# Vertrauenswürdiger mobiler Zugriff auf Unternehmensnetze im VOGUE-Projekt

Prof. Dr. Kai-Oliver Detken[1], Günther Diederich[2], Adrian Nowak[3]

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

[2]Hochschule Bremen, Flughafenallee 10, D-28199 Bremen
guenther.diederich@hs-bremen.de

[3]OTARIS Interactive Services GmbH, Fahrenheitstr. 1, D-28359 Bremen
nowak@otaris.de

## Zusammenfassung

Durch Einführung von mobilen Endgeräten wächst der IT-Schutzbedarf stark. Während sich früher Angriffe vor allem gegen die Server richteten, verlagern sie sich heute nicht nur auf die Firewall und das VPN-Gateway, sondern wenden sich auch direkt gegen Endgeräte, die sich zeitweilig außerhalb des sicheren Netzes befinden. Denn wer sie kompromittiert, der erlangt in vielen Fällen zugleich einen bequemen Zugang ins Unternehmensnetz. Natürlich haben sich bereits Lösungen etabliert, die helfen sollen mobile Geräte abzusichern. Allerdings sind diese meist plattformspezifisch (Symbian OS, Blackberry oder Windows Mobile). Anforderungen und Maßnahmen an mobile Endgeräte in Sicherheitsstandards (z.B. ISO27001, IT-Grundschutz) fokussieren den Einsatz innerhalb einer Arbeitsumgebung, berücksichtigen jedoch nicht deren Einsatz in Umgebungen verschiedener Betreiber (z.B. beim einem Dienstleister oder dessen Kunden). Neben mehr Interoperabilität wäre daher eine Distributionsplattform wünschenswert, die Software an mobile Endgeräte sicher verteilt und dabei die Installation von Schadsoftware verhindert. Der Beitrag geht daher kurz auf die neuen Sicherheitsbedrohungen mobiler Endgeräte ein und zeigt die Standards im Umfeld Trusted Computing auf. Darüber hinaus werden die ersten Ergebnisse des Projektes VOGUE präsentiert, das ein höheres mobiles Sicherheitsniveau erreichen will.

# 1 Einleitung

Mobile Endgeräte, z.B. Mobiltelefone oder Smartphones, werden zunehmend mit integrierten Anwendungen wie Terminplanung, elektronische Notizblöcke oder E-Mails eingesetzt. Dabei werden zunehmend Unternehmensdaten auf den elektronischen Begleitern mitgenommen. Allerdings sind die mobilen Endgeräte im Unterschied zu normalen Arbeitsplatzrechnern schlechter in herkömmliche betriebliche IT-Infrastrukturen integriert. Der Zugriff und die Synchronisation der Daten der mobilen Endgeräte erfolgen durch spezielle Software. Zudem sind die wenigen vorhandenen Sicherheitsmechanismen kaum ausreichend, um vertrauliche persönliche oder geschäftskritische Daten zu schützen. Der Verlust eines Gerätes bringt fast immer auch den Verlust der Vertraulichkeit der Daten mit sich.

P. Horster (Hrsg.) · D.A.CH Security 2010 · syssec (2010) pp.

Folgende Entwicklungen lassen sich heute im mobilen Umfeld ausmachen:

a. **Mobiler Endgeräte:** Die technische Entwicklung ermöglicht sowohl eine zunehmende Integration von Funktionalitäten und Schnittstellen in mobile Endgeräte als auch die Zusammenführung ursprünglich verschiedener Geräteklassen wie beispielsweise Mobiltelefon und PDA in ein einziges Gerät. Darüber hinaus werden die Geräte immer leistungsfähiger und der Grad der Vernetzung wächst sowohl quantitativ durch die Anzahl zur Verfügung stehender Kommunikationskanäle als auch qualitativ durch gesteigerte Übertragungsraten oder andere Übertragungsformen wie Ad-hoc-Vernetzung. Im Kommunikationsbereich werden die Teile, die heute in Hardware realisiert sind, zunehmend in Software realisiert werden. Mobile Endgeräte werden zudem immer mehr als digitale Assistenten oder persönliche Hilfsmittel eingesetzt.

b. **Dienste:** Im Bereich der Dienste ist eine verstärkte Verbreitung von echten mobilen Diensten festzustellen. Das heißt, es werden immer mehr Dienste eingesetzt, die sich der spezifischen Eigenschaften und Fähigkeiten der mobilen Endgeräte bedienen. Neue Benutzungsparadigmen wie „Digital Lifestyle“ oder „Ubiquitous Computing“ verändern dabei die Anforderungen an mobile Dienste. Bedienbarkeit und Kommunikationsfähigkeit spielen hierbei eine hervorgehobene Rolle. Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet und in vielen Fällen zur Verlagerung der Funktionalitäten.

Aus diesen Entwicklungen lässt sich ableiten, dass sich neue Sicherheitsanforderungen ergeben bzw. die Bedrohungslage sich verändert. Es ist abzusehen, dass ähnliche Angriffe, wie sie heute bei PCs und anderen Rechnersystemen bekannt sind, in Zukunft in deutlich stärkerem Umfang auch bei mobilen Endgeräten auftreten werden. Monokulturen von Software und Hardware können diese Bedrohungslage drastisch verschärfen. Da der Einsatzbereich eines mobilen Endgerätes vom Arbeitsgerät hin zum persönlichen Life-Style-Produkt reicht, entstehen neue Anwendungsaspekte, wie Mobilität, langer Batteriebetrieb und neue Kommunikationstechnologien. Im Vergleich zu klassischen Rechnern entstehen durch die Veränderung der Benutzungsparadigmen und wegen neuer Anwendungsszenarien neuartige Bedrohungen. [BSI06]

