Zutritt nur nach Aufforderung

Die Absicherung von Smartphones ist keine leichte Aufgabe

Kai-Oliver Detken

Schön, was Smartphones heute alles können. Eben noch im Netz des Arbeitgebers, wenig später im Netz des Kunden, abends wieder retour – weil es nützlich ist zur Erledigung der Aufgaben. Aber auch ein Albtraum für IT-Verantwortliche, denn es lauert Ansteckungsgefahr. Deshalb geht es nicht ohne Regeln. Man kennt sie aus dem Krankenhaus: Patienten mit unklarem Krankheitsbild kommen vorsorglich erst einmal auf die Quarantänestation. So auch hier. Der Beitrag beschreibt die für mobile Endgeräte im Vogue-Forschungsprojekt erarbeiteten Lösungen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Unternehmen stellen heute hohe Anforderungen an die Mobilität und Flexibilität ihrer Arbeitnehmer. Der Anspruch, auch über die Unternehmensgrenzen hinweg mit Daten verschiedener Betriebe arbeiten zu können, birgt jedoch auch neue Herausforderungen und Risiken. Er führt zu einer Ausdehnung der digitalen Unternehmensgrenzen, von traditionellen Perimeter-Einrichtungen bis hin zu den mobilen Endgeräten der Arbeitnehmer. Neben der obligatorischen Kontrolle von Benutzerdaten brauchen Unternehmen die Gewissheit, dass sensible Firmendaten, die sich im Netz sowie auf den Geräten selbst befinden, nicht durch kompromittierte oder gefährdete Endgeräte bedroht werden. Zu diesem Zweck ist ein Mechanismus erforderlich, der den Zustand der Endgeräte vor dem Zugriff auf kritische Ressourcen erfasst und mit dem ggf. angemessen reagiert werden kann.

Generisches Anwendungsszenario

Im Rahmen des Vogue-Projekts (www.vogue-project.de) werden die Möglichkeiten des Einsatzes von Trusted-Computing-Konzepten auf mobilen Endgeräten untersucht. Dazu wurde eine Sicherheitsarchitektur für mobile Endgeräte und die Infrastruktur definiert, die es ermöglichen soll, die vorher im Projekt definierten Sicherheitsanforderungen zu erfüllen. So soll mobilen Geräten in verschiedenen Einsatzumgebungen der sichere Zugriff auf Ressourcen unterschiedlicher Unternehmen ermöglicht werden. Das Beispiel nach *Bild 1* wurde als generisches Szenario in Vogue entwickelt und setzt sich aus verschiedenen realen Szenarien zusammen. Es zeigt verschiedene IT-Infrastrukturen, die einen Service-Mitarbeiter betreffen, wenn er ein mobiles Gerät für die sichere Verbindung zur BI-Plattform (BI – Business Intelligence) eines Kundenunternehmens verwendet. Anfangs nutzt der Mitarbeiter die Infrastruktur des Dienstleistungsunternehmens und ist mit seinem mobilen Endgerät ein Teil davon. Der Mitarbeiter hat hier System- und Datenzugriffe entsprechend der Sicherheitsrichtlinie seines Arbeitgebers. Der sichere Einsatz und der sichere Betrieb des Gerätes erfolgt dabei entsprechend eines standardisierten Informationssicherheitsmanagements (z.B. ISO 27001).

Im Rahmen der Auftragsbearbeitung wird das mobile Endgerät zudem außerhalb der sicheren Infrastruktur des Dienstleisters verwendet, z.B. im Unternehmensnetz des Kunden. Um nach der Auftragsbearbeitung wieder Zugriff auf das Netz des Dienstleisters zu erhalten, muss das mobile Gerät vertrauenswürdig sein, d.h. die Sicherheitsanforderungen des Dienstleistungsunternehmens im vorgeschriebenen Umfang erfüllen (z.B. Versionsstand des Betriebssystems, der Anti-Viren-Software, der Firewall und die Sicherheitseinstellungen). Um dies festzustellen, wird der Zustand des mobilen Endgeräts unter Verwendung von Trusted Network Connect (TNC) vor seiner Rückkehr ins Netz des Dienstleisters überprüft [1]. Sollten diese Anforderungen nicht erfüllt sein, kann ein sicher abgetrennter Bereich im Netz, eine sog. Quarantänezone, verwendet werden, um den vertrauenswürdigen Zustand wieder herzustellen (z.B. durch Rücksetzen von Konfigurationen oder Aktualisierung von Software) [2].

