Sichere Integration mobiler Nutzer in Unternehmensnetzwerke

Malte Hesse · Norbert Pohlmann
{hesse | pohlmann}@internet-sicherheit.de

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen

Zusammenfassung

Die Herausforderung der sicheren Integration mobiler Nutzer in bestehende Unternehmensnetzwerke setzt sich aus mehreren Teilaspekten zusammen. Um eine Ende-zu-Ende Prozesssicherheit zu erreichen ist es wichtig alle Teilaspekte und den Kontext zwischen den Akteuren zu betrachten. Wir wollen diese Ende-zu-Ende Prozesssicherheit daher als Integrative-Prozesssicherheit bezeichnen. Dies ist mitunter schwierig, weil nicht alle Aspekte im gleichen Verantwortungsbereich liegen und keine einheitliche aufeinander abgestimmte Lösung verfügbar ist. Der Analyseprozess der diesem Abstract zugrunde liegt prüft die Ausgangssituation für den Benutzer, die mobile Endgeräte, die Zugangsebene und das Unternehmensnetzwerk mit seinen Diensten. Darauf aufbauend werden zunächst die zusätzlich auftretenden Bedrohungen erarbeitet - also die Probleme die eine Integration mobiler Geräte erst entstehen lässt. Im nächsten Schritt werden dann die zugehörigen Sicherheitsmaßnahmen erörtert. Dabei wird erarbeitet, dass die Hauptherausforderung in nächster Zeit sichere Hard- und Softwarelösungen sein werden. Es gibt zwar jetzt schon eine Reihe von „Tools“ und Lösungen die für die verschiedenen Teilaspekte verwendet werden könnten, doch erzielt man damit keine Integrative-Prozesssicherheit. Dazu zählen zum einen die gegenseitige Authentikation der Kommunikationspartner und zum anderen der Einsatz von zertifikatsbasierter Verschlüsselung. Jedoch ist es ebenso wichtig, dass die vorliegende Hard- und Softwarekonfiguration gegenseitig zuverlässig abgefragt werden kann, um eine Aussage über die Integrität des Systems treffen zu können. Leider sind die dafür benötigen sicheren Betriebssysteme noch in der Entwicklung und noch keine Hardware-Sicherheitsmodule für mobile Geräte verfügbar. Da zurzeit keine sichere Integration der Geräte möglich ist, fordern wir die Entwicklung solcher Systeme und Module. Nichtsdestotrotz verlangt die Praxis den Einsatz von mobilen Geräten. Dabei gibt es eine Reihe von Faktoren, die im fortlaufenden IT-Sicherheitsprozess des Unternehmens beachtet werden sollten und bei denen dieser Artikel eine Hilfe sein soll.

1 Einleitung

Von überall und zu jeder Zeit auf alle aktuellen Unternehmensdaten zugreifen und in Echtzeit fundierte Business-Entscheidungen treffen zu können, ist wohl der Wunsch jedes auf Mobilität angewiesenen Mitarbeiters. Die Unternehmen versprechen sich davon eine Steigerung der Produktivität ihrer Mitarbeiter und damit eine höhere Wertschöpfung. Technisch möglich ist heute aufgrund kleiner leistungsfähiger mobiler Endgeräte schon vieles. Neue E-Mails werden dem Nutzer bequem aufs Endgerät „gepusht“. Termine können von unterwegs geplant und direkt in die Kalender der beteiligten Mitarbeiter eingetragen werden. Das globale Adressbuch ermöglicht auch den Zugriff auf Adressdaten, die bisher nicht auf dem mobilen Ge-

P. Horster (Hrsg.) · DACH Mobility 2006 · syssec (2006) pp.

rät verfügbar waren. Außerdem gibt es Lösungen für den Zugriff auf Informationssysteme, welche zum Beispiel bei Gesprächen mit Kunden vor Ort Einblick in das eigene Customer Relations Management System oder Lagersystem erlauben.

Diese Integration von mobilen Nutzern bringt jedoch eine Reihe von Sorgen und Problemen mit sich.

2 Ausgangssituation in Unternehmen

Es wird nun der Zugriff der mobilen Nutzer auf ein Unternehmensnetzwerk betrachtet. Es lassen sich einige entscheidende Teilaspekte herausfiltern (vgl. Abbildung 1). In den nächsten Unterabschnitten wird zunächst betrachtet, welche Gegebenheiten für diese Aspekte vorliegen. Diese Analyse ist wichtig als Grundlage für die darauf folgende Betrachtung.