Aus den neuen Sicherheitskriterien heraus, die auch mobile Teilnehmer mit einbeziehen müssen, ergeben sich neue Anforderungen an mobile Endgeräte. Diese ergeben sich alleine schon durch ihre Mobilität, im Gegensatz zu fest installierten Endgeräten. Diese macht die Endgeräte leichter angreifbar und auch die Nutzung unterschiedlicher Netzzugänge lassen PDAs, Laptops etc. nicht wie statische Endgeräte im administrativen Alltag handhaben:

a. **Recovery:** Notebooks – lassen sich beispielsweise mit Hilfe einer Recovery-Partition auf einer lokalen Festplatte oder durch einen externen Datenträger wiederherstellen, den Mitarbeiter immer mitführen. Damit ist es möglich, bei intakter Hardware Fehler im Bereich des Betriebssystems oder der Anwendungssoftware zu beheben. Smartphones und ähnliche Geräte lassen sich über eine Speicherkarte leicht mit einem neuen System versorgen.

b. **Remote-Installation:** Sie erfordert ein Minimal-Betriebssystem mit den nötigen Treibern für die Konnektivität. Damit kann das Endgerät eine Verbindung zur Zentrale aufnehmen und die benötigten Programme von dort installieren. Das erfordert eine Software-Verteilerlösung, die auch über Firmengrenzen hinweg funktioniert. Ein

Problem stellt hier allerdings die Datenmenge beziehungsweise die nötige Downloadzeit bei einer schmalbandigen Verbindung dar.

c. **Patchlevel:** Damit ein mobiles Endgerät die Erlaubnis erhält, sich mit dem Firmennetz zu verbinden, sollte es einen bestimmten Patchlevel nachweisen können. Die Patches kann beispielsweise eine Software-Verteilerlösung bereitstellen. Je nach Strenge der Security Policys kann das in einer Quarantänezone erfolgen.

d. **Quarantänezone:** Dabei handelt es sich um einen vom Firmennetz getrennten Bereich mit einem Mechanismus für die Softwareverteilung. Er hält alle aktuellen Patches vor, dazu Daten für sicherheitsrelevante Dienste wie Anti-Viren- oder Anti-Spy-Definitionen. Das mobile Gerät muss diese Quarantänezone passieren, um in das lokale Netz zu kommen. Fehlen ihm Patches, aktualisiert es hier seinen Bestand.

Die Authentifizierung der mobilen Mitarbeiter kann auf Benutzer- wie auf Hardwareebene erfolgen. Sie überprüft zum einen, ob das Gerät im Firmennetz erlaubt ist und in einer zweiten Stufe, ob der jeweilige Teilnehmer berechtigt ist, der sich anzumelden versucht. Diesen Ansatz verfolgt der Standard „Trusted Network Computing“ (TNC), der im Folgenden kurz dargestellt wird. [DGBS08]

# 2 Die TNC-Spezifikation

Die Trusted Computing Group (TCG) entwickelte mit der Spezifikation Trusted Network Connect (TNC) einen Ansatz, um die „Reinheit“ von Endpunkten sicherstellen zu können. Das heißt, es kann durch Authentifizierungs- und Autorisierungsinformationen eine Zustandsprüfung („Health Check“) erfolgen, die sicherstellt, dass das Endgerät den IT-Sicherheitsregeln des Unternehmens entspricht. Die TNC-Architektur ist somit die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten. Die Architektur bezieht dabei schon bestehende Sicherheitsaspekte, wie Virtual Private Network (VPN), IEEE 802.1x (802.1x), Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), Hyper-Text Transfer Protocol Security (HTTPS) und RADIUS mit ein.

Als Besonderheit bietet TNC optionale Hardwareunterstützung mit dem Trusted Platform Module (TPM) oder dem Mobile Trusted Module (MTM) an, mit dem die Sicherheit von TNC erhöht werden kann. So machte das TPM es unter anderem möglich, dass nur signierte Software auf einem System aufgeführt werden kann. Während das TPM schon serienmäßig in Hardware (z.B. von IBM) eingebaut wird, existiert jedoch das MTM bisher noch als Entwurf. Die Einführung des MAP-Servers ermöglicht zusätzlich noch das Weglassen einer dedizierten Hardwareunterstützung bei ähnlichem Sicherheitsgrad. [EUD09]

Die Architektur des Trusted Network Connects ist von der Trusted Computing Group in der Spezifikation 1.4 (Revision 4) vom Mai 2009 veröffentlicht worden [TNC01]. Wie in Abb. 1 zu erkennen 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 zusam-

mengefasst. Diese drei abstrakten Layer sind waagerecht über die Komponenten der drei Einheiten gelegt worden. Das Zusammenwirken der einzelnen Komponenten wird durch Interfaces realisiert. Neu in der aktuellen Spezifikation ist der Metadata Access Point (MAP), der die zusätzlichen Sicherheitskomponenten von MAP-Clients mit anbindet.

