SCHUTZ MOBILER IT-CLIENTS IM UNTERNEHMENSEINSATZ

eingereicht von:

Hannes Slanar

DIPLOMARBEIT

zur Erlangung des akademischen Grades
Diplom Ingenieur (FH)
(Dipl. Ing. (FH))

Fachhochschule St. Pölten

Studienrichtung: Telekommunikation und Medien

Begutachter:
Dipl.-HTL-Ing. Andreas Schaupp MSc MAS

St. Pölten, im September 2007

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der vom Begutachter beurteilten Arbeit überein.

St. Pölten, am 13. September 2007 Unterschrift:

Abstract

In den letzten Jahren ist der Gebrauch von Notebooks stark angestiegen. Vielen Mitarbeitern wird von ihren Unternehmen ein mobiler Desktopersatz zur weltweiten Kommunikation und Datenverarbeitung bereitgestellt. Der Einsatz dieser bringt auch neue Angriffsmöglichkeiten um in sensible Unternehmensdaten einsehen zu können.

Angreifer bedrohen mobile IT-Clients nicht nur über Netzwerke, sondern auch mittels lokaler Angriffsmöglichkeiten, da diese Endgeräte durch ihre Mobilität leicht in die Hände von unerwünschten Personen fallen können. Es muss daher dafür gesorgt werden, dass bei Diebstahl oder Verlust eines Clients keine sensiblen Daten ausgelesen werden können. Mobile IT-Clients werden oft in unsicheren öffentlichen Netzwerken eingesetzt. Diese müssen daher besonders gut gegen Angreifer aus dem selben Kommunikationsnetz abgesichert werden. Außerdem darf nicht vergessen werden, dass die Anwender der Clients so wenig wie möglich durch Sicherheitsvorkehrungen an ihrer Arbeit gehindert werden.

Diese Diplomarbeit stellt, nach einer Erläuterung typischer Angriffsmethoden, Schutzmechanismen vor, welche mobilen IT-Clients mehr Sicherheit bieten sollen. Es wurden gewisse Schutzmöglichkeiten unterschiedlicher Kategorien gegen bekannte Angriffsmöglichkeiten getestet und evaluiert. Ziel dieser Arbeit war es, Möglichkeiten zu finden, welche mobilen IT-Clients im Unternehmenseinsatz ausreichend Schutz bieten können.

Weiters werden Vorschläge erbracht, wie Unternehmen ihre mobilen IT-Clients vor Angriffen unterschiedlicher Arten schützen können. Außerdem wird gezeigt, mit welchen Mitteln eine sichere Kommunikation über öffentliche Netzwerke eingerichtet werden kann.

Abstract

In the past few years the use of notebooks has increased considerably. A large part of employees are provided with Notebooks by their companies for worldwide communication and data processing. But the use of mobile devices also creates new opportunities to access confidential company data.

Attackers pose a threat to mobile IT-clients not only via networks but also by local attacks as these terminals - due to their mobility - may easily fall into the hands of unauthorized persons. Therefore measures have to be taken to prevent access to data in the case of theft or loss of a client. In many cases mobile IT-clients are used in insecure public networks. As a consequence these must be protected against attacks from the same communication network. Besides, one has to keep in mind that the users of the clients will not be inhibited in their work through security measures.

This diploma thesis lists possible methods of attacks and introduces respective security measures to give mobile devices a high degree of protection. Different mechanisms of protection against known possibilities of attacks were tested and evaluated. It is the aim of this work to find ways which can offer mobile IT-clients used in companies sufficient protection.

Furthermore, suggestions are made as to how companies can protect their mobile IT-clients against various kinds of attacks. Also means for secure communication via public networks are shown.

Danksagung

In der Zeit, in der ich diese Diplomarbeit verfasst habe, wurde ich von vielen Menschen unterstützt. Ganz besonders möchte ich meinem Diplomarbeitsbetreuer, Herrn Dipl.-HTL-Ing. Andreas Schaupp MSc MAS, für seine wertvolle Hilfe, fachliche Unterstützung und Geduld bei der Erstellung dieser Arbeit danken.

Großen Dank spreche ich auch meiner Familie aus, die mich während meines gesamten Studiums unterstützt hat und mir besonders beim Zustandekommen der vorliegenden Arbeit immer wieder Mut zugesprochen und mein Durchhaltevermögen gestärkt hat.

St. Pölten, am 13. September 2007 Hannes Slanar

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

In den letzten Jahren hat die Nachfrage nach mobilen Endgeräten stark zugenommen. Für Unternehmen und deren Mitarbeiter sind Notebooks zu einem wichtigen Arbeitsmittel geworden. Durch Zunahme von Funktionalität kann das Notebook heutzutage sogar als Desktopersatz verwendet werden. Da der Preis stark sinkt, nimmt ihre Zahl immer schneller zu. Im Jahr 2004 ergab sich durch Unternehmensnachfragen ein Wachstum von 14,5% in diesem Marktsegment.[1]

Die Entwicklung von mobilen Kommunikationstechnologien wie der Mobilfunk hat in den letzten Jahren rasante Fortschritte gemacht. Für viele Leute wurde es zum Ziel, immer und überall erreichbar zu sein und bestimmte Dienste nützen zu können.

Mobile Kommunikation ist ein sehr wichtiger Faktor für weltweit erfolgreiches Wirtschaften geworden. Unternehmen reduzieren durch den Einsatz neuer mobiler Kommunikationsmittel massiv die Kosten ihrer Arbeitsprozesse und erreichen eine sehr starke Effizienz- und Flexibilitätssteigerung. Sie können ihre Daten schneller aktualisieren und dadurch Geschäftsprozesse schneller abwickeln und Entscheidungen treffen. Unternehmen werden so konkurrenzfähiger und können dem Kunden ein besseres Produkt bzw. eine bessere Dienstleistung anbieten.

1.1 Einsatz mobiler IT-Clients

Mobile Kommunikation wird für österreichische Unternehmen immer wichtiger. Jeder fünfte Mitarbeiter in Österreich ist im Durchschnitt mindestens einmal pro Woche im Außendienst unterwegs.[2] Das Notebook stellt für diese Mitarbeiter eine wichtige Kommunikationsschnitt-

[1] vgl. wienweb.at, [wie07].
[2] vgl. Salzburger Nachrichten, [sal07].

stelle zum Unternehmen dar. Dem Außendienstmitarbeiter stehen mit Hilfe des Notebooks alle IT-Ressourcen des Unternehmens zur Verfügung. Andererseits kann dadurch die zentrale Unternehmensniederlassung immer über die geschäftliche Tätigkeit ihrer Mitarbeiter Bescheid wissen, auch wenn diese sich gerade nicht in der Niederlassung befinden. Somit wird die Performance des Unternehmens stark erhöht.

Der häufigste Einsatz mobiler Kommunikationsprodukte findet in den Bereichen Logistik, Vertrieb, Produktion, Kundendienst und Informationsmanagement Anwendung.[3]

1.2 Warum Sicherheit?

Mit neuen Technologien gibt es daher auch immer neue Möglichkeiten Angriffe auf diese durchzuführen. In der mobilen Kommunikation spielt Sicherheit eine sehr große Rolle. Unter IT-Sicherheit selbst versteht man, dass sowohl die gespeicherten Daten als auch das IT-System vor unbefugtem Zugriff geschützt werden.

Mobile IT-Clients stellen in den meisten Fällen eine Verbindung zum Unternehmen über eine öffentliche Datenleitung her. Diese Datenleitung muss daher immer als unsicher angenommen werden.

In den vergangenen Jahren ist die Zahl der IT-Sicherheitsvorfälle exponentiell angestiegen. Zwischen den Jahren 2000 und 2003 meldete der im deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) angesiedelte Community Emergency Response Team/Coordination Center- (CERT/CC) Bund eine mehr als Verzehnfachung der weltweiten IT-Sicherheitsvorfälle. Abbildung 1.1 zeigt graphisch deren Anstieg in den Jahren 1988 bis 2003.

> *„Eines der größten Probleme bei der Computersicherheit ist, dass die meisten Anwender überzeugt sind, ihnen werde nichts passieren.“*[Cor07]

Am wenigsten ist der Sicherheitsgedanke bei Klein- und Mittelunternehmen verbreitet. Diese argumentieren meistens damit, dass sie keine wichtigen Daten besitzen, die geschützt werden müssten. Ein Angreifer kann aber schon mit auch nicht so wichtigen Daten für das Unternehmen Schaden anrichten, sei es z.B. nur die Kreditkartennummer eines Kunden. Jedes Unternehmen mit einer IT-Infrastruktur muss sich heutzutage über die IT-Sicherheit Gedanken machen, da bereits ein kleiner Sicherheitsvorfall einen großen Verlust für ein Unternehmen bedeuten kann.

[3] vgl. FTK Dortmund, [Dor07].

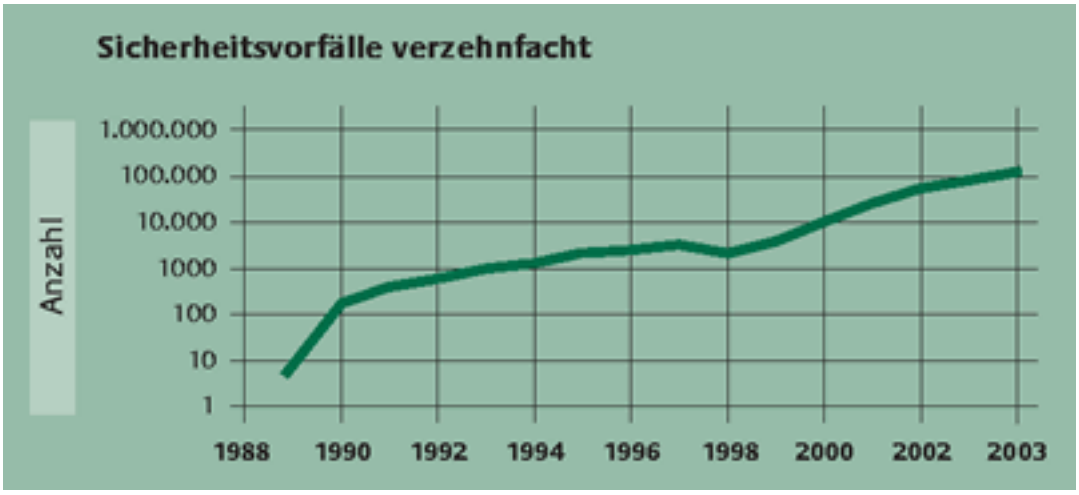

Abbildung 1.1: Sicherheitsvorfälle der letzten Jahre, Quelle: CERT/CC

1.3 Grundelemente der Datensicherheit

Das BSI veröffentlichte 1992 das IT-Sicherheitshandbuch, in dem zunächst drei Grundbedrohungen unterschieden werden, der Verlust von Vertraulichkeit, Verfügbarkeit und Integrität.[4] Durch das starke Ansteigen der Datenkommunikation in den darauf folgenden Jahren wurde zu diesen drei Grundschutzzielen noch die Authentizität hinzugefügt.

Vertraulichkeit

Hierbei handelt es sich um die Geheimhaltung der Daten vor Unbefugten. Es müssen daher Maßnahmen ergriffen werden, um Daten vor unberechtigtem Zugriff zu schützen. In der mobilen Kommunikation ist dies ein wichtiger Punkt, da es für Angreifer leichter ist, Daten auf einem mobilen IT-Client einsehen zu können als auf Rechnern, welche sich am Unternehmensstandort befinden.

Authentizität

In diesem Fall muss eine Überprüfung derjenigen erfolgen, die auf die Daten zugreifen wollen. Dies können nicht nur Personen sein, sondern auch andere Geräte. Es muss möglich sein, Informationen sicher einem Benutzer oder Gerät zuordnen zu können.

[4] vgl. Datenschutz Berlin, [Ber04].

Verfügbarkeit

Unter Verfügbarkeit versteht man, dass die gewünschte Funktion oder die Daten eines Systems für die Benutzer bei Bedarf bereitgestellt werden. Es muss daher verhindert werden, dass Daten abhanden kommen oder auf sie kein Zugriff erfolgen kann. Auch ist sicherzustellen, dass Hard- bzw. Software funktionsbereit sind, sobald sie aufgerufen werden.

Integrität

Unter Integrität versteht man die Unverfälschtheit der Daten. Sie dürfen nicht von Unbefugten im System manipuliert werden können. Es muss daher verhindert werden, dass verfälschte Daten von einem System verarbeitet werden. Da mobile IT-Clients meist in der Öffentlichkeit zum Einsatz kommen, ist es besonders wichtig, die Verfälschung von transportierten Daten zu verhindern.

Kapitel 2

Gefährdungslage mobiler Systeme

Notebooks sind im Regelfall großen Gefahren und Angriffsmöglichkeiten ausgesetzt. Viele Benutzer sind leitende Mitarbeiter, die mit sehr sensiblen Daten arbeiten und sich um Sicherheit in den meisten Fällen nicht kümmern wollen.

Die Gefahren in der mobilen Kommunikation, speziell mit Notebooks, sind vielfältig und lassen sich in Gruppen einteilen. Im Folgenden werden diese näher erläutert.[5]

Diebstahl

Eine der am häufigsten auftretenden Sicherheitsprobleme ist der Diebstahl bzw. Verlust des mobilen Endgerätes. Der Dieb kommt dadurch nicht nur an teure Hardware, sondern in den meisten Fällen auch an sensible Daten des Unternehmens. Dieser Aspekt ist weitaus schlimmer als der reine Verlust der Hard- und Software bzw. der Daten. Aber nicht nur Diebstahl ist ein großes Sicherheitsrisiko in der mobilen Kommunikation, auch durch Unvorsichtigkeit können unerwünschte Personen in sensible Daten einsehen.

> *„In Londoner Taxis wurden im 1. Halbjahr 2001 29000 Laptops, 1300 PDAs und 63000 Mobiltelefone vergessen.“*[Jüp01]

Observation

Das Abhören und Mitschneiden von Datenverbindungen stellt in der mobilen Kommunikation ein großes Problem für die Sicherheit dar. Durch mobile Technologien wie Wireless Local Area Network (WLAN) wird es dem Angreifer enorm erleichtert, die Kommunikation eines mobilen Clients mitzuschneiden. In öffentlichen WLANs kann der Angreifer jeglichen Datenverkehr des Opfers belauschen. Dies erfolgt meistens völlig unbemerkt.

[5] vgl. Eren, S. 145, [Det06].

Manipulation

Der nächste Schritt nach dem Lauschangriff ist die Manipulation der Daten des Opfers. Der Angreifer kann die gesendeten und empfangenen Daten des Opfers zu seinen Gunsten verändern. In diesem Fall glaubt das Opfer, dass es mit seinem gewollten Kommunikationspartner Daten austauscht. In Wirklichkeit empfängt diese Daten der Angreifer, manipuliert sie und sendet sie an die gewollte Kommunikationsgegenstelle weiter.

Impersonation

Eine weitere Angriffsmethode besteht darin, die Identität des Opfers anzunehmen. Hierbei muss der Angreifer nicht die Erscheinung oder Unterschrift des Opfers imitieren. Manchmal reichen die Daten, welche über das Netzwerk geschickt werden aus, um die Identität des Opfers vortäuschen zu können. Der Angreifer genießt dessen Bonität und kann mit dessen Namen Verträge unterschreiben.

Er kann aber auch nur die Infrastruktur des Opfers nutzen wollen. Das beste Beispiel dafür ist eine Breitband-Internetanbindung, welche den Benutzern über WLAN zur Verfügung gestellt wird. Wenn die Sicherheitsvorkehrungen nicht gut genug sind, kann der Angreifer über dieses Netzwerk einsteigen und die Kommunikationsinfrastruktur nutzen.

In letzter Zeit sind die Angriffsstrategien immer ausgeklügelter und raffinierter geworden. Abbildung 2.1 zeigt die Entwicklung der Angriffstechnologien der vergangenen Jahre.

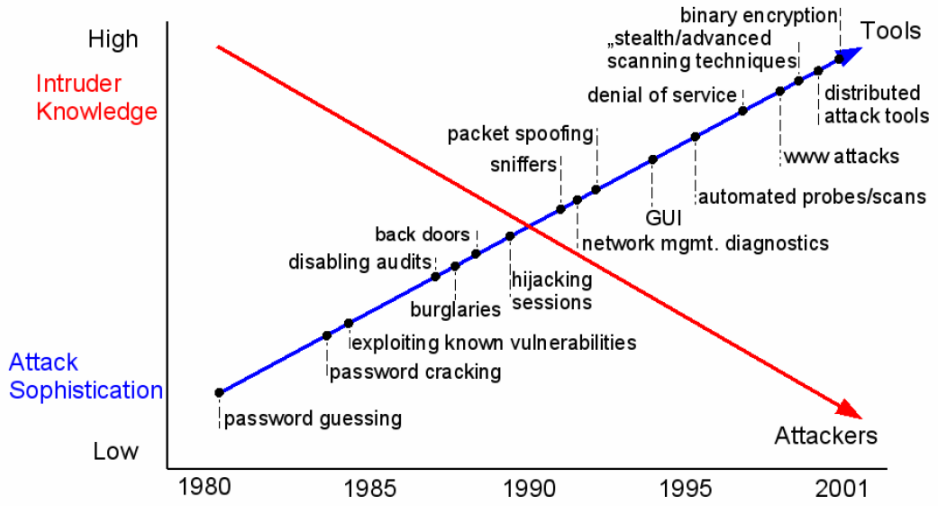

Abbildung 2.1: Entwicklung der Angriffstechnologien, Quelle: Krieger, 2006, S. 8

Die ersten Angriffsmethoden bestanden in einfachem Ausprobieren von Passwörtern. Eine Weiterentwicklung bestand darin das Passwort des Opfers herauszufinden ohne viele Möglichkeiten ausprobieren zu müssen. Durch das große Wachstum des Internets ergaben sich

auch für Angreifer immer schneller neue Wege. Es wurden Tools entwickelt, welche ganz bestimmte Sicherheitslücken ausnützen. Dadurch können wiederum Personen Angriffe durchführen, welche eigentlich kaum großes Wissen über Angriffstechnologien besitzen.

In dieser Arbeit wird grob zwischen zwei unterschiedlichen Angriffsmöglichkeiten unterschieden. Der *lokale Angriff* setzt voraus, dass der Angreifer physischen Zugang zu dem mobilen Client besitzt. Der *Netzwerkangriff* hingegen findet über eine Datenleitung von einem remote Angreifer statt.

2.1 Lokale Angriffe auf Daten

Um einen lokalen Angriff durchführen zu können, muss der mobile IT-Client in den Besitz des Angreifers kommen. Dies geschieht in den meisten Fällen durch Diebstahl oder Verlust des Endgerätes. Der Angreifer hat dadurch nicht nur sachlichen Wert erlangt, sondern er verfügt auch über alle Daten, welche auf dem mobilen Client gespeichert sind. Dies ist sehr problematisch, da in vielen Fällen äußerst sensible Daten auf den Clients gespeichert werden.

Lokale Angriffe sind besonders gefährlich, da der Angreifer sehr viele Möglichkeiten hat, um in die Daten des mobilen Clients Einblick zu bekommen. Er hat in vielen Fällen genügend Zeit und kann sehr viele Angriffsmethoden ausprobieren. Dabei kann er auf der untersten Schicht anfangen.[6]

Im Folgenden werden die Angriffsmethoden auf lokale Daten von mobilen Clients näher beschrieben.