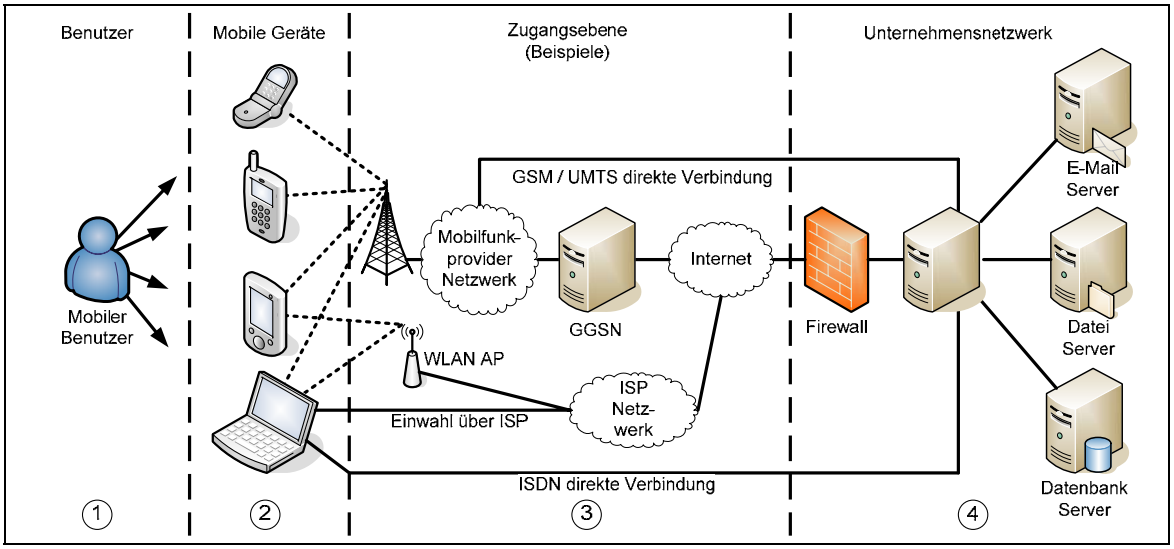

Abbildung 1 - Ausgangssituation bei der Integration mobiler Geräte

2.1 Benutzerbedürfnisse

Es ist wichtig, die Echtzeit-Bedürfnisse des Benutzers nach Information durch benutzerfreundliche Lösungen zu erfüllen. Der Benutzer wünscht eine einfache und praktikable Lösung, die ihm das weltweite mobile Arbeiten erleichtern soll. Sicherheit ist für den Benutzer zweitrangig und bedeutet Mehraufwand. Bekommt ein Benutzer keine Lösung vom Unternehmen gestellt, sucht er sich selbst eine oft auch unsichere Lösung. Beispiele für derartige Benutzer sind nicht mehr länger nur Manager oder Außendienstmitarbeiter, sondern inzwischen fast jeder Mitarbeiter eines Unternehmens, der beruflich einige Zeit im Monat außerhalb seines Büros verbringen muss.

2.2 Mobile Endgeräte

Der Markt der mobilen Endgeräte ist kaum noch zu überblicken. Für diese Betrachtung sind jene Endgeräte interessant, welche dem Benutzer unabhängig von dessen Aufenthaltsort den Zugriff auf unternehmenseigene Daten und Dienste ermöglichen. Dazu zählen u. a. Mobiltelefone, Smartphones, PDAs und Notebooks. Dabei kann die Anbindung über verschiedenste

Zugriffsszenarien erfolgen, welche im Abschnitt 2.3 genauer erläutert werden. Die Anbindung muss dabei jedoch nicht zwangsläufig über eine drahtlose Lösung erfolgen.

Abhängig vom Grad der Mobilität, dem vorhandenen Speicher oder der CPU-Leistung und von verfügbaren Ein- und Ausgabemöglichkeiten ergeben sich verschiedene Klassen der Mobilität der Geräte. All diese Geräte haben unterschiedliche Hard- und Softwarearchitekturen, verfügen über unterschiedliche Anwendungen und Daten und haben verschiedene Schnittstellen zur Außenwelt. Außerdem könnten die Geräte auch das persönliche Eigentum der Benutzer sein. Dies ist für die Betrachtung der Sicherheitsmaßnahmen ebenfalls relvant.

