Mobil, aber bitte sicher

Sichere Einbindung mobiler Endgeräte in Unternehmensnetze

Kai-Oliver Detken

Mobile Endgeräte sind immer weiter verbreitet. Dabei werden auch zunehmend sicherheitskritische Geschäftsprozesse über sie abgewickelt und sensible Daten auf ihnen verwaltet. Zudem werden sie zunehmend in Unternehmensnetze integriert. Mit ihrer steigenden Funktionalität wächst aber auch das Risiko von Sicherheitsproblemen. Es gibt zwar verschiedene Sicherheitslösungen im Bereich mobiler Anwendungen und Netze. Viele von ihnen sind aber proprietär und behandeln häufig nur einen bestimmten Sicherheitsaspekt wie z.B. Verschlüsselung, Virenschutz, mobiles VPN. Oftmals fehlen auch Mechanismen, um eine zentrale und sichere Distribution von Anwendungen und Sicherheitsrichtlinien in Netzen mobiler Endgeräte zu ermöglichen.

Dr. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Der Schutzbedarf von IT-Infrastrukturen steigt ständig, da immer mehr Geschäftsprozesse von ihnen abhängen. Durch die Einführung mobiler Endgeräte verschärfen sich diese Anforderungen zusätzlich. Während früher die Angriffsvektoren auf die erreichbaren Serversysteme gerichtet waren, haben sie sich heute auf die Firewall und das VPN-Gateway verlagert. Hinzu kommen direkte Attacken auf die Endgeräte, die sich außerhalb des sicheren Netzes temporär aufhalten und über die man gesicherte Zugänge ins Unternehmensnetz aufbauen könnte (*Bild 1*).

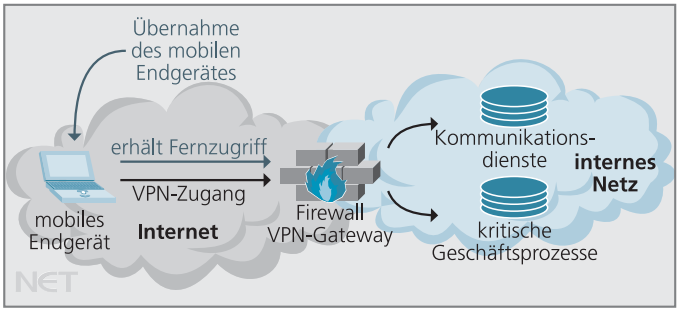

Bild 1: Angriffsvektor auf mobile Endgeräte

Um mobile Netze abzusichern, gibt es bereits verschiedene Lösungen. Diese sind aber meist auf eine Plattform (SymbianOS, BlackBerryOS oder Windows Mobile) beschränkt. So gibt es beispielsweise zwar eine Nokia-Lösung für mobile VPNs, die aber keine anderen Plattformen unterstützt. Ähnliches gilt für Personal-Firewall-Lösungen. Die Firma Research in Motion (RIM) stellt zwar umfangreiche Sicherheitsmechanismen – von der Verschlüsselung bis zu Aspekten der Fernadministration – für die Blackberry-Plattform zur Verfügung, allerdings gibt es solche Sicherheitsmechanismen in dieser Durchgängigkeit nicht für die anderen Plattformen. Zusätzlich ist die Blackberry-Lösung proprietär und fiel bereits durch einige Sicherheitslücken auf. Besonders wünschenswert wäre darüber hinaus ein Werkzeug zur sicheren Fernadministration von mobilen Netzen und eine Distributionsplattform, mit der Software an die einzelnen mobilen Endgeräte abgesichert verteilt wird. Bösartige Software (Malware) kann auf diese Weise nicht einfach auf den mobilen Endgeräten installiert werden.

Anforderungen an mobile Endgeräte

An mobile Endgeräte werden spezielle Forderungen gestellt, denn durch ihre Mobilität werden sie leichter angreifbar. Auch durch die Nutzung unterschiedlicher Netzzugänge sind PDA, Laptop usw. nicht einfach handhabbar:

- Ein *Recovery* von mobilen Endgeräten kann z.B. bei Notebooks durch eine Recovery-Partition auf der lokalen Festplatte oder durch einen Datenträger, den der Mitarbeiter immer mitführen müsste, realisiert werden. Um ein Recovery erfolgreich durchführen zu können, muss sich die physische Hardware in ein-

