User-Centric Identity Management in mobilen Szenarien im SIMOIT-Projekt

Prof. Dr.-Ing. Kai-Oliver Detken[1], Prof. Dr.-Ing. Evren Eren[2]

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

[22]FH Dortmund, FB Informatik, Emil-Figge-Straße 42, D-44227 Dortmund
eren@fh-dortmund.de

Zusammenfassung

Mobile Lösungen und Systeme werden heute zunehmend in Unternehmen eingesetzt. Leider fehlen aber dabei ausgereifte und plattformunabhängige Werkzeuge, die zur Absicherung von mobilen Netzen angewandt werden können. Dies gilt insbesondere auch für einen Einsatz in mittelständisch geprägten Unternehmen (KMU). Im Gegensatz zu Großunternehmen können sich mittelständische Unternehmen oft keine speziellen Abteilungen für die IT-Sicherheit leisten. KMUs müssen oft mit einem sehr eingeschränkten Budget und wenig 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. Dieser Beitrag diskutiert die wesentlichen Elemente von „Identity and Access Management“ vor dem Hintergrund der spezifischen Anforderungen in mobilen Umgebungen und Anwendungsszenarien. Die Autoren stellen den State-of-the-art beim Identity Management, die zugehörigen Standards sowie die Initiativen im Kontext des SIMOIT-Projekts vor. Darüber hinaus setzt sich der Beitrag mit den Ergebnissen des Projekts und der Prototyp-Implementierung hinsichtlich generischer Anforderungen auseinander.

1 Einleitung

Transparentes und zentral gesteuertes Identity und Access Management (IAM) gewinnt zunehmend an Bedeutung für zukünftige Netze und Dienste, insbesondere für mobile Szenarien. Bedingt durch die Tatsache, dass feste und drahtlose Kommunikationsnetze zusammenwachsen, und der Zugang zu Services zeit- und raumunabhängiger wird (Stichwort: Ubiquitous Computing), sind multimodale und standardisierte Lösungen vonnöten. Durch die Vielfalt der Netzzugangstechnologien sowie durch die steigende Zahl der Dienste (aber auch deren unerlaubte Nutzung), sind mobile Endgeräte (und die Benutzer als solche) Sicherheitsrisiken ausgesetzt. Verlässliche Identifikation, sowohl des Benutzers als auch des Endgerätes zur Autorisierung und Authentifizierung bei Zugängen zu Netzen und Diensten, ist zwingend erforderlich. IT-basierte Geschäftsprozesse verlangen Administration und Steuerung von Zugangsberechtigungen mit automatisierter und rollenbasierter Zuweisung und Rücknahme von Benutzerprivilegien – das sogenannte “User-Provisioning” bzw. “De-Provisioning”.

P. Horster (Hrsg.) · D.A.CH Security 2009 · syssec (2009) pp.

Das Trusted Network Connect (TNC) adressiert diesen Sachverhalt. Von der Trusted Computing Group (TCG) spezifiziert, zielt TNC auf die Schaffung eines gemeinsamen Standards ab. Neben der Authentifizierung (Benutzer- und Geräteidentifikation) definiert sie eine Quarantänezone für ungesicherte Geräte. TNC verhindert jedwede Modifikation von Endgeräten und schließt somit Sicherheitslöcher aus, die durch fehlerhafte und schwache Gerätekonfigurationen sowie Sicherheitsprobleme in Softwareanwendungen und Betriebssystemen mobiler Endgeräte verursacht werden. Der Konfigurationsstatus des Endgerätes wird einem dedizierten Server kommuniziert, der über dessen Vertrauenswürdigkeit bzw. Zuverlässigkeit entscheidet.

Die TNC-Kernspezifikation wurde bereits abgeschlossen und einige Produkte wie beispielsweise Switches, Router und VPN-Gateways sind ansatzweise am Markt verfügbar. Jedoch ist eine nahtlose Integration von mobilen Benutzern in Unternehmen das sogenannte „User-Centric Identity Management" noch nicht durchgängig möglich. Es fehlen plattformunabhängige Lösungen. Auch sind Authentifizierungsmechanismen und Synchronisation von Benutzeridentitäten sowie -rechten nicht kompatibel. Ganz besonders für kleine und mittelständische Unternehmen (KMU) ist „Identity Management and Access" ein komplexes Thema und stellt eine große Herausforderung dar. Diese Zielgruppe kann sich keine eigenen Abteilungen für die IT-Sicherheit leisten und muss mit beschränktem Budget sowie wenig personellen Ressourcen auskommen. Auch die steigende Komplexität von mobilen Netzen erfordert Mechanismen zur zentralen Administration und Konfiguration. Das Forschungs- und Entwicklungsprojekt SIMOIT identifizierte diese Problematik und implementierte den TNC-Ansatz teilweise in Form eines herstellerneutralen Prototyps. [DGBS08]

2 IT-Sicherheitsfaktoren

Sicherheit ist ein Grundbedürfnis des Menschen - und damit unserer Gesellschaft. Damit ist auch IT-Sicherheit ein wichtiges Thema in der Informations- und Kommunikationsbranche. Wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in Folge von IT-Vorfällen erhöhen den Handlungsbedarf in Sachen „aktives IT-Sicherheitsmanagement". Dabei beschränkt sich IT-Sicherheit keineswegs auf die jeweiligen IT-Fachabteilungen sondern zieht sich durch sämtliche Abteilungen. Ganzheitliche Sicherheit in einer IT-Infrastruktur verlässt sich im Wesentlichen auf folgende Faktoren: [DEER06], [ITW05]