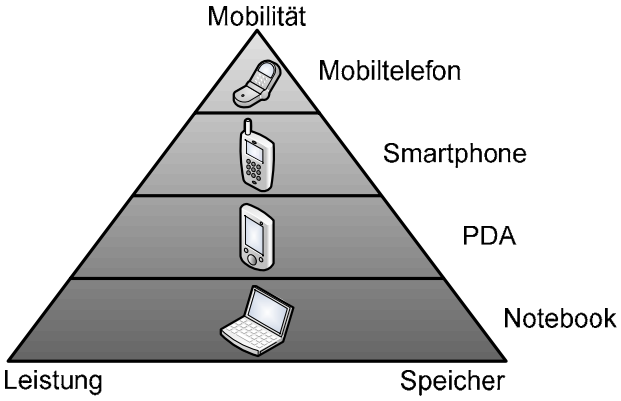

Abbildung 2 - Mobilitätsklassen

Allgemein befinden sich eine ganze Reihe von Anwendungen auf mobilen Geräten, die auch mit Hilfe von Diensten aus dem Unternehmen abgerufen werden. Dazu zählen verschiedene Text- und Multimedianachrichten, außerdem Kontakt- und Kalenderdaten. Bei einem Zugriff auf Informationssysteme kommen noch eine Vielzahl von Kunden- und anderen Stammdaten hinzu. Des Weiteren gibt es eine lange Liste von möglichen Anwendungen, die der Benutzer auf dem Gerät installieren kann. Dies reicht von Navigationssystemen über Wörterbücher bis hin zu Spielen.

Außerdem können Videos, Fotos oder Sprache gespeichert werden. Die Geräte erlauben den Zugriff auf das Internet, z.B. über einen Webbrowser. Auch verfügen die Geräte über eine Telefon- oder Modemfunktion.

Ein modernes mobiles Gerät hat eine Vielzahl von unterschiedlichen Schnittstellen. Dazu gehören neben Tastatur und Display, als offensichtliche Schnittstellen zum Benutzer, oft die Anbindungen an Mobilfunkbetreiber über GSM/(E)GPRS und UMTS/HSDPA. Außerdem sind inzwischen einige Geräte mit WLAN und LAN Anschlüssen ausgestattet.

Im Personal Area Network Umfeld gibt es eine ganze Reihe von Verbindungsmöglichkeiten. Darunter fallen Bluetooth, die Infrarotschnittstelle, USB und serielle Kabelverbindungen. Austauschbare Speicherkarten sind ebenfalls eine Schnittstelle des Geräts nach außen. Speicherkarten können entfernt und über einen Kartenleser oder andere Geräte ausgelesen werden.

2.3 Zugangsebene auf das Unternehmensnetz

Es gibt diverse Szenarien für den Zugriff von mobilen Geräten auf das Unternehmensnetzwerk. Allgemein kann davon ausgegangen werden, dass dies über ein oder mehrere ungesicherte Netzwerke geschieht. Diese können fremde Unternehmensnetzwerke sein, öffentliche Internet-Zugangspunkte in Cafés oder Flughafenlounges. Der Zugriff kann über WLAN oder

Bluetooth erfolgen oder direkt paket- oder leitungsvermittelt über die Infrastruktur eines Mobilfunkbetreibers oder per Einwahl über eine Telefonleitung.

2.4 Unternehmensnetzwerk

Ein Unternehmensnetzwerk bietet einem Mitarbeiter eine Reihe von Diensten, die durch den Zugriff auf mehrere Server bereitgestellt werden. Dazu zählen Exchange Server, Datenbanken, Customer Relation Systeme, Groupware Lösungen und Dateiserver. Das Unternehmensnetzwerk muss ggf. angepasst werden, um den Zugriff von außen auf diese Server zu ermöglichen. Dadurch waren Unternehmensnetzwerke bisher i.d.R. gegen Bedrohungen von außen geschützt.

3 Schutzbedarfsfeststellung

Das Grundschutzhandbuch vom Bundesamt für Sicherheit in der Informationstechnik bietet die Module „Mobiltelefon“, „PDA“, „Laptop“, „mobiler Arbeitsplatz“ und „häuslicher Arbeitsplatz“. Daraus lassen sich eine Reihe von Bedrohungen und auch entsprechende Lösungen ableiten. Leider kann das Grundschutzhandbuch keine einheitliche Integrative-Prozesssicherheit liefern. Wir wollen daher nun betrachten, welche besonderen Bedrohungen für unsere Teilaspekte vorliegen.