2.1.1 Boot mit spezieller Software

Bei Notebooks, welche nicht nach einem hohen Sicherheitsstandard konfiguriert sind, wird erst nach dem Starten von Windows ein Passwort verlangt. Für einen Angreifer stellt das aber kein Problem dar.

Es gibt einige Tools, welche es erlauben, unter einem anderen System von einem Datenträger zu booten. In den meisten Fällen sind dies Systeme, welche einen Unix Kernel besitzen und New Technology File System- (NTFS) Treiber mitbringen. Mit diesen kleinen Betriebssystemen ist es möglich, auf die Windows Registry zuzugreifen. Man kann also den Passworthash jedes Windows Accounts auslesen bzw. löschen. Windows XP verwendet folgende Schritte, um die gespeicherten Passwörter zu codieren:

[6] Als unterste Schicht ist hier die direkte Steuerung der Hardware bzw. der Ausbau der Festplatte gemeint.

1. Konvertierung zu Unicode.[7]
2. Bildung eines MD4-Hash aus dem Unicode.
3. Verschlüsselung des Hashwertes mit dem DES-Algorithmus. Es wird dabei die RID (Relative Identifier) als Schlüssel verwendet.[8] Das Ergebnis ist ein Hashwert mit einer Länge von 16 Bytes.

Das Passwort kann daher von solchen Tools geändert und der Hashwert kann ausgelesen werden. Mit dem Hash des Passwortes kann eine Offline Brute-Force-Attacke durchgeführt werden.[9] Dies ermöglicht es, in einer akzeptablen Zeit das Passwort herauszufinden. Der Angreifer bekommt dadurch vollen Zugriff auf das Betriebssystem, solange der Benutzer des Notebooks keine weiteren Sicherheitsvorkehrungen getroffen hat.

Umgehen eines BIOS- und Boot-Passwortes

Wenn der Benutzer des Notebooks im BIOS nicht angegeben hat, dass geprüft werden soll, ob von externen Medien gebootet werden kann, muss der Angreifer dies umkonfigurieren, um die Windows Registry bearbeiten zu können. In den meisten Fällen wird aber ein BIOS Passwort verlangt. Man kommt also nur in das BIOS, wenn dieses Passwort bekannt ist.

Viele Hersteller implementieren ein Backdoor-Passwort, welches es ermöglicht, ohne Wissen des momentan gesetzten Passwortes in das BIOS zu gelangen. Diese Passwörter findet man nach Herstellern geordnet sehr oft im Internet.[10] Außerdem ist es bei manchen Herstellern möglich, durch Setzen eines Jumpers am Motherboard das BIOS Passwort zu löschen.

Wenn die Möglichkeit besteht, von einem anderen Medium außer der Festplatte zu booten, ohne das BIOS Passwort eingeben zu müssen, kann das Passwort mit einem kurzen Programm gelöscht werden. Es muss nur der CRC-Wert des CMOS-RAM in einen falschen Wert geändert werden. Beim nächsten Power On Self Test (POST) verifiziert das Notebook diesen Wert mit seinem errechneten. Stimmt dieser nicht überein wird eine CRC-Fehlermeldung ausgegeben. Dies hat zur Folge, dass das Passwort neu gesetzt werden muss. Diese Methode bewirkt jedoch, dass alle Werte aus dem BIOS gelöscht werden und wieder ihren Standardwert annehmen.

Es ist möglich, im BIOS ein Boot-Passwort zu setzen. Der User muss bei dieser Einstellung immer vor dem booten des Systems sein Passwort eingeben. Um diese Sicherheitsvorkehrung zu umgehen, gibt es Dongles, welche während des Starts des Notebooks angeschlossen

[7] Unicode ist ein internationaler Standard, welcher jedem sinntragenden Zeichen einen Code zuweist.
[8] Ein Benutzer in einem Windows System besteht aus einem SID (Security Identifier) und einem RID. Der SID wird dem RID vorangestellt und ergibt so die interne Identifikation des Benutzers.
[9] Bei dieser Angriffsmöglichkeit werden nach der Reihe Passwörter ausprobiert.
[10] vgl. FileStorm, [Fil04].

sein müssen.[11] Dadurch wird das Boot-Passwort nicht abgefragt und es kann auf dem Notebook ein System gestartet werden.

Umgehen eines Harddisk Passwortes

Wenn auf dem mobilen Client ein Harddisk- (HD) Passwort gesetzt ist, muss dieses immer vor dem Zugriff auf die Festplatte eingegeben werden. Dieses Passwort kann einfach im BIOS aktiviert werden. Damit also ein Angreifer die Daten auf der Festplatte einsehen kann, muss er dieses Passwort umgehen. Es ist möglich, mit einem speziellen System zu booten und mit einer Software dieses Passwort zu deaktivieren.[12]

Eine zweite Möglichkeit ist, den Festplattenzugriff mit einem Standard Master Passwort zu aktivieren. Die meisten Hardware Hersteller haben ein Standard Passwort für ungewollt gesperrte Festplatten.[13]

Außerdem ist es mit einer speziellen Hardware möglich, diesen Passwortschutz zu umgehen. Solch eine Hardware wird z.B. von der Firma Vogon bereitgestellt.[14] Die geschützte Festplatte wird an das Gerät angeschlossen. So kann jedes Passwort, ohne Verlust der Daten auf der Festplatte, umgangen werden.

2.1.2 Wechselmedien

Ein sehr beliebtes Wechselmedium für Daten sind heutzutage USB-Sticks. Sie werden häufig als vorübergehende Datenspeicher verwendet. Es kommen auch immer mehr Multifunktionsgeräte als USB-Speicher zum Einsatz, wie z.B. MP3-Player und ähnliches.

Für Angriffe über Wechselmedien wird vorausgesetzt, dass der Angreifer sehr kurze Zeit Zugriff auf den mobilen Client hat. Dies kann vorkommen, wenn der Inhaber des Notebooks kurz seinen Arbeitsplatz verlassen hat oder eine Datei auf dem USB-Stick des nicht vermuteten Angreifers einsehen will. Wenn dem Angreifer so eine Chance geboten wird, kann dieser ohne viel Aufwand die Daten unauffällig von dem Notebook auf seinen Datenträger kopieren. Der Angreifer muss auf seinem Stick nur ein Autorun-Script ausführen. Sobald der Benutzer des mobilen Clients im Windows Explorer versucht, mittels Doppelklick auf das Wechselmedium zuzugreifen, wird das Script gestartet. Um einen USB-Stick für solche Angriffe vorzubereiten bedarf es nicht viel Aufwand.[15] Es muss lediglich eine autorun.inf-

[11] Ein Dongle wird über eine Schnittstelle an die Hardware angeschlossen und kann so einen speziellen Zustand des Systems bewirken.
[12] vgl. Rockbox, [Roc03].
[13] vgl. Vidström, S. 19, [Vid05].
[14] vgl. Vogon, [Vog07].
[15] vgl. USB Hacks, [Hac06].

Datei auf dem Datenträger erstellt werden, welche weitere .bat-Dateien ausführt. Es wird direkt nach dem Ausführen der autorun.inf nach Dateien eines speziellen Dateityps gesucht und auf den USB-Stick kopiert. Der Angreifer ist nun im Besitz einiger Daten des mobilen Clients.

Neue Angriffsmöglichkeiten bietet der neue U3-Standard. U3 steht für *„Simplified for You, Smarter about You, As mobile as You“*.[16] Mit diesem Software- und Hardware-Standard ist es möglich, ohne vorherige Installation auf dem Rechner Programme direkt von dem USB-Speicher auszuführen. Die U3-Software führt Anwendungen aus, liest und schreibt auf die Festplatte und löscht danach wieder ihre geschriebenen Dateien. Der Wechseldatenträger besteht aus zwei logischen Speichermedien. Auf dem einen befindet sich die schreibgeschützte U3-Software. Auf dem anderen befinden sich die Anwendungsdaten.

Es ist nun möglich, über die Update Prozedur ein falsches Image in die schreibgeschützte Partition einzuspielen. Es kann also jedes Image, welches auf der Partition Platz hat, eingespielt werden. Hier kann mittels Autorun Funktion bösartiger Code ausgeführt oder in die Daten des mobilen Clients eingesehen werden. Da sich die schreibgeschützte Partition des U3 fähigen Gerätes wie eine Compact Disk-Read Only Memory (CD-ROM) verhält, wird bei aktiviertem Autostart das bösartige Programm ausgeführt, ohne dass der Benutzer den Start des Programms bestätigen muss.[17] Der Angreifer kann daher durch einfaches Anstecken des USB-Sticks gewünschte Daten auf den Speicher herunterladen ohne manuell ein Programm starten zu müssen.

2.1.3 Social Engineering

> *„Der Begriff Sozialkonstruktion bzw. Social Engineering (auch Social Hacking) bezeichnet in der Informatik das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher oder gespielter Kontakte.“*[Waa05]

Der Mensch ist generell das unsicherste Glied in der Sicherheitskette. Die Kunst des Social Engineering ist es, eine Vertrauensbasis zu seinem Opfer aufzubauen. Social Engineering Angriffe können mit keiner Technologie verhindert werden. Sie sind daher eine der gefährlichsten Angriffsformen.

Es werden in der Regel drei unterschiedliche Formen des Social Engineering unterschieden. Bei *Computer Based Social Engineering* hat der Angreifer in den meisten Fällen keinen sozialen Kontakt zu seinem Opfer. Es wird in diesem Fall eine falsche Identität bzw. Vertrau-

[16] vgl. Hama GmbH, [Gmb07b].
[17] vgl. MCGrew Security, [Sec06].

ensbasis ausgenutzt. Das beste Beispiel hierfür sind die so genannten Phishing Attacken.[18]

Human Based Social Engineering ist der eigentliche Social Engineering Angriff. Der Angreifer steht mit dem Opfer in diesem Fall in direktem sozialen Kontakt. Der Täter gibt sich in den meisten Fällen als Autoritäts- bzw. Vertrauensperson aus. Er versucht, eine hektische Situation vorzutäuschen, z.B. einen Serverausfall, der sofortiges Handeln erfordern würde. In solch angespannten Situationen steht das Opfer unter Stress und gibt in den meisten Fällen zu viele Informationen preis.

Die dritte Form ist das so genannte *Reverse Social Engineering*. Bei dieser Methode täuscht der Angreifer ein Problem vor und bietet seine Hilfe an, dieses zu lösen. Das Opfer sieht den Täter somit als den Helfer in Not. Durch das Vortäuschen eines gemeinsamen Feindes bekommt der Angreifer das Vertrauen seines Opfers.

Ein erfolgreicher Social Engineering Angriff setzt sich aus mehreren Stufen zusammen.[19]

1. *Informationsbeschaffung:* Der Angreifer versucht Informationen über sein Opfer zu bekommen. In dieser Stufe ist noch kein Kontakt zum Opfer notwendig.
2. *Aufbauen von Kontakten/Identität fälschen:* Jetzt muss der Täter in eine andere Rolle schlüpfen, vorzugsweise in die Rolle einer Person, die gegenüber dem Opfer höher gestellt ist.
3. *Informationen über das Ziel erarbeiten:* In dieser Phase versucht der Angreifer mit geschickten Fragen an Informationen zu gelangen.
4. *Informationen logisch zusammensetzen:* Alle gesammelten Teilinformationen werden nun zusammengesetzt und entweder als brauchbar oder unbrauchbar eingestuft.

2.2 Netzwerkangriffe

Netzwerkangriffe sind in der Regel leichter zu starten als lokale. Der Angreifer hat keinen physischen Zugriff auf den mobilen Client des Opfers und versucht daher Angriffe über das Netzwerk durchzuführen. IBM meldete im Jahr 2004, zwischen Juli und September, einen Anstieg um 55% der Netzwerkangriffe auf von IBM betreute Systeme.[20]

Besonders durch den Einsatz von mobilen IT-Clients wird es Angreifern erleichtert, Netzwerkangriffe erfolgreich durchzuführen. Da diese oft über öffentliche Datennetze kommunizieren, kann sich der Angreifer im gleichen Netzwerk wie der Client aufhalten.

[18] Beim Phishing wird das Opfer auf Internetseiten gelockt, welche einer vertrauenswürdigen Seite sehr ähnlich sehen. Wenn der Benutzer auf dieser Seite seine Benutzerdaten angibt, kann der Angreifer diese einsehen.
[19] vgl. Waas, S. 4, [Waa05].
[20] vgl. PCDirekt, [PCD04].

Dadurch kann er versuchen, die vom mobilen Client gesendeten bzw. empfangenen Daten zu lesen oder sogar zu verändern. Er kann in Daten einsehen oder falsche Daten an das Opfer senden. Außerdem kann er versuchen, remote Zugriff auf den mobilen Client zu bekommen oder bösartigen Code einzuspielen. In den folgenden Abschnitten wird auf die wichtigsten Angriffsmöglichkeiten über ein Netzwerk eingegangen.

2.2.1 Angriffe auf WLANs

Sehr häufig werden Wireless Local Area Networks von mobilen IT-Clients verwendet. Diese komfortable Technologie ermöglicht es, kabellos Zugriff auf das Internet und zur IT-Infrastruktur des Unternehmens zu erlangen. Sie werden oft auf Flughäfen, in Bahnhöfen oder anderen öffentlichen Einrichtungen angeboten. Diese werden häufig von Telekommunikationsunternehmen in Form von HotSpots bereitgestellt.[21]

Der kabellose Zugang ermöglicht aber einem Angreifer sehr gute Angriffsmöglichkeiten, da Pakete einfach mitgeschnitten werden können. Um in die gesendeten und empfangenen Daten des Opfers Einsicht zu erlangen, muss sich der Angreifer nur in dem Radius, in welchem der Access Point (AP) sendet, aufhalten. Er kann daher eine *Man In The Middle Attacke* (MITM) starten. In diesem Fall gibt er sich als AP aus und wartet bis sich der mobile Client bei ihm einloggt.[22] Der Angreifer verbindet sich über eine zweite Netzwerkschnittstelle mit dem echten AP. So kann der Angreifer Daten mitlesen und falsche Daten weiterleiten. Diese Form des Angriffs wird in Abschnitt 2.2.2 weiter erläutert. Es gibt noch einige Techniken, den WLAN-Dienst zu unterbinden. Diese werden aber in dieser Arbeit nicht erläutert, da durch solche Attacken nur der Service nicht zur Verfügung steht, sie aber keine direkte Bedrohung für die mobilen Clients bedeuten.

Natürlich gibt es auch Verfahren, um WLANs vor Unbefugten zu schützen. Eine oft eingesetzte, aber veraltete Möglichkeit ist die Verschlüsselung mittels WEP (Wired Equivalent Privacy). Dies war das Standard Verschlüsselungsprotokoll welches im ersten IEEE 802.11-Standard im Jahre 1999 eingeführt wurde. WEP basiert auf dem Rivest Cipher 4- (RC4) Verschlüsselungsalgorithmus mit einer Schlüssellänge von 40 bzw. 104 Bit.[23] Durch eine Schwäche in diesem Verfahren kann eine WEP-Verschlüsselung mit Tools wie *WEPCrack* in einer akzeptablen Zeit umgangen werden.[24]

In den meisten Fällen wird heutzutage ein besseres Verfahren verwendet, um Daten, welche

[21] HotSpots sind öffentliche Internetzugangspunke, welche von mobilen IT-Clients über WLAN genutzt werden können.

[22] Diese Art von AP wird oft auch als rogue AP bezeichnet.

[23] Bei RC4 wird eine Zufallsfolge aus einem Schlüssel erzeugt. Diese wird danach mit den zu verschlüsselnden Daten XOR verknüpft.

[24] Das Tool WEPCrack befindet sich auf der beigelegten CD-ROM.

über eine Luftschnittstelle übertragen werden, zu verschlüsseln. Dieses Verfahren nennt sich Wi-Fi Protected Access (WPA) und ist der Nachfolger von WEP. Wenn WPA mittels Pre-Shared keys (PSK) konfiguriert ist, kann diese Schutzvorkehrung von Angreifern eventuell umgangen werden.[25] Durch das Abhören der ersten zwei Handshake Pakete, welche bei einem Verbindungsaufbau zwischen Client und AP ausgetauscht werden, ist es möglich, eine Offline Brute-Force- bzw. Wörterbuchattacke durchzuführen.[26] Dieser Angriff kann mit Hilfe des Tools *Aircrack* durchgeführt werden.[27] In vielen Fällen ist diese Angriffsmöglichkeit aber nur dann erfolgreich, wenn der verwendete PSK simpel gehalten ist.[28]

2.2.2 Man In The Middle Attacken

Bei Man In The Middle Attacken befindet sich der Angreifer zwischen seinem Opfer und der Gegenstelle, mit der das Opfer kommuniziert. Heutzutage ist es aber nicht mehr unbedingt zwingend, dass sich der Angreifer physisch zwischen seinem Opfer und der Kommunikationsgegenstelle befindet. Dadurch, dass sich die Datenpakete ihren Weg durch das Netzwerk selbst suchen, müssen nur ein paar Wegweiser so umgestellt werden, dass das Opfer seine Daten zuerst an den Angreifer schickt, und dieser die Daten dann an die Gegenstelle weiterleitet. Das heißt, der Angreifer muss sich nur in dem selben Netzwerk wie sein Opfer befinden. Im Speziellen müssen beide über die selbe Broadcast Domain kommunizieren. Dies ist in den meisten öffentlichen Netzwerken, wie z.B. auf Flughäfen oder in Hotels, der Fall.

Es gibt mehrere Techniken, eine MITM-Attacke durchzuführen. Ziel ist immer, dass der Angreifer die gesendeten Datenpakete des Opfers empfängt und an die Gegenstelle weitersenden kann. Das Opfer muss daher dazu gebracht werden, dass es seine zu sendenden Daten an den Angreifer adressiert.

Bei einem *Dynamic Host Configuration Protocol* (DHCP) *basierenden Angriff* werden dem Opfer über DHCP falsche Informationen mitgeteilt. Der Angreifer startet bei dieser Methode einen zweiten DHCP-Server im Netzwerk, welcher auf die DHCP-Anfrage des Opfers mit falschen IP-Informationen antwortet. Voraussetzung dafür ist aber, dass der DHCP-Server des Angreifers schneller antwortet als der richtige Server im Netzwerk. Der Angreifer kann dem Opfer z.B. seine IP-Adresse als Gateway mitteilen. Dadurch werden alle Pakete, welche der mobile Client über das Internet senden will, zuerst an den Angreifer adressiert. Dieser kann in die Daten einsehen, sie verändern und weiterleiten. Es kann dem Opfer aber auch nur eine falsche DNS-Server Adresse mitgeteilt werden. In diesem Fall bringt der Angrei-

[25] Ein PSK muss auf jedem Client vorkonfiguriert sein, um Zugriff auf das WLAN zu erlangen.
[26] vgl. Gerwing, S. A-23, [Ger06].
[27] Das Tool Aircrack befindet sich auf der beigelegten CD-ROM.
[28] vgl. Ahlers, [Ahl06].

fer mittels Auflösen falscher IP-Adressen das Opfer auf bösartige Pharming Seiten. Diese Möglichkeit wird in Abschnitt 2.2.3 näher erläutert.