- **Zugangssteuerung/Zugriffskontrolle:** Dieser Mechanismus beinhaltet das Spektrum der Tools, die benutzt werden, um digitale Identitäten hinsichtlich des Zugangs in ein Netzwerk und dessen Ressourcen zu limitieren. Ressourcen können dabei Objekte wie Rechner, Server, Drucker etc. sowie Softwaredienste sein. Die Zugangssteuerung bzw. Zugriffskontrolle kann mittels Benutzerauthentifizierungsmethoden erfolgen, wobei die Echtheit von Benutzern und deren Privilegien überprüft wird – beispielsweise durch EAP (Extensible Authentication Protocol). Nach erfolgreicher Authentifizierung folgt die Autorisierung, die bestimmt, auf welche Objekte Benutzer zugreifen dürfen. In der Regel sind es Dienste.
- **Integrität:** Die Integrität umfasst die Maßnahmen, die dafür sorgen, dass die geschützten Daten während der Verarbeitung oder Übertragung nicht manipuliert, d.h. beschädigt oder verändert werden können. Hauptziel ist somit die Gewährleistung von korrekten und vollständigen Daten. Sowohl die Daten selbst, also auch Hard- und Software, müssen vor unberechtigtem Zugriff geschützt werden. Auf sensible Daten dürfen nur befugte Personen Zugriff erhalten. Die Verwendung von kryptografischen

Hashfunktionen gewährleistet die Integrität von sensiblen Daten. Im Allgemeinen kann bei dem Gebrauch von Hashes eine Veränderung der Daten nicht verhindert werden, es kann lediglich nachträglich festgestellt werden, dass eine Manipulation der Daten stattgefunden hat.

- **Originalität (Authentizität):**Die Authentizität/Originalität von sensiblen Daten und die sichere Zuordnung zum Sender sowie der Nachweis, dass die Informationen auf dem Kommunikationsweg nicht manipuliert worden sind und keine Kopien ohne Wissen des vermeintlichen Absenders verbreitet werden, sind Faktoren, die den Begriff der Originalität im Umfeld von IT-Sicherheit beschreiben.
- **Authentifizierung:** Die Authentifizierung dient zur Feststellung von Identitäten einer Person oder einem Gerät, um beispielsweise den Zugang zu technischen Systemen zu kontrollieren. In der Kommunikation lässt sich durch die Authentifizierung verifizieren, dass der Kommunikationspartner (Benutzer oder Gerät) auch derjenige ist, für den er sich ausgibt. Die Prüfung der Authentizität, also die Herkunft und Unverfälschtheit von Dokumenten und Informationen gehört ebenfalls zum Begriff der Authentifizierung.
- **Autorisierung:** Die Autorisierung ist eine Berechtigung, die sich auf Person, IT-Komponente oder Anwendung bezieht. Sie definiert, wer was in einem Netzwerk tun darf oder welche System-Ressourcen genutzt werden dürfen. Bei der Autorisierung werden dem Nutzer Rechte zugewiesen. Diese erlauben es dem Benutzer eine bestimmte Aktion auszuüben. Um einen wirksamen Schutz zu erreichen, sollte der Nutzer bei der Rechtevergabe nur für die Ressourcen autorisiert werden, die er unbedingt benötigt.
- **Vertraulichkeit:** Unter Vertraulichkeit versteht man, dass eine Nachricht oder bestimmte Daten nur für Befugte zugänglich gemacht werden. Unbefugte haben dagegen keinen Zugang zu diesen übertragenen Informationen. Um die Vertraulichkeit zu gewährleisten, müssen die im System gespeicherten oder die auf dem Übertragungsweg befindlichen Daten durch Verschlüsselung vor unberechtigtem Zugriff geschützt werden.
- **Verfügbarkeit:** Die Verfügbarkeit umfasst die Hardware ebenso wie die Software, das Betriebssystem und die Datenspeicherung, die Netzwerkkomponenten und die Sicherheit vor unberechtigten Zugriffen. Der Begriff der Verfügbarkeit ist somit ein weiterer Eckpfeiler der IT-Sicherheit.
- **Audit:** Auditing ist ein Verfahren, das alle sicherheitsrelevanten Ereignisse betrachtet und protokolliert. Das Auditing befasst sich mit allen Benutzeraktivitäten in einem geschützten Bereich. Ressourcen können dabei Objekte wie Rechner, Server, Drucker etc. sowie Softwaredienste sein.

3 Lösungen für Endpunkt-Sicherheit

Das Wachstum des Internets in den letzten Jahren brachte neue Technologien und demzufolge neue Herausforderungen für die Sicherheit mit sich. Eine dieser Herausforderungen betrifft, zusätzlich zur gewöhnlichen Benutzerauthentifizierung, die zunehmende Notwendigkeit für Maschine-Maschine-Identifikation sowie Authentifizierung und Netzwerkzugangssteuerung

in der IP-Schicht. Maschinenbasierte und Plattform-Authentifizierung ist wesentlich für die Sicherheit und Autorisierung bei Netzwerkzugangsanfragen in den ISO-OSI-Ebenen 2 und 3. Darüber hinaus besteht das Problem der Endpunkt-Integrität, was bedeutet, dass Angriffe auf höheren OSI-Ebenen (Malware wie Viren und Trojanische Pferde) zunehmen. Das Problem der Endpunkt-Integrität betrifft die Vertrauenswürdigkeit/Zuverlässigkeit der kommunizierenden Endpunkte (z.B. Client und Server) hinsichtlich der Integritätsbedingungen und ihrer Identitäten. Unter Integrität verstehen wir die relative „Reinheit“ von Endpunkten bezüglich der eingesetzten (installierten) Software und Hardware. Ein Paradigma für schädliche Software sind Viren und Trojanische Pferde, die insbesondere Unternehmensnetze angreifen. Heutzutage haben viele Mitarbeiter ihre mobilen Endgeräte wie Laptops, PDAs, etc. im Mischbetrieb, d.h., sowohl im privaten Bereich zu Hause als auch am Arbeitsplatz im Einsatz. [TCG08]

Endpunkt-Sicherheitslösungen nutzen Router, Switches, WLAN-Access-Points, Software und Security-Appliances. Es werden Authentifizierungs- und Autorisierungsinformationen beispielsweise über mobile Endgeräte an einen Richtlinienserver weitergeleitet, der dann entscheidet, ob das Gerät einen Zugang erhalten darf oder nicht. Der Zugriffsschutz ermöglicht weiterhin, eine Zustandsprüfung („Health Check“) am Client durchzuführen. Ein solcher Health Check besteht üblicherweise aus der Abfrage bestimmter Informationen über die Client-Plattform. Ermittelt werden unter anderem die Version des Virenscanners, Einstellungen der Personal Firewall und anderer Programme sowie der Patch-Status des Endgerätes (u.a. Betriebssystems). Falls der Client nicht den IT-Richtlinien entspricht, kann er in ein Virtual LAN (VLAN) isoliert werden, wo dann eine „Sanierung“ durchgeführt werden kann.