3.1 Der Benutzer als Bedrohung

Allgemein sind „social engineering“ Techniken, wie sie u.a. beim Phishing eingesetzt werden, sehr erfolgreich. Durch eine Mischung aus Gutgläubigkeit, Hilfsbereitschaft und Neugierde ist der Benutzer eine ernstzunehmende Bedrohung. So wurden in einem Experiment auf einem Firmengelände gezielt 20 mit Trojanischen Pferden infizierte USB-Sticks „verloren“ [HEIS06]. Davon wurden 15 Stück von Angestellten gefunden und auch in ihre Rechner gestöpselt. Mit dem so gewonnen Zugriff auf Arbeitsplatzrechner konnten weitere Systeme des Unternehmens in dem Test kompromittiert werden. Darüber hinaus ist der Benutzer anfällig für soziale Interaktion z.B. beim Bier nach einem gemeinsamen Training im Sportstudio. Des Weiteren könnte die Identität eines Benutzers gestohlen und von Angreifern missbräuchlich verwendet werden. Auch gehört die Erstellung von Bewegungsprofilen zu den Bedrohungen. Durch das Bewegen eines mobilen Gerätes durch die zellulare Struktur des Netzes eines Mobilfunkproviders werden so genannte Mobility Management Informationen über das Gerät und damit über den Benutzer erfasst. Diese werden auch im Idle-Mode des Gerätes beim Wechsel zwischen Location Areas im GSM Netz erfasst.

3.2 Das mobile Endgerät als Spionagewerkzeug

Mobile Engeräte haben eine besonders große Angriffsfläche, da der Benutzer so sie in allen Lebenssituationen bei sich hat. Bei diesen Geräten kommt es zwecks Spionage sogar zu Manipulation von Gerätehardware [BSI03]. Dabei wird z.B. direkt die Platine des Gerätes angezapft, als Strom oder sogar Datenlieferant. Auch gibt es mit FlexiSpy [FlexiSpy] nun ein kommerzielles Produkt für Symbian Telefone, um hinter Personen herzuspionieren. Vermarktet wird dies als eine Art „Privatdetektiv“ für den Partner. Es bedarf keiner großen Phantasie, dass im nicht kommerziellen Umfeld ähnliche Lösungen verborgen vor der Öffentlichkeit auch auf anderen Systemen eingesetzt werden. In den ersten fünf Monaten des Jahres 2006

hat sich nach F-Secure die Anzahl der mobilen Schadsoftware auf 200 verdoppelt. Es ergeben sich Bedrohungen durch Softwarefehler, und es besteht immer die Möglichkeit von Hintertüren in oft nicht offenen Systemen.

Einige zusätzliche Bedrohungen liegen aufgrund der Schnittstellen der Systeme vor. Bluetooth scheint geradezu Schadsoftware anzuziehen, auch gefördert durch fehlerhafte Implementierungen der Spezifikation durch die Hersteller. Auch werden mobile Geräte gerne liegen gelassen und sind leicht zu stehlen.

3.3 Zugangsebene als Angriffsfläche

Bedrohungen sind gegeben durch die unberechtigte Benutzung von Diensten. Außerdem sind an mobile Transaktionen besondere Anforderungen gestellt. Die Luftschnittstellte, die bei drahtlosen Zugangsmethoden gegeben ist, bietet ein enormes Angriffspotential. Eine Reihe von drahtlosen Systemen weist enorme Sicherheitsprobleme auf. Bei GSM sind die verwendeten Schlüssellängen inzwischen viel zu kurz und auch der verwendete Verschlüsselungsalgorithmus weist einige Probleme auf. Bei Bluetooth ist es nicht so sehr die Spezifikation, sondern die eigentliche Implementierung von einigen Herstellern in den Geräten, die immer wieder zu kritischen Sicherheitsproblemen geführt hat. Um Kosten zu sparen oder um nicht mit Exportbeschränkungen belastet zu sein wird zusätzlich teilweise auf die Implementierung von Verschlüsselung komplett verzichtet, was dem Kunden jedoch meist noch nicht einmal angezeigt wird. Betrachtet man WLAN, gibt es eine Reihe von Faktoren, wie die Designfehler älterer WLAN Standards. Zusätzlich gibt es inzwischen einen kaum noch zu überblickenden WLAN-Markt und die Benutzer sind bei der Konfiguration schlichtweg überfordert. Für öffentliche Netzwerke gibt es eine Reihe von Gesetzesnormen, die sicherstellen sollen, dass ein gewisses Maß an Sicherheit umgesetzt wird (TKG §§ 88, 89, 109), jedoch gibt es dort auch die gesetzliche Vorschrift zur technischen Umsetzung von Überwachungsmaßnahmen (TKG §110). Abschließend lässt sich feststellen, dass die Zugangsebene sich als nicht vertrauenswürdig einstufen lässt.