Durch eine *Address Resolution Protocol* (ARP) *Cache Vergiftung* kann der Angreifer auf Layer 2 des ISO/OSI Modells sein Opfer dazu bringen, dass alle Pakete, welche über das Gateway gesendet werden müssen, zuerst zu ihm gelangen. Der Angreifer sendet in diesem Fall einen ARP-Response an sein Opfer. Dieser beinhaltet seine MAC-Adresse und die IP-Adresse des Gateway. Nun glaubt das Opfer, dass das Gateway die MAC-Adresse des Angreifers hat. Alle Pakete, welche vom Opfer über das Internet geschickt werden sollen, werden auf Layer 2 an den Angreifer adressiert. Wenn ein Switch im Einsatz ist, schickt dieser die Pakete direkt auf jenem Port aus, auf welchem der Angreifer angeschlossen ist. Nachdem die Pakete des Opfers empfangen wurden, können diese eventuell verändert an das richtige Gateway gesendet werden. Der Angreifer befindet sich also logisch zwischen dem Opfer und dem Gateway.

Durch die *Vorspiegelung eines WLAN-APs* kann in WLANs einfach eine MITM-Attacke durchgeführt werden. Der Angreifer simuliert einen öffentlichen AP mit guter Signalqualität und wartet, bis sich sein Opfer mit dem vorgespielten AP verbindet. Sobald dies der Fall ist, muss der Angreifer nur mehr den Traffic des Opfers an den richtigen AP weiterleiten.[29]

2.2.3 Pharming

Pharming ist eine Angriffsmöglichkeit, bei der der Angreifer durch Täuschung seines Opfers an sensible Daten, wie Kreditkartennummern und Passwörter, gelangen kann.

Bei dieser Methode wird das Opfer trotz Eingabe eines richtigen Uniform Resource Locator (URL) mit einer falschen Seite verbunden. Es gibt zwei Möglichkeiten, diese Art von Angriff umzusetzen. Eine Möglichkeit besteht darin, dem Opfer einen Trojaner einzuspielen, welcher in die hosts-Datei des Systems falsche Einträge schreibt.[30] Wenn das Opfer nun eine Verbindung mit einer Seite, welche in der hosts-Datei aufzufinden ist und durch den Angreifer manipuliert wurde, herstellen will, wird es mit einem falschen Server verbunden. Diese Angriffsmöglichkeit setzt aber voraus, dass es der Angreifer schon vorher geschafft hat, einen Trojaner auf dem System des Clients einzuschleusen, was bei vorsichtigen Benutzern schwierig ist. Eine zweite Möglichkeit, Pharming Attacken durchzuführen, besteht mittels *Domain Name System-* (DNS) *Spoofing*. In diesem Fall wird das Opfer ohne Einschleusen von Code auf falsche Seiten gelenkt.[31]

[29] vgl. Sicherheitskultur, [Sch06].

[30] In der hosts-Datei speichert ein System die Zugehörigkeit von Hostnamen zu IP-Adressen. Bevor das System versucht einen Hostnamen mittels DNS aufzulösen, schaut es in der hosts-Datei nach ob dem angeforderten Host eine IP-Adresse zugeordnet ist.

[31] vgl. McAfee Inc., [Inc06].

Beim DNS-Spoofing versucht der Angreifer, die Zuordnung von einer Domain zu einer falschen IP-Adresse im mobilen Client zu erreichen. Bevor der Client eine gewisse Domain aufrufen kann, muss er den konfigurierten DNS-Server nach der IP-Adresse dieser Domain fragen. Dieses System kann von Angreifern ausgenutzt werden, um ihre Opfer auf falsche Server zu leiten.

Damit ein Angriff erfolgreich durchgeführt werden kann, ist in der Regel kein großer Aufwand nötig. Diese Technik ist bislang schlecht gegen Manipulation abgesichert. Dies ist der Fall, da im Internet viele DNS-Server untereinander kommunizieren, und daher alle nach dem gleichen simplen System funktionieren müssen. Um Verbesserungen in DNS zu implementieren, müssten viele Server weltweit umgestellt werden. Ein Angriffspunkt stellt das Faktum dar, dass die meisten DNS-Server keine Möglichkeit haben, die Authentizität eines Kommunikationspartners zu überprüfen.

Ein Client stellt an seinen konfigurierten DNS-Server eine rekursive Anfrage. Wenn dieser Server keinen Eintrag zu der nachgefragten Domain hat, schickt dieser an den nächsten DNS-Server eine iterative Anfrage. Der Client erhält die IP-Adresse von dem Server, an den er seine Anfrage gesendet hat. Aus Effizienzgründen erfolgt die DNS-Kommunikation immer über das User Datagram Protocol (UDP). Dies lässt das Fälschen und Einstreuen von Paketen zu.

Wenn der DNS-Server die angefragten Daten nicht kennt, muss er andere Server fragen. Eine Angriffsmöglichkeit wäre es, wenn der Angreifer einen eigenen DNS-Server in seiner Domain betreibt. Wenn er nun bei dem DNS-Server des Opfers seine Domain nachfragt, schickt dieser einen DNS-Request an den Server des Angreifers. Der DNS-Server des Angreifers kann dem DNS-Server des Opfers nicht nur seine Domain mitteilen, sondern auch noch andere gefälschte Einträge übertragen. Der DNS-Server des Opfers hat nun gefälschte Daten in seinem Cache. Diese Attacke funktioniert aber nicht mehr bei aktuellen Nameservern, da diese nicht angeforderte Daten verwerfen.

Es gibt aber natürlich noch weitere Möglichkeiten, um den Cache des DNS-Servers zu vergiften. Der Angreifer muss zuerst eine Anfrage an den anzugreifenden DNS-Server schicken, in der er nach seiner Domain fragt. Daraufhin kontaktiert der Server des Opfers den DNS-Server des Angreifers und fragt ihn nach der IP-Adresse der Domain des Angreifers. So weiß der Angreifer, welchen Query Identifier (QID) der DNS-Server des Opfers gerade benutzt hat.[32] Nun schickt der Angreifer eine Anfrage nach der Domain, welche er umleiten will, an den zu vergiftenden DNS-Server. Wenn dieser nun eine iterative Anfrage an die angegriffene Domain schickt, antwortet der Angreifer mit einem DNS-Response indem er die vorher aus-

[32] Ein QID dient zur Unterscheidung von mehreren DNS-Anfragen. Der Client schickt eine Anfrage mit einem 16 Bit langen QID. Der Server antwortet mit der gleichen QID. So weiß der Server bzw. der Client auf welche Anfrage sich eine Antwort bezieht.

gelesene QID fortlaufend erhöht. Der angegriffene DNS-Server verwendet nun die Antwort, welche der Angreifer verschickt hat und die den passenden QID enthält. Daher muss der Angreifer mehrere Antworten mit immer aufsteigendem QID versenden. Jene Antwort, die zu spät vom richtigen DNS-Server kommt, wird verworfen. Wenn nun das Opfer seinen DNS-Server nach dieser Domain fragt, wird ihm die IP-Adresse mitgeteilt, welche der Angreifer dem DNS-Server vorher übermittelt hat.[33]

Eine einfachere Angriffsmöglichkeit kann erfolgen, wenn der Angreifer die Leitung des Opfers abhören kann. In Abschnitt 2.2.2 wurde auf einige Techniken eingegangen wie dies umgesetzt werden kann. Der Angreifer muss nur die DNS-Anfrage des Opfers mitlesen und schneller mit dem richtigen QID die gefälschte Antwort an das Opfer senden.[34] Er kann auch eine *Denial of Service-* (DoS) *Attacke* auf den angefragten Server starten, damit dieser nicht in einer entsprechenden Zeit antworten kann.[35]

Pharming Angriffe können so, vom Benutzer eines mobilen IT-Clients vollkommen unbemerkt, durchgeführt werden. Der User wird trotz manueller Eingabe der URL auf falsche Server geleitet.

2.2.4 Angriffe mittels Online Updates

Viele Anwendungen können über das Internet aktualisiert werden. Ein zentraler Server stellt aktuelle Updates für Software zur Verfügung. Diese oft aktivierte Funktion kann bei unzureichenden Schutzmaßnahmen von Angreifern dazu genutzt werden, bösartigen Code, ohne Wissen des Anwenders auf dem mobilen IT-Client zu installieren.

Diese Updatemöglichkeit wird von Windows XP eingesetzt. Ein Angreifer kann daher die Verbindung eines Clients zu einem Update Server über ein öffentliches Netzwerk überwachen und eventuell Dateien verändern, welche vom mobilen Client ausgeführt und installiert werden. Dies wird einem Angreifer, wie in Abschnitt 2.2.2 erläutert, durch das Umleiten von Paketen ermöglicht. Außerdem können Programme auf den automatischen Update Dienst des mobilen IT-Clients zugreifen und von einem bestimmten Server bösartigen Programmcode auf den mobilen IT-Client herunterladen und installieren.[36] Windows XP übermittelt standardmäßig seine Updates über das unverschlüsselte Hypertext Transfer Protocol (HTTP). Dies wurde festgestellt, indem auf einem mobilen IT-Client mit Microsoft Windows XP Service Pack (SP) 2 ein automatisches Update durchgeführt und gleichzeitig der

[33] vgl. Wismüller, [Wis07].
[34] vgl. Mraz, [VM97].
[35] Bei einer DoS-Attacke startet ein Client sehr viele Anfragen innerhalb einer kurzen Zeit. Der angegriffene Server ist daher lange mit diesen Anfragen beschäftigt und kann sich keinen anderen Clients zur Verfügung stellen.
[36] vgl. Keizer, [Kei07].

übertragene Datenverkehr mittels dem Sniffer Tool Ethereal aufgezeichnet wurde.[37] Wenn bösartige Software schon auf dem System installiert wurde, kann diese im Hintergrund willkürlich Programmcode herunterladen und installieren, ohne eine Interaktion des Benutzers zu benötigen.

Nicht nur das Betriebssystem muss mittels Updates auf aktuellem Stand gehalten werden. Auch Software wie Anti-Virus Scanner, müssen über aktuelle Virensignaturen und Programmupdates verfügen, um verlässlich zu funktionieren. Da heutzutage meistens schon täglich neue Virendefinitionen erhältlich sind, ist es nahe liegend diese Updates online durchzuführen, um immer auf dem aktuellsten Stand zu bleiben. Bei schlechter Implementierung durch die Softwarehersteller kann diese Funktion als Angriffspunkt dienen, um bösartigen Code auf dem Client zu installieren.

[37] Die aufgezeichneten Daten sowie Ethereal befinden sich auf der beigelegten CD-ROM.

Kapitel 3

Schutzmechanismen

Es gibt heutzutage viele Möglichkeiten mit Hard- bzw. Software, seine mobilen IT-Clients vor ungewollten Zugriffen zu schützen. Es muss aber nicht nur darauf geachtet werden, dass die eingesetzten Schutzmechanismen richtig konfiguriert sind. Man darf ebenfalls nicht vernachlässigen, die Mitarbeiter dementsprechend zu schulen, und eine gute Passwortpolitik umzusetzen. In den folgenden Abschnitten werden einige Schutzmechanismen für mobile IT-Clients näher erläutert.

3.1 Sicherheit durch Hardware

Sicherheit kann schon auf der Hardwareebene implementiert und umgesetzt werden. Dadurch ist es möglich schon sehr früh, während dem Bootvorgang des mobilen IT-Clients, gewisse Sicherheit zu gewährleisten. Im folgenden Abschnitt werden Möglichkeiten für Sicherheitsmechanismen, welche mittels Hardware umgesetzt wurden, beschrieben.

3.1.1 BIOS Mechanismen

In jedem Fall muss Sicherheit auf den untersten Layern anfangen. Man sollte es dem Angreifer so schwer wie möglich machen, besonders wenn dieser physischen Zugriff auf das Gerät hat. Daher ist das BIOS in erster Linie vor ungewollten Zugriffen zu schützen.

Das BIOS wird direkt nach dem Einschalten des Gerätes geladen und ausgeführt. Es befindet sich in einem nichtflüchtigen Chipsatz direkt auf dem Motherboard des mobilen Gerätes. Es enthält Daten, um die Hardware des Notebooks ansteuern zu können. Der Benutzer kann diese Daten bzw. einige Sicherheitseinstellungen ändern, indem er nach dem POST mit einer speziellen Tastenkombination in das BIOS einsteigt.

Natürlich sollte so gut wie möglich verhindert werden, dass Angreifer diese Einstellungen ändern können.

3.1.1.1 Zugriffsschutz für das BIOS

Es kann heutzutage bei jedem BIOS eine Passwortabfrage aktiviert werden. Der Benutzer kommt daher nur in das BIOS, wenn er das Passwort kennt. Dies verhindert unter anderem das Booten des Notebooks von einem anderen Medium. Standardmäßig sollte es nur möglich sein, das Betriebssystem von der Festplatte booten zu können. Diese Schutzvorkehrung kann aber mit einigen Methoden umgangen werden, wie in Abschnitt 2.1.1 beschrieben.

3.1.1.2 Schutz vor ungewollten Bootmechanismen

Eine weitere Schutzvorkehrung, welche das BIOS zur Verfügung stellt, ist das Festlegen eines Boot-Passwortes. Wenn dieses vom Benutzer gesetzt ist, muss während dem POST ein Passwort eingegeben werden, damit das Notebook bootet. Wenn dieses Passwort nicht bekannt ist, kann daher von keinem Medium gebootet werden. Diese Schutzvorkehrung kann aber, wie in Abschnitt 2.1.1 beschrieben, umgangen werden.

3.1.1.3 Harddisk-Passwortschutz

Das BIOS stellt eine Möglichkeit zur Verfügung, um die Festplatte mit einem Passwortschutz zu versehen. Dieses Passwort wird nach jedem Start des mobilen Clients, vor dem ersten Zugriff auf die Festplatte, abgefragt. Diese Option wird vom BIOS unterstützt und kann dort auch aktiviert werden. Der Hashwert des Passwortes wird direkt auf der Festplatte abgespeichert. Das heißt, es hilft dem Angreifer nichts, wenn er die Festplatte ausbaut und in einem anderen System darauf zugreifen will.

Das BIOS kommuniziert direkt mit dem Festplattencontroller über den ATA-Befehlssatz.[38] Man kann zwei unterschiedliche Passwörter für den Festplattenzugriff setzen. Das *User-Passwort* sollte im Normalfall verwendet werden. Wenn dieses Passwort nicht bekannt ist kann auch das *Master-Passwort* verwendet werden. Wie dieses Passwort die Festplatte entsperrt, hängt von dem aktivierten Sicherheitsmodus ab. Wenn *High Security Mode* verwendet wird, kann die Festplatte nach Eingabe des Master-Passwortes wieder verwendet werden. Im *Maximum Security Mode* werden durch dieses Passwort alle gesetzten Passwörter gelöscht und der Inhalt der Festplatte wird mit lauter Nullen überschrieben. Es kann im Maximum Security Mode die Entsperrung also nur mit einem gültigen User-Passwort erfolgen. Abbil-

[38] Dieser Befehlssatz wird für die Kommunikation mit ATA-Festplattencontrollern verwendet.

dung 3.1 zeigt ein Flussdiagramm, wie bei unbekanntem User-Passwort auf die Festplatte zugegriffen werden kann.

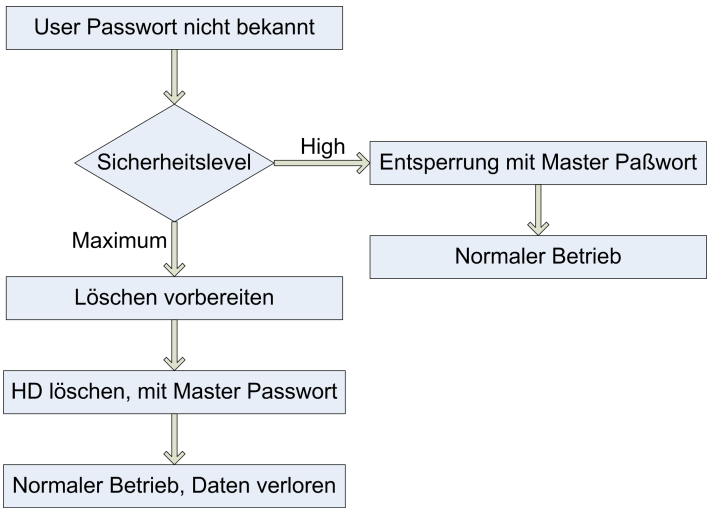

Abbildung 3.1: Flussdiagramm bei unbekanntem User-Passwort

Wenn High Security Mode aktiviert ist, kann man entweder mit einem Backdoor Master-Passwort oder mit einem speziellen Programm, wie in Abschnitt 2.1.1 erklärt, diese Sicherheitsvorkehrung umgehen.

Im Maximum Security Mode kann nur mittels User-Passwort auf die Daten zugegriffen werden. Durch Eingabe des Master-Passwortes kann die Festplatte verwendet werden, doch werden alle Daten vorher gelöscht. Um diese Konfiguration zu umgehen, benötigt man spezielle Hardware.[39]

In den meisten Fällen kann man im BIOS nicht direkt den Sicherheitsmode des Festplattenschutzes angeben. Standardmäßig wird High Security Mode verwendet, welcher um einiges leichter umgangen werden kann als Maximum Security Mode. Um diesen aktivieren zu können, benötigt man spezielle Software wie das *ATA Security eXtension BIOS*.[40] Dieses erweiterte BIOS lässt es zu, Maximum Security Mode zu aktivieren.[41]

3.1.2 Trusted Platform Module

Sicherheit kann durch den Einsatz von spezieller Hardware geleistet werden. Ein sehr effektives Mittel wird seit 1999 von der Trusted Computed Platform Alliance (TCPA) entwickelt. TCPA veröffentlichte das so genannte *Trusted Platform Module* (TPM), welches durch erweiterte Hardware mehr Sicherheit, speziell auf mobilen IT-Clients, bereitstellt.

[39] vgl. Vogon, [Vog07].
[40] ATA Security eXtension BIOS befindet sich auf der beigelegten CD-ROM.
[41] vgl. Fitzenreiter, [Fit05].

Die TPM-Hardware stellt dem System eine Grundlage für vertraute Informationen zur Verfügung. Es ist möglich, die Vertrauenswürdigkeit auf andere Teile der Hardware auszuweiten und so eine Kette zu erstellen, welcher vertraut werden kann. Das TPM besteht aus einem Mikrocontroller, der kryptographische Funktionen unterstützt. Dadurch ist es möglich, derartige Operationen ausschließlich in dem TPM durchzuführen. Es werden anderer Hard- und Software Sicherheitsoperationen zur Verfügung gestellt ohne, dass diese Einsicht in die Funktionen bekommen. Der Rivest Shamir Adleman- (RSA) Accelerator des TPM führt die Ver- bzw. Entschlüsselung von mittels RSA verschlüsselten Daten aus. Durch den Random Number Generator kann die Hardware zufällige Schlüssel erzeugen.

Ziel eines TPM ist es, das Computersystem, in welchem es implementiert ist, als vertrauenswürdig oder fremd zu erkennen. Durch den Einsatz eines TPM ist es also möglich, ein Computersystem gegenüber einem Kommunikationspartner zu authentifizieren. Im Gegensatz zur SmartCard ist ein TPM an eine Plattform und nicht an einen bestimmten Benutzer gebunden. Jede Aktion der Hardware muss über eine Schnittstelle zum TPM angefragt werden. Dafür dient der so genannte Low Pin Count- (LPC) Bus, der eine Anbindung des TPM an das Mainboard darstellt.[42]

Bei Entfernung des TPM aus dem System wird der Mikrocontroller unbrauchbar. Das System weist daher bei fehlendem TPM keine einwandfreie Funktion auf. Außerdem kann nicht mehr auf die mittels TPM geschützten Daten zugegriffen, bzw. können Aktionen, welche durch das TPM geschützt sind, ebenfalls nicht durchgeführt werden.