Neben den lizenzpflichtigen Softwarelösungen Ciscos Network Admission Control (NAC) und Microsoft Network Access Protection (NAP), gibt es Open-Source-Lösungen, wie den Ansatz Trusted Network Connect (TNC).

Alle genannten Technologien unterstützen die sichere Authentifizierungsmethode auf Basis des 802.1x-Authentifizierungsstandards. Diese beinhaltet die Identifizierung des Endsystems direkt am Switch-Port. Eine solche Authentifizierung erfordert entsprechende Funktionen auf Seiten des Switches, des Clients und einer lokalen Authentifizierungsinstanz, beispielsweise einem RADIUS-Server. Eine weitere Lösung ist die MAC-basierte Authentifizierung: Hier wird dieselbe Infrastruktur genutzt wie bei einer 802.1x-Infrastruktur – es wird lediglich auf Zertifikate und/oder Anmeldedaten verzichtet. Der Switch verwendet die MAC-Adresse als Ersatz für den Benutzernamen und gleicht diese mit dem RADIUS-Server ab. In 802.1x-fähigen Netzen kann dieses Verfahren verwendet werden, um Endsysteme ohne „Supplicant“ (802.1x-Endgeräteschnittstelle) gegen einen RADIUS-Server abzugleichen. Die Web-basierende Authentifizierung lagert die Anmeldung der Endgeräte auf ein Web-Portal aus, an dem sich der Benutzer anmelden kann. Somit können sich Geräte und Systeme ohne erforderliche Voraussetzungen am Netzwerk registrieren und gegebenenfalls Zugriff auf den sicheren Netzbereich erhalten. [NISP08]

4 Benutzerzentriertes Identity Management mittels Trusted Network Connect

Identity Management beinhaltet das Spektrum der Tools, die benutzt werden, um digitale Identitäten zu repräsentieren, administrieren und deren Zugangskontrolle durchzusetzen. Ac-

cess Management repräsentiert die zentralisierte Authentifizierung und Autorisierung für die bereitgestellten Netzwerkressourcen. Diese Funktionalität wird auch als Extranet Access Management (EAM) bezeichnet. Hauptziel von Identity- und Accessmanagement (IAM) ist die Verbesserung des angebotenen Dienstes und somit ein einheitlicher Zugriff auf Ressourcen. Die Benutzerauthentifizierung wird auf Basis des IEEE 802.1x Standards realisiert. Hierbei werden die Benutzeridentitäten und -privilegien geprüft. In der Regel übernimmt ein Authentifizierungsserver wie z.B. RADIUS den Authentifizierungsprozess. IEEE 802.1x wurde entwickelt, um eine sichere Plattform für die Benutzerauthentifizierung zu schaffen. Als Portbasiertes Zugriffssteuerungsprotokoll, das auf Portebene zwischen einer beliebigen Authentifizierungsmethode und einem restlichen Netzwerk verläuft, basiert es im Wesentlichen auf dem Extensible Authentication Protocol (EAP) und bietet einen Mechanismus für die Zugangsautorisierung einzelner Benutzer an ihren Endpunkten. Es erfolgt eine Übersetzung der Nachrichten der jeweils gewählten Authentifizierungsmethode in das korrekte Nachrichtenformat.

In Verbindung mit IEEE 802.1x und dem Trusted Platform Module (TPM) gewährleistet die Trusted-Network-Connect-Technologie, dass lediglich zertifizierte (digital signierte) Anwendungssoftware operieren kann. Die TNC-Architektur wurde mit dem Ziel entwickelt, eine vertrauenswürdige Verbindung zwischen unsicheren (öffentlichen) Medien wie zum Beispiel dem Internet herzustellen. Das Kombinieren weiterer Sicherheitsmechanismen ist durch die offene und herstellerunabhängige Entwicklung des TNC-Standards möglich. Mit Hilfe des Trusted Platform Moduls (TPM), welches auf dem TCG-Standards basiert, wird zusätzlich ein Hardware-seitiger Schutz geboten und der Sicherheitsanspruch der Technik erhöht. Desweiteren arbeitet die TNC-Technologie mit einem Autorisierungstoken (z.B. X.509-Zertifikat), der ebenfalls mit den vom TP-Modul gesammelten Informationen über den Zustand des Client-Systems übertragen wird. Die übertragenen Informationen werden am Zielsystem auf Richtlinienkonformität geprüft. Eine Zugriffsentscheidung kann somit auf Basis der Identität und des Zustands des Systems getroffen werden. Neben der höherwertigen Authentifizierung, die durch Benutzer- und Hardware-Identifizierung ermöglicht wird, ist auch der Mechanismus einer Quarantänezone für unsichere Endsysteme 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. [ITW05], [MUEL08], [TCG05]

Der technisch-strukturelle Aufbau teilt sich in drei Hauptaufgaben auf:

- **Access Requestor (AR):** Das Client-System wird um eine Softwarekomponente, den TNC-Client, erweitert. Dieser ermittelt den aktuellen Zustand des Systems und schickt diesen an den TNC-Server (Network Policy Server). Die Messung der einzelnen Komponenten des Rechnersystems findet durch sog. Integrity Measurement Collectors (IMC) statt. Für jede zu messende Komponente existiert dabei ein passender IMC, z.B. einer für den Virenscanner und einer für die Personal Firewall. Zum Systemstart werden die IMCs vom TNC-Client auf dem zugreifenden Rechnersystem initialisiert, um bei einem Verbindungsaufbau Messwerte von den jeweiligen Komponenten sammeln zu können.
- **Policy Enforcement Point (PEP):** Der PEP ist das TNC-Element am Eintrittspunkt des Netzwerkes; in der Regel eine aktive Netzwerkkomponente (z.B. WLAN Access-Point, Switch oder Router) mit 802.1x-Unterstützung. Aufgaben der Komponente ist die Entgegennahme und Weiterleitung von Verbindungsanfragen sowie die Ausführung der

Handlungsentscheidung des Policy Decision Point (PDP). Der PEP stellt als Eintrittspunkt den zuerst adressierten Verbindungspunkt des Netzwerkes dar. Ankommende Verbindungsanfragen eines AR werden direkt an den PDP weitergeleitet. Im Falle einer Negativüberprüfung gibt es zwei Optionen: Abweisen des anfragenden Clients oder Verschieben in ein vordefiniertes Netzwerksegment zur anschließenden Wiederherstellung des gewünschten Zustandes.

- **Policy Decision Point (PDP):** Dieser ist für die Bewertung der durch die Integrity Measurement Collectors ermittelten und durch den TNC-Client übertragenen Messdaten zuständig. Hierfür wird das System um eine Softwarekomponente, den TNC-Server, erweitert, der die Daten vom Client entgegen nimmt. Die eigentliche Bewertung erfolgt durch die Integrity Measurement Verifiers (IMV).

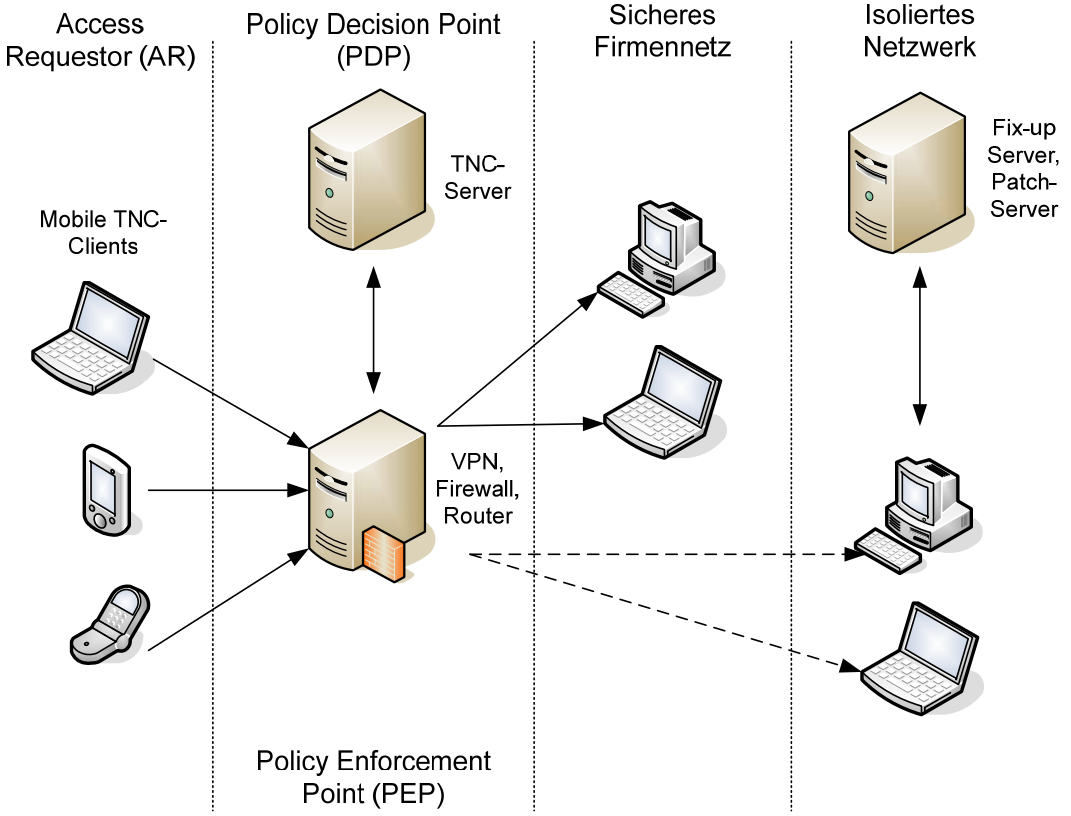

Abb. 1: Trusted Network Connect (TNC) Architektur

5 Der SIMOIT-Ansatz

Das SIMOIT-Projekt (http://www.simoit.de) zielt auf die Entwicklung einer auf Standards basierten mobilen IT-Sicherheitsplattform ab, die sich in heterogenen mobilen Umgebungen einsetzen lässt. Die in diesem Projekt erarbeiteten Lösungen sollen in unterschiedlichsten Unternehmen einsetzbar sein. Ziel war es, technische und auch nicht technische Lösungen als Baukastensystem zu entwickeln, die herstellerunabhängig entwickelt werden. Die nicht technischen Lösungen zielen darauf ab die Unternehmensführung über die Notwendigkeit der mobilen IT-Sicherheit zu überzeugen und die Akzeptanz der Mitarbeiter bzw. Benutzer zu erlangen.