Nimmt der Service-Mitarbeiter die Tätigkeit für den Kunden wieder auf oder setzt diese fort, verlässt der Mitarbeiter hierfür die Infrastruktur seines Arbeitgebers und verbindet sich mit dem Netz des Kundenunternehmens. Dieses unterliegt ebenfalls einem standardisierten Informationssi-

cherheitsmanagement, unterscheidet sich jedoch in den verwendeten Sicherheitsrichtlinien (z.B. sicherheitsrelevante Einstellungen, Softwareanforderungen). Daher muss der Mitarbeiter die entsprechenden, vordefinierten Sicherheitsrichtlinien seines mobilen Endgerätes wechseln. Anschließend nimmt er zunächst Verbindung zum Sicherheits-Gateway des Kundenunternehmens auf und authentifiziert sich. Das Sicherheits-Gateway überprüft die Authentifizierung und vergleicht die Informationen zum Systemzustand des mobilen Endgerätes mit den Sicherheitsanforderungen des Kundenunternehmens. Für den Fall, dass dem mobilen Endgerät unabdingbare Sicherheitsmerkmale fehlen (z.B. VPN-Client, aktuelle Fassung der Sicherheitsrichtlinie), wird das mobile Endgerät nur mit einer Quarantänezone verbunden, in der fehlende Daten oder Software zur Verfügung gestellt werden können und die Überprüfung wiederholt werden muss.

Wenn der Zustand des Clients der Sicherheitsrichtlinie des Kundenunternehmens entspricht, wird eine sichere VPN-Verbindung zwischen dem mobilen Endgerät und einem Portal der BI-Lösung in der DMZ – der sog. demilitarisierten Zone – des Kundennetzes aufgebaut. Unter Verwendung der Dienste des BI-Portals hat der Mitarbeiter eingeschränkten Zugriff auf die BI-Plattform im Intranet des Kundenunternehmens. Der Zugriff des Mitarbeiters ist auf jene Systemdienste beschränkt, die zur Erfüllung seines Vertrages erforderlich sind, z.B. einen Auftrag abrufen, auf auftragsrelevante Daten zugreifen, Ergebnisse abliefern (neue Daten, Berichte) oder eigene offene Aufträge schließen. Die wesentlichen Herausforderungen in diesem Anwendungsszenario betreffen das sichere Wechseln von Sicherheitseinstellungen durch nicht-privilegierte Nutzer, das Management der Quarantänezonen und Netzzugehörigkeiten, die zuverlässige Zusammenstellung und sichere Übertragung des Zustands des mobilen Endgerätes sowie die Anwendungsfreundlichkeit und Transparenz der entsprechenden Funktionen. Das Management der zwei Quarantänezonen muss, mit Blick auf die Kontrolle des mobilen Endgeräts, den unterschiedlichen Rollen des Mitarbeiters im Dienstleistungs- und Kundenunternehmen entsprechen. Das Dienstleistungsunternehmen, als tatsächlicher Eigentümer des mobilen Endgerätes, wird z.B. wesentliche Software-Updates wie Betriebssystem- und Anti-Virensoftware-Updates zur Verfügung stellen, während jegliche kundenspezifische Software, z.B. der VPN-Client, vom Kundenunternehmen zur Verfügung gestellt wird. Fordert beispielsweise ein mobiles Endgerät mit einer veralteten Virendatenbank eine Verbindung zum Kundennetz an, wird die Verbindung verweigert und der Mitarbeiter darüber informiert, dass er sich mit dem Netz seines Arbeitgebers (des Dienstleisters) verbinden und seine Virendatenbank aktualisieren muss, bevor eine Verbindung zum Kundennetz gestattet wird.