Die Grundlage der Sicherheit, welche dieses Modul bereitstellt, ist der Endorsement Key (EK), welcher aus einem public/private Schlüsselpaar besteht. Dieses wird in der TPM Hardware abgelegt wobei der private key diese niemals verlässt. Es gibt zwei Möglichkeiten, ein solches Schlüsselpaar zu erzeugen. Es kann entweder einmalig durch einen bestimmten Befehl erzeugt oder schon bei der Produktion des Moduls generiert werden. Die Echtheit des TPM wird durch das Endorsement Zertifikat bestätigt, welches den EK beinhaltet.

Durch den Attestation Identity Key (AIK), welcher aus dem EK gebildet wird, wird das System authentifiziert. Der Benutzer muss zuerst ein Zertifikat erstellen und dieses von einer dritten Instanz verifizieren und unterschreiben lassen. Nun wird die unterschriebene ID im TPM abgespeichert. Über den AIK eines mobilen Clients kann z.B. eine remote Gegenstelle sicherstellen, dass es mit dem richtigen System kommuniziert. Mit dieser Methode lassen sich auch Daten an einzelne Plattformen binden. Nur so ist es möglich, dass diese Daten nur mit dem berechtigten System ausgelesen werden können.

Das Platform Zertifikat wird vom Hersteller des mobilen IT-Clients ausgestellt und bestätigt, dass die eingebauten Komponenten der Trusted Computing Group- (TCG) Spezifikation

[42] LPC wird verwendet, um Geräte, die nur eine geringe Datenrate benötigen, an Mainboards anzubinden.

entsprechen sowie die Implementierung eines gültigen TPM erfolgt ist.[43] Dieses Zertifikat bescheinigt die Vertrauenswürdigkeit der Plattform.

Durch das Conformance Zertifikat wird die korrekte Implementierung des TPM in die Plattform bestätigt.

Das Platform Configuration Register (PCR) dient zur Speicherung von Zustandsabbildern der aktuellen Soft- bzw. Hardware Konfiguration des Systems.[44] In Abbildung 3.2 werden die Basiskomponenten eines TPM dargestellt.

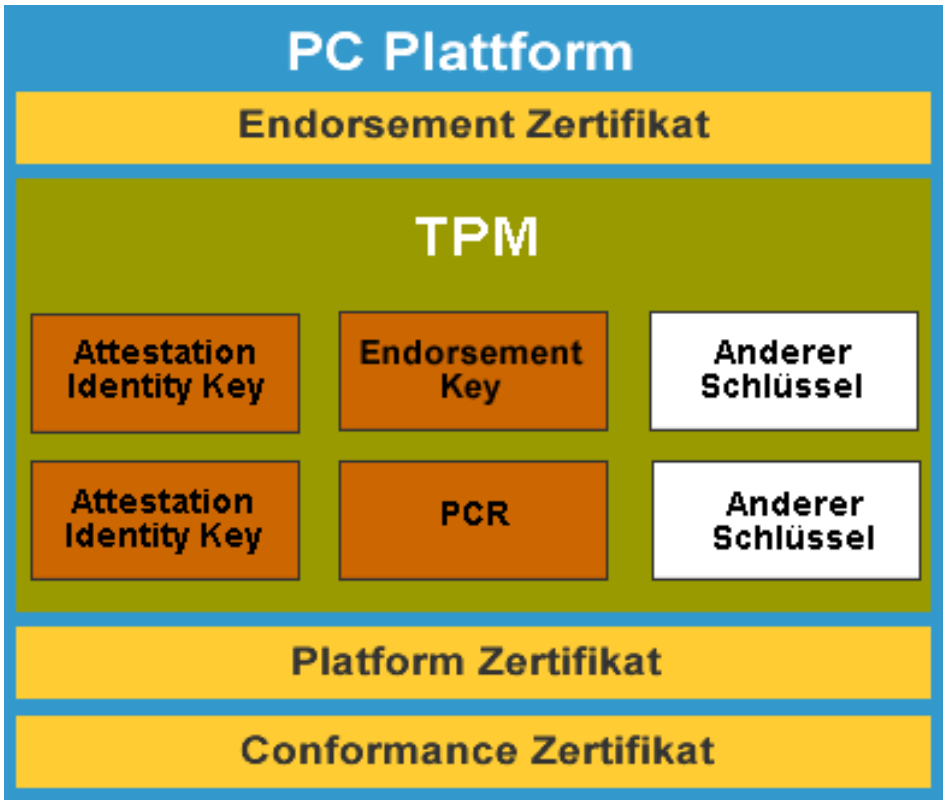

Abbildung 3.2: Basiskomponenten eines TPM, Quelle: Intel Corp., 2002

Es gibt mehrere Möglichkeiten, wie das TPM sehr sensible Daten abspeichert. Es wird ein symmetrischer Schlüssel erstellt, mit dem sehr kleine Datenmengen verschlüsselt und direkt im TPM abgespeichert werden. Bei größeren Daten werden diese in Blöcke transformiert, welche einzeln verschlüsselt und auf der Festplatte gespeichert werden, wobei der Schlüssel dafür im TPM gespeichert ist.[45]

Das TPM kann ebenfalls während dem Bootvorgang einen BIOS-Code Integrity Check durchführen, damit keine falschen Daten in diesen Code gelangen können.

[43] TCG ist eine internationale Standardisierungsorganisation, welche nach einem Industriestandard Hardware zertifiziert.
[44] vgl. BSI Trusted Platform Module, [fSidI07a].
[45] vgl. Intel Corp., [Baj02].

Ein TPM verfügt über einen Trusted Software Stack (TSS), welcher eine Softwareschnittstelle bereitstellt, über die die Anwendungen des Benutzers die Funktionen dieser Hardware nutzen können. Mit Hilfe eines TPM kann sich ein System z.B. bei einem VPN-Gateway oder einem Zugangskontollsystem in einem WLAN authentifizieren. Die Kommunikationsgegenstelle kann durch Prüfen des AIK sicherstellen, dass sie mit der richtigen Plattform kommuniziert. Es kann durch den Einsatz eines TPM Daten signiert werden. Es kann außerdem sichergestellt werden, dass diese nicht verändert werden können. Mittels TPM verschlüsselte Daten können nur auf der Plattform, auf welcher sie verschlüsselt wurden, wieder entschlüsselt werden.[46]

3.2 Spezielle Softwaresicherheitsmechanismen

Um einen mobilen IT-Client vor lokalen bzw. Angriffen über ein Netzwerk zu schützen, stehen einige Sicherheitstechniken zur Verfügung. Es wird grob zwischen zwei Techniken unterschieden. Der Anwender des mobilen Clients muss seine Daten vor dem Einsehen durch unautorisierte Personen schützen, auch wenn diese durch Diebstahl den physischen Zugriff auf den mobilen IT-Client erlangt haben. Die zweite Sicherheitstechnik muss vor Angriffen schützen welche über das Internet oder ein lokales Netzwerk durchgeführt werden können. In den folgenden Abschnitten wird auf die wichtigsten Sicherheitstechniken für den Schutz von mobilen IT-Clients eingegangen.

3.2.1 Zugriffsschutz für Daten

Einer der wichtigsten Sicherheitsaspekte ist, dass Daten nicht von unbefugten Personen eingesehen werden können. Das folgende Kapitel beschäftigt sich mit dem Fall, dass einem Außendienstmitarbeiter, welcher sehr sensible Unternehmensdaten auf seinem Notebook gespeichert hat, das mobile Gerät gestohlen wurde. Es wird nun erläutert, welche Maßnahmen gesetzt werden können, um unbefugten Personen, welche physischen Zugriff auf das Gerät haben, den Zugriff auf sensible Daten zu verweigern.

3.2.1.1 Data Encryption

Einem Angreifer, der einen mobilen IT-Client physisch besitzt, sollte das Einsehen in auf die Festplatte gespeicherte Daten unmöglich gemacht werden. Das Verschlüsseln dieser Daten stellt eine geeignete Schutzmaßnahme dar.

[46] vgl. Krauß, [Kra06].

Es gibt unterschiedliche Verfahren, wie Hard- bzw. Software Datensicherheit zur Verfügung stellen kann.[47] File Level Encryption verschlüsselt nur einzelne Dateien. Der Schlüssel, mit welchem auf die Datei zugegriffen werden kann, befindet sich im Header der geschützten Datei. Bei Container based Encryption wird auf ein bestehendes Dateisystem ein zusätzliches Dateisystem aufgesetzt, welches loop device genannt wird. Dieses zusätzliche Dateisystem funktioniert wie ein Container, welcher Dateien enthält. Für das Dateisystem, welches sich direkt auf der Festplatte befindet, sieht dieser Container aus, wie eine große Datei mit zufälligem Inhalt. Eine weitere Methode ist die Verschlüsselung der ganzen Festplatte mittels Software. Bei diesem Verfahren wird das Betriebssystem aufgefordert, jeden Block, welcher auf die Festplatte geschrieben werden soll, zu verschlüsseln, bzw. beim Lesen wieder zu entschlüsseln. Es müssen hierfür Verschlüsselungsalgorithmen verwendet werden, welche im Systemkernel implementiert sind. Eine vierte Möglichkeit ist das Verschlüsseln mittels Hardware. In diesem Fall ist das Betriebssystem nicht direkt in die Verschlüsselung der Daten involviert. Dies funktioniert mit Hilfe eines speziellen Mikrocontrollers. Jeder Block, den das Betriebssystem auf die Festplatte schreibt, wird vorher völlig unbemerkt von der Hardware verschlüsselt bzw. bei einem Lesevorgang entschlüsselt.[48]

Die letzten beiden angeführten Methoden zur Datenverschlüsselung bieten den sichersten Schutz und sind für den Benutzer transparent. Durch Verschlüsselung der gesamten Festplatte werden nicht nur Benutzerdaten sondern auch Systemdaten vor unautorisierten Zugriffen geschützt. Der Benutzer muss sich in diesem Fall während dem Bootvorgang authentifizieren, damit das System gestartet werden kann.

Um Daten sicher zu verschlüsseln, sollte ein starker Algorithmus gewählt werden. In den letzten Jahren haben sich Verfahren wie Advanced Encryption Standard (AES), 3 Data Encryption Standard (3DES) und Twofish durchgesetzt. In vielen Fällen werden AES und Twofish eingesetzt, da seit der Standardisierung von AES, 3DES als veraltet gilt. AES und Twofish sind Block Cipher Verfahren, welche Daten mit einem symmetrischen Schlüssel verschlüsseln.

Das NIST (National Institute of Standards and Technology) wählte im Jahre 2000 den vom Belgier Rijndael entwickelten Block Cipher Algorithmus als AES aus. AES hat eine fixe Blockgröße von 128 Bit und eine Schlüssellänge von 128, 192 oder 256 Bit. Jeder Block wird in 10 bis 14 Runden verschlüsselt, abhängig von der Länge des Schlüssels.[49] Dieser Algorithmus weist wie Twofish eine gute Diffusion auf.[50] Ein großer Vorteil von AES ist, dass jeder Schritt Operationen enthält, welche parallel durchgeführt werden können. Durch diese

[47] vgl. Sennhauser, [AS07].
[48] vgl. Abschnitt 3.1.2.
[49] vgl. Schneier S. 55, [FS03].
[50] Eine Funktion ist diffus, wenn durch eine geringe Änderung des Inputs eine große Änderung des Outputs erfolgt.

Eigenschaft können Geschwindigkeitskriterien erfüllt werden. Die Verschlüsselung unterscheidet sich in der Implementierung aber stark von der Entschlüsselung. Daher müssen in jedem System Verschlüsselung und Entschlüsselung separat implementiert werden.

Twofish unterstützt, wie AES auch, Schlüssellängen von 128, 192 und 256 Bit. Die Blocklänge beträgt 128 Bit und der Algorithmus basiert auf einem Feistelnetzwerk.[51] Der 128 Bit lange Plaintext wird in 32 Bit Werte aufgespaltet, wodurch die meisten Operationen mit einem 32 Bit Wert durchgeführt werden können.[52]

Wegen seiner Komplexität wird Twofish als eine Spur sicherer betrachtet als AES. AES bietet gegenüber Twofish einen Geschwindigkeitsvorteil.

Um eine Festplatte zu ver- bzw. entschlüsseln, muss aber auch der Schlüssel in irgendeiner Form gespeichert sein. Dieser Schlüssel wird als master key bezeichnet. Eine Möglichkeit ist, diesen Schlüssel mittels public key verschlüsselt auf der Festplatte abzuspeichern. Als bessere Methode erweist sich, den master key auf einer SmartCard oder in einem TPM abzuspeichern. Bei Verwendung einer SmartCard sollte der Benutzer noch zusätzlich ein Passwort angeben, um diese vor dem Lesen durch unautorisierte Personen zu schützen. Dies ist eine der besten Methoden, um Festplatten zu verschlüsseln, da sich der master key nicht auf dem selben Speichermedium wie die verschlüsselten Daten befindet.

Windows XP stellt eine integrierte Option zur Verschlüsselung von Daten zur Verfügung. Das so genannte *Encrypting File System* (EFS) ermöglicht es, Benutzerdaten auf NTFS formatierten Datenträgern mittels File Level Encryption zu verschlüsseln und so das Einsehen durch unbefugte Personen zu verhindern. Nach dem Systemstart wird EFS in das NTFS eingehängt und arbeitet als integrierter Systemdienst zur Ver- und Entschlüsselung von sensiblen Daten. Die FSTRL (File System Run Time Library) ist ein Modul des EFS-Treibers und wird von NTFS verwendet, um das Lesen, Öffnen und Schreiben von verschlüsselten Dateien zu ermöglichen. Wenn NTFS nun auf eine verschlüsselte Datei trifft kommuniziert es mit der FSTRL, um die gewünschte Operation ausführen zu können. Da sich EFS im Kernel des Systems befindet, kann es auch verhindern, dass der Schlüssel in die Auslagerungsdatei geschrieben wird. Alle zur Ver- und Entschlüsselung benötigten Daten werden von Windows XP in einen Bereich des Hauptspeichers abgelegt, der nicht in die Auslagerungsdatei geschrieben wird, wenn diese länger nicht benötigt werden. Eine Schwachstelle stellt jedoch der Ruhezustand dar, welcher bei mobilen Clients öfters verwendet wird. Wenn das Notebook in diesen Zustand wechselt, wird der gesamte Hauptspeicher auf der Festplatte abgespeichert. Wenn sich zu diesem Zeitpunkt der Schlüssel gerade im Hauptspeicher befindet, wird dieser ebenfalls in dieser Datei abgelegt. Außerdem speichern die meisten Anwen-

[51] Mit einem Feistelnetzwerk ist es möglich, Daten zu verschlüsseln und zu entschlüsseln ohne die Umkehrfunktion bilden zu müssen.

[52] vgl. Schneier S. 59, [FS03].

dungen temporäre Dateien, welche dann den Klartext der verschlüsselten Datei enthalten. Das macht einen Zugriff für unautorisierte Personen möglich.[53]

EFS kombiniert symmetrische sowie asymmetrische Verschlüsselungsverfahren. Um eine Datei zu verschlüsseln, wird zuerst ein zufälliger Schlüssel kreiert. Mit diesem wird nun die Datei verschlüsselt und kann damit auch wieder entschlüsselt werden. Es wird für jede zu verschlüsselnde Datei ein eigener Schlüssel, der so genannte File Encryption Key (FEK), erstellt. Dieser wird nun asymmetrisch für jeden Benutzer, der Zugriff auf die Datei haben soll, verschlüsselt. Jeder Benutzer hat ein Schlüsselpaar, welches aus einem public und einem private key besteht. Der public key ist jedem Benutzer bekannt, wobei den private key nur der Benutzer kennt, für den er erzeugt wurde. Es können dadurch nur Daten mit dem private key entschlüsselt werden, welche mit dem dazugehörigen public key verschlüsselt wurden. Für jeden Benutzer, der Zugriff auf die verschlüsselte Datei haben soll, wird eine Data Decryption Field- (DDF) Struktur hinterlegt. Diese Struktur enthält eine Kopie des FEK sowie SID des Benutzers. In Abbildung 3.3 wird dieses Verfahren grafisch dargestellt.

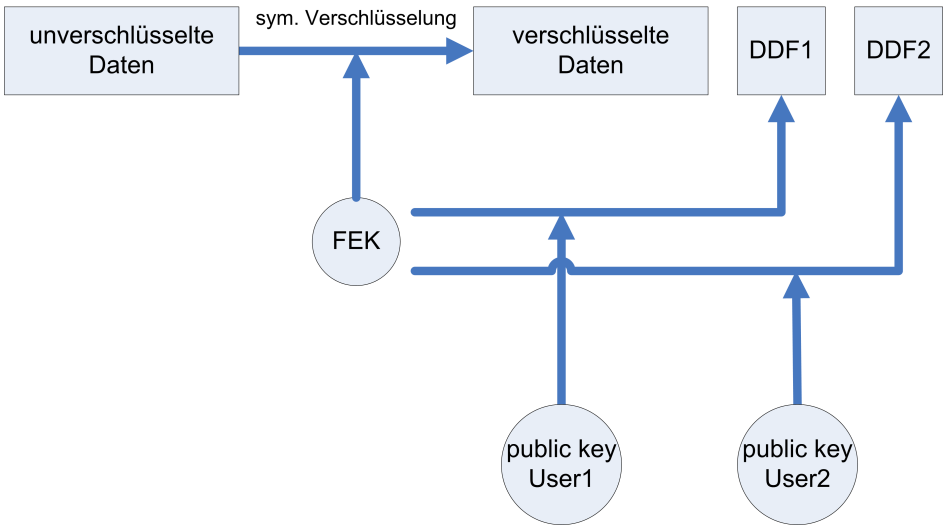

Abbildung 3.3: Dateiverschlüsselung mit EFS

Wenn ein Benutzer auf die verschlüsselte Datei zugreifen will, wird zuerst mit seinem private key sein DDF entschlüsselt. Jetzt kann er den FEK aus dem DDF auslesen und damit die Datei mit dem symmetrischen Verfahren entschlüsseln.

Die symmetrische Verschlüsselung wird ab Windows XP SP2 mit AES-256 realisiert. Um den FSK asymmetrisch zu verschlüsseln, wird das RSA-Verfahren angewendet. Diese Methode stellt einen starke Verschlüsselungsalgorithmus zur Verfügung.

Bevor ein Benutzer Dateien verschlüsseln kann, muss ein EFS-Zertifikat vom System für ihn erstellt werden. Dieses Zertifikat enthält den public key, welcher von allen anderen Benutzern

[53] vgl. BSI Sichere Nutzung von EFS, [fSidI07b].

gelesen werden kann, sowie den private key, der nur vom Inhaber des Zertifikates gelesen werden darf. Der private key des Benutzers muss daher mit einem Algorithmus geschützt werden, damit nur der Inhaber des Zertifikates diesen Schlüssel lesen kann. Dies erfolgt mit dem so genannten User Master Key. Dies ist ein symmetrischer Schlüssel, welcher zufällig vom System erzeugt wird. Von diesem Schlüssel werden weitere Schlüssel abgeleitet, welche den private key des Benutzers verschlüsseln.