Das Thema in Kürze

Mobile Endgeräte werden verstärkt in Unternehmensnetze integriert. Doch nimmt damit auch das Risiko von Sicherheitsproblemen zu. Leider fehlen immer noch ausgereifte, plattformunabhängige Werkzeuge, die zur Sicherung von mobilen Netzen eingesetzt werden können. Mit dem TNC-Ansatz, auf dem z.B. das Simoit-Projekt bereits herstellerunabhängig aufsetzt, könnte ein höheres Sicherheitsniveau erreicht werden.

wandfreiem Zustand befinden, d.h., der Recovery-Vorgang kann nur bei defektem Betriebssystem vorgenommen werden. Bei den mobilen Endgeräten wie z.B. Smartphones kann ein neues System z.B. über eine Speicherkarte wiederhergestellt werden.

- Die *Remote Installation* ist erforderlich, wenn auf dem mobilen Endgerät ein Minimalbetriebssystem lauffähig ist, in dem auch die nötigen Treiber für die Konnektivität vorhanden sein müssen. Ist das erfüllt, kann das Endgerät eine Verbindung zum Hauptsitz aufnehmen und die benötigten Programme installieren lassen. Hierzu ist serverseitig eine Softwareverteilungslösung erforderlich, die in diesem Fall die Software auch über die Firmengrenzen hinweg transportieren muss. Ein Problem stellt allerdings die Datenmenge bzw. die benötige Downloadzeit bei schmalbandiger Verbindung des Endgerätes dar.
- Damit sich ein mobiles Endgerät erfolgreich am Hauptsitz anmeldet und auch die Berechtigung besitzt, das interne Netz zu nutzen, muss ein bestimmter *Patchlevel* der verschiedenen Anwendungen vorhanden sein. Das Bereitstellen von Patches kann von einer Softwareverteilungslösung analog zur Remote Installation vorgenommen werden. Je nach Strenge der Security Policys kann normal gearbeitet werden oder man befindet sich in einer Quarantänezone.
- Eine *Quarantänezone* ist ein vom Firmennetz abgeschlossener Bereich in dem sich eine Softwareverteilungslösung befindet. Die Softwareverteilung hält alle aktuellen Patches von Anwendungen und sicherheitsrelevanten Diensten wie Antiviren- und Antispy-Definitionen. Das mobile Endgerät muss diese Quarantänezone passieren, um in das lokale Netz zu kommen. Sollten auf dem Endgerät einige Patches fehlen, so werden diese installiert und der Client aktualisiert.

Die Authentifizierung der mobilen Mitarbeiter kann auf Benutzer- und Hardwareebene erfolgen. Zum einen wird überprüft, ob das Gerät im Firmennetz erlaubt ist, zum anderen wird der anzumeldende Benutzer überprüft. Heutige Authentifizierungsarten bieten die wissensbasierte (Passwort, PIN), die besitzorientierte (Hardware-Token), die biometrische (Fingerabdruck, Iris-Scan) und die Multifaktor-Authentifizierung (Kombination verschiedener Arten). Diese können über verschiedene Authentifizierungstechniken umgesetzt bzw. implementiert werden:

- IEEE 802.1x ist eine portbasierte Zugangssteuerungsmethode, die die Authentifizierung auf höheren Ebenen erlaubt (ULAP – Upper Layer Authentication Protocol), um direkt zwischen Client und Authentifizierungsserver zu wirken. Sie definiert letztendlich ein Rahmenwerk zur Authentifizierung und Zugangskontrolle sowie zum Verhalten der Ports (authentifiziert/nicht authentifiziert).
- Remote Access Dial-in User Service (Radius) wurde ursprünglich von der Livingston Enterprise Inc. entwickelt und stellt ein Authentifizierungs- und Autorisierungsprotokoll für Zugangsserver dar. D.h., Radius wurde mit der Prämisse entwickelt, Benutzern den Fernzugang zu diversen Ressourcen z.B. über eine Wählverbindung auf einen NAS bzw. RAS zu ermöglichen.
- Extensible Authentication Protocol (EAP) ist ein allgemeines Rahmenwerk für multiple Authentifizierungsmethoden, um Benutzer auf unterschiedlichste Arten (Passwort, Token, SmartCard, PKI, biometrisch usw.) authentifizieren zu können.