5.1 Technische Plattform

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 sollte. Die Hauptplattform stellt dabei das Mobile Security Gateway (MSG) dar, welches aus verschiedenen Modulen (VPN, Firewall, TNC, RADIUS, LDAP) besteht. Dabei wurden speziell Open-Source-Software (OSS) Projekte und Ansätze untersucht, um eine offene, standardkonforme Umsetzung zu ermöglichen. Gleichzeitig ist man so flexibel geblieben, dass bestehende Komponenten wie z.B. Firewall-Systeme eingebunden werden können. In diesem Fall würde man das jeweilige SIMOIT-Modul nicht verwenden, sondern nur eine Schnittstelle zur Verfügung stellen. Die Anbindung an eine bestehende Inventory-Datenbank wurde ebenfalls vorgesehen, um die erlaubten Software-Versionen und Patch-Level abfragen zu können. Beim Pilotkunden war zusätzlich die Anbindung an einen internen Active-Directory-Server (ADS) notwendig, weshalb über LDAP auch hier eine Schnittstelle zur Verfügung gestellt wurde. Darüber werden auch sämtliche Benutzerprofile abgefragt, die für die Authentifizierung wichtig sind, und an den MSG weitergeleitet.

Um eine möglichst hohe Flexibilität auch für die Zukunft zu erhalten, wurde bei SIMOIT hauptsächlich Server-seitig die Entwicklung vorangetrieben, da man davon ausging, dass die Hersteller mobiler Endgeräte eigene Zugangssoftware in naher Zukunft bereitstellen werden. Auf Seite des Servers ist man dann so flexibel, dass beliebige TNC-Implementierungen angepasst werden können.

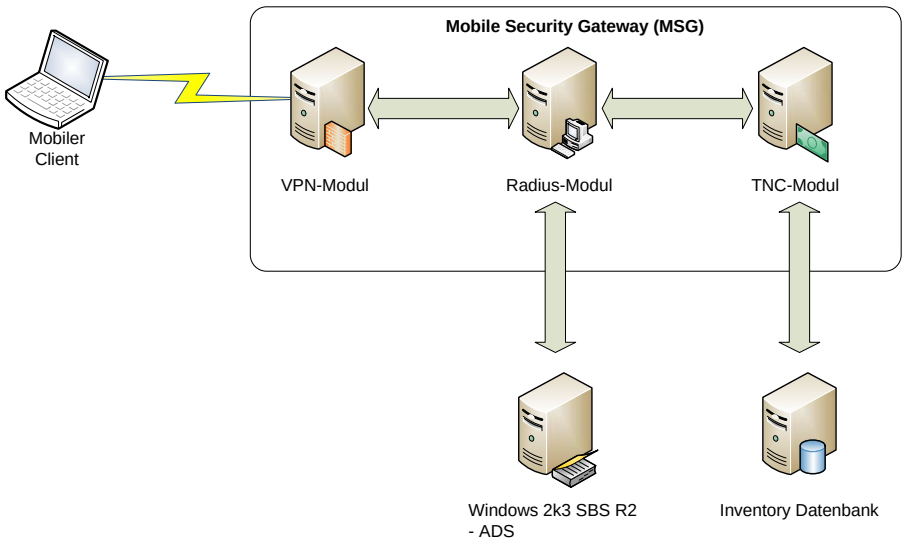

Abb. 2: Übersicht über die SIMOIT-Module

Der Kommunikationsablauf stellt sich bei SIMOIT nun wie folgt dar. In der Variante 1 versucht sich ein Mitarbeiter mit einem veralteten Softwarestand eines mobilen Systems in das Unternehmensnetz einzuwählen. Dabei wird zuerst eine Benutzerauthentifizierung vorgenommen, die er erfolgreich besteht. Auf Basis von Daten in der Softwareverteilung wird das mobile System in allerdings in die Quarantänezone verschoben. Der Mitarbeiter hat nun ausschließlich nur Zugriff auf Software-Updates, kann aber keinen internen Server erreichen. Dazu wird automatisch eine VPN-Verbindung aufgebaut und das VPN-Modul stellt einen „Radius Access Request“ an das RADIUS-Modul. Das RADIUS-Modul führt anschließend

eine Autorisierungsabfrage durch mittels Überprüfung durch einen „LDAP Request“ an den Windows 2003 Server. Erst dann fragt das TNC-Modul die Inventory-Datenbank auf kritische Softwarepakete ab. Die Authentifizierung wird durch das RADIUS-Modul mittels User und Passwort überprüft. Das RADIUS-Modul sendet die notwendigen Firewall-Einstellungen an das VPN-Modul zurück und die Regeln werden gesetzt.

In der Variante 2 wählt sich ein mobiler Mitarbeiter nach der Aktualisierung seines Systems erneut ein. Die Softwareverteilung meldet, dass das Gerät sich auf dem aktuellen Stand befindet und der Mitarbeiter erhält den vollen Zugriff auf das Unternehmensnetz.

In der Variante 3 wird das mobile Gerät von einem Hacker übernommen oder wird von einem Mitarbeiter missbraucht. Das Endgerät erlangt den Vollzugriff auf das Unternehmensnetz und startet einen Angriff. In diesem Fall wird das integrierte Intrusion Detection System (IDS) aktiv werden, welches im VPN-Modul integriert ist. Das IDS registriert den Angriff auf die Unternehmensressourcen und unterbindet den Zugriff im ersten Schritt. Mitarbeiter der IT können benachrichtigt werden, um weitere Aktionen zu veranlassen. [DGBS08]

5.2 Mechanismen der Quarantänezone

Auf dem Client wird der Zustand des aktuellen Softwarebestandes erfasst, um auf Basis dieser Informationen eine Integritätsentscheidung durchführen zu können. Außerdem sind Mechanismen vorhanden, die für das Update veralteter oder die Installation fehlender Software sorgen. Im Einzelnen gibt es folgende Komponenten auf dem Client, wie auch in Abb. 3 dargestellt ist:

- **Integrity Measurement Collectors:** Erfassen den aktuellen Zustand des Systems für definierte Teilbereiche, wie z.B. den Stand der Virendefinitionen oder die Version von Sicherheitssoftware.
- **TNC-Client:** Sammelt auf Anfrage die Informationen der Kollektoren, um diese für Integritätsentscheidungen des TNC-Servers weiterzuleiten.
- **Network Access Requestor:** Verbindet den Client für das VPN mit dem Unternehmensnetz. Bietet in der Authentisierungsphase den Kanal für die Übertragung von Zustandsinformationen zum TNC-Server und Sicherheitsrichtlinien zum TNC-Client.
- **Softwareverteiler-Client:** Falls der Client die Softwarebestandsanforderungen nicht erfüllt, lässt der TNC-Client anhand der Security Policy die jeweilige Komponente neue Softwarepakete installieren.
- **Software-/Datenempfänger:** Empfängt Benachrichtigungen über neue Softwareversionen und aktualisierte Security Policies, um automatisiert den Softwarebestand auf dem aktuellen Stand zu halten. Außerdem ruft diese Komponente nach Anweisung durch den Softwareverteiler-Client die Softwarepakete ab und stellt sie der Softwareinstallation zur Verfügung.
- **Softwareinstallation:** Nach dem Abruf von Installationspaketen sorgen automatisierte Installationsabläufe für eine möglichst geringe Belastung des Endanwenders.

Die aktuellen Sicherheitsrichtlinien sollten dabei im Unternehmensnetz zum Abruf bereitstehen. Falls die Installation des mobilen Sicherheits-Clients mit der Verbindung zum Unternehmensnetz erfolgt, wird die aktuelle Version der Security Policy direkt geladen. Alternativ muss erst eine VPN-Verbindung zum Unternehmensnetz hergestellt werden. Hierbei scheitert die Überprüfung der Zuverlässigkeit des mobilen Systems, da bisher keine Sicherheitsüber-

prüfung angewandt wurde und damit wahrscheinlich auch der Softwarebestand nicht ausreichend ist. Im Quarantänebereich kann der Sicherheits-Client die Security Policy aber erhalten und anwenden, so dass bei der nächsten Verbindung mit dem VPN-Server ein voller Zugang zum Unternehmensnetz ermöglicht werden kann.

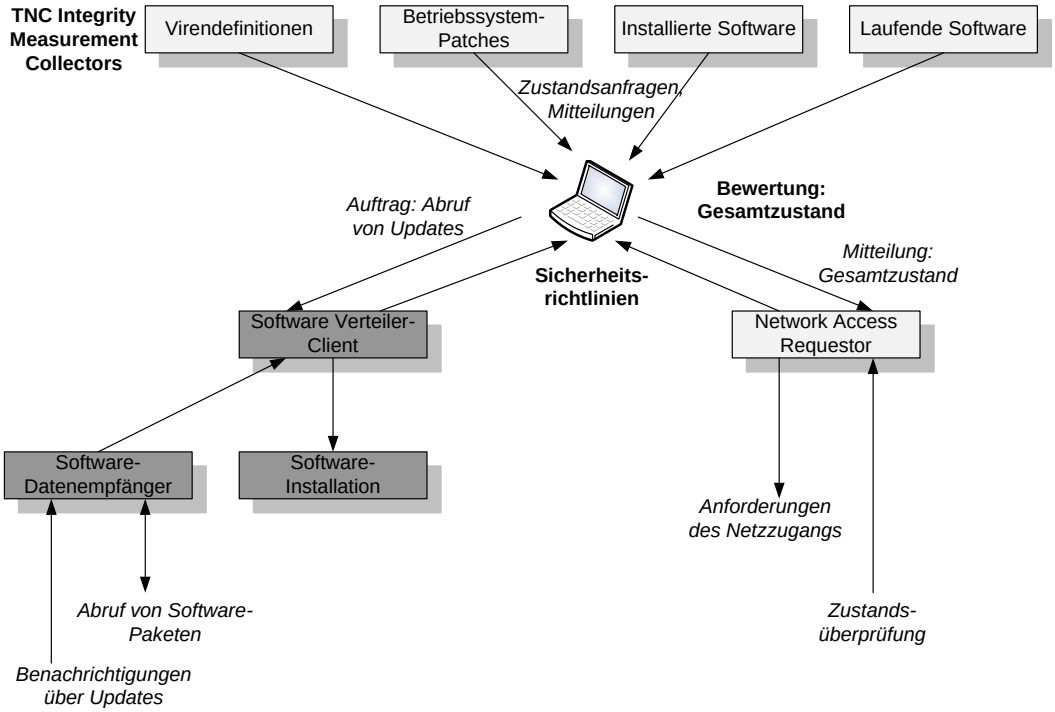

Abb. 3: Client-Architektur

Zur Überprüfung des Client-Zustandes werden entsprechend der Sicherheitsrichtlinie Software-Versionsstände, zusätzlich installierte Software, laufende Sicherheitsapplikationen und deren Zustand (z.B. Aktualität von Virendefinitionen) analysiert. Der TNC Integrity Measurement Collector liefert dabei jeweils komponentenspezifische Zustandsinformationen, die vom mobilen Sicherheits-Client zusammengetragen werden. Dadurch kann sichergestellt werden, dass diese Zustandsüberprüfung zu einem identischen Ergebnis kommt wie die Überprüfung des Autorisierungs-Servers.

Auf Serverseite werden die Zustände der Clients während der Authentisierung überprüft. Wenn diese nicht ausreichen, werden entsprechende Softwarepakete zur Verfügung gestellt, die zum Erreichen des benötigten Zustandes führen.

Der mobile Sicherheits-Client ist für die Einhaltung der Sicherheitsrichtlinien des Unternehmens zuständig. Hier muss formuliert und beschrieben sein, in welchem Zustand das mobile Gerät sich befinden darf, um Zugriff auf das Unternehmensnetz zu erhalten. Die Sicherheitsrichtlinie beinhalten dabei Informationen, wie z.B. notwendige Software in verschiedenen Versionen und zu startende Sicherheitsapplikationen.