Unter Windows XP SP2 ist es möglich Recovery Agents zu aktivieren. Benutzer dieser Gruppe können auf alle verschlüsselten Dateien zugreifen. Wenn ein Benutzer mittels EFS Daten verschlüsselt, wird ein Data Recovery Field (DRF), das mit dem public key des Recovery Agents verschlüsselt wird, generiert. Wenn der Recovery Agent nun das DRF entschlüsselt, kennt er den FEK und kann auf die verschlüsselte Datei zugreifen. Auf mobilen Clients empfiehlt es sich aber Recovery Agents zu deaktivieren, damit mehr Schutz geboten werden kann.[54] In Abschnitt 4.2.1.1 wird auf die Sicherheit von EFS eingegangen.

3.2.1.2 Verbesserte Authentifizierungsmethoden

Im mobilen Einsatz ist die Authentifizierung von Benutzern gegenüber dem System besonders wichtig, da der mobile Client vielen Personen physisch zugänglich ist. Authentifizierungsmethoden sind Technologien zur Feststellung der behaupteten Identität des Benutzers. Aufgrund der festgestellten Identität muss das mobile System den Benutzer Aktionen durchführen lassen, für welche er autorisiert ist.[55] Die Autorisierung erfolgt nach der Authentifizierung des Benutzers. Damit die Authentifizierung erfolgreich ist, muss das System etwas Einzigartiges des Benutzers, der sich gegenüber dem mobilen Client authentifizieren will, überprüfen. Hierfür gibt es drei wichtige Methoden:

- *Wissen:* Dies sind alle Daten, welche der Benutzer weiß, und die bei der Authentifizierung zwischen dem System und einem User ausgetauscht werden. Diese Daten können z.B. Passwörter, PINs oder Antworten auf eine spezielle Frage sein.
- *Besitz:* Der Benutzer muss sich gegenüber dem System mit etwas authentifizieren, was er inne hat. Nur der Inhaber eines gewissen Mediums kann sich erfolgreich gegenüber dem System authentifizieren. Dies können SmartCards, USB-Tokens oder ähnliches sein.
- *Biometrisches Merkmal:* Dies sind personenbezogene Merkmale, welche aufgrund der individuellen körperlichen Eigenschaften eindeutig einer gewissen Person zugeordnet werden können. Das können Fingerabdrücke, Irisbeschaffenheit oder ähnliches sein.

[54] vgl. Gerstner, [Ger03].

[55] Autorisierung ist der Vorgang indem geprüft wird, ob der authentifizierte Benutzer gewisse Aktionen durchführen darf.

Die Sicherheit der einzelnen Authentifizierungsmethoden ist unterschiedlich. Methoden, welche den Benutzer mittels Wissen oder Besitz authentifizieren, lassen sich prinzipiell leichter abfragen. Allerdings können solche Nachweise entwendet werden oder verloren gehen bzw. vergessen werden. Die Sicherheit der Authentifizierungsmethode ist abhängig von der abgefragten Information. Je wahrscheinlicher es ist, dass der Benutzer der einzige ist, welcher diese Information besitzt, und diese schwer gefälscht bzw. erraten werden kann, desto sicherer ist die Methode.

Um die Sicherheit zu erhöhen, kann auch eine hybride Authentifizierungsmethode eingesetzt werden, bei der mehrere Methoden kombiniert werden. Es ist für einen Angreifer leicht möglich, an ein Passwort oder eine SmartCard zu gelangen. Bei einem hybriden Verfahren werden z.B. neben einem Passwort noch eine SmartCard bzw. auch noch eine biometrische Erkennung verlangt.[56]

Hybride Methoden erschweren es dem Angreifer beträchtlich, sich als ein autorisierter Benutzer gegenüber einem System zu authentifizieren. Eine als sehr sicher geltende und häufig eingesetzte Methode ist die Authentifizierung mittels *One Time Password* (OTP). In diesem Fall muss sich der Benutzer gegenüber dem System durch etwas, das er weiß und inne hat, authentifizieren. Die Firma *RSA Security* stellt SecurID Tokens zur Verfügung, welche alle 60 Sekunden einen neuen einmalig gültigen Code berechnen und diesen auf einem kleinen Display anzeigen. Dieser Zahlenwert muss zum Loginzeitpunkt an das übliche Passwort des Benutzers angehängt werden, damit sich dieser erfolgreich authentifizieren kann. Da der SecurID Token mit dem Server zeitsysnchronisiert ist, weiß der Server immer, zu welchem Zeitpunkt der Benutzer welches Passwort eingeben muss. Diese Authentifizierungsmethode verfügt über sehr hohe Sicherheit.[57]

Für eine Authentifizierung mittels Fingerabdruck stellt unter anderem Lenovo, in vielen ihrer business Notebooks, einen integrierten Fingerabdruckscanner bereit.[58] Verbesserte Authentifizierungen mittels SmartCard bzw. USB-Token werden unter anderem von der Firma Aladdin zur Verfügung gestellt. Diese können in eine bestehende Public Key Infrastructure (PKI) implementiert werden und unterstützen eine RSA-1024 Bit Authentifizierung.[59]

Authentifizierungen über eine SmartCard oder einen USB-Token bzw. Fingerabdruck werden von Microsoft Windows XP SP2 standardmäßig unterstützt. Dadurch kann der Benutzer eines mobilen IT-Client beim Login Vorgang des Betriebssystems durch erweiterte Sicherheitsmechanismen authentifiziert werden.

[56] vgl. Eren, S. 176, [Det06].
[57] vgl. RSA Security Inc., [Inc07b].
[58] vgl. Lenovo, [Len07].
[59] vgl. Aladdin GmbH, [Gmb07a].

3.2.2 Schutz im Netzwerk

Viele Angriffe erfolgen über das Internet bzw. ein lokales Netzwerk. Solche Attacken sind leicht zu starten, da sich der Angreifer entweder in dem gleichen Netzwerk seines Opfers befindet, oder gar nur eine Internetverbindung zu seinem Opfer benötigt. Im Gegensatz zu lokalen Angriffszenarios muss sich der Angreifer nicht erst physischen Zugriff zum mobilen Client verschaffen. Angriffe über ein Netzwerk sind daher besonders gefährlich und mobile Clients sollten dagegen gut geschützt werden.

In den nachfolgenden Abschnitten werden die wichtigsten Schutzmechanismen vor Angriffen in Netzwerken erläutert.

3.2.2.1 Schutz in WLANs

Viele Unternehmen bieten ihren Mitarbeitern neben einem kabelgebundenen Netzwerkzugang auch die Möglichkeit, über ein Wireless LAN die IT-Infrastruktur zu nützen. Das WLAN muss dementsprechend abgesichert werden, damit Angreifer keine Möglichkeiten haben, Daten aus dem Netzwerk auszulesen bzw. in die IT-Infrastruktur des Unternehmens über einen unauffälligen, kabellosen Client einzudringen.

Eine der besten Sicherheitsvorkehrungen gegenüber Angreifern besteht darin das WLAN örtlich abzugrenzen. Es sollte daher so konfiguriert werden, dass der Radius des kabellosen Netzwerks nur so weit gehalten wird, wie er wirklich benötigt wird. Dies schränkt die Anzahl der potenziellen Angreifer ein.

Für Sicherheit im WLAN müssen die Bereiche Verschlüsselung, Authentifizierung sowie Schlüsselmanagement implementiert werden. Der Standard IEEE 802.11i bietet Lösungen, um diese Voraussetzungen umzusetzen. Wie in Abschnitt 2.2.1 beschrieben, ist WEP sehr unsicher und WPA-PSK eventuell zu umgehen. Eine gute Sicherheitslösung bietet WPA2-Enterprise. In diesem Fall kommt das Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) für die Verschlüsselung und Integritätsprüfung zum Einsatz. Dieses Protokoll arbeitet mit AES und gilt daher als sehr sicher. Das Verschlüsselungsergebnis entsteht durch die AES-Verschlüsselung eines Zählers, welcher mit einem Klartextblock XOR verknüpft wird. Die Schlüssellänge beträgt 128 Bit und wird über IEEE 802.1X zur Verfügung gestellt. Durch die Integritätsprüfung wird sichergestellt, dass Daten während der Übertragung nicht verändert wurden.

IEEE 802.1X spezifiziert eine portbasierende Zugriffskontrolle für Netzwerke nach dem IEEE 802-Standard. Abbildung 3.4 zeigt die Funktionsweise von IEEE 802.1X in einer WLAN Umgebung. Bei diesem Standard wurden folgende Rollen der beteiligten Netzelemente spezifiziert:

- *Supplicant*: Der Client, welcher den Netzwerkzugang anfordert.
- *Authenticator*: Dieser stellt den Clients einen Zugang zum Netzwerk zur Verfügung. Im Falle eines WLANs ist dies ein AP.
- *Authentication Server*: Dieser Server stellt einen Authentifizierungsdienst bereit und wird meist mittels Radius-Server implementiert.

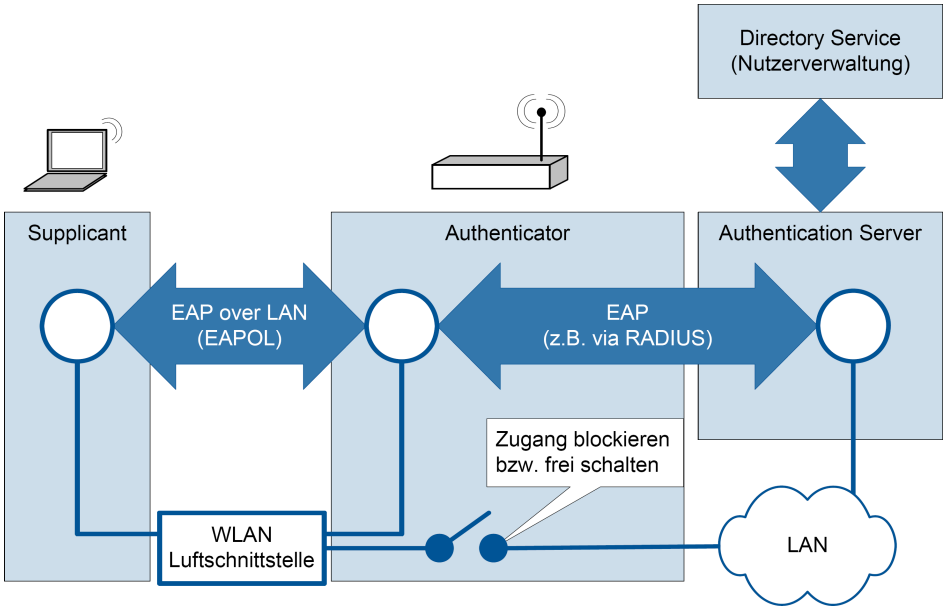

Abbildung 3.4: Funktionsweise von IEEE 802.1X, Quelle: Gerwing, 2006, S. A-16

Die Authentifizierung der mobilen Endgeräte erfolgt über das Extensible Authentication Protocol (EAP). Die Kommunikation der Authentifizierungsphase wird mittels EAP over LAN (EAPOL) durchgeführt. Dadurch kann sich der Client auf Layer 2 authentifizieren, ohne, dass ihm eine Layer 3-Adresse zugewiesen werden muss. EAP wird in WLANs außerdem eingesetzt, um die Verteilung von Schlüsselmaterial zu gewährleisten. Die EAP-Transport Layer Security (EAP-TLS) Methode bietet eine beidseitige Authentifizierung mittels X.509-Zertifikaten.[60] Es muss daher eine PKI im Unternehmensnetzwerk bestehen. Jeder Client, dem es gestattet sein soll, das WLAN zu nützen, benötigt ein gültiges Zertifikat. Weitere Schlüssel werden nun mittels public/private key Verschlüsselung zwischen Client und Server ausgetauscht.[61]

WPA2-Enterprise bietet guten Schutz für WLANs in größeren Unternehmen. Es wird dadurch sichergestellt, dass mobilen Clients über eine Luftschnittstelle ein sicherer Übertragungskanal zur Verfügung steht.

[60] Ein X.509-Zertifikat enthält Daten über den Server, wie Namen der Organisation, den public key dieses Servers, usw. Dies wird von einer vertrauenswürdigen Certificate Authority (CA) signiert und als echt bestätigt. Dadurch kann jeder dieses Zertifikat auf Echtheit überprüfen.

[61] vgl. Gerwing, [Ger06].

3.2.2.2 Group Policy

Group Policy (GP) wurde von Microsoft entwickelt, um es Systemadministratoren zu ermöglichen, jeder Benutzergruppe in einem Active Directory Netzwerk genau spezifizierte Tätigkeiten zu erlauben oder zu verweigern. Dies gilt nicht nur für den Benutzer, sondern auch für Programme, welche dieser ausführt. Diese Schutzmöglichkeit kann Benutzer von Tätigkeiten abhalten, welche eine Sicherheitslücke im System hervorrufen könnten. Ein Systemadministrator kann mittels Group Policy Management Console (GPMC) die verschiedenen Group Policy Objects (GPO) konfigurieren und verwalten. In der folgenden Auflistung werden die wichtigsten sicherheitsrelevanten Einstellungen erläutert.[62]

- *Internet Explorer*: Diese Einstellungen können dazu verwendet werden, dass bestimmte Benutzer gewisse Internet Explorer Sicherheitseinstellung verwenden müssen.
- *Windows Firewall*: Der Administrator kann die Windows Firewall des Benutzers genau konfigurieren, bestimmten Programmen den Zugriff auf das Netzwerk gestatten oder verweigern und gewisse Ausnahmen bei gewissen Szenarien, wie z.B. remote Administration, konfigurieren. Es können zwei unterschiedliche Profile für die Windows Firewall erstellt werden: ein Domain Profil, welches aktiv ist, wenn sich der Benutzer in dem Active Directory des Unternehmens befindet, sowie ein Standard Profil, das aktiviert wird, wenn der Benutzer sein Notebook außerhalb der Unternehmensdomain benutzt.
- *Internet Communication Management*: Diese Komponente ist zuständig für die Konfiguration der Kommunikation des mobilen Clients. Hier kann angegeben werden, wie die unterschiedlichen Komponenten von Windows XP SP2 über das Internet bzw. das lokale Netzwerk kommunizieren sollen.
- *Security*: Mit diesen Einstellungen kann ein Client, der sich zu seiner Domain verbinden will, zuerst darauf überprüft werden, ob er das aktuellste Sicherheitsupdate besitzt. Falls eine bekannte Sicherheitslücke auf dem Client besteht, wird er entsprechend gewarnt.
- *Infrastructure*: Damit kann verhindert werden, dass Benutzerpasswörter automatisch auf der Festplatte des mobilen IT-Clients abgespeichert werden.
- *Network*: Mit dieser Einstellung ist es möglich den Background Intelligent Transfer Service (BITS) zu deaktivieren.[63] Es können mit dieser Komponente auch Remote Procedure Calls (RPC) blockiert werden.[64]

[62] vgl. Microsoft Corp., [Cor04].

[63] BITS wird von Windows Betriebssystemen verwendet, um im Hintergrund Daten von einem Server zu transferieren.Eine typische Anwendung dafür ist die automatische Windows Update Funktion.

[64] RPC ist ein Protokoll, welches zum Aufruf einer Funktion, die von einem entfernten Rechner durchgeführt

Weiters kann mit GP auch der Zugriff auf den Registry Editor und auf die Konsole verhindert werden. Es ist auch möglich, Wechseldatenträger zu deaktivieren, damit keine Angriffe über USB-Sticks oder ähnliches durchgeführt werden können. Außerdem kann GP dafür sorgen, dass gewisse Programme wie z.B. Anti-Virus oder ähnliche Software auf dem mobilen Client ausgeführt werden.

Um diese Sicherheitsvorkehrungen auf mobilen IT-Clients effektiv einsetzen zu können, sollte *GPAnywhere* verwendet werden. Dies ermöglicht es GPs auf mobilen Clients, welche nicht immer eine Verbindung zur Domain haben, einzusetzen. Wenn der Client nun eine Verbindung zum Active Directory des Unternehmens hat, werden die Sicherheitsrichtlinien für den Benutzer des mobilen IT-Clients aktualisiert. Dieses Feature trägt besonders zur Sicherheit auf mobilen IT-Clients bei. Es kann so das GP-Service in einer bestehenden IT-Infrastruktur eines Unternehmens auf die mobilen Geräte erweitert werden und diesen dadurch mehr Sicherheit gewähren.[65]

3.2.2.3 Sicherheit in öffentlich zugänglichen Netzwerken

In vielen Fällen nützen mobile IT-Clients öffentliche Internetanbindungen. Da der mobile Benutzer nicht weiß, wer und was sich hinter diesem Netzwerk befindet, muss er sich gegen Angriffe besonders gut schützen. Öffentliche Netzwerke stehen sehr vielen Personen zur Verfügung, und der Betreiber ist nicht verpflichtet, den Clients Sicherheit zu gewähren. Der Benutzer muss daher selbst für die Sicherheit seines Clients und seiner Daten sorgen.

Um einen mobilen Client in öffentlichen Netzwerken ausreichend schützen zu können, darf auf Sicherheitssoftware nicht verzichtet werden. Was auf keinen Fall fehlen darf, ist eine *Personal Firewall*, welche den IT-Client vor ungewollten Zugriffen über ein Netzwerk schützen soll. Diese Softwarelösung schließt sämtliche Ports, welche nicht benötigt werden. Es werden auch Programmzugriffe vom mobilen Client auf andere Rechner im Netzwerk kontrolliert und überwacht. Außerdem verhindert die Firewall auf Grund der nicht benötigten geschlossenen Ports den Zugriff von außerhalb. Die Voraussetzung, dass eine Firewall wirklich guten Schutz vor dem Einschleusen von Würmern oder Trojanern bietet, ist eine richtige und gewissenhafte Konfiguration. Die Personal Firewall lässt Datenpakete entweder durch oder verwirft diese nach bestimmten Regeln. Diese Regeln können Portnummern, Protokolle, Richtung oder andere Eigenschaften der Datenpakete sein. Diese Software filtert ungewollte Pakete heraus, sodass Angreifer nicht so ohne weiteres gefälschte Daten an den mobilen Client senden können.

Microsoft Windows XP SP2 bietet eine integrierte Firewall, welche standardmäßig aktiviert

wird, dienen soll.

[65] vgl. Business Wire, [Wir05].

ist. Diese in das Betriebssystem integrierte Software stellt dem mobilen IT-Client einen gewissen Basisschutz vor Angriffen aus dem Netz zur Verfügung. Sie schließt nach der Aktivierung jeden Port, welcher nicht von der Windows Firewall freigegeben ist, und macht es Angreifern schwerer in das System einzudringen. Es wird dem Benutzer auch ermöglicht, Datenpakete nach Absender IP-Adressen zu filtern. Die Firewall muss natürlich so konfiguriert werden, dass der Benutzer des mobilen Clients uneingeschränkt arbeiten kann. Jedes Programm, welches auf die Netzwerkschnittstelle zugreifen will, muss zuerst in der Windows Firewall registriert werden.

Es wird dadurch ein Systemtool zur Verfügung gestellt, welches den Datenverkehr des mobilen Clients auf Layer 3 und 4 des ISO/OSI Modells überwacht. Außerdem kann die Windows Firewall zentral von einem Systemadministrator mittels Group Policy konfiguriert werden.[66] Der Benutzer des mobilen IT-Clients muss sich daher keine Gedanken um die richtige Konfiguration seiner Firewall machen. Abbildung 3.5 zeigt eine erweiterte Konfiguration erlaubter Dienste, welche über das Netzwerk von anderen Benutzern genutzt werden dürfen.