3.4 Unternehmensnetzwerk als Geldquelle

In diesem Artikel werden nur die durch die Integration von mobilen Geräten zusätzlich entstehenden Bedrohungen für das Unternehmensnetzwerk betrachtet. Es wird auf ein bestehendes Sicherheitskonzept (z.B. nach Grundschutzhandbuch) aufgebaut. Für die zusätzliche Bedrohung durch mobile Geräte sind zwei Szenarien denkbar. Zum einen kann das mobile Gerät einen entfernten Zugriff auf das Unternehmensnetzwerk aufbauen oder es wird von einem Benutzer zurück in das Unternehmen gebracht und lokal verbunden. In beiden Fällen kann ein durch Schadsoftware verseuchtes Gerät versuchen andere Rechner anzugreifen. Gestohlene oder gefundene Geräte können missbraucht werden, um auf Unternehmensdaten zuzugreifen. Außerdem können die mobilen Geräte begünstigt durch ihre diversen Schnittstellen auch Hintertüren vorbei an der Unternehmens-Firewall aufreißen. Damit können zum einen gezielt Daten aus dem Unternehmen geschleust werden und Angriffe auf ein anderes System in dem Unternehmen durchgeführt werden.

4 Notwendige Sicherheitsmaßnahmen

Diese zusätzlich notwendigen Sicherheitsmaßnahmen werden erst durch die Integration mobiler Nutzer im Unternehmen benötigt. Bereits existierende Sicherheitskonzepte müssen zusätz-

lich überprüft und im fortlaufenden Sicherheitsprozess des Unternehmens neu angepasst werden.

4.1 Der sensible und aufmerksame Benutzer

Am besten sollten mobile Geräte physikalisch mit den Benutzern verbunden werden. Da dies möglicherweise nicht ganz so einfach zu realisieren ist, muss auf das Bewusstsein des Benutzers gesetzt werden, gut auf das Gerät aufzupassen und das Gerät nur gemäß der Sicherheitsrichtlinien des Unternehmens zu verwenden. Diese Sicherheitsrichtlinien müssen zunächst durch einen Evaluierungsprozess, z.B. anhand des Grundschutzhandbuches erarbeitet werden. Doch nüchtern betrachtet ist der Benutzer der einzige Teilaspekt, der nicht durch eine Technik „sicher gemacht“ werden kann. Daher sind die Aufklärung und die positive Motivation des Benutzers wichtig. Ohne seine Mitarbeit lässt sich keine sichere Integration bewerkstelligen. Dies gilt auch für die Sensibilisierung des Benutzers gegen „social engineering“ Techniken.

4.2 Mobiles Endgerät als privater Tresor mit Airbag

Die Zahl mobiler Schadsoftware nimmt in letzter Zeit stark zu. In Fällen von Wirtschaftsspionage wird auch vor der physikalischen Veränderung von Geräten nicht zurückgeschreckt. Immer häufiger wird Schadsoftware gezielt für ein Opfer entwickelt, was das erkennen durch herkömmliche Virenscanner nahezu unmöglich macht. Geht man bei mobilen Geräten von einem ähnlichen Verlauf aus wie es bei Arbeitsplatzrechnern zu beobachten war, so werden bald die meisten Geräte mit einer Firewall, Virenscannern, Festplattenverschlüsselung und weiteren Sicherheitsanwendungen von Drittanbietern ausgestattet sein. Nur wie soll ein Unternehmen mit Geräten umgehen, die dem Benutzer, also dem Mitarbeiter, privat gehören? Verantwortlich und bei Fahrlässigkeit persönlich haftbar für die Sicherheit im Unternehmen ist die Unternehmensführung. Dies umfasst auch die mobilen Geräte, auch wenn sie vielleicht weder im Besitz noch Eigentum des Unternehmens sind. Der richtige Ansatz für Geräte, die Eigentum von Mitarbeitern sind ist wohl, den Zugriff auf das Unternehmen von der Kontrolle der IT über das Gerät abhängig zu machen. Dies wird zur Konsequenz haben, dass der Besitzer auf seinem eigenen Gerät keine eigenen Programme, wie Spiele aus dem Internet, installieren darf. Diese könnten Schadsoftware enthalten und die Integrative-Prozesssicherheit gefährden. All diese zusätzlichen Produkte verursachen Kosten für die Anschaffung und Wartung. Zusätzlich bieten sie wiederum durch möglicherweise fehlerhafte Implementierungen eine weitere Angriffsfläche.