Die Softwareverteilung kommt zum Einsatz, wenn mobile Clients per Aktualisierung der Sicherheitsrichtlinien oder nach der Ablehnung des aktuellen Systemzustandes zum Installieren von Softwarepaketen angehalten werden. Eine Distributionsplattform hält die aktuell zu verteilenden Softwarepakete bereit, so dass mobile Clients diese per HTTP unter den in der Security Policy angegebenen Adressen abrufen können. Der Zugriff ist bei Konnektivität zum Unternehmensnetz oder bei bestehender Quarantäne-VPN-Verbindung möglich. [DETK08]

5.3 Implementierung

Die Implementierung der Hardwareplattform wurde mit vier Servern realisiert, wobei zwei Server für die Einwahl zuständig sind und zwei weitere Server die Daten für die Authentizierung vorhalten (Nutzerdaten und Softwarestand des einzuwählenden Gerätes):

- **VPN-Gateway:** dient als Endpunkt des IPsec und nutzt X.509-Zertifikate für die Endgeräte. Durch den IPsec-Tunnel wird mittels L2TP mit PPP die Authentifizierung durchgeführt. Auch die Zertifikats-ID des VPN-Tunnels wird ermittelt und mit den Anmeldedaten an den RADIUS-Server weitergeleitet.
- **RADIUS-Server:** übernimmt die Autorisierung und Authentifizierung des Benutzers und des Gerätes. Er entscheidet aufgrund der Antwort des TNC-Moduls, ob der eingewählte Client Vollzugriff erhält oder lediglich in das Quarantänenetz gelangt.
- **Windows 2003 Active Directory Server:** Im Active Directory liegen die Benutzerdaten, die vom RADIUS-Server abgefragt werden. Es kann auch ein LDAP-Server verwendet werden.
- **Softwareverteilung:** hält die Informationen der installierten bzw. nicht installierten Paketen vor. Diese Informationen werden vom RADIUS-TNC-Modul ausgewertet.

Das TNC-Modul bei SIMOIT ist ein FreeRadius-Modul. Das Modul dient als Serverkomponente des TNC-Systems und entscheidet als PDP, aufgrund der Daten, die vom Inventory Integrity Measurement Validator (Inventory-IMV) zurückgeliefert werden, in welches Netz der TNC-Client gelangen wird. Als Komponenten enthalten sind neben FreeRadius und der Inventory-IMV, der TNC-Server mit der libtnc (Open-Source-Bibliothek).

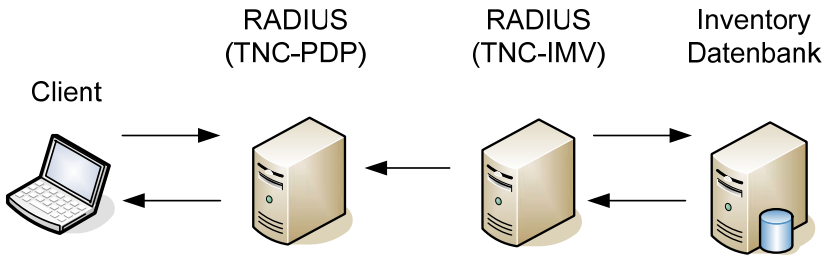

Abb. 4: TNC-Kommunikation

Die TNC-Implementierung ist auf die Serverseite konzentriert. Dem RADIUS-Server werden über das FreeRadius-Modul TNC-Server auf Anfrage Zustandsinformationen der sich anmeldenden Geräte mitgeteilt. Dazu wurde das TNC-Framework „libtnc“ eingebunden.Es kann entsprechend der Konfiguration dynamisch verschiedene Validatoren zur Zustandsermittlung heranziehen. Implementiert wurde der Validator Inventory-IMV, der die Inventardatenbank zum Softwarestand des Endgerätes anfragt und das Ergebnis mit den aktuell notwendigen kritischen Updates für das Gerät vergleicht.

Der Inventory-IMV wurde mit Hilfe der HTTP(s)GET/XML-Methode implementiert. Es werden dafür folgende Abfragen benötigt:

- **Softwarepakete:** Die zugehörige HTTP-URI lautet „inventory/packages“. Als Antwort wird eine XML-Datenstruktur zurückgegeben, die die verschiedenen Softwarepakete enthält.

- **Softwarestände auf Gerät:** Die zugehörige HTTP-URI lautet „/inventory/device/[device-id]/packages. Als Antwort wird auch hier eine XML-Datenstruktur zurückgegeben.

Über den Statuscode kann die erfolgreiche Übermittlung (Code 200), der Fehlerfall (Codes 404) für ein unbekanntes Gerät, sowie das Nichterreichen des Inventory-Servers (Code 503) erkannt werden. Diese Abfragen werden automatisch vom Radius-TNC Modul bei einer Einwahl durchgeführt.

Die Paketverwaltung der Software-Stände wurde mithilfe der relationalen Datenbank SQLite realisiert. SQLite hat nicht wie die meisten anderen Datenbanksystem einen Serverprozess, sondern liest die Daten bei Bedarf aus regulären Dateien aus. Hier werden alle Daten der Endgeräte (MAC-Adresse, fortlaufende Nummer, ID des Gerätetyps) und der installierten Softwarebasis (Software-ID, Status-ID) gehalten. Es können dabei unterschiedliche Softwareverteilungslösungen verwendet werden. Allerdings muss dabei jeweils eine Anpassung der Datenbankfelder durchgeführt werden. Dabei müssen folgende Informationen vorhanden sein: welches Softwarepaket muss auf dem Client installiert werden, ist das Paket bereits installiert und wird das Paket als kritisch eingestuft. Diese Informationen werden verwendet, um die XML-Dateien zu erstellen, die der TNC-IMV-Server zwecks Netzzuordnung benötigt.