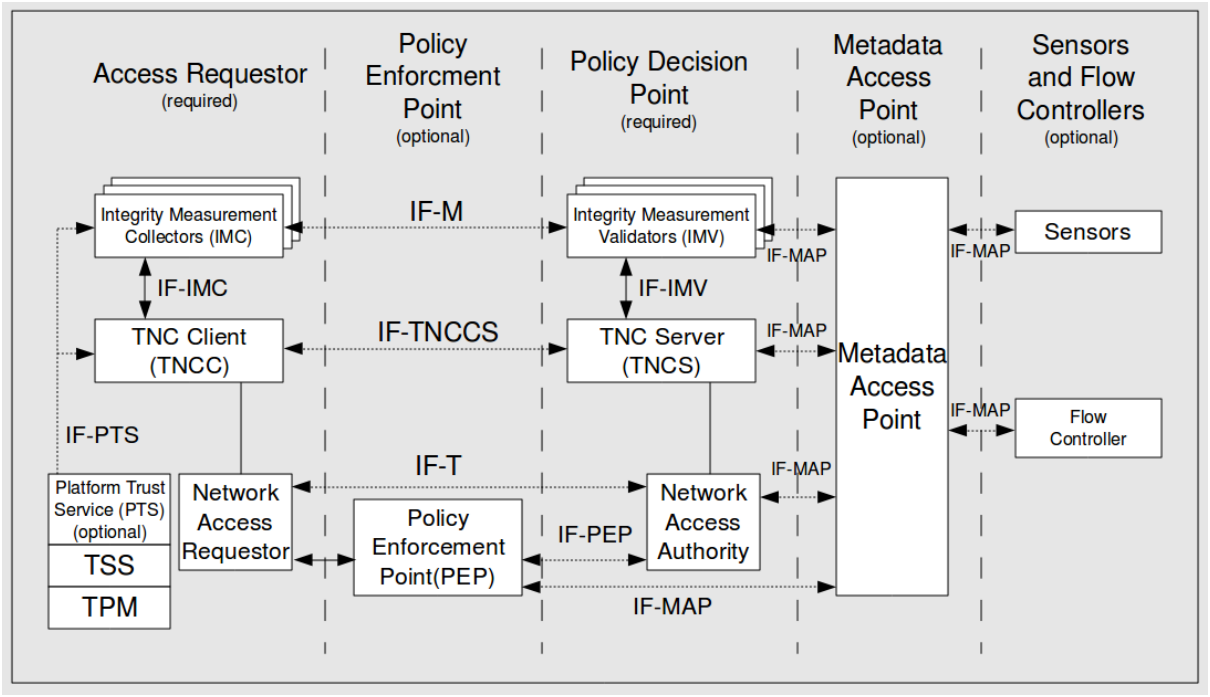


**Abb. 1:** TNC-Architektur [TNC02]

Die Einheiten besitzen die folgenden Aufgaben:

a. **Access Requestor (AR):** Der Access Requestor stellt die Verbindung in ein geschütztes Netzwerk her. Er muss in der TNC-Architektur auf jeden Fall umgesetzt werden.

b. **Policiy Decision Point (PDP):** Der PDP entscheidet für die Anfrage des AR, wie die Zugriffsrechte für die Verbindung aussehen. Er muss in der TNC-Architektur ebenfalls umgesetzt werden.

c. **Policy Enforcement Point (PEP):** Der PEPbildet die von dem PDP erhaltenen Zugriffsberechtigung des AR ab. Er wird als optional angesehen.

d. **Metadata Access Point (MAP):** Der MAP speichert und liefert Zustandsinformationen über die ARs. Der MAP wird ebenfalls als optionaler Bestandteil angesehen.

e. **MAP-Client (MAPC):** Die Rolle des MAP-Clients beinhaltet das Veröffentlichen oder das Konsumieren der Zustandsinformationen des MAP über die ARs. Auch dieser Bereich wird als optional angesehen.

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. Der AR beinhaltet in der Architektur die folgenden Komponenten:

a. **Network Access Requestor (NAR):** Der NAR ist eine Einheit (z.B. Software-Komponente), welche die Verbindung zu einem Netzwerk herstellt. Es ist nicht ausge-

schlossen, dass auf einem AR mehrere NARs installiert sind, die die Verbindung zu verschiedenen Netzwerken ermöglichen.

b. **TNC Client (TNCC):** Der TNC-Client (Software-Komponente) sammelt die von den IMCs erhaltenen Daten und sendet diese an den TNC-Server. Sind nicht alle Statusinformationen über die IMCs abrufbar, kann der TNC-Client zusätzlich selbst Informationen über den Status des Systems abrufen.

c. **Integrity Measurement Collector (IMC):** Die Integrity Measurement Collectoren sind Software-Komponenten, die den Status des AR (z.B. aktuelle Patch-Infos, aktuelle Viren-Signaturen, Software-Versionen oder den Firewall-Status) an den TNC-Client melden. In der TNC-Architektur ist vorgesehen, dass mehrere IMCs auf einem AR installiert sein können und das diese IMCs auch ihre Status-Informationen an mehrere TNC-Clients melden können.

Der PEP beinhaltet als Komponente nur den Policy Enforcement Point. Diese Komponente regelt die Zugriffe auf das Netzwerk (z.B. durch Access-Listen oder durch VLANs). Der PEP erhält die Berechtigungen für den AR von dem PDP.

Der PDP beinhaltet in der Architektur die folgenden Komponenten:

a. **Network Access Authority (NAA):** Der NAA entscheidet, ob der AR Zugang zu dem Netzwerk erhält. Er kontaktiert den TNCS und fragt dort den Sicherheitsstatus des AR ab.

b. **TNC Server (TNCS):** Der TNC-Server steuert den Datenaustausch zwischen den IMV und dem IMC, sammelt die Empfehlungen (z.B. von dem IMV) und leitet daraus eine Sicherheitsstufe für den NAA ab.

c. **Integrity Measurement Verifier (IMV):** Der IMV verifiziert (z.B. mit Hilfe eines Integritätstests) den AR anhand der Daten von den IMCs.