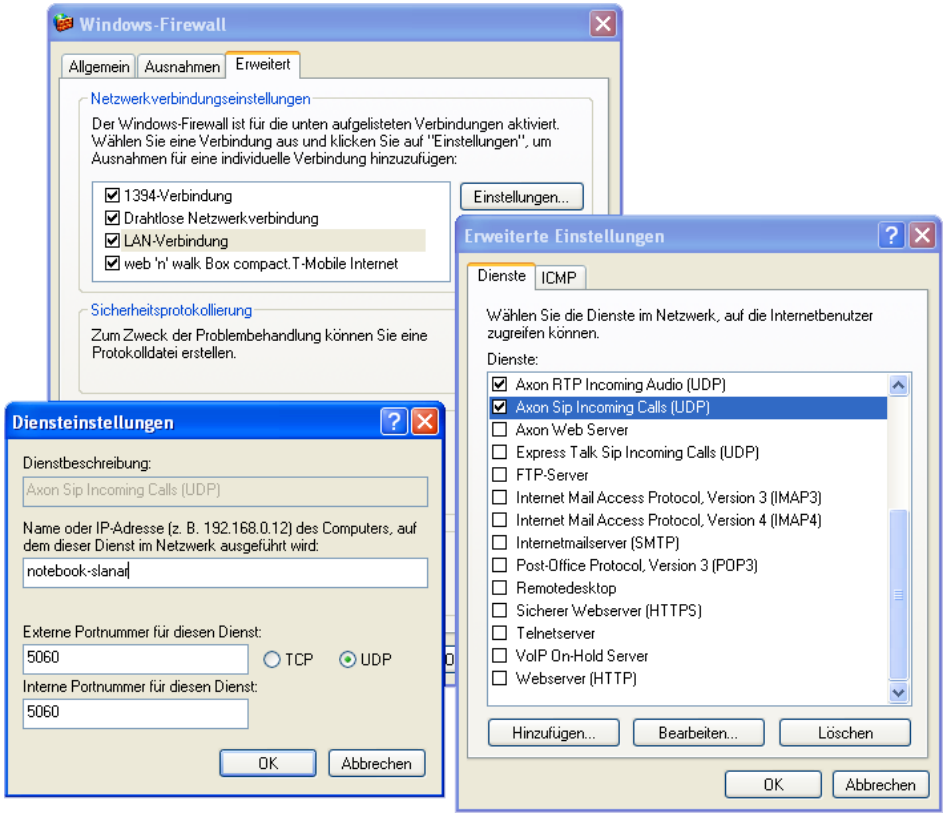

Abbildung 3.5: Konfiguration von erlaubten Diensten der Windows Firewall

Die Windows Firewall kann als Grundschutz verwendet werden. Es sollte aber nicht darauf verzichtet werden, mittels weiterer Software den mobilen Client zu schützen, wie z.B. mit

[66] Für Informationen über Group Policy siehe Abschnitt 3.2.2.2.

einem Host Intrusion Detection System.[67]

3.2.2.4 Schutz mittels VPN, IPSec und SSL

Unternehmen müssen sicherstellen, dass ihre mobilen IT-Clients Daten über öffentliche Netzwerke sicher übertragen können. Es ist daher dafür zu sorgen, dass der Client eine gute Verschlüsselung, sowie Authentifizierung der Kommunikationsgegenstelle durchführt. Einem potenziellen Angreifer, welcher sich ebenfalls in dem öffentlichen Netzwerk befinden kann, ist es daher nicht möglich, in gesendete bzw. empfangene Daten des Clients einzusehen oder diese während der Übertragung zu verändern. Diese Schutzmöglichkeit kann mittels *Virtual Private Networks* (VPNs) umgesetzt werden.

VPNs sind in den letzten Jahren für mobile IT-Clients immer wichtiger geworden. Mit dieser Technologie wird es einem mobilen Client ermöglicht, über das Internet eine Verbindung zu dem privaten Netzwerk des Unternehmens herzustellen. Dem mobilen Benutzer steht so die IT-Infrastruktur des Betriebes von überall, wo ihm eine Internetverbindung bereitgestellt wird, zur Verfügung.

Da bei diesem Verfahren sehr sensible Daten des Unternehmens über öffentliche Datenleitungen geschickt werden, und in den meisten Fällen der VPN-User Zugriff auf die gesamte IT-Infrastruktur des Unternehmens hat, muss ein VPN auch dementsprechend gut abgesichert werden. Dies geschieht oftmals mittels *Internet Protocol Security* (IPSec). Dieses Protokoll stellt bei richtiger Konfiguration einen sehr sicheren Kommunikationskanal bereit.

Um Daten mittels IPSec sicher über ein VPN übertragen zu können, wird der Encapsulating Security Payload (ESP) verwendet. Mittels ESP werden die Datenpakete verschlüsselt sowie authentifiziert. Ein Angreifer kann somit die Datenpakete nicht verändern und einsehen. Bevor aber Daten mit ESP übertragen werden können, müssen die Kommunikationspartner (VPN-Gateway und Client) authentifiziert und die ESP-Parameter ausgehandelt werden. Dies geschieht durch das *Internet Key Exchange*- (IKE) Protokoll.

Das IKE-Protokoll arbeitet in zwei Phasen. In der ersten Phase authentifizieren sich die beiden Kommunikationspartner gegenseitig. Außerdem werden in dieser Phase die Schlüssel, welche für die ESP-Kommunikation benötigt werden, ausgehandelt. Ebenso wird eine so genannte Security Association (SA) aufgebaut, welche dazu benutzt wird, nachfolgenden IKE-Verkehr zu verschlüsseln und zu authentifizieren. In der zweiten Phase des IKE-Protokolls werden die Security Parameter für ESP ausgehandelt. Hier wird entschieden, welcher Verschlüsselungsalgorithmus verwendet wird, und welcher Traffic verschlüsselt werden soll.[68]

Ein sehr wichtiger Aspekt bei der Kommunikation über VPNs ist die Authentifizierung. Es

[67] Für Informationen über Host Intrusion Detection Systems siehe Abschnitt 3.2.2.5.
[68] vgl. Snyder, [Sny01].

muss sichergestellt sein, dass der Client mit dem richtigen Server, sowie der Server mit einem autorisierten Client kommuniziert. Hierfür muss sich der Client gegenüber dem Server, und der Server gegenüber dem Client authentifizieren. Um dies mittels IPSec durchzuführen, gibt es zwei Möglichkeiten: entweder mit Pre -Shared keys oder mit digitalen Zertifikaten. Bei der Authentifizierung mit Pre-Shared keys hat jeder VPN-Client einen Schlüssel auf dem Notebook konfiguriert, mit welchem er sich gegenüber dem VPN-Gateway authentifiziert. Die überschaubarere und sicherere Möglichkeit ist die Authentifizierung mittels digitalem Zertifikat. Diese sehr sichere Methode setzt voraus, dass das Unternehmen eine Public Key Infrastructure besitzt.[69]

Mittels PKI wird der Einsatz von digitalen Zertifikaten und Signaturen bereitgestellt. Die PKI stellt Sicherheitsinformationen wie die aktuelle Gültigkeit der eingesetzten Zertifikate zur Verfügung. Jeder, der ein Zertifikat erhält, kann durch die Signatur der Certificate Authority die Gültigkeit überprüfen. Wenn ein Unternehmen eine PKI besitzt, kann jeder Server sowie mobile Client über ein digitales Zertifikat authentifiziert werden. Die Authentifizierung mittels digitalen Zertifikaten ist eine gut skalierbare und sichere Lösungsmethode.

Mit solchen Zertifikaten können der mobile Client und der Server authentifiziert werden. Nun muss sich aber auch noch der Benutzer des Clients gegenüber dem Server authentifizieren, damit bei Diebstahl des Notebooks der Angreifer nicht in das VPN einsteigen kann. Natürlich kann das digitale Zertifikat des Benutzers auch auf einer SmartCard gespeichert werden, damit der Angreifer bei Diebstahl des Clients nicht das Zertifikat einsehen kann. Trotzdem sollte nicht auf eine gute Authentifizierung des Benutzers mittels OTP verzichtet werden.[70]

Die Authentifizierung ist der schwierigste Teil beim Betrieb eines VPN. Wenn diese nach den erwähnten Kriterien erfolgt, kann das VPN als sicher eingestuft werden. Erfolgreiche Angriffe auf die Verschlüsselung von IPSec sind gegenwärtig nicht bekannt.

VPNs sind eine sehr praktische Technologie für Unternehmen mit Außendienstmitarbeitern. Auf der anderen Seite werden dadurch aber auch neue Angriffsmöglichkeiten geboten. Man sollte daher bei der Sicherheit von VPNs nicht sparen und den finanziellen sowie fachlichen Aufwand auf sich nehmen.

Secure Socket Layer (SSL) wird oft eingesetzt, um Daten zwischen einem Webserver und einem Client sicher zu übertragen. Bei SSL muss sich während dem Aufbau einer Verbindung der Server gegenüber dem Client und eventuell auch der Client gegenüber dem Server mittels eines X.509-Zertifikates authentifizieren. Der Sender verschlüsselt die Daten mit dem public key des Empfängers, welche dieser mit seinem private key wieder entschlüsseln kann. Mit diesem Verfahren wird ein symmetrischer Schlüssel zwischen den kommunizierenden End-

[69] vgl. Networkworld, [Lor00].
[70] Für Informationen über OTP siehe Abschnitt 3.2.1.2.

geräten ausgetauscht, mit dem der restliche Datenverkehr verschlüsselt wird. Diese Technologie macht es möglich, dass sich Webserver gegenüber einem Client sicher authentifizieren und die zu übertragenden Daten verschlüsselt übertragen können.[71]

3.2.2.5 Spezifische Sicherheitssoftware

Wie in Abschnitt 3.2.2.3 beschrieben, bieten Personal Firewalls einen Basisschutz vor Angriffen aus dem Netzwerk. Eine Firewall alleine stellt aber keinen ausreichenden Schutz des mobilen IT-Clients dar. Angriffe auf Applikationsebene können diese Firewalls nicht mehr erkennen. Um auch diese Art von Angriffen abwehren zu können, sollte auf dem Client ein *Host Based Intrusion Detection System* (HIDS) installiert werden. Ein HIDS überwacht einen Host mittels so genannten Software Agents. Diese Agents überwachen den Systemkernel und schlagen Alarm, sobald etwas verdächtiges im System des mobilen IT-Clients festgestellt wird. Außerdem wird der Benutzer alarmiert, wenn Konfigurationsdateien geändert werden. Ein HIDS liest sämtliche Log-Dateien aus und benachrichtigt seinen User über ungewöhnliche Vorgänge.

Einen Schritt weiter gehen die so genannten *Host Based Intrusion Prevention Systems* (HIPS). Diese Softwareprodukte können nicht nur Angriffe erkennen, sondern auch verhindern. Die Agenten bilden einen so genannten Wrapper um den Betriebssystemkern.[72] So können diese den Zugriff auf die Betriebssystemressourcen überwachen und kontrollieren. Darunter fällt z.B. der Schreibzugriff auf Systembibliotheken, die Speicherzuweisung für Applikationen und der wechselseitige Zugriff von Applikationen. Eine wichtige Voraussetzung für die einwandfreie und sinnvolle Funktion eines HIPS ist die richtige Konfiguration, da dem Benutzer nicht nur gemeldet wird, dass ein Angriff erfolgt ist, sondern auch gleich eine Schutzmaßnahme getroffen wird. Bei falscher Konfiguration kann dies zum Fehlschlagen von Prozessen führen.[73]

Um ausreichenden Schutz in einem öffentlichen Netzwerk zu erlangen, sollte auf jedem mobilen Client eine Personal Firewall und ein HIDS bzw. ein HIPS installiert werden. Diese Software muss aber genau an die Bedürfnisse des Benutzers angepasst werden, damit sie ihren Zweck erfüllt. In vielen Fällen werden diese Produkte, die eine Personal Firewall und ein HIPS besitzen, angeboten. Software wie Kaspersky Internet Security oder Norton Internet Security bieten dem Benutzer einen Komplettschutz.

[71] vgl. Heinzmann, [Hei05].

[72] Ein Wrapper ist eine Schnittstelle zwischen zwei Programmcodes. In diesem Fall stellt der Wrapper eine Schnittstelle zwischen dem Systemkernel und den darauf zugreifenden Applikationen dar.

[73] vgl. Todt, [Tod04].

3.3 Gegenüberstellung

Die in diesem Kapitel erläuterten Schutzmöglichkeiten stellen unterschiedlich starke Sicherheit auf mobilen IT-Clients zur Verfügung. Unter Wahrung sämtlicher Sicherheitsvorkehrungen, sollte die Konfiguration dieser Schutzmaßnahmen zentral erfolgen, damit sich der Benutzer des mobilen Gerätes so wenig wie möglich mit Sicherheit beschäftigen muss. Es sollte auf keinen Fall vernachlässigt werden, dass auch Außendienstmitarbeiter, die einen mobilen IT-Client einsetzen, dementsprechend im Umgang mit diesem unter Berücksichtigung von Sicherheitsaspekten gut geschult sind.

Tabelle 3.1 zeigt eine Bewertung sowie deren Funktion der lokalen Schutzmechanismen, welche in diesem Kapitel behandelt wurden.

Schutzmechanismus	Funktionsweise	grobe Bewertung
TPM	bindet Informationen an Plattformen	bietet eine starke Basis für Schutzmaßnahmen, die darauf aufbauen
EFS	verschlüsselt Dateien und Ordner	bietet eine schwache Schutzvorkehrung bei unzureichender Windows Login Authentifizierung, ist aber einfach zu konfigurieren und zu verwenden
Boot/BIOS-Passwort	fragt ein Passwort ab, bevor in das BIOS eingestiegen, bzw. das System gebootet werden kann	macht den Angreifer langsam, bietet aber keine starke Schutzvorkehrung
Harddisk-Passwort	verlangt eine gültige Authentifizierung vor dem ersten Zugriff auf die Festplatte	bietet schwachen Schutz, kann aber den Angreifer sehr viel Zeit kosten
Harddisk-Encryption	verschlüsselt Daten auf der gesamten Festplatte	ist für starke Datensicherheit auf mobilen IT-Clients unerlässlich
Verbesserte Authentifizierung	Benutzer müssen sich mit verbesserten Merkmalen an dem mobilen System authentifizieren	bietet starken Schutz auf mobilen Geräten

Tabelle 3.1: Bewertung der lokalen Schutzmechanismen

In Tabelle 3.2 werden die Funktionen der verschiedenen Schutzmechanismen für Netzwerkangriffe beschrieben und deren Schutzvorkehrung bewertet. Manche Maßnahmen können

sowohl für lokalen Schutz, als auch für Sicherheit in Netzwerken eingesetzt werden.

Schutzmechanismus	Funktionsweise	grobe Bewertung
TPM	authentifiziert Plattformen	bietet einen starken Schutzmechanismus um Plattformen zu authentifizieren
Verbesserte Authentifizierung	Benutzer müssen sich mit verbesserten Methoden an remote Systemen authentifizieren	bietet starke remote Benutzerauthentifizierung
Group Policy	Benutzern werden bestimmte Tätigkeiten erlaubt oder verboten	kann zentral verwaltet werden und auch auf mobilen Clients für starken Schutz sorgen
VPN	stellt eine sichere Verbindung zum Unternehmensstandort her	ist eine starke Schutzmöglichkeit, um Daten authentifiziert sowie verschlüsselt zu übertragen und sollte auf mobilen Geräten zum Einsatz kommen
SSL	authentifiziert Server und Clients und verschlüsselt die auszutauschenden Daten	bietet starken Schutz und sollte für sichere Kommunikation mit Webservern eingesetzt werden
Windows Firewall	verbietet den Zugriff auf den mobilen Client nach vordefinierten Regeln	stellt Grundschutz gegenüber Angriffen über Netzwerke dar, bietet aber insgesamt zu schwache Sicherheit
spezifische Software	bemerkt Netzwerkangriffe auf das mobile System	hilft Angriffe früh zu erkennen und zu verhindern und bietet starken Schutz

Tabelle 3.2: Bewertung der Schutzmechanismen für Netzwerkangriffe

Es gibt viele Schutzmöglichkeiten, welche mobilen IT-Clients gute Sicherheit bieten können. Je mehr Schutzmechanismen eingesetzt werden, um das System besser zu schützen, desto komplexer wird die Konfiguration und der Einsatz des Systems. Da die Folgen von unsicheren mobilen IT-Clients aber verheerend sein können, sollte man diesen zusätzlichen Aufwand in kauf nehmen.

Kapitel 4

Sicherheitstests

Das folgende Kapitel beschäftigt sich mit dem Testen der Sicherheit von unterschiedlichen Schutzmöglichkeiten. Es soll getestet werden, welche Implementierungen von gewissen Schutzmaßnahmen wirklich Sicherheit bieten oder eventuell sogar andere Angriffspunkte hervorrufen.

Diese Tests sollen zeigen, ob sich die in der Theorie bewährten Technologien auch in der Praxis bewähren können. Es wird spezielle Sicherheitssoftware auf ihre Funktion und Sicherheit getestet. Im Laufe des Kapitels wird gezeigt welche Softwareansätze und Technologien mobilen IT-Clients wirklich Schutz bieten können.

4.1 Durchführungskonzept für Sicherheitstests

Es muss zuerst eine Testumgebung aufgesetzt werden. Diese besteht aus zwei Standrechnern und einem Notebook, welches den zu schützenden mobilen IT-Client darstellt. Auf diesem Notebook wird das Betriebssystem Microsoft Windows XP SP2 eingesetzt, da dieses das meist verbreitete System auf mobilen Clients ist.

Der erste Standrechner dient als Schnittstelle zwischen simuliertem Internet und der IT-Infrastruktur des Unternehmens. Auf diesem Rechner wird Microsft Windows Enterprise Server 2003 eingesetzt. Der dritte Rechner dient als Angreifer und führt das Linux Betriebssystem Debian Etch aus.[74] Dieses System wurde gewählt, da es viele Konfigurationsmöglichkeiten bietet, besonders für das Durchführen von Angriffszenarios. Mit diesem Rechner werden Angriffe auf den mobilen Client bzw. den Server des Unternehmens gestartet.

Auf dem Rechner des Angreifers läuft spezielle Software, um Angriffe durchführen zu können, sowie ein Nessus Server, welcher remote Computer auf Sicherheitslücken untersuchen

[74] Etch ist der Codename für die Version 4 des Debian Betriebssystems.

kann.[75]

Der mobile IT-Client wird mit unterschiedlichen Schutzmechanismen versehen, welche durch den Rechner des simulierten Angreifers auf ausreichenden Schutz getestet werden kann.

4.2 Clientschutzsoftware

Der Markt der Anbieter von Clientschutzsoftware ist sehr groß, so dass daher IT-Verantwortlichen von Unternehmen eine große Auswahl an unterschiedlichen Softwareprodukten zur Verfügung steht. Durch die große Konkurrenz in diesem Marktsegment werden Entwicklerfirmen solcher Softwarelösungen gezwungen, immer bessere Schutzlösungen auf den Markt zu bringen.

