplexität von TNC genügend verringert, um auch kleinen und mittleren Unternehmen ohne großes Sicherheitsbudget den Einsatz einer einfachen TNC-Lösung zu ermöglichen. Durch das Nutzen standardisierter Schnittstellen kann durch das Hinzufügen weiterer Integrity Measurement Verifier die Integritätsprüfung bei erhöhten Si-

cherheitsbedarf auch auf dem Client stattfinden, so dass das Unternehmen die Möglichkeit hat langsam auf eine vollständige TNC-Lösung zu migrieren.

Doch da es vorkommen kann, dass erfolgreich auf Integrität geprüfte mobile Endgeräte von Angreifer übernommen oder von Mitarbeitern missbraucht werden, existiert im MSG noch ein optionales Intrusion Detection Modul. Wenn von Endgeräten mit Vollzugriff Angriffe auf das Unternehmensnetz gestartet werden, registriert das eingesetzte Network Intrusion Detection System (NIDS) Snort (www.snort.org) den Angriff auf die Unternehmensressourcen und unterbindet optional den Zugriff. Es wird so der gesamte ankommende Netzwerkverkehr mitgelesen. Der Inhalt der Datenpakete wird mit charakteristischen Mustern von bekannten Angriffen verglichen – diese Muster werden allgemein Signaturen genannt, die beim NIDS Snort in „Rules“ (Regeln) festgehalten werden. Zur Mustererkennung wird bei Snort der Aho-Corasick-Algorithmus verwendet. Mitarbeiter der IT können so benachrichtigt werden, um weitere Aktionen zu veranlassen.

7 Fazit

Zusammenfassend betrachtet, fehlen mithin noch immer ausgereifte und plattformunabhängige Werkzeuge, die zur Absicherung von mobilen Netzen eingesetzt werden können. Dies gilt insbesondere auch für einen Einsatz in mittelständisch geprägten Unternehmen. Im Gegensatz zu Großunternehmen können sich mittelständische Unternehmen oft keine speziellen Abteilungen für die IT-Sicherheit leisten. Mittelständische Unternehmen müssen oft mit einem sehr eingeschränkten Budget und Personal für die IT-Sicherheit auskommen. Insofern sind einfach zu bedienende, plattformübergreifende Sicherheitswerkzeuge erforderlich. Da mobile Netze immer komplexer werden, ist die Administration dieser Netze immer aufwändiger und fehleranfälliger (insbesondere hinsichtlich der IT-Sicherheit). Aus diesem Grunde sind Mechanismen, die eine zentrale Administration von mobilen Netzen ermöglichen, immer wichtiger.

Der vorgestellte TNC-Ansatz ist eine Möglichkeit ein höheres Sicherheitsniveau zu erreichen. Die Kern-Spezifikationen sind bereits abgeschlossen und erste Produkte wie Switche, Router, VPN-Gateways werden unterstützt. Allerdings sind noch Lücken bzgl. Veränderungen der Agenten auf Endgeräten vorhanden. Auch gehen die Herstelleransätze noch zu weit auseinander. Allerdings wurde Microsofts Statement-of-Health-Protokoll integriert, so dass man zukünftig auch mit höherer Interoperabilität rechnen kann. Bisher ist allerdings kaum Know-how zum Thema TNC in den Unternehmen vorhanden.

Der SIMOIT-Ansatz setzt bereits auf den TNC-Ansatz und die Teilumsetzung auf Serverseite. Die Entscheidung über die Integrität der Endgeräte wird aufgrund der vorhandenen Infrastrukturinformationen getroffen. Die Lösung ist modular aufgebaut, so dass sie auch andere Herstellerlösungen (z.B. Softwareverteilung, VPN) mit integrieren kann. Für einen reibungslosen Verlauf sollten die Herstellerkomponenten (besonders im Bereich Firewall und VPN) allerdings den TNC-Ansatz unterstützen. In Zukunft werden auf der mobilen Endgeräteseite einige TNC-Clients integriert werden, so dass beliebige Betriebssysteme eingebunden werden können. Momentan ist man in der Entwicklung aber noch nicht soweit, so dass man bei Herstellerlösungen auf proprietäre Systeme zugreifen müsste. Dies wird sich aber durch das Vorantreiben des TNC-Standards weiter ändern.

Literatur

[DeEr06] Detken, Eren: Mobile Security - Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit; 672 Seiten; Hardcover; Hanser Verlag; ISBN 3-446-40458-9; München 2006

[HPFS02] Housley, Polk, Ford, Solo: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; RFC-3280; Updated: RFC-4325, RFC-4630; Network Working Group; IETF April 2002

[NAP01] http://www.microsoft.com/technet/network/nap/default.mspx, zuletzt besucht: 11.4.2008

[NAP02] TNC IF-TNCCS: Protocol Bindings for SoH; TCG Trusted Network Connect; Specification Version 1.0; 21. May 2007

[NAC01] http://www.cisco.com/go/nac, zuletzt besucht: 11.4.2008

[NAC02] Network Endpoint Assessment (nea), http://www.ietf.org/html.charters/nea-charter.html, zuletzt besucht: 11.4.2008

[NeDe07] Nelson, DeKok: Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes; RFC-5080 (Proposed Standard); Updates: RFC-2865, RFC-2866, RFC-2869, RFC-3579; Network Working Group; IETF December 2007

[ScHa07] Schmidt, Axel; Haase, Andreas: Hochmobiler Mitarbeiter – Entwicklung einer dedizierten Infrastruktur für die mobile Kommunikation; Diplomarbeit an der Hochschule Bremen; Bremen 2007

[Serm06] J. Sermersheim: Lightweight Directory Access Protocol (LDAP): The Protocol; RFC-4511 (Proposed Standard); Network Working Group; IETF June 2006

[TNC01] https://www.trustedcomputinggroup.org/specs/TNC, zuletzt besucht: 11.4.2008

[TNC02] http://www.trustedcomputinggroup.org/groups/network, zuletzt besucht: 11.4.2008

[X509] X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks; ITU-T Standard; August 2005