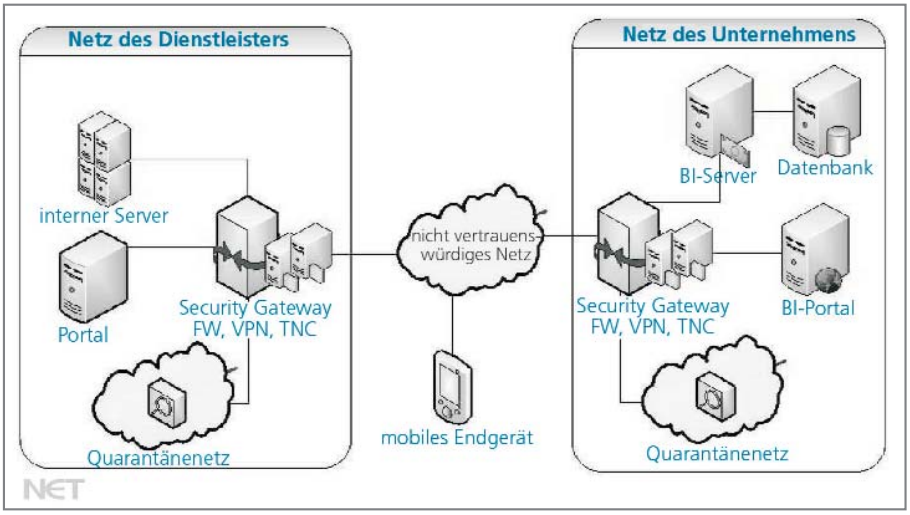

Bild 1: Unterschiedliche Sicherheitsanforderungen in mobilen BI-Infrastrukturen

Solche zusätzlichen Sicherheitsanforderungen wirken sich auf die Verfügbarkeit von Netzwerkverbindungen aus und in Folge dessen auf die Anwendungsfreundlichkeit des mobilen Endgerätes. Daher müssen die entsprechenden Sicherheitsmaßnahmen sorgfältig implementiert werden. Erlaubt man z.B. gleichzeitig eine Verbindung in beide Quarantänenetze, kann dies helfen, häufige Wechsel zwischen den beteiligten Netzen zu vermeiden, und die Herstellung des erforderlichen Systemzustandes kann dem Nutzer als ein einziger Prozess präsentiert werden.

Absicherungsmechanismen im Vogue-Projekt

Wie bereits in der Szenario-Beschreibung erklärt, ist das zentrale Thema des Projekts ein Nutzer, der im Auftrag eines Unternehmens mit einem mobilen Gerät Zugriff zu Ressourcen eines weiteren Unternehmens erhalten soll. Nachdem zunächst über einen VPN-Gateway mit Benutzernamen und Passwort der eingeschränkte Zugang zum fremden Netz gewährt wird, ist als nächster Schritt die Identität des mobilen Geräts anhand des entsprechenden Zertifikats zu prüfen (Remote Attestation). Daraufhin ist festzustellen, welche Richtlinien auf dem mobilen Gerät erfüllt sind und inwiefern diese für den Zugriff auf die gewünschten Ressourcen ausreichen oder angepasst werden müssen. Durch Einsatz eines Quarantänenetzes sollen gegebenenfalls Änderungen der Eigenschaften des Geräts (z.B. Versionen der Firewall- und Virenschutzsoftware) ermöglicht werden und somit eine Anpassung hinsichtlich der Richtlinien durchsetzen. Erst wenn die Richtlinien (Policies) glaubhaft überprüft wurden, können die Zugriffsrechte des mobilen Geräts auf die geschützten Ressourcen erweitert werden.

Durch die Anwendung von mobilen Geräten in fremden Netzen und der

daraus resultierenden Einflüsse verschiedener Rollen ergeben sich besondere Anforderungen an die Strategie der Sicherheitsrichtlinien. Nicht nur das Gerät für sich, sondern zusätzlich auch der Nutzer des Geräts muss verifiziert, sein Zugriff ggf. eingeschränkt werden. In Vogue wird dies durch eine Aufteilung der Kontrollmechanismen der Richtlinie und somit durch eine zusätzliche Richtlinienkontrolle auf dem mobilen Gerät erreicht. So soll allen Partnern ermöglicht werden, Einfluss auf die sicherheitskritischen Einstellungen des mobilen Geräts zu erhalten. Nur dadurch wird eine Vertrauensbeziehung zwischen der Infrastruktur und dem Nutzer möglich. Bei diesem Ansatz ist es wichtig, die Richtlinien in einer einheitlichen und eindeutigen Semantik zu verfassen, um Kohärenz zu gewährleisten.