Es kann in dieser Arbeit nicht auf alle führenden Softwareprodukte eingegangen werden. Die Funktionsweise ist aber bei den unterschiedlichen Softwarelösungsansätzen meist die gleiche. Zuerst wird auf Schutzmechanismen für lokale Sicherheit der Daten auf einem mobilen IT-Client eingegangen. Der nächste Abschnitt behandelt spezifische Lösungen mittels spezieller Software von Drittanbietern. Danach wird auf Schutz im Netzwerk eingegangen, wo nicht nur Betriebssystem- und spezielle Softwarelösungen, sondern auch Kommunikationstechnologien getestet werden.

4.2.1 Produkte für Zugriffsschutz

In den folgenden Abschnitten werden die wichtigsten Möglichkeiten für Schutz vor lokalen Angriffen getestet. Es wird angenommen, dass der Angreifer durch Diebstahl oder ähnliches in den Besitz des mobilen IT-Clients gekommen ist und daher vollen physischen Zugriff auf das System hat. Das Ziel dieser Schutzmaßnahmen ist nur, den Angreifer daran zu hindern, die auf dem Client gespeicherten Daten einzusehen, jedoch nicht, die Hardware vor unbefugtem Gebrauch zu schützen.

4.2.1.1 Betriebssystemlösungen

Wie schon in Abschnitt 3.2.1.1 erwähnt, wird EFS von Windows zur Verfügung gestellt, um einzelne Dateien zu verschlüsseln. Wenn nun der mobile Client in die Hände eines Angreifers fällt, kann dieser die verschlüsselten Dateien nicht so ohne weiteres einsehen.

[75] Nessus ist ein Sicherheitsscanner, welcher bekannte Angriffsmöglichkeiten auf Computer über das Netzwerk durchführt. Um immer die aktuellsten Angriffsmethoden verwenden zu können, kann diese Software über das Internet aktualisiert werden.

Der Angreifer kann jedoch z.B. mit dem Tool *Offline NT Password & Registry Editor* das Passwort jedes Benutzeraccounts zurücksetzen.[76] Das heißt, es wird ihm ermöglicht, sich erfolgreich auf dem System als beliebiger Benutzer einzuloggen. Das Passwort kann aber mit solchen Tools nur überschrieben und nicht ausgelesen werden.[77] Unter Windows XP SP2 ist durch das Zurücksetzen des Passwortes das Zertifikat und daher auch der private key des Benutzers nicht mehr dechiffrierbar; alle mit EFS verschlüsselten Dateien sind somit nicht mehr zu entschlüsseln. Ein Angreifer könnte sich daher mit diesem Tool Zugang zum Administrator Account schaffen und nicht zu dem Benutzer, welcher die mittels EFS verschlüsselten Dateien erstellt hat. Es ist möglich, den Hashwert des Benutzerpasswortes auszulesen und z.B. mit dem Tool *Ophcrack* als Plaintext darzustellen.[78] Dieses Programm versucht mittels Brute-Force-Attacke das Passwort zu erraten. Es wird von jedem möglichen Passwort der Hashwert gebildet und mit dem auf dem System gespeicherten Wert verglichen. Ergibt sich eine Übereinstimmung, wurde das Passwort gefunden.[79] In diesem Fall kann der Angreifer nun alle verschlüsselten Dateien, welche dieser Benutzer einsehen darf, auslesen. Diese Angriffsmöglichkeit versucht, nicht das EFS zu umgehen, sondern den Schutz des Login-Verfahrens.[80] Eine gute EFS-Verschlüsselung setzt also voraus, dass eine sehr starke Benutzerauthentifizierung verwendet wird.

Eine Möglichkeit, um Daten mittels EFS gut zu schützen besteht darin, die private keys der Benutzer zu exportieren. Es befinden sich daher keine Schlüssel für das EFS auf dem mobilen IT-Client. Das Notebook kann so konfiguriert werden, dass sich der Benutzer bei jedem Login mit einer SmartCard bzw. USB-Zoken authentifizieren muss.[81] Auf dieser Karte befindet sich der private key, mit dem der Benutzer den Zugriff auf all seine verschlüsselten Daten bekommt.

4.2.1.2 Spezifische Softwarelösungen

Es gibt eine Vielzahl an Verschlüsselungssoftware, welche mit sicheren Verfahren einzelne Daten bzw. ganze Partitionen verschlüsseln können. Ein gutes Tool ist *TrueCrypt* welches unter der General Public License (GPL) zur Verfügung steht.[82] Mit diesem Open Source Tool ist es möglich, Daten automatisch on the fly zu ver- bzw. entschlüsseln. Dieses Programm ist unter anderem auch für Microsoft Windows XP erhältlich.[83]

[76] Offline NT Password & Registry Editor befindet sich auf der beigelegten CD-ROM.
[77] vgl. Petter Nordahl-Hagen, [NH04].
[78] Ophcrack befindet sich auf der beigelegten CD-ROM.
[79] vgl. Ophcrack, [Oph07].
[80] Heutzutage ist kein öffentlicher Algorithmus bekannt, welcher in akzeptabler Zeit den Schlüssel eines EFS berechnen kann.
[81] vgl. Abschnitt 3.2.1.2.
[82] GPL ist eine Lizenz zur Lizenzierung von freier Software.
[83] TrueCrypt befindet sich auf der beigelegten CD-ROM.

Es bietet viele unterschiedliche Verschlüsselungsalgorithmen, um die Sicherheit der Daten zu gewährleisten. Diese Software unterstützt zwei unterschiedliche Methoden. Es kann entweder eine ganze Partition oder ein einzelner Container verschlüsselt werden. Das Betriebssystem sieht diesen Container als eine Datei mit zufälligem Inhalt. Innerhalb solch einem Container verwaltet TrueCrypt ein eigenes Dateisystem. Wenn ein Benutzer nun Daten eines Containers oder einer ganzen verschlüsselten Partition schreiben oder lesen will, muss diese zuerst als ein virtuelles Laufwerk gemountet werden.

TrueCrypt hat noch ein paar Features für mehr Sicherheit implementiert. Die erstellten Container haben keinen eigenen Dateiheader. Dadurch wird es Angreifern erschwert, verschlüsselte Container auf dem Dateisystem aufzufinden. Die Datei, welche als Container dient, hat immer die Maximalgröße, mit der sie erstellt wurde, da der unbenutzte Bereich mit Zufallswerten aufgefüllt wird. Außerdem ist es möglich, ein so genanntes hidden Volume zu erstellen. Dies ist ein eigener Speicherbereich in einem Container. Genauer gesagt, ein hidden Volume ist daher ein eigener verschlüsselter Speicherbereich in einem verschlüsselten Container. Wenn nun der Besitzer des mobilen IT-Clients gezwungen wird, das Passwort für einen Container weiterzugeben, kann dieser nur das Passwort des Containers und nicht das des hidden Volumes bekannt geben. In einem hidden Volume sollten besonders sensible Daten gespeichert werden.

TrueCrypt kann so eingesetzt werden, dass der Benutzer beim mounten einer verschlüsselten virtuellen Partition nicht nur ein Passwort sondern auch ein key file angeben muss. Dadurch wird eine hybride Authentifizierungsmethode zum Einsatz gebracht, bei der der Benutzer durch Wissen des Passwortes und Besitz des key files authentifiziert wird.[84] Dieses key file sollte auf einer SmartCard oder ähnlichem gespeichert sein.

Bekannte Angriffe auf dieses System sind nur Brute-Force-Attacken. Bei einem starken Passwort, oder bei Verwendung eines key files, ist es praktisch unmöglich, die Daten in einer akzeptablen Zeit zu entschlüsseln. TrueCrypt muss von dem Benutzer des mobilen IT-Clients richtig verwaltet und eingesetzt werden. Es steht dem Administrator der IT-Infrastruktur des Unternehmens keine Möglichkeit zur Verfügung, den Einsatz dieser Software mobilen Clients zu überprüfen und zu verwalten.

Eine spezielle Enterpriselösung für diesen Einsatz bietet *Safeboot*. Mit dieser Software ist es möglich, Datensicherheit der mobilen IT-Clients zu gewährleisten, wobei die Verwaltung der Softwaremodule zentral erfolgt. Das Herzstück ist das so genannte Management Center. Diese Softwarekomponente bietet Administratoren eine zentrale Konfigurationsmöglichkeit der einzelnen Safeboot Sicherheitselemente der mobilen IT-Clients. Um einzelne Komponenten auf den Clients zentral aktivieren und konfigurieren zu können, muss nur eine Datei auf dem mobilen Gerät installiert werden. Die Kommunikation zwischen Management Cen-

[84] vgl. TrueCrypt, [Tru07].

ter und Client erfolgt verschlüsselt. Bei Verbindung mit dem Management Center sucht der Client nach Änderungen in der Konfiguration. Safeboot unterstützt electronic Identity (eID), wodurch ermöglicht wird, sich mit einer elektronischen ID- (Identity) Card anzumelden. Es kommt bei diesem Produkt eine Richtliniendatenbank zum Einsatz, mit deren Hilfe Administratoren bestimmten Benutzern spezifische Rechte übertragen können.

Eine weitere Komponente dieser Enterpriselösung ist die Device Security Software. Diese führt eine Pre-Boot Authentifizierung durch, sowie die Verschlüsselung der kompletten Festplatte.[85] Dafür kann eine Zwei-Faktor Authentifizierung eingerichtet werden. Durch Application Control kann der Administrator zentral steuern, welche Programme auf dem mobilen IT-Client ausgeführt werden dürfen. Mittels Device Encryption wird die Verschlüsselung auf dem Client zentral konfiguriert. Es wird nicht nur die Festplatte verschlüsselt, sondern auch Wechseldatenträger, damit chiffrierte Dateien nicht von Unbefugten über transportable Medien eingesehen werden können. Zur Zwei-Faktor Authentifizierung können SmartCards, USB-Tokens sowie Zertifikate einer PKI eingesetzt werden. Durch den Einsatz von Port Control wird es dem Administrator ermöglicht, gewisse Hardwareschnittstellen auf dem mobilen Client zu deaktivieren bzw. nur für gewisse Geräteklassen oder Hersteller IDs zu erlauben.

Ebenfalls eine wichtige Softwarekomponente ist Network Security. Diese bietet eine Datenverschlüsselung, unabhängig davon, wo sich die Daten in der IT-Infrastruktur des Unternehmens befinden.[86]

Das britische Unternehmen *Becrypt* bietet ebenfalls eine Datensicherheitslösung, welche zentral gesteuert und konfiguriert werden kann. Mit Hilfe des Protect Managers ist es möglich, die beiden Komponenten DISK Protect und Connect Protect zu verwalten.

Mit DISK Protect kann eine Pre-Boot Authentifizierung sowie das Verschlüsseln der gesamten Festplatte verlangt werden. Es ist auch möglich, Daten auf Wechseldatenträgern verschlüsselt abzuspeichern. Der Schlüssel wird mittels RSA geschützt an eine zentrale Datenbank übertragen. Wenn sich der Benutzer nicht nach der angegebenen Anzahl von Versuchen erfolgreich authentifiziert hat, wird das mobile System gesperrt. Der Benutzer des Clients muss in diesem Fall mit dem Administrator in Kontakt treten, welcher den mobilen Client über das Internet wieder freischalten kann.

Connect Protect steuert die angeschlossenen Wechselmedien auf dem mobilen IT-Client. Dadurch kann die Kommunikation mit diesen Geräten teilweise oder gänzlich eingeschränkt werden.[87]

Eine Enterpriselösung hat gegenüber einer stand alone Implementierung wie TrueCrypt ei-

[85] Bei einer Pre-Boot Authentifizierung muss sich er Benutzer vor dem Bootvorgang gegenüber dem System authentifizieren.

[86] vgl. Safeboot, [Saf07].

[87] vgl. Becrypt, [Bec07].

nige Vorteile. Der mobile Benutzer wird bei Lösungen wie Safeboot und Becrypt mit der Software nicht direkt konfrontiert, da das Programm für ihn transparent läuft. Ein weiterer großer Vorteil gegenüber TrueCrypt ist die Pre-Boot Authentifizierung. Sehr effektiv ist die zentrale Verwaltung der Software, welche speziell im mobilen Bereich ein großer Vorteil zu stand alone Lösungen ist. Einziger geringer Vorteil von TrueCrypt ist die Unterstützung von hidden Volumes. Solch ein Feature kann von Enterpriselösungen nicht implementiert werden, da diese meist Single Sign On (SSO) verwenden.[88] Tabelle 4.1 zeigt eine Gegenüberstellung der zwei beschriebenen Enterpriselösungen.

Safeboot	Becrypt
keine automatische Sperrung	Sperrung nach einer gewissen Anzahl von fehlerhaften Authentifizierungsversuchen
nur erlaubte Applikationen können ausgeführt werden	alle Applikationen können ausgeführt werden
Verschlüsselung von zentralen Daten und Wechselmedien	nur Verschlüsselung von lokalen Daten und Wechselmedien

Tabelle 4.1: Gegenüberstellung von Datensicherheitssoftware

Ein Vorteil von Safeboot gegenüber Becrypt ist die Kontrolle über Applikationen. Außerdem ermöglicht Safeboot das Verschlüsseln von Daten in der gesamten IT-Infrastruktur des Unternehmens. Die Sperrung nach einer gewissen Anzahl von fehlerhaften Authentifizierungsversuchen wird hingegen nur von Becrypt unterstützt.

Wenn mobile IT-Clients eine sichere Konfiguration besitzen, sollte dieser natürlich immer beibehalten werden. Eine Änderung in solch einem System kann es unsicher machen. Das Unternehmen *Tripwire* hat Softwareprodukte entwickelt, welche es ermöglichen, Daten auf Servern bzw. Clients zu überwachen. Es können dadurch Systemdateien, Sicherheitskonfigurationen oder andere Dateien auf deren Richtigkeit überprüft werden.

Auf dem Notebook muss Tripwire for Servers, welches auch auf Desktops und Clients eingesetzt werden kann, installiert werden. Administratoren können mittels Tripwire Manager jede Installation von Tripwire for Servers zentral verwalten.[89]

Wenn sich der Client in einem sicheren Zustand befindet, kurz nachdem dieser aufgesetzt und konfiguriert wurde, sollte der IT-Administrator des Unternehmens diesen Status mittels Tripwire Manager in die zentrale Verwaltung einlesen und abspeichern. Wenn sich der

[88] SSO ermöglicht es dem Benutzer, mit nur einer einzigen erfolgreichen Authentifizierung auf alle benötigten Ressourcen zugreifen zu können.

[89] Eine Testversion von Tripwire for Servers und Tripwire Manager befindet sich auf der beigelegten CD-ROM.

mobile IT-Client, nach einem längeren Außendienst wieder in der IT-Infrastruktur des Unternehmens befindet, können im Hintergrund Integritätsprüfungen durchgeführt werden, durch welche unautorisierte Veränderungen auf dem überwachten Client festgestellt werden können.

Oft verändern Systemupdates oder andere Prozesse die überwachten Daten des Clients. In diesem Fall muss der Administrator mittels Tripwire Manager diese Änderungen autorisieren, damit bei der nächsten Integritätsprüfung keine unautorisierten Änderungen gemeldet werden. Wenn nun solche während einer Integritätsprüfung festgestellt werden, können diese zentral wieder rückgängig gemacht werden.

Mittels Tripwire können Unternehmen ihre sensiblen Daten und Konfigurationen auf mobilen IT-Clients überwachen und bei Fehlern den Client in den letzten vertrauenswürdigen Zustand zurücksetzen. Dadurch kann dem mobilen Benutzer mehr Sicherheit gewährt werden, da ungewollte Änderungen am System erkannt werden.[90]

4.2.2 Produkte für Schutz im Netzwerk

Für Sicherheit im Netzwerk sollte der mobile IT-Client nicht nur mit dementsprechender Software ausgestattet sein, sondern sollte auch die wichtigsten Protokolle für sichere Übertragungskanäle unterstützen. Im Folgenden werden Tests von Softwareprodukten sowie Übertragungstechnologien auf deren ausreichende Sicherheit beschrieben.

4.2.2.1 Betriebssystemlösungen

Microsoft Windows XP SP2 stellt durch die integrierte Windows Firewall dem Benutzer eine grundlegende Netzwerksicherheit zur Verfügung. Wie in Abschnitt 3.2.2.3 erwähnt, kann die integrierte Firewall Datenpakete nach IP-Adressen bzw. Portnummern filtern.

Es wurden mit Hilfe des Nessus Servers auf dem Debian System Sicherheitsscans durchgeführt. Auf den Server kann mit Hilfe eines Clients, welcher in diesem Fall auf dem selben System installiert wurde, zugegriffen werden. Es wurde ein Scan mit aktivierter, standardmäßig konfigurierter Windows Firewall durchgeführt.[91] Da normalerweise kein Port offen ist, hat Nessus keine Sicherheitslücken gemeldet.

Um zu zeigen, vor welchen Angriffsmöglichkeiten die integrierte Firewall den mobilen IT-Client schützt, wurde auch ein Scan mit deaktivierter Firewall durchgeführt. Dieser ergab drei Sicherheitslücken, welche es einem Angreifer ermöglichen, willkürlichen Code auf dem

[90] vgl. Tripwire Inc., [Inc07c].
[91] Nessus Server und Client befinden sich auf der beigelegten CD-ROM.

mobilen Client ohne Authentifizierung ausführen zu können. Dies ist über den Server Message Block (SMB) möglich.[92] Außerdem ist es einem Angreifer möglich an Information zu kommen, wie z.B das verwendete Betriebssystem oder die eingestellte Uhrzeit des mobilen Clients, was aber keine direkte Sicherheitslücke bedeutet.[93]

Da die Windows Firewall oft so konfiguriert wird, dass die Verwendung des oft benutzen SMB-Dienstes möglich ist, ist diese Angriffsmöglichkeit mit der Aktivierung der Systemfirewall nicht eliminiert. Nessus weist bei dieser Sicherheitslücke auf drei Updates von Microsoft hin, welche diese Probleme lösen.[94] Wenn diese drei Updates installiert werden, sind die genannten Angriffsmethoden nicht mehr möglich. Der Sicherheitsscan des mobilen Clients bei aktivierter Windows Firewall und erlaubten SMB-Dienst weist keine großen Gefährdungen mehr auf.[95]

Um mobile IT-Clients mit Microsoft Windows XP sicher zu halten, sind regelmäßig Updates zu installieren. Diese Updates werden von Microsoft im Internet zur Verfügung gestellt. Standardmäßig ist Windows XP so konfiguriert, dass regelmäßig nach neuen Updates gesucht wird. Diese Funktion wurde mit BITS realisiert und kann von der Windows Firewall nicht geblockt werden, unabhängig davon wie diese konfiguriert ist. Es ist daher sinnvoll, eine Software Firewall von Drittanbietern, wie z.B. Kaspersky Internet Security, zu installieren, die den gesammten Traffic des mobilen IT-Clients überwachen kann.