Bei den Arbeitsplatzrechnern gibt es nun erste lauffähige Implementierungen für sichere Betriebssysteme, wie z.B. das EMSCB-Projekt mit der Sicherheitsplattform Turaya [EMSCB], welches von einem durch das Wirtschaftsministerium gefördertes Konsortium entwickelt wird. Mit Hilfe von einem standardisierten und inzwischen auf vielen Rechnern verfügbaren Hardwaremodul, dem Trusted Platform Modul (TPM), kann das System mit Beginn des Bootvorgangs seinen Zustand erfassen und überprüfen. Zusätzlich ist es über Virtualisierungstechniken möglich, oberhalb des Turaya-Sicherheitskerns (Security Kernel) herkömmliche Betriebssysteme (Legacy Operating System) auszuführen oder auch Anwendungen mit einem hohen Sicherheitsbedarf isoliert zustarten (vgl. Abbildung 3).

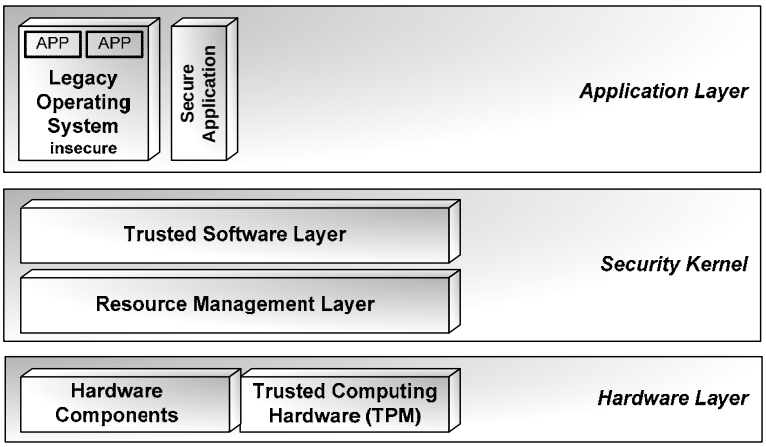

Abbildung 3 - Sicherheitsplattform Turaya

Durch die Verwendung von sicheren Betriebsystemen kann die Integrität der Systeme sichergestellt werden. Anwendungen laufen isoliert und so kann auch Schadsoftware nur in abgesteckten nicht kritischen Bereichen aktiv werden und keinen nennenswerten Schaden anrichten. Da wir bei mobilen Geräten ebenfalls verstärkt mit „mobile malware“ zu rechnen haben, muss auch der Trend bei diesen Geräten in Richtung sicherer Betriebssysteme gehen. Selbst das Anzapfen von der Geräteplatine durch zusätzliche Hardware wäre so zumindest in der Theorie feststellbar. Da der Sicherheitsplattform ein Secure-Boot Vorgang zugrunde liegt kann auch der Hardwarezustand erfasst werden. Natürlich hat auch diese Technik seine Grenzen. In der Praxis wird es immer Manipulationsmöglichkeiten für einen Angreifer geben, wenn dieser physikalischen Zugriff auf ein Gerät hat. Jedoch lässt sich der Aufwand für den Angreifer durch eine vernünftige Sicherheitsplattform erhöhen und der mögliche Aktionsradius im Bezug auf den Zugriff auf Daten lässt sich minimieren.

Leider ist für kleine mobile Geräte - abgesehen von Notebooks - bisher kein Sicherheitsmodul verfügbar, und auch die Entwicklung von sicheren Betriebssystemen für diese Geräte hat, wie man es bei der Sicherheitsplattform Turaya sieht, gerade erst begonnen. Einige Ansätze gibt es von verschiedenen Gruppierungen, leider meist mit sehr unterschiedlichen und teilweise gegensätzlichen Interessen [PiRR05]. Oft wird Trusted Computing auch in den direkten Zusammenhang mit Digitale Rights Management (DRM) gebracht und damit wird die Angst der Benutzer vor ungewollten Restriktionen geweckt.

Der Aufwand, welcher für die Sicherheit getrieben wird, sollte zudem immer dem eigentlichen Schutzbedarf angemessen sein. Daher muss betrachtet werden, welche Daten überhaupt schützenswert sind, wie hoch ein möglicher Schaden ist und wie wahrscheinlich das Eintreten überhaupt ist. Viele der heute verfügbaren Lösungen lassen sich mit einigen Tools wie einer Verschlüsselung, Virenscanner und Firewall erweitern und erfüllen so den notwendigen Schutzbedarf. Jedoch haben Daten, die bei Verlust eine beachtliche Bedrohung für das Unternehmen bedeuten, auf mobilen Geräten nichts zu suchen.