Bild 2 zeigt die Teilung der Richtliniendomänen in Infrastruktur und Gerät. Dabei steht PDP für Policy Decision Point, also die Instanz, die Informationen erhält und gegen die Richtlinie prüft. Die Durchsetzung der Richtlinien wird durch die Policy Enforcement Points (PEP) erreicht, die außerdem zum Sammeln der nötigen Information dienen. Die Entscheidung und Durchsetzung von Richtlinien bez. Infrastrukturressourcen muss auf Infrastrukturseite geschehen. Entsprechend müssen die Richtlinien der mobilen Domäne auf dem mobilen Gerät entschieden und durchgesetzt werden. Im Falle des Einsatzes von Software und Daten auf dem mobilen Gerät, deren Nutzung insbesondere auch nach bzw. ohne Zugang zur Infrastruktur (durch den PEP derselben) unter der Einhaltung der entsprechenden Richtlinien erfolgen soll, ist es also zusätzlich nötig, dass Richtlinienentscheidungen der Infrastrukturdomäne auch auf dem Gerät repräsentiert sind.

Die Architektur von Vogue *(Bild 3)* lässt sich in die Komponenten der Infrastruktur und in die des mobilen Geräts gliedern. Als mobiles Endgerät könnte ein Smartphone mit einem Linux-basierten Betriebssystem, beispielsweise Android, zum Einsatz kommen. Zur Absicherung der Kommunikation eines mobilen Endgeräts mit einer Infrastruktur können Virtual Private Networks (VPN) eingesetzt werden. Diese übernehmen die Prüfung des Nutzers mit sicheren Authentifizierungsverfahren sowie die Sicherung der Vertraulichkeit und der Integrität von ausgetauschten Nachrichten zwischen zwei VPN-Endpunkten durch geeignete Kryptoverfahren. Für die Realisierung des VPN werden somit die Komponenten VPN-Client und VPN-Gateway sowie ggf. auf Infrastrukturseite eine entsprechende Management-Architektur (z.B. ein Zertifikatsserver, ein AAA-Server und ein Verzeichnisdienst) benötigt. Auf dieser Verbindung basierend können daraufhin weitere Eigenschaften des mobilen Geräts geprüft bzw. nachgewiesen werden. Um den aktuellen Zustand des Endgeräts glaubwürdig messen und erfassen zu können, wird der Trusted-Computing-Ansatz Trusted Network Connect (TNC) eingesetzt. Dabei ist hervorzuheben, dass TNC unabhängig vom VPN ist. Letzteres ermöglicht nur die verschlüsselte, authentifizierte Kommunikation zwischen den Komponenten des mobilen Endgeräts und der Infrastruktur; es wäre also theoretisch auch eine andere Technologie einsetzbar.

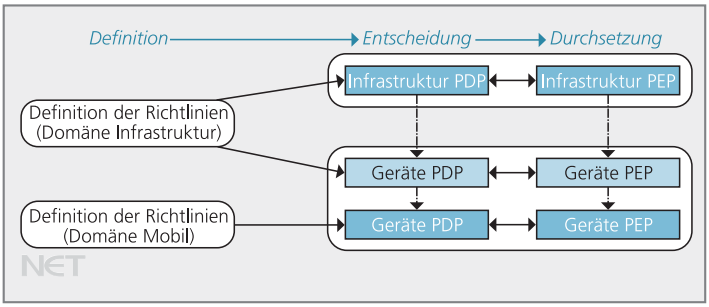

Bild 2: Aufteilung von PEP und PDP auf Gerät bzw. Infrastruktur

Hat sich der Benutzer authentifiziert, wird per TNC Remote Attestation geprüft, ob sich das Endgerät in einem vertrauenswürdigen Zustand befindet. Ein vertrauenswürdiger Zustand ist gegeben, wenn die Software des Endgeräts der auf der Infrastrukturseite festgelegten Richtlinie entspricht. Eine solche Richtlinie kann verschiedene Programme zulassen oder verbieten, Versionsnummern vorschreiben oder Datenzugriffsrechte festlegen. Für diese Überprüfung werden die Komponenten TNC-Client und TNC-Server benötigt [1].