Demnach sind die wichtigsten Bestandteile einer TNC-Architektur der Access Requestor (AR) und der Policy Decision Point (PDP). Erweitern lässt sich diese Infrastruktur zusätzlich mit dem Plattform Trust Service (PTS), dem Policy Enforcement Point (PEP) und dem Metadata Access Point (MAP) sowie daran angeschlossenen Metadata Access Point Clients (MAP-C). [DET09]

Folgendes kurzes Szenario kann zum besseren Verständnis herangezogen werden. Der AR versucht auf ein geschütztes Netzwerk zuzugreifen. Der PDP vergleicht nun die vom dem AR gelieferten Informationen über sich selbst (z.B. Plattform, Benutzerzertifikate, Passwörter, etc.) mit den im Netzwerk geltenden Zugriffsbeschränkungen und entscheidet dann, ob und wie dieser AR Zugriff zu dem Netzwerk bekommt oder nicht. Wenn ein PEP im Netzwerk vorhanden ist, wird die Entscheidung des PDP zuerst an diesen weitergeleitet und dieser legt fest, aufgrund der Entscheidung des PDP, wie mit diesem AR weiter zu verfahren ist. Über den MAP können MAP-Clients den Zugriff des AR weiter einschränken bzw. dessen Sicherheitsstatus beobachten und aufgrund von Sicherheitsverletzungen den PDP oder, wenn vorhanden, den PEP dazu auffordern, den AR in einen anderen Bereich des Netzwerks unterzubringen bzw. ihm den Zugang teilweise oder komplett zu verweigern.

Man kann daher die Aufgaben von TNC wie folgt zusammenfassen:

a. Eindeutige Erkennung von Zugangsversuchen und die Identifizierung der Endgeräte

b. Vergleich mit den und das Umsetzen von Sicherheitsrichtlinien
c. Isolierung und im besten Fall die automatische Korrektur bei fest gestellten Richtlinienverletzungen
d. Erstellung und Verwaltung der Richtlinien sowie die Auswertung der Ereignisse und gesammelten Daten

# 3 Das VOGUE-Projekt

Bei der Komplexität des TNC-Ansatzes, stellt sich natürlich die Frage der Umsetzbarkeit. Bereits die erste Phase des Verbindungsaufbaus enthält die Problematik, dass die zuverlässige Erkennung der Verbindungsart und des Endgerätes garantiert werden muss. Anschließend muss das Endgerät anhand der MAC- oder IP-Adresse dem Netzwerk zugeordnet werden, indem man den ARP-Datenverkehr ausliest. Bei einem Tunnelaufbau mittels VPN kann die Verbindungsanfrage durch den VPN-Mechanismus klar zugeordnet werden. Ohne VPN-Technik ist man auf das Erkennen von DHCP-Anfragen im Netz angewiesen. Eine zusätzliche Schwierigkeit kommt hinzu, wenn man nicht voraussetzt, dass der Teilnehmer mit seinem Endgerät ausschließlich gute Absichten verfolgt. Wenn das Endgerät mit Malware infiziert ist oder ein Angreifer direkt versucht in das Unternehmensnetz zu gelangen, wird der offizielle Verbindungsversuch unterdrückt werden. Der TNC-Ansatz muss dann beurteilen, ob das Endgerät den Zugang erhält oder nicht. Zusätzlich muss er dem Endgerät das Netz ein Stück weit öffnen. Sobald dann der Angreifer eine Verbindung erhält, besitzt er auch weitere Möglichkeiten, um Sicherheitslücken auszukundschaften. Es gibt hier mannigfaltige Angriffsmöglichkeiten. Problematisch ist auch, dass der Quarantänebereich für unsichere Endgeräte die Möglichkeit bietet andere Teilnehmer anzugreifen, die ebenfalls nicht eingelassen werden. Da auch diese Endgeräte Sicherheitsschwächen haben werden, ist die Chance auf Erfolg höher, als in sicherer Umgebung. [TOER09b]

An diesem einfachen Beispiel sieht man bereits, dass eine Umsetzung nicht per Installationsroutine durchgeführt werden kann. Man sollte konzeptionell die Anforderungen an ein solches System im Vorfeld erarbeiten und dann die technischen Systeme dementsprechend umsetzen. Aufgrund der neuen und wachsenden Herausforderungen, die an die Vertrauenswürdigkeit von Mobiltelefonen gestellt werden, wird in dem VOGUE-Projekt (http://www.vogue-project.de) eine Plattform zur Absicherung mobiler Endgeräte entwickelt, die auf mobilen Endgeräten nutzbar ist. Aufgrund der Quelloffenheit und definierten Schnittstellen, wurde dafür exemplarisch das Google-Betriebssystem Android (http://www.android.com) ausgewählt. VOGUE wird eine Sicherheitsplattform zur Verfügung stellen, die Mechanismen für eine vertrauenswürdige Geräteauthentisierung enthält. Anhand des definierten generischen Szenarios, das im nächsten Unterkapitel dargestellt wird, soll der Sicherheitsgewinn nachgewiesen werden, der durch die Ergebnisse des VOGUE-Projektes erzielt werden kann. Die in VOGUE entwickelte Sicherheitslösung für Mobiltelefone wird aber nicht nur auf das nachfolgende Anwendungsszenario beschränkt bleiben, sondern kann grundsätzlich zur Absicherung mobiler Applikationen eingesetzt werden können.

## 3.1 Generisches Anwendungsszenario

Im ersten Schritt wurden im VOGUE-Projekt verschiedene technik- und anwendungsorientierte Szenarien mit unterschiedlicher Sichtweise definiert und zusammengestellt, um ein Si-

cherheitsszenario entwickeln zu können. Dabei wiesen alle unterschiedlichen Szenarien eine Gemeinsamkeit auf, die zu einem generischen Szenario zusammengefasst wurden. So wurden beispielsweise in allen Szenarien mobile Geräte für den Zugriff auf vertrauenswürdige Infrastrukturen eingesetzt. Ein Teil der Verbindung erfolgt dabei über ein unbekanntes und somit nicht vertrauenswürdiges Netz, die Art der Verbindung ist dabei nicht auf eine bestimmte Technik festgelegt (z.B. WLAN oder UMTS). Eine Maßnahme zur Absicherung, die nach derzeitigem Stand der Technik in allen Szenarien eingesetzt werden kann, ist die VPN-Technik (Virtual Private Network). Das VPN-Szenario ist somit grundlegender Teil aller Szenarien und damit auch des generischen Szenarios, in dem als Bestandteil ein Sicherheitsgateway eingesetzt wird.