Betrachtet man einige der verfügbaren Lösungen, so gibt es erste Funktionen für ein Managen der Geräte über die Luftschnittstelle (Remote Device Management over the air). Damit lassen sich auch Funktionen zum Löschen oder Sperren von Geräten implementieren, die jedoch immer abhängig von der Erreichbarkeit des Gerätes über die Luftschnittstelle sind. Ein Angreifer wird kaum dafür sorgen, dass das Gerät nach dem Diebstahl so lange wie möglich eine gute Netzabdeckung behält, sondern wird sich mit dem ausgeschalteten Gerät auf den Weg in

ein Speziallabor machen. Dort können die gewünschten Informationen direkt aus dem Speicherbaustein ausgelesen werden. Nichtsdestotrotz sind diese Sicherheitsfunktionen wichtig, da sich dieser Aufwand für einen Angriff nur bei besonders schützenswerten und daher für den Angreifer wertvollen Daten überhaupt lohnt.

4.3 Eine vertrauenswürdige Zugangsebene

Betrachtet man einige der zurzeit verfügbaren Lösungen für mobile E-Mail, so ist schon einiges getan. Die Kommunikation genügt aufgrund zertifikatsbasierter Verschlüsselung bereits sehr hohen Sicherheitsanforderungen. Die Zertifikate müssen zuvor offline zwischen Client und Server ausgetauscht werden. Sowohl Server als auch Client werden authentisiert. Die unsichere Zugangsebene bereitet bei der Betrachtung allgemein keine weiteren größeren Probleme. Problematisch ist einzig die Nichtverfügbarkeit des Dienstes wegen fehlender Netzabdeckung oder Störungen im Netz.

4.4 Ein gerüstetes Unternehmensnetzwerk

Zu dem Sicherheitskonzept für das Unternehmensnetzwerk kommt eine Reihe von Anforderungen durch die Integration mobiler Nutzer hinzu. Dies bedeutet natürlich auch einen erhöhten Aufwand für die IT und erhöhte Ausgaben für die IT-Sicherheit, was bei der Betrachtung der Wertschöpfung durch mobile Geräte auch betrachtet werden muss.

Wenn wir nun auf Seiten der mobilen Geräte sichere Betriebssysteme fordern, ist die logische Konsequenz, dass wir dies auf Seiten der Server auch tun. Zurzeit kann der angemessene Schutzbedarf jedoch noch mit anderen Mitteln realisiert werden. Diese Geräte befinden sich schließlich in der direkten Kontrolle der IT des Unternehmens und können ganz anders gesichert und gewartet werden als mobile Geräte. Mit dem Aufbau der Tunnelverbindung zwischen mobilen Gerät und Unternehmen und zusätzlich zu der dabei durchgeführten Authentikation, muss es für den Server und für das mobile Gerät die Möglichkeit geben, den Zustand der Hard- und Software des jeweils anderen abzufragen. Bestimmte Softwarekonfigurationen werden zuvor von einem Administrator attestiert, und den Systemen mit diesem vertrauenswürdigen Zustand wird der Zugriff auf das Netzwerk gestattet.

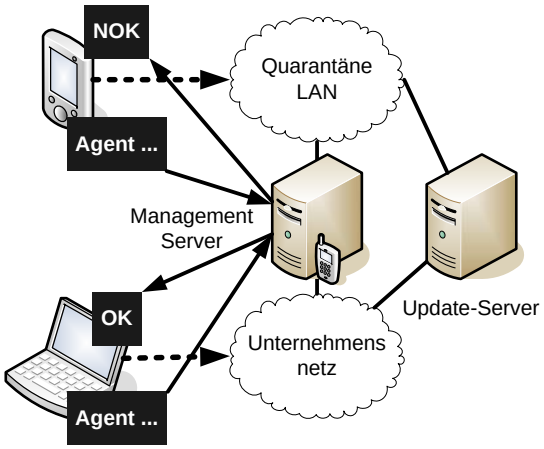

Abbildung 4 - Agenten basierte Zugangsregelung

Ist der Zustand für das mobile Gerät nicht wie erwartet, kann das Gerät in ein virtuelles Netzwerk in eine Quarantäne geleitet werden, in der es nur Zugriff auf einen Updateserver hat.

Erste Realisierungsideen hierfür gibt es z.B. von Microsoft mit NAP, von Cisco mit Cisco Trust Agent (CTA) und von Nortel mit TunnelGuard. Diese Lösungen arbeiten jedoch nicht auf sicheren Betriebssystemen, sondern mit auf den Clients installierten Agenten. Die Agenten erfassen den Status von einem System und geben diesen über unterschiedliche Nachrichtenformate weiter an einen Management Server, welcher den Zugriff regelt. Wer garantiert jedoch dem Management Server, dass nicht ausgerechnet ein Angriff auf den Agenten stattgefunden hat? Ein weiteres Problem ist ein Mangel der Verfügbarkeit von Agenten für verschiedene Plattformen, auf die wir im Bereich mobiler Geräte stoßen.