Der TNC-Ansatz

Die Trusted Computing Group (TCG) entwickelte mit der Spezifikation Trusted Network Connect (TNC) einen standardisierten Ansatz zur Realisierung vertrauenswürdiger Verbindungen z.B. über das Internet. Die TNC-Architektur ist die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten. Sie bezieht dabei schon bestehende Sicherheitstechniken wie VPNs, IEEE 802.1x, EAP und Radius mit ein.

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

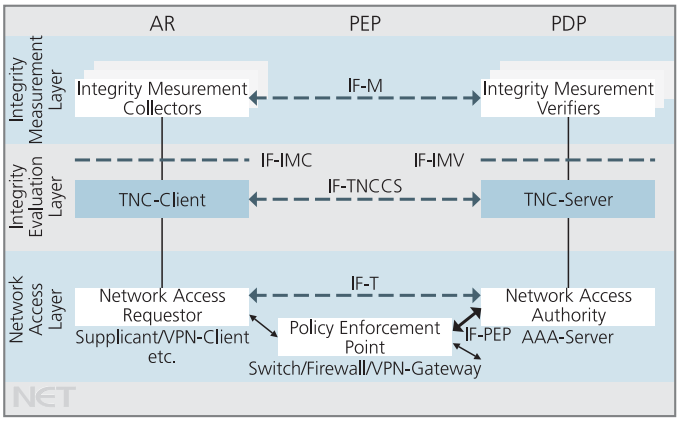

Bild 2: TNC-Architektur

Wie in *Bild 2* zu sehen ist, besteht die TNC-Architektur aus verschiedenen Einheiten. Ähnliche Funktionen oder Rollen in der TNC-Architektur sind durch den Network Access Layer, den Integrity Evaluation Layer und den Integrity Measurement Layer zusammengefasst. Diese drei abstrakten Layer wurden waagerecht über die Komponenten der drei Einheiten gelegt; das Zusammenwirken der einzelnen Komponenten wird über Interfaces realisiert.

Die Einheiten besitzen folgende Aufgaben:

- Der *Access Requestor* (AR) stellt die Verbindung in ein geschütztes Netz her. Hier sorgt der Network Access Requestor für den sicheren Kommunikationskanal zum entfernten Netz und dem PDP. Der TNC-Client ist für das Sammeln von Informationen

zum Gerätezustand zuständig. Diese Informationen werden von Integrity Measurement Collectors an den TNC-Client geliefert.

- Der *Policy Decision Point* (PDP) entscheidet für die Anfrage des AR, wie die Zugriffsrechte für die Verbindung aussehen. Die Network Access Authority ist dabei für die Kommunikation zum anfragenden Gerät und das Setzen der entsprechenden Policy im PEP zuständig. Die Basis für die Policy bildet die Empfehlung des TNC-Servers, der dazu mit dem TNC-Client kommuniziert und Daten vom TNC-Client an die Integrity Measurement Verifiers zur Entscheidungsfindung weiterleitet.
- Der *Policy Enforcement Point* (PEP) bildet die vom PDP erhaltene Zugriffsberechtigung des AR ab.

Alle Einheiten und Komponenten in der Architektur sind logische und nicht physische Einheiten oder Komponenten. Ihre Realisierung kann daher unterschiedlich erfolgen.

Vergleichbare Realisierungen kommen u.a. von Cisco Systems und Microsoft. Die Network-Access-Protection-Architektur (NAP) ist die Implementierung von Network Access Control durch das Unternehmen Microsoft. Cisco Systems nennt seinen Ansatz Network-Admission-Control-Architektur (NAC). Beide Architekturen sind mit der des TNC zu vergleichen, wobei sich aber die Schnittstellen und die Bezeichnungen der einzelnen Einheiten unterscheiden. Der Einsatz von NAC erfordert bisher eine vollständige Cisco-Hardwareinfrastruktur und Cisco-Softwarekomponenten. Dank eines Lizenzaustauschabkommens zwischen Cisco und Microsoft wird der NAP-Client von Microsoft jedoch in Zukunft auch das Protokoll des Cisco Trust Agent unterstützen. In Hardwarekomponenten wird NAC dagegen in absehbarer Zeit nur von Cisco angeboten werden.

Umsetzung im Simoit-Projekt

Im Simoit-Projekt (**www.simoit.de**) wurde anhand der Anforderungen an mobile Endgeräte und der Anwendungsfälle beim Pilotkunden eine Entwicklungs- und Testplattform aufgesetzt, die den TNC-Ansatz praktisch evaluieren soll. Aufgrund der hohen Anforderungen an die organisatorische Sicherheit der Unternehmen bei der Einführung einer vollständigen TNC-Architektur, wurde dabei eine Lösung entwickelt, die eine schrittweise Migration auf TNC ermöglicht. Die Hauptplattform stellt dabei das Mobile Security Gateway (MSG) dar, das aus verschiedenen Modulen besteht (*Bild 3*).