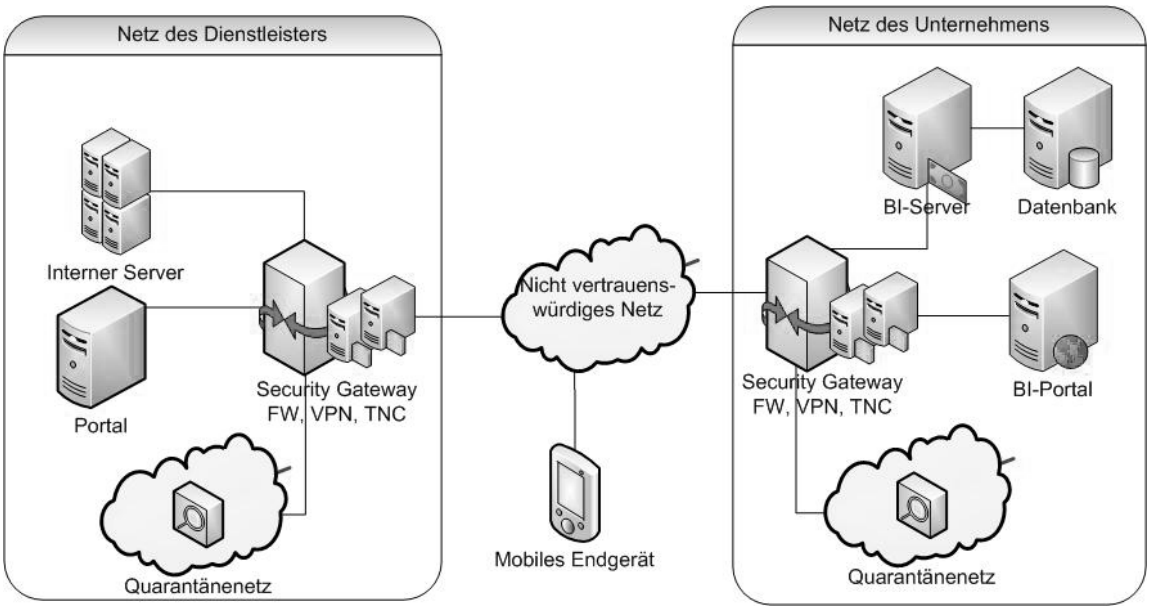


**Abb. 2:** Kooperation von Dienstleister und Unternehmen zum sicheren Datenaustausch

Alle Szenarien fokussieren ganz oder teilweise die sichere Einbindung externer Fachkräfte, genauer deren mobiler Endgeräte, in sensible Infrastrukturen. Unterliegen diese Infrastrukturen einem Sicherheitsmanagement, und wird der Zustand des mobilen Endgerätes vor einer vollständigen Einbindung angemessen überprüft, ist die sichere Einbindung möglich. Dies wird im generischen Szenario dadurch abgebildet, dass vom Endgerät zwar eine sichere Verbindung in ein Grenznetz, jedoch nicht in ein internes Netz erfolgen soll. Umgekehrt soll auch ein Zugriff vom Unternehmensnetz auf sensible Daten und Informationen des Dienstleisters nicht möglich sein, die sich im internen Netz des Dienstleisters oder auf dem mobilen Endgerät befinden können. Kann ein mobiles Gerät mittels VPN und TNC durch das Sicherheitsgateway nicht als vertrauenswürdig eingestuft werden, wird eine Verbindung entweder abgelehnt oder ausschließlich zu einem sog. Quarantänenetz hergestellt. Die Einbindung in ein Quarantänenetz soll die Behebung identifizierter Fehler ermöglichen, z.B. die Aktualisierung von Virenschutzprogrammen. Ein Sicherheitsmanagement fokussiert jedoch nur die Sicherheit einer einzelnen Arbeitsumgebung, ein sicherer Wechsel der Arbeitsumgebung und der entsprechenden Einstellungen wird nicht ausreichend berücksichtigt, auch wenn beide Umgebungen einem Sicherheitsmanagement unterliegen. Dieser sichere Wechsel ist unter anderem Gegenstand des Projektes VOGUE.

Für den Zeitraum der Dienstleistung entsteht zusätzlich zu den Strukturen „Dienstleister“ und „Unternehmen“, die eigenen und im allgemeinem verschiedenen Richtlinien unterliegen, eine temporäre Struktur für die Kooperation. Diese unterliegt einer eigenen Richtlinie, die sich wiederum von den (internen) Richtlinien des Dienstleisters und des Unternehmens unterscheidet. In einer solchen ad hoc Struktur wäre eine dynamische Aushandlung dieser Kooperationsrichtlinie eine allumfassende Lösung. Hierfür ist ein sicherer Wechsel zwischen Richtlinien (z.B. im Übergang von der internen Richtlinie des Dienstleisters zur Richtlinie für die Kooperation) erforderlich. Die zugrunde liegende Technologie wird jedoch erst mit diesem Projekt weiterentwickelt bzw. zum Einsatz gebracht. Für das vorliegende Projekt wird somit zunächst von einer bereits vereinbarten Richtlinie zwischen Dienstleister und Unternehmen ausgegangen (z.B. auf der Grundlage eines Dienstleistungsvertrages). Auf einer solchen Basis kann eine Weiterentwicklung zur sicheren Anwendung von mehr als zwei Richtlinien oder zur dynamischen Gestaltung von Richtlinien erfolgen.