Da die mobilen Geräte auch zurück in das Unternehmen geführt werden, muss auch das Netzwerk gegen Angriff von innen besser geschützt werden. Firewallsysteme oder Instrusion Dectection Systeme helfen da wenig, da sie zum Schutz vor Angriffen von außen entwickelt wurden. Lösungen wie Self-Defending Network von Cisco oder IntraPROTECTOR von der COMCO sind darauf ausgelegt, interne Angriffe zu erkennen.

5 Fazit

Auf welche Daten sollte welcher Mitarbeiter wann Zugriff bekommen? Diese zentrale Frage sollte gestellt werden, bevor jeder Mitarbeiter mit einem mobilen Gerät ausgestattet wird. Mobiles Arbeiten kann die Produktivität und die Wertschöpfung steigern, jedoch führt dies auch zu einem erhöhten Management- und Sicherheitsaufwand für die IT eines Unternehmens. Dies kann bei schlechter Planung schnell dazu führen, dass die erhoffte Wertschöpfung durch die Integration der Geräte ausbleibt. Mit der Einführung der mobilen Geräte muss das hoffentlich schon bestehende Sicherheitskonzept angepasst werden. Wichtig ist die Implementierung einer Integrativen-Prozesssicherheit. Das umfasst alle vorgestellten Teilaspekte und die Einbeziehung des Kontexts zwischen ihnen. Muss ein mobiler Mitarbeiter die gleichen Zugriffsrechte haben, die er auch an seinem festen Arbeitsplatz hat? Welche Daten sind für einen mobilen Zugriff einfach zu sensibel?

Wichtigste technische Herausforderungen in nächster Zeit werden jedoch sichere Hard- und Softwarelösungen für mobile Endgeräte sein. Neben der gegenseitigen Authentikation und dem Einsatz von zertifikatsbasierter Verschlüsselung für die Kommunikation, muss die vorliegende Hard- und Softwarekonfiguration überprüfbar sein und gegenseitig zuverlässig abgefragt werden können. Daher fordern wir die Entwicklung der dafür benötigten sicheren Betriebsysteme und Hardware-Sicherheitsmodule für mobile Geräte. Eine wirklich sichere Integration der mobilen Nutzer ist bis dahin nicht realisierbar. Das wird jedoch kaum die Antwort eines mit der Integration mobiler Geräte beauftragten Administrators an seinen Vorgesetzten sein.

Abhängig vom Schutzbedarf der Daten müssen weitere verschiedene Sicherheits-Tools verwendet werden, um das Gerät gegen Gefahren zu härten. Die Ausgaben für solche Sicherheits-Tools und der Wartungsaufwand können die Kosten für die mobilen Geräte schnell in die Höhe treiben.

Literatur

[BSI03] Bundesamt für Sicherheit in der Informationstechnik (BSI). GSM-Mobilfunk Gefährdungen und Sicherheitsmaßnahmen. Referat III Mobilfunksicherheit (2003).

[CáSa06] Cáceres, Sailer. Trusted Mobile Computing, IBM T.J. Watson Research Center (2006).

[EMSCB] European Multilaterally Secure Computing Base (EMSCB). Homepage. (2006).

[FlexiSpy] FlexiSpy. http://www.netzwelt.de/news/73907-flexispy-der-kostenpflichtige-handytrojaner.html (2006).

[GSHB05] Bundesamt für Sicherheit in der Informationstechnik (BSI), Grundschutzhandbuch (2005).

[HEIS06] Heise News vom 12.06.2006, USB-Sticks als Trojanische Pferde der Neuzeit, http://www.heise.de/newsticker/meldung/74135 (2006).

[IMNR06] Homepage des Innenministeriums des Landes NRW. Informationen zu Wirtschaftsspionage. http://www.im.nrw.de (2006).

[LiPo06] M. Linnemann, N. Pohlmann, Die vertrauenswürdige Sicherheitsplattform Turaya, InP. Horster (Hrsg.): DACH Security 2006, syssec (2006) 302-313.

[PiRR05] Pisko, Rannenberg, Rossnagel. Trusted Computing in Mobile Platforms. DuD 29/2005. (2006).

[TCG] Trusted Computing Group. Homepage. (2006).