Die Anbindung an den Verzeichnisdienst des Unternehmens kann auf Basis von LDAP oder Active Directory (AD) erfolgen. Im Fall der AD-Nutzung musste für die Zuordnung der Netzzugänge (internes Firmennetz, Quarantäne) eine kleine Schemaänderung des Active Directory vorgenommen werden, da es in AD-Attributen keine Auswahl für das Netz gibt. Durch die positive Überprüfung des Softwarestandes des Clients durch das TNC-Modul wird dann das Attribut geändert, das an das AAA-Modul und anschließend an das VPN-Modul weitergeleitet wird. Dieses setzt dann die Firewall-Regeln entsprechend für den Client und ermöglicht abschließend den Zugriff auf das interne Firmennetz. [ROSE09]

6 Fazit

Der TNC-Ansatz wird immer noch speziiert, liegt aber seit 2008 auch endlich in der Version 1.3 [TCG08] vor. Die führenden Hersteller wie Microsoft und Cisco Systems gingen dabei zuerst eigene Wege. Unter dem Stichwort Network Admission Control (NAC) hat Cisco Systems eine Enforcement- und Quarantäne-Technologie auf API-Ebene entwickelt, die in die Cisco-Netzwerkinfrastruktur eingebaut ist. Um eine Authentifizierung und Autorisierung der Benutzer zu realisieren, wird das vertrauenswürdige Modul (Cisco Trusted Agent) verwendet, das auf den Endsystemen installiert und in Cisco-Routern und Switches eingebaut sein muss. NAC erfordert also eine aktuelle IOS-Version auf der Cisco-Infrastruktur. Eine Vielzahl von Prozessen wird von der Cisco-Architektur realisiert, um Zugang zum Netz zu ermöglichen und gleichzeitig Sicherheit gewährleisten zu können.

Der Ansatz von Microsoft lautet Network Access Protection (NAP) und ist in der Funktionsweise nahezu identisch mit der TNC-Architektur. Jedoch unterscheidet sich die entwickelte NAP-Technologie durch die Namensvergabe einzelner Komponenten. Der NAP-Client entspricht hierbei dem TNC-Client und der TNC-Server dem Network Policy Server (NPS). Der Integrity Measurement Collector ist mit dem System Health Agent (SHA) vergleichbar. Die Aufgabe des Integrity Measurement Verifiers wird vom System Health Validator ersetzt. Nachdem Microsoft sich erst vom TNC-Ansatz trennen wollte, um eigene Wege zu beschrei-

ten, hat man sich inzwischen wieder dazu bekannt. Somit steht momentan der Netzwerkhersteller Cisco Systems alleine mit einem proprietären Ansatz dar, den auch die anderen Hersteller haben sich zu den TNC-Spezifikationen bekannt.

Das ursprüngliche SIMOIT-Projekt hat die Bedeutung von TNC bereits früh erkannt und eigene Wege beschritten. Aufgrund der fehlenden TNC-Client-Implementierungen wurde deshalb eine reine Serverlösung umgesetzt, die modular aufgebaut ist und mit anderen Sicherheitskomponenten genutzt werden kann. Durch den Einsatz einer Softwareverteilung wird das Fehlen des TNC-Clients kompensiert. Wenn die Entwicklung hier weitergeht und Betriebssystemhersteller die notwendige TNC-Implementierung liefern, kann SIMOIT dementsprechend erweitert werden. Bis dahin muss eine geeignete Softwareverteilungslösung die fehlende TNC-Clientfunktion kompensieren. Durch die zentrale Erfassung der Benutzer und Softwarestände auf einem internen AD-Server sowie in der Softwareverteilung, ist mittels des TNC-Ansatzes im SIMOIT-Projekt ein Identity Management möglich geworden, das sich nicht nur auf mobile Endgeräte beziehen muss. Durch Einführung dieser Mechanismen kann ein Unternehmen seine Sicherheitsrichtlinien auf die mobilen Endgeräte erweitern, die bislang ein Eigenleben führen, da sie nicht permanent für den IT-Administrator erreichbar sind.

7 Literaturverzeichnis

[DEER06] Detken, Eren: Mobile Security - Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit. 672 Seiten; Hanser Verlag; ISBN 3-446-40458-9; München 2006

[DETK08] K.-O. Detken: Trusted Network Connect - die sichere Einwahl mobiler Mitarbeiter ins Unternehmen; Handbuch der Telekommunikation; Deutscher Wirtschaftsdienst; 129. Ergänzungslieferung von April; Köln 2008

[DGBS08] Detken, Gitz, Bartsch, Sethmann: Trusted Network Connect - sicherer Zugang ins Unternehmensnetz; D.A.CH Security 2008: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven; Herausgeber: Patrick Horster; syssec Verlag; ISBN 978-3-00-024632-6; Berlin 2008

[ITW05] IT-Wissen http://www.itwissen.info/,http://www.itwissen.info/definition/lexikon/IT-Sicherheit-IT-security.html

[MUEL08] Müller, T.: Trusted Computing Systeme Konzepte und Anforderungen, Springer Verlag 2008, ISBN 978-3-540-76409-0, Berlin Heidelberg

[NISP08] Markus Nispel; Enterasys Secure Networks: Was Sie über NAC wissen sollten. http://www.computerwoche.de/knowledge_center/security/1871427/index.html

[ROPR08] Ben Rothke und Peter Riedelberge: Endpoint-Security-Lösungen verschiedener Hersteller im Vergleich, http://www.searchsecurity.de/ 18.03.2008

[ROSE09] Raphael Rosendahl: Mobile Netzwerksicherheit, Diplomarbeit, Hochschule Bremen, Studiengang: Technische Informatik, Bremen Februar 2009

[TCG08] TCG Trusted Network Connect TNC Architecture for Interoperability; Specifcation 1.3; Revision 6; April 2008

[TCG05] Trusted Computing Group, https://www.trustedcomputinggroup.org/home/