Im Rahmen der Kooperation muss der mobile Mitarbeiter mit seinem Endgerät in das Netz des Unternehmens integriert werden, um Daten mittels eines Portals den unternehmensinternen Anwendungen übermitteln zu können. Darüber hinaus ist es zur Aufgabenerfüllung für den mobilen Mitarbeiter erforderlich, Daten aus solchen Anwendungen abrufen zu können. Insgesamt entsteht somit folgendes Bild, nach Abb. 2. Der Anwendungsfall auf der Grundlage des generischen Szenarios wird die Basis für die Entwicklung in VOGUE darstellen.

## 3.2 Business Intelligence (BI)

Am Beispiel eines BI-Szenarios soll der TNC-Ansatz für das generische Szenario verdeutlicht werden. Unter Business Intelligence (BI) werden alle softwaregestützten und analytischen Auswertungen verstanden, die einen schnellen, visuell unterstützen Zugriff auf Unternehmensdaten liefern und bei der Entscheidungsfindung das Management unterstützen.

Im Unternehmen fallen in den unterschiedlichsten Bereichen Daten an, die in firmeninternen Datenbanken gesammelt werden. Hierzu zählen beispielsweise CRM-Tools, ERP-Systeme oder das Controlling. Diese Daten werden intern im Unternehmen erhoben und gepflegt. Darüber hinaus existieren Datenbanken, die aus unternehmensexternen Datenquellen gespeist werden können. Dazu zählen Inputs durch Zulieferer, Unternehmen in der Logistikkette oder mobile Zugriffe durch Mitarbeiter im Vertrieb etc. Alle Datenbanken liefern ihre Daten an ein Data Warehouse, welches die Aufgabe hat, die Daten zu bündeln, zu bereinigen und den Zugriff für Analysesysteme zu ermöglichen.

Die Analysesysteme werten die Daten sowohl mit einfachen als auch komplexen statischen Methoden aus. Diese gehen über Harmonisierung, Filterung oder Anreicherung der Daten bis hin zu Data Mining Techniken, in denen explorative Analysemethoden zum Forecast von Trends eingesetzt werden. Oftmals werden mit BI-Systemen auch Wissensmanagementsysteme verknüpft. Hierbei werden qualitative Daten gesammelt und für eine statistische Analyse aufbereitet, die dem Management für Entscheidungsprozesse zur Verfügung stehen können.

Die analysierten Daten stehen in BI-Portalen zur Auswertung bereit. BI-Systeme zeichnen sich durch eine hohe Benutzerfreundlichkeit aus, da sie in der Regel auch von Managern ohne statistische Vorbildung und ohne Informatikwissen bedient werden können müssen. Mit Hilfe von visuellen Darstellungen, in Form von Grafiken, Dashboards, Thermometern, Ampeln und

Diagrammen werden Informationen übersichtlich dargestellt und erleichtern so die Entscheidungsfindung.

Anwendungsfälle sind hier:

- Zusammenführung von Unternehmensdaten
- Feedback zur Effizienz von Marketingmaßnahmen
- Analyse von Verkaufszahlen
- Effizienzanalyse von Produktlinien
- Vergleich von Anbietern zur Kostenkontrolle
- Attraktiver Überblick über das klassische Unternehmenscontrolling

Der Zugriff auf die Daten erfolgt in der Regel über Webportale. Somit können Informationen zur Entscheidungsfindung jederzeit und überall zur Verfügung gestellt werden. Das Management erhält die Informationen häufig aufbereitet in Form von Berichten. Eine zeitnahe Informationsbereitstellung erhöht die Produktivität im Unternehmen. Daher ist auch im BI-Anwendungsbereich die Anbindung von mobilen Endgeräten mittlerweile ein integraler Bestandteil der Lösungen. Häufig stellen auch externe Dienstleister Daten für das BI-System bereit oder dürfen an spezifischen Unternehmensinformationen partizipieren. Dies erfolgt häufig über heterogene Netze hinweg.

Durch den im Projekt VOGUE verfolgten TNC-Ansatz, lassen sich auch für den BI-Bereich Lösungen umsetzen, die die Integrität und Konformität von mobilen Endgeräten und deren Verbindung in Bezug auf die vereinbarten Richtlinien sicherstellen. Somit können auch in unternehmenskritischen Bereichen mobile Lösungen sicher eingesetzt und die Produktivität gesteigert werden.

## 3.3 Einsatz des TNC-Ansatzes im BI-Szenario

Die Vorteile von TNC zeigen sich vor allem aus Sicht von VOGUE in einem solchen BI-Szenario, wenn die Lösung auch von externen Mitarbeitern (von Fremdfirmen) mit genutzt und/oder die Anwender der Suite sich außerhalb der Unternehmens-IT-Infrastruktur bewegen. Akteure sind jeweils (mindestens) ein Administrator in jedem der beiden Unternehmen und ein externer Mitarbeiter.

Ein externer Mitarbeiter von Unternehmen A führt Audits mit seinem mobilen Endgerät durch. Die dabei ermittelten Daten möchte der Mitarbeiter an einen Datenbank-Server in Unternehmen B übertragen. Zudem erfolgt eine Aktualisierung der für ihn bestimmten Audit-Anweisungen auf seinem mobilen Client. Danach kehrt der externe Mitarbeiter wieder zurück zum eigenen Unternehmen und betritt somit wieder das eigene Netz. Die beiden Unternehmen haben bereits ein gemeinsames Vertragsverhältnis, so dass keine „ad-hoc“-Aushandlung von Sicherheitsrichtlinien erfolgen muss. Bei der Einbindung von externen Mitarbeitern in andere Netze kommt es zwangsweise zu einem Wechsel der Sicherheitspolitik.