Wird bei der Attestierung der Zustand des Endgeräts als unsicher bewertet, erhält das Gerät keinen Zugriff auf die Zielressourcen, sondern wird in einem Quarantänenetz isoliert. Dies kann auf Seiten des VPN-Gateways beispielsweise mit einem Paketfilter realisiert werden. Innerhalb des Quarantänenetzes kann das Endgerät mithilfe einer Softwareverteilungslösung auf den geforderten aktuellen Stand gebracht werden. Anschließend kann das Gerät gemäß den Spezifikationen von TNC eine erneute Attestierung anfordern.

Für die Richtlinienentscheidung bzw. -durchsetzung ergibt sich eine Ambivalenz. Es müssen in den Policy Decision Points (PDP) die von den beiden Domänen „Mobil“ und „Infrastruktur“ vorgegebenen Richtlinien evaluiert und durch die Policy Enforcement Points (PEP) entsprechend durchgesetzt werden. Der Entscheidungspunkt der Richtlinien der Domäne „Mobil“ gibt den kleinsten gemeinsamen Nenner der Sicherheitsanforderungen der verschiedenen Domänen vor. Policies der Domäne „Infrastruktur“, die nicht mit den Policies der Domäne „Mobil“ vereinbar sind, können folglich nicht umgesetzt werden. Dies ist sinnvoll, da der Eigentümer des Endgeräts letztendlich die Kontrolle über das Gerät behalten muss. In solchen Situationen muss infrastrukturseitig der Zugang zu den Zielressourcen verweigert werden.

Sind alle Voraussetzungen erfüllt, erhält der Nutzer des mobilen Endgeräts mithilfe der Infrastruktur Zugriff auf die gewünschte Zielapplikation und somit auf die Zielressourcen. Während des gesamten Prozesses vom Aufbau der VPN-Verbindung bis zum Zugriff auf die Zielressourcen muss der aktuelle Zustand des Verbindungsaufbaus dem Benutzer jederzeit deutlich gemacht werden. Außerdem muss dem Nutzer immer klar sein, welche Richtlinien auf seinem Gerät erfüllt sind,