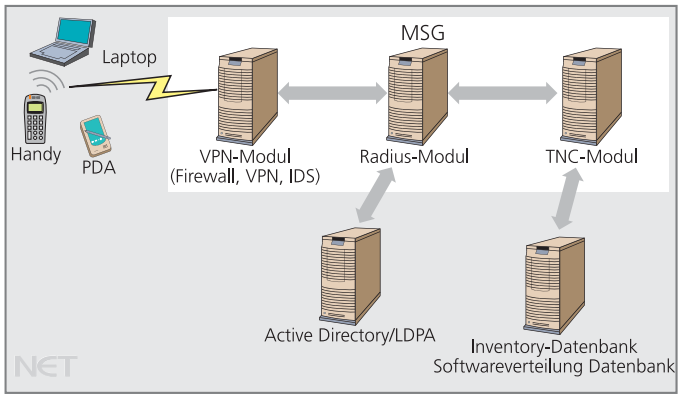

Bild 3: Übersicht der Simoit-Module

Dabei wurden speziell Open-Source-Software-Projekte und -Ansätze (OSS) gewählt, um eine offene, standardkonforme Umsetzung zu ermöglichen. Gleichzeitig konnte die Flexibilität gewahrt bleiben, so dass bestehende Komponenten wie z.B. Firewall-Systeme eingebunden werden können. In diesem Fall würde das jeweilige Simoit-Modul nicht verwendet, sondern nur eine Schnittstelle zur Verfügung gestellt werden.

Beim Pilotkunden war zusätzlich die Anbindung an einen internen Active Directory Server (ADS) notwendig, weshalb über LDAP auch hier eine Schnittstelle zur Verfügung gestellt wurde. Darüber werden sämtliche internen Benutzerprofile abgefragt, die für die Authentifizierung wichtig sind, und an den MSG weitergeleitet. Beide Systeme gleichen sich gegeneinander mehrmals am Tag ab, da der ADS innerhalb des Unternehmensnetzes zu finden ist und unabhängig vom MSG arbeitet.

Während vollständige TNC-Architekturen Software-Agents und Integrity Measurement Collectors auf Client-Seite voraussetzen, arbeitet die Simoit-Plattform auch mit unveränderten Clients zusammen, die nur über eine Standardinstallation verfügen. In diesem Fall wird zusätzlich zur gewohnten Nutzerauthentifizierung die verwendete Hardware über ein X.509 identifiziert. Der im Simoit-Projekt verwendete FreeRadius-Server (**www.freeradius.org**) wurde dafür so erweitert, dass er über standardisierte Schnittstellen mit einem TNC-Server verbunden ist. Der TNC-Server baut auf die Open-Source-Bibliothek „libtnc" auf und nutzt speziell entwickelte Integrity Measurement Verifier zur Integritätsprüfung. Diese sind an die Softwareverteilung des Pilotkunden angepasst und ermitteln den gewünschten und vorhandenen Softwarestand eines Endgerätes, um über diese Informationen den Zugriff auf das Unternehmensnetz zu regeln. Es können allerdings beliebige Softwareverteilungssysteme angebunden werden.

Fazit

Zusammenfassend betrachtet, fehlen mithin noch immer ausgereifte und plattformunabhängige Werkzeuge, die zur Absicherung von mobilen Netzen eingesetzt werden können. Da mobile Netze immer komplexer werden, wird ihre Administration immer aufwendiger und fehleranfälliger, insbesondere hinsichtlich der IT-Sicherheit. Aus diesem Grund werden Mechanismen, die eine zentrale Administration von mobilen Netzen ermöglichen, immer wichtiger. Der vorgestellte TNC-Ansatz ist eine Möglichkeit, ein höheres Sicherheitsniveau zu erreichen. Das Simoit-Projekt setzt bereits herstellerunabhängig auf ihn auf.

Leider ist der TNC-Ansatz noch nicht endgültig spezifiziert, so dass er noch unterschiedlich interpretierbar ist und proprietäre Implementierungen entstehen können. Dies wird sich aber durch das Vorantreiben des TNC-Standards verbessern. *(bk)*