Folgende Abläufe müssen durchgeführt werden, bevor die Daten übermittelt werden können:

1. Mitarbeiter betritt fremdes Netz und nimmt eine Verbindung zum Sicherheitsgateway auf.

2. Die Sicherheitsparameter des mobilen Endgerätes werden gesammelt und an das Sicherheitsgateway übertragen.

3. Je nach Zustand des mobilen Endgerätes entscheidet das Sicherheitsgateway, ob das Endgerät eine Verbindung zum Datenbank-Server aufbauen darf oder erst einmal in ein Quarantäne-Netz kommt, von wo aus z.B. Aktualisierungen aufgespielt werden können.

4. Werden alle Sicherheitsrichtlinien erfüllt, dann erfolgt die Übertragung der Daten an den Datenbank-Server und die Aktualisierung der Audit-Anweisungen auf dem Client des Mitarbeiters. Hierbei gelten verschärfte Sicherheitsrichtlinien, welche besagen, dass der Mitarbeiter nur eine Internet-Verbindung auf einmal geöffnet haben darf.

5. Im Folgenden kehrt der Mitarbeiter in das eigene Unternehmen zurück und betritt das eigene Netz. Hier gelten andere Sicherheitsrichtlinien, die wiederum vom mobilen Endgerät erfüllt werden müssen, damit eine Verbindung ins interne Netz aufgebaut werden kann.

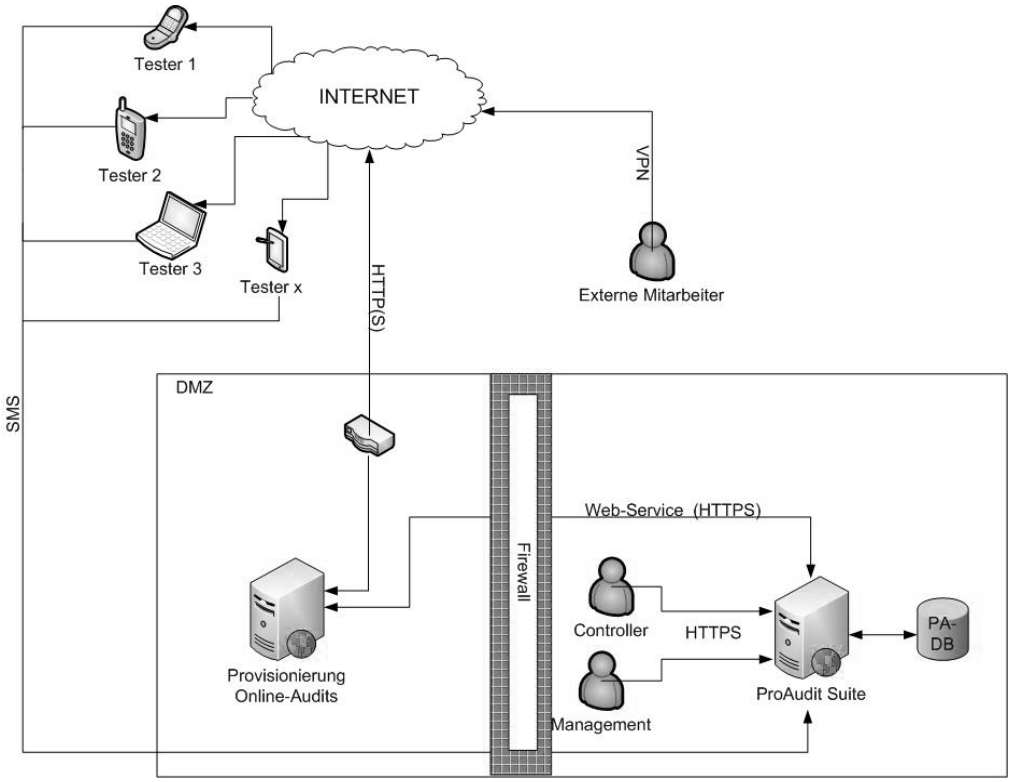


**Abb. 3:** Architektur des BI-Szenarios

Im Rahmen des VOGUE-Projektes stellt ein Partner seine BI-Lösung zur Verfügung und wird diese auch für Android-Betriebssystem weiter entwickeln. Die BI-Lösung stellt somit die Rahmenanwendung für VOGUE bereit und ermöglicht den sinnvollen Einsatz der TNC-Technologie. Das Forschungsprojekt zielte dabei auf die Entwicklung einer auf Standards basierten mobilen IT-Sicherheitsplattform ab, die sich in heterogenen mobilen Umgebungen einsetzen lässt. Ziel ist es, technische und auch nicht technische Lösungen als Baukastensystem anzubieten, die herstellerunabhängig entwickelt werden können.

Im VOGUE-Projekt sollte die Hauptplattform ein zentrales Security Gateway umfassen, welches aus verschiedenen Modulen (VPN, Firewall, TNC, RADIUS, LDAP) besteht. Dabei werden speziell Open-Source-Software (OSS) Projekte und Ansätze untersucht, um eine offene, standardkonforme Umsetzung zu ermöglichen. Gleichzeitig erhält man sich die Flexibilität, so dass bestehende Komponenten wie z.B. Firewall-Systeme eingebunden werden kön-

nen. Eine Anbindung an eine bestehende Inventory-Datenbank sollte in Erwägung gezogen werden, um erlaubte Software-Versionen und Patch-Level abfragen zu können. Darüber hinaus sollten auch sämtliche Benutzerprofile abgefragt werden, die für die Authentifizierung wichtig sind. Die genauen Spezifikationen werden derzeit im VOGUE-Projekt erarbeitet.