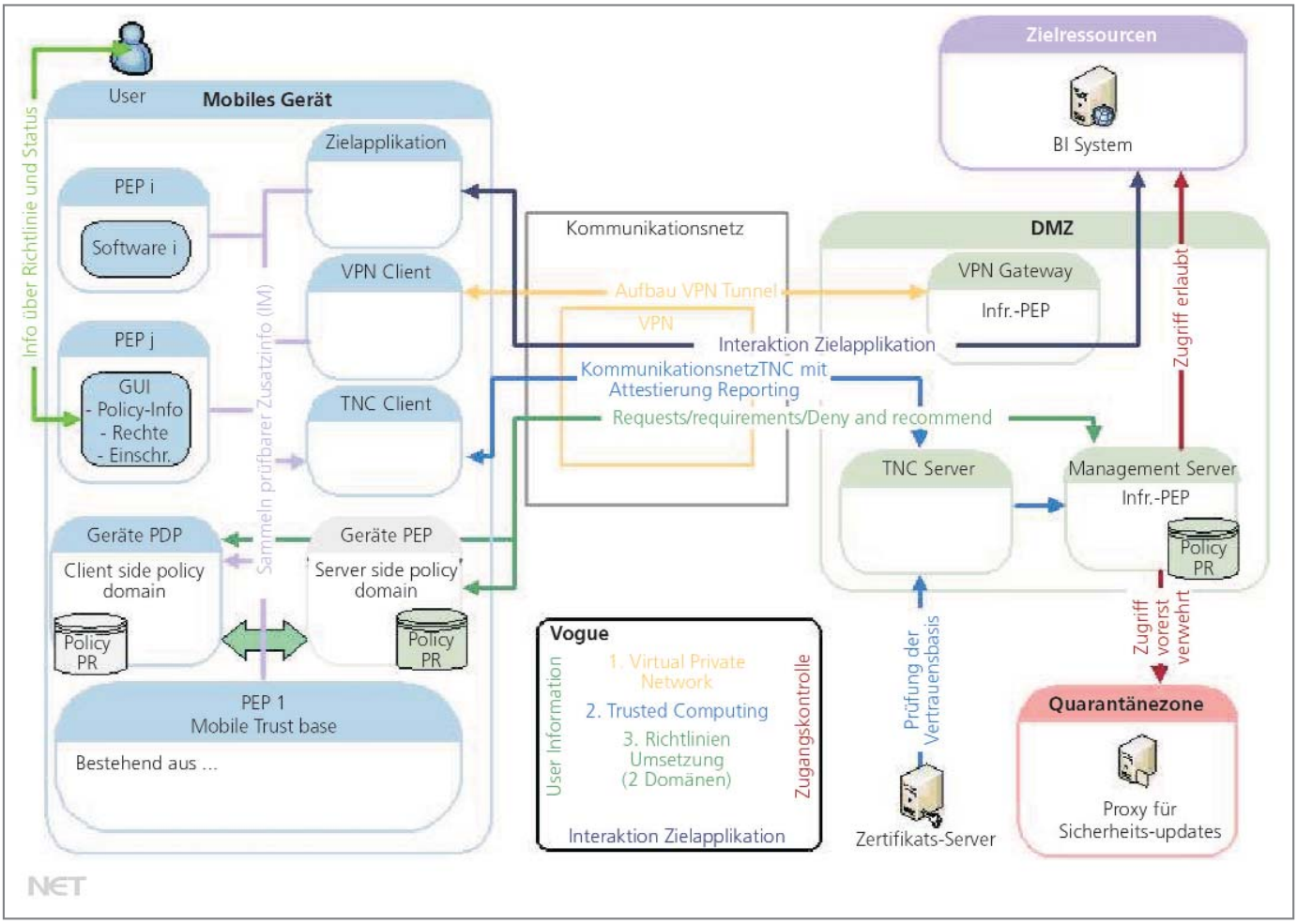

Bild 3: Architektur von Vogue, eine Übersicht

bzw. welche Einschränkungen er mglw. für die Dauer des Zugangs zur fremden Infrastruktur hinnehmen muss. Nur so kann gewährleistet werden, dass der Benutzer des Endgeräts Vertrauen in das Gesamtsystem hat [3].

Ausblick

Im Rahmen des vom BMBF geförderten Verbundprojekts Vogue wurden die Möglichkeiten des Einsatzes von Trusted-Computing-Konzepten auf mobilen Endgeräten untersucht. Das Projekt befindet sich derzeit in der Endphase. Die entworfene Sicherheitsarchitektur kann die notwendigen Sicherheitsanforderungen erfüllen und so möglichen Bedrohungen begegnen. Der zentrale Ansatz ist hierbei die authentische Attestierung des Zustands des Endgeräts gegenüber der Infrastruktur. Im Gegensatz zu den bisher verfügbaren, proprioritären NAC-Lösungen (NAC – Network Access Control) – u.a. von Cisco und Microsoft – basiert der Vogue-Ansatz auf der standardisierten TNC-Architektur und quelloffenen Softwarekomponenten. Dazu muss auch der Zustand der Komponenten der TNC-Architektur vertrauenswürdig nachweisbar sein, weshalb eine auf der Basis eines Secure Boots gründende Vertrauenskette in die Architektur integriert wurde. Mit Secure Boot wird nun gewährleistet, dass auf dem Endgerät ein vom Herausgeber zertifizierter Betriebssystem-Kernel gestartet wird, dessen Authentizität und Integrität gesichert ist. In Verbindung mit bereits etablierten Standardtechnologien, wie MAC Policy Enforcement und VPN, kann so der Sicherheitsstandard beim unternehmensübergreifenden Einsatz von mobilen Endgeräten weiter erhöht werden. Das ist auch dringend notwendig, da es bei bisherigen Herstellerlösungen weder vertrauenswürdige Authentifizierung auf TNC-Basis noch zentrale Verwaltungsmöglichkeiten mobiler Endgeräte gibt. *(bac)*

Literatur

[1] Trusted Computing Group, TCG Specification Architecture Overview, Revision 1.3, März 2007

[2] Detken, K.-O.; Diederich, G.; Nowak, A.: Vertrauenswürdiger mobiler Zugriff auf Unternehmensnetze im Vogue-Projekt. DACH Security 2010: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Hrsg.: Schartner, P., Weippl, E., Syssec-Verlag, Wien, 2010

[3] Detken, K.-O. ; Diederich, G.; Heuser, S.: Sichere Plattform zur Smartphone-Anbindung auf Basis von TNC. DACH Security 2011: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Hrsg.:Schartner, P; Weippl, E., Syssec-Verlag; Wien 2010