# 4 Ausblick

Das VOGUE-Projekt steht aktuell noch am Anfang seiner Entwicklung. Während in der ersten Phase die Anforderungen anhand des BI-Szenarios definiert wurden, arbeitet man zurzeit an der Definition der Sicherheitsplattform auf Basis des Standards Trusted Computing. Dabei werden auch Sicherheitsanalysen des verwendeten mobilen Betriebssystem Android durchgeführt. Allerdings haben die verschiedenen Ansätze und noch nicht fertige Standards bisher dazu beigetragen, dass sich Trusted Computing nicht durchsetzen konnte. Auch verlangt der Einsatz von TNC ein globales Netzkonzept im Unternehmen, was die Integration komplexer gestaltet. Zusätzlich haben sich andere Zugriffstechnologien im direkten Umfeld weiter entwickelt. Aktuelle Betriebssysteme bieten inzwischen viele Reglementierungsmöglichkeiten an, was die Benutzermechanismen und Updates des Kernels betrifft. Auch gibt es Lösungen zur Zugriffskontrolle auf Schnittstellen wie USB oder Speicherkarten. Deshalb geht der Trend eher in die Realisierung von Teilbereichen des Trusted Computing, wie dies beispielsweise durch Authentisierungslösungen mittels RADIUS-Server und 802.1x ermöglicht wird.

Zusätzlich haben Forschungsprojekte das Thema Trusted Computing in den letzten Jahren immer mehr fokussiert. Folgende Projekte setzen sich neben VOGUE ebenfalls mit der Thematik auseinander: [EUD09]

a. **SIMOIT (http://www.simoit.de):** war ein gefördertes Projekt des Landes Bremen. Das Projekt zielte auf die Entwicklung einer auf Standards basierenden mobilen IT-Sicherheitsplattform ab, die sich in heterogenen mobilen Umgebungen einsetzen lässt. Die in diesem Projekt erarbeiteten Lösungen können in unterschiedlichen Unternehmen eingesetzt werden, auf Basis von Trusted Computing. Aktuell wird an der Kommerzialisierung gearbeitet.

b. **TNC@FHH (http://trust.inform.fh-hannover.de/joomla/):** ist auch eine Open-Source-Implementierung der TNC-Architektur zur Integritätsprüfung von Endgeräten im Rahmen der Netzwerkzugangskontrolle 802.1x. Damit eine offene und standardkonforme Umsetzung ermöglicht werden konnte, wurde speziell Open Source Software untersucht und analysiert. Auch hier können bestehende Komponenten wie z.B. spezielle Firewall-Systeme mit eingebunden werden.

c. **tNAC (http://www.tnac-project.org):** ist ein vom BMBF gefördertes Projekt, welches eine vertrauenswürdige Network-Access-Lösung entwickelt. Durch die Integration von Turaya, einer Trusted-Computing-Plattform, soll ein signifikant höheres Sicherheitsniveau erreicht werden. Forschungsschwerpunkte ist dabei insbesondere die sinnvolle und praxistaugliche Verwendung von Trusted-Computing-Funktionen im Rahmen einer interoperablen NAC-Lösung, basierend auf dem TNC-Standard.

Die TNC-Ansätze der Projekte SIMOIT und TNC@FHH sind unterschiedliche „Trusted Computing“-Implementierungen für mobile Szenarien. Sie erlauben ein relativ hohes Sicherheitsniveau für mobiles Identity und Access Management. Die Ansätze sind modular aufgebaut, so dass auch andere Herstellerlösungen (z.B. VPN-Gateways oder Firewalls) integriert

werden können. VOGUE wird jetzt in die nächste Phase dieser Entwicklung gehen und die Sicherheitsanbindung der mobilen Endgeräte auf Smartphones erweitern. Dabei sollen TNC-Clients für das mobile Betriebssystem Android entwickelt werden, so dass der Einsatzbereich nicht nur auf Laptops beschränkt bleibt.

## Danksagung

Das VOGUE-Projekt (http://www.vogue-project.de) ist ein gefördertes BMBF-Projekt mit einer Laufzeit von zwei Jahren, das im Oktober 2009 seine Arbeiten begonnen hat und im September 2011 endet. An dieser Stelle möchten sich die Autoren beim BMBF für die Unterstützung der Forschungsarbeiten bedanken. Ebenso gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten diesen Bericht erst ermöglicht haben.

## Literatur

[BSI06] Bundesamt für Sicherheit in der Informationstechnik (BSI): Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, BSI-Studie, Bonn 2006

[DET09] Kai-Oliver Detken: Mobiles Trusted Computing; Linux Technical Review, URL: http://www.linuxtechnicalreview.de, Verlag Linux New Media AG, München 2009

[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

[DETK08] Detken: Mobil, aber bitte sicher: Sichere Einbindung mobiler Endgeräte in Unternehmensnetze, NET 06/08, NET Verlagsservice GmbH, Woltersdorf 2008

[EUD09] Eren, Uhde, Detken: Mobile Identity Management auf Basis des SIMOIT-Projekts und der TNC@FHH Entwicklung, Buch „Wireless Communication and Information – Radio Engineering and Multimedia Applications“, Herausgeber: Jürgen Sieck und Michael A. Herzog, ISBN-13: 978-3-940317-51-3; S. 283-297, vwh Verlag Werner Hülsbusch, Berlin 2009

[EREN09] Endpunkt Sicherheit: TNC-basiertes Identitäts- und Access-Management für mobile Anwendungen, NET 10/08, NET Verlagsservice GmbH, Woltersdorf 2009

[TNC01] TCG Trusted Network Connect, Federated TNC, Specification 1.0, Revision 26, May 18, 2009, https://www.trustedcomputinggroup.org/specs/TNC

[TNC02] TCG Specification Architecture Overview, Specification, Revision 1.4, 2nd August 2007, https://www.trustedcomputinggroup.org/developers/infrastructure

[TOER09a] Török, Elmar: Sicheres Netzwerk durch Network Access Control, NAC-Grundlagen, Teil 2, TecChannel, 10.08.2009, München 2009

[TOER09b] Török, Elmar: Basiswissen: Die Technik hinter Network Access Control, NAC-Grundlagen, Teil 2, TecChannel, 30.09.2009, München 2009