Es sollte auf mobilen IT-Clients trotzdem das automatische Windows Update eingesetzt werden, um möglichst schnell an Sicherheitsupdates zu gelangen. Um in einem Unternehmen in die Aktualisierungsprozedur der Clients mehr Sicherheit und Überschaubarkeit zu bringen, kann *Windows Server Update Services* (WSUS) eingesetzt werden.[96] Dafür muss ein Windows Server, auf welchem WSUS in Betrieb ist, in die IT-Infrastruktur des Unternehmens implementiert werden. Der Server lädt Updates von einer vertrauenswürdigen Quelle herunter und speichert sie auf einer Festplatte. Die Clients müssen so konfiguriert werden, dass sie ihre Windows Updates vom Server beziehen. Dies kann mit Gruppenrichtlinien oder durch Umschreiben der Registry am Client geschehen. Der Administrator kann über ein Webinterface den Server konfigurieren und bestimmen, welche Updates die Clients herunterladen sollen. Der WSUS-Server muss seine Updates von einem WSUS-Upstreamserver beziehen. Die Konfiguration sollte so erfolgen, dass für die Authentifizierung des WSUS-Upstreamservers SSL verwendet wird.

[92] SMB wird von Windows XP verwendet, um anderen Netzwerkteilnehmern Freigaben zur Verfügung zu stellen.

[93] Der Nessus Report für den Scan bei deaktivierter Windows Firewall befindet sich auf der beigelegten CD-ROM.

[94] Folgende Updates haben diese Probleme gelöst: KB896422, KB917159, KB921883.

[95] Der Nessus Report für den Scan bei aktivierter Windows Firewall und erlaubtem SMB-Dienst befindet sich auf der beigelegten CD-ROM.

[96] WSUS befindet sich auf der beigelegten CD-ROM.

Windows Updates bestehen sowohl aus Metadaten, welche Informationen über das Updatepaket enthalten, als auch aus dem eigentlichen Updatefile. Die Metadaten sollten über SSL vom Upstreamserver auf den WSUS-Server des Unternehmens übertragen werden. Das Updatefile wird von Microsoft signiert und kann daher über HTTP übertragen werden. Die Kommunikation zwischen dem WSUS-Server und den Clients erfolgt genauso.[97] Dadurch kann der Systemadministrator steuern, welche Updates die Clients installieren und bestimmen, dass sie diese von einer sicheren Quelle beziehen. Um besonders hohe Sicherheit zu gewähren, sollte dieser Dienst nur im internen LAN des Unternehmens zur Verfügung gestellt werden. Ein Update ist daher nur möglich, wenn sich der mobile IT-Client am Unternehmensstandort befindet.

4.2.2.2 Sicherheitsprotokolle

Für eine sichere Übertragung von Daten über das Internet stellt VPN, wie in Abschnitt 3.2.2.4 erläutert, eine sichere Lösung dar. Beim Einsatz eines VPN stellt die Authentifizierung des remote Benutzers den einfachsten Angriffspunkt dar. Daher muss auf deren starke Ausprägung besonderer Wert gelegt werden.[98]

SSL wird häufig eingesetzt, um die Kommunikation zwischen einem Webserver und einem Client zu authentifizieren und zu verschlüsseln. Wie in Abschnitt 3.2.2.4 erläutert, kommen für die Authentifizierung X.509-Zertifikate zum Einsatz. Im Folgenden wird demonstriert, wie mittels MITM-Attacke auf eine SSL-Verbindung mit Server Authentifizierung der Benutzername und das Passwort des Opfers für die Nutzung einer Website mitgelesen werden können. Voraussetzung hierfür ist, dass sich Angreifer sowie Opfer im selben öffentlichen Netzwerk befinden.

Um die Attacke durchzuführen, wird das Programm *dsniff* auf dem PC des Angreifers installiert.[99] Dieses besteht unter anderem aus folgenden Teilprogrammen:

- *arpspoof:* wird benötigt um den ARP-Cache des Opfers zu vergiften
- *dnsspoof:* antwortet auf die DNS-Anfragen des Opfers
- *webmitm:* leitet den Traffic des Opfers bzw. des Servers weiter

Zuerst muss der Angreifer veranlassen, dass sein Opfer alle Pakete, welche für sein Gateway bestimmt sind, an ihn sendet. Dies geschieht mittels ARP-Cache Vergiftung. Der Angreifer sendet permanent ARP-Replies mit der Zuordnung von seiner MAC-Adresse zur IP-Adresse des Gateway. Das Opfer hat daher in seinem ARP-Cache eine falsche MAC-IP-Zuordnung. Alle Pakete, die das Opfer nun zum Gateway schickt, werden von diesem selbst

[97] vgl. Microsoft TechNet, [Tec07].
[98] Für Informationen über Authentifizierung siehe Abschnitt 3.2.1.2.
[99] vgl. dsniff, [dsn07].

mit der MAC-Adresse des Angreifers adressiert.[100] Der Switch schickt daher diese Pakete über den physischen Port, an dem der Angreifer angeschlossen ist. Dies soll durch das folgende ausgetestete Beispiel näher erläutert werden. Bei Ausführen des Befehls `arpspoof -t 192.168.0.245 192.168.0.1` auf dem Computer des Angreifers werden andauernd ARP-Replies mit der IP-Adresse des Gateway (z.B. 192.168.0.1) und der MAC-Adresse des Angreifers an die IP-Adresse des Opfers (z.B. 192.168.0.245) versendet. Nach Beendigung des Befehls `arpspoof` werden mit der richtigen Layer 2-Adresse des Gateway noch drei ARP-Replies an das Opfer gesendet, damit nach der Attacke die Internetverbindung des mobilen Clients nicht abbricht und somit das Opfer keinen Angriff vermutet.[101]

Nachdem nun der Traffic des Opfers über den Angreifer fließt, muss der DNS-Server gestartet werden, der auf die DNS-Responses des Opfers antwortet. Durch das Ausführen des Befehls `dnsspoof` leitet der Rechner des Angreifers die Anfragen des Clients an den richtigen DNS-Server weiter. Die Antwort wird natürlich dem Opfer mit der scheinbar richtigen IP-Adresse des DNS-Servers, die der DHCP-Server den Clients übermittelt, mitgeteilt. In diesem Beispiel hat das Opfer zuerst die Startseite (*www.orf.at*) und danach den ECampus der FH-St. Pölten (*ecampus.fh-stpoelten.ac.at*) aufgerufen.[102] In der Datei `/usr/share/dsniff/dnsspoof.hosts` wurde angegeben, dass sich der ECampus auf der IP-Adresse des Angreifers befindet. Wenn der Befehl `dnsspoof -f /usr/share/dsniff/dnsspoof.hosts` ausgeführt wird, prüft der Computer des Angreifers zuerst in dieser Datei, ob hier die angefragte DNS-Zuordnung angegeben wurde.[103] Wenn ja, antwortet er mit der falschen IP-Adresse des nachgefragten Servers, anstatt den DNS-Response an den richtigen DNS-Server weiterzuleiten.

Es muss auch noch der Webserver gestartet werden, welcher dem mobilen IT-Client den richtigen Server simuliert. Der Befehl `webmitm -dd` startet den Webserver und gibt detaillierte Debuginformationen aus.[104] Diese enthalten unter anderem den Benutzernamen und das Passwort, mit welchem sich der mobile User auf der Website *ecampus.fh-stpoelten.ac.at* eingeloggt hat.[105]

Der Rechner des Angreifers braucht ein X.509-Zertifikat, um eine SSL-Verbindung zu dem Client aufbauen zu können. Dies sind in den meisten Fällen self signed Zertifikate.[106] Da in

[100] Für weitere Informationen zu MITM-Attacken siehe Abschnitt 2.2.2.

[101] Das Listing für den Befehl `arpspoof -t 192.168.0.245 192.168.0.1` befindet sich auf der beigelegten CD-ROM.

[102] Das Listing für den Befehl `dnsspoof` befindet sich auf der beigelegten CD-ROM.

[103] Das Listing für den Befehl `dnsspoof -f /usr/share/dsniff/dnsspoof.hosts` befindet sich auf der beigelegten CD-ROM.

[104] Das Listing für den Befehl `webmitm -dd` befindet sich auf der beigelegten CD-ROM.

[105] Das Listing des Befehls `webmitm -dd` beinhaltet in Zeile 427 den Benutzernamen und das Passwort des Benutzers.

[106] self signed Zertifikate wurden nicht von einer gültigen CA signiert, sondern von einem unautorisierten System.

diesem Fall kein gültiges Zertifikat vorliegt, bekommt der Benutzer des mobilen IT-Clients eine Warnung von seinem Webbrowser. Durch Social Engineering kann das Opfer dazu gebracht werden, dem ungültigen self signed Zertifikat trotzdem zu vertrauen.[107] Besonders raffinierten Angreifern gelingt es in seltenen Fällen, ihr Zertifikat von einer gültigen CA mittels gefälschter Identität signieren zu lassen.[108] Dies ist aber nicht der Regelfall. Der Benutzer eines mobilen IT-Clients sollte das Zertifikat des Servers auch manuell überprüfen, um sicher zu gehen, dass der Besitzer des Zertifikates wirklich der von ihm vermutete ist.

4.2.2.3 Spezifische Softwarelösungen

Um sich heutzutage gegen bösartige Software abzusichern, sollte jeder Client ein Anti-Virus Programm installiert haben. Dieses sucht in regelmäßigen Abständen nach Viren, die sich bereits auf dem System befinden. Da immer wieder neue Vorgangsweisen entwickelt werden, um Viren zu programmieren, müssen daher auch immer neue Techniken implementiert werden, die sie aufspüren können. Um einen Virenscanner immer wieder auf den neuesten Stand zu bringen, wird dieser in den meisten Fällen mittels Online Update aktuell gehalten. Die neuen Virensignaturen und Programmupdates werden regelmäßig durch die Software heruntergeladen und installiert.

Es wurde getestet, ob diese Updatefunktionen einen Angriffspunkt bieten, um bösartige Software einschleusen zu können. Auf dem mobilen IT-Client wurde der kostenfreie Virenscanner *AVG Anti-Virus Free Edition 7.5* installiert.[109] Nun wurde ein Updateprozess dieser Software mittels Ethereal belauscht.[110] AVG lädt zuerst die Datei `/softw/70free/update/avginfo.ctf` vom Updateserver über HTTP herunter und prüft, ob neue Updates zur Verfügung stehen. Sollten solche gefunden werden, werden diese vom selben Server aus dem gleichen Ordner ebenfalls über HTTP heruntergeladen und installiert. Dieser Server wurde mit identer Ordnerstruktur und mittels Apache 2.0 gespiegelt. Durch Vergiftung des ARP-Caches und einer falschen Antwort auf ein DNS-Response wurde dieser Server vom Client während des Updatevorgangs kontaktiert. Auf ihm befindet sich ebenfalls eine Updateliste sowie eine veränderte Updatedatei. Wenn der mobile IT-Client ein Update durchführt, prüft er diese gefälschte Datei auf die Signatur des Softwareherstellers und gibt eine Fehlermeldung aus, da diese durch die Änderungen eine ungültige Signatur enthält.[111] Der bösartige Code wird daher auf dem Client nicht installiert.

Die Updateprozeduren der Anti-Virus Softwarehersteller sind so mittels Signatur gut gegen manipulierte Updatedateien abgesichert. Es wird dadurch einem Angreifer erschwert, bösar-

[107] Für Informationen über Social Engineering siehe Abschnitt 2.1.3.
[108] vgl. Heise Online, [Onl06].
[109] AVG Anti-Virus Free Edition 7.5 befindet sich auf der beigelegten CD-ROM.
[110] Die Snifferdaten des Virenupdates befinden sich auf der beigelegten CD-ROM.
[111] vgl. Slazenger, [Sla05].

tigen Code auf einem mobilen System über ein Anti-Virus Update zu installieren.

Speziell Benutzer von mobilen IT-Clients sollte nicht auf die Installation eines HIPS verzichtet. Dadurch können bekannte Angriffsmöglichkeiten früh erkannt und verhindert werden. Es wurde auf dem mobilen Client eine 15 Tage-Demoversion der Software *Kaspersky Internet Security 7.0* installiert.[112] Um die einwandfreie Funktion dieses HIPS zu testen wurde mittels Nmap ein Portscan auf dem Client durchgeführt.[113] Damit Ergebnisse der Portscans aussagekräftiger sind, wurden mehrere Ports auf dem Client geöffnet.[114] Wenn ein Portscan auf ein mit dieser Software geschütztes System durchgeführt wird, wird dieser nach 60 gescannten Ports erkannt.[115] Daraufhin wird die IP-Adresse des Absenders, der den Scan durchgeführt hat, standardmäßig für 60 Minuten auf dem Client gesperrt, und es wird ein Log-Eintrag getätigt.[116] Wenn die IP-Adresse des Angreifers auf dem Zielsystem noch nicht gesperrt ist, kann dieser genau 60 Ports scannen, bevor dies mit der gleichen Adresse nicht mehr möglich ist.

Es wurde auch getestet, nach welchem Zeitintervall zwischen den SYN-Paketen Kaspersky Internet Security dies nicht mehr als Portscan erkennt. Der Test ergab, dass bei einer Wartezeit von 0,5 Sekunden zwischen den gesendeten SYN-Paketen dies nicht mehr als Portscan erkannt wird.[117] Dies wurde durch Mitsniffen der Datenpakete festgestellt.[118] Da sich mobile IT-Clients in den meisten Fällen nicht besonders lange in öffentlichen Netzwerken aufhalten, reicht diese Sicherheitsvorkehrung meist aus. Angreifer können dadurch bekannte Kommunikationsports auf dem mobilen Client ausspionieren, indem wenige, aber dafür bestimmte Ports geprüft werden. Kaspersky Internet Security ist aber trotzdem ein HIPS, welches mobilen IT-Clients in öffentlichen Netzwerken Schutz bieten kann.

Es wurde weiters das HIPS *Norton Internet Security 2007* mittels 15 Tage-Demoversion getestet.[119] Nun wurde ebenfalls wieder mittels Nmap getestet, ob auch dieses HIPS den Portscan erkennt und unterbindet. Dabei zeigte sich das gleiche Verhalten wie bei Kaspersky Internet Security 7.0. Einziger Unterschied ist, dass Norton Internet Security 2007 standardmäßig die IP-Adresse eines vermutlichen Angreifers nur für 30 Minuten sperrt.

Solche Produkte bieten nicht nur Schutz vor Angriffen über Netzwerke, sondern auch vor Malware, Spyware und sonstiger sicherheitsgefährdender Software. Die Untersuchungen er-

[112] Kaspersky Internet Security befindet sich auf der beigelegten CD-ROM.
[113] Nmap befindet sich auf der beigelegten CD-ROM.
[114] Das Listing für den Portscan ohne HIPS befindet sich auf der beigelegten CD-ROM.
[115] Das Listing für den Portscan, auf ein mit Kaspersky Internet Security 7.0 geschütztes System, befindet sich auf der beigelegten CD-ROM.
[116] Der Log-Eintrag von Kaspersky Internet Security für einen Portscan befindet sich auf der beigelegten CD-ROM.
[117] Das Ergebnis dieses Portscans befindet sich auf der beigelegten CD-ROM.
[118] Die Snifferdaten für den Portscan mit 0,5 Sekunden Wartezeit zwischen den SYN-Paketen befinden sich auf der beigelegten CD-ROM.
[119] Norton Internet Security befindet sich auf der beigelegten CD-ROM.

gaben, dass Norton Internet Security 2007 gegenüber Kaspersky Internet Security 7.0 einen großen Performanceverlust des mobilen IT-Clients aufweist.

Die amerikanische Firma *Altiris* entwickelte ein Produkt namens *Endpoint Security Solution*.[120] Diese Software ermöglicht Unternehmen ein zentralisiertes Sicherheitsmanagement für alle Endpunkte einer vorhandenen IT-Infrastruktur. Durch eine zentrale Konfiguration können auf mobilen IT-Clients individuelle Security Policies durchgesetzt werden. Diese Sicherheitsrichtlinien können je nach Aufenthalt des mobilen Benutzers automatisch geändert werden. Auf dem Client muss der Endpoint Security Agent installiert sein, welcher Security Policies von der Central Management Console bei Verbindung herunterlädt und aktualisiert. Endpoint Security Solution besteht aus den folgende Basiskomponenten, um Schutz zu gewährleisten:

- Advanced firewall enforcement
- Wireless connectivity control
- Enterprise-managed endpoint integrity checking
- Removeable data storage device control

Advanced firewall enforcement ermöglicht es Administratoren, Firewall- und HIPS-Konfigurationen mittels Policies auf dem mobilen IT-Client festzulegen. Die Funktionen der Firewall werden in den Network Device Interface Specification (NDIS) Treiber der Network Interface Card (NIC) implementiert.[121] Dadurch kann Netzwerkdatenverkehr auf der untersten Ebene des Betriebssystems untersucht und eventuell gestoppt werden. Dies ermöglicht ein frühes Erkennen von Netzwerkangriffen und bietet daher dem mobilen IT-Client in öffentlichen Netzwerken guten Schutz.

Wireless connectivity control kann eingesetzt werden, um den IT-Client vor unsicheren oder rogue APs zu schützen. Administratoren können einstellen, dass sich Geräte nicht zu unzureichend geschützten oder nur zu gewissen APs verbinden dürfen. Im Falle des mobilen IT-Clients macht dies aber nicht viel Sinn, da die meisten öffentlichen APs keine gute Schutzvorkehrung besitzen. Der mobile Benutzer kann aber gezwungen werden, ein VPN über eine unsichere WLAN-Verbindung herzustellen, um alle gesendeten und empfangenen Daten ausreichend zu schützen.

Enterprise-managed endpoint integrity checking stellt sicher, dass der mobile IT-Client alle Sicherheitspolicies erfüllt, bevor der Benutzer eine unsichere Datenverbindung verwenden kann. Es wird geprüft, ob installierte Sicherheitssoftware alle aktuellen Virensignaturen und Updates besitzt, und ob diese zum Zeitpunkt der Verbindung ausgeführt werden. Erst nachdem das System mit allen verfügbaren Updates ausgestattet wurde, wird die Verbindung für

[120] Altiris Endpoint Security Solution Evaluation Version befindet sich auf der beigelegten CD-ROM.
[121] NDIS definiert ein standard Application Programming Interface (API) für NICs.

den User freigegeben.

Removeable data storage device control bietet den Administratoren Kontrolle über die Verwendung von Wechseldatenträgern. Es können alle Datenträger erlaubt werden oder nur spezielle, welche mittels Hersteller-ID oder Typ des Datenträgers identifiziert werden können. Außerdem wird es Administratoren ermöglicht, dass angeschlossene Speichermedien nicht beschrieben werden dürfen.

Administratoren können mittels Endpoint Security Solution verhindern, dass unautorisierte Anwendungen auf dem mobilen IT-Client ausgeführt werden. Es ist ebenfalls möglich, bestimmten Applikationen den Zugang zum Internet zu untersagen.[122]

Es besteht die Möglichkeit, je nachdem in welchem Netzwerk sich der Client befindet (zu Hause, im Unternehmen oder in einem öffentlichen Netzwerk), unterschiedliche Sicherheitspolicies für verschiedene Standorte zu aktivieren. Dies kann manuell durch den mobilen Benutzer geschehen oder automatisch erkannt werden. Für die automatische Erkennung werden Layer 2- und Layer 3-Adressen des Gateway, DHCP-Servers und DNS herangezogen. Theoretisch wäre es möglich, ein öffentliches Netzwerk nach genau diesen Parametern zu konfigurieren, damit der mobile IT-Client eine schwächere Sicherheitspolicy aktiviert. Aber das wiederum ist sehr unwahrscheinlich, da der Angreifer Informationen benötigt, welche ihm nicht sehr leicht zugänglich sind.

[122] vgl. Altiris Inc., [Inc07a].

Kapitel 5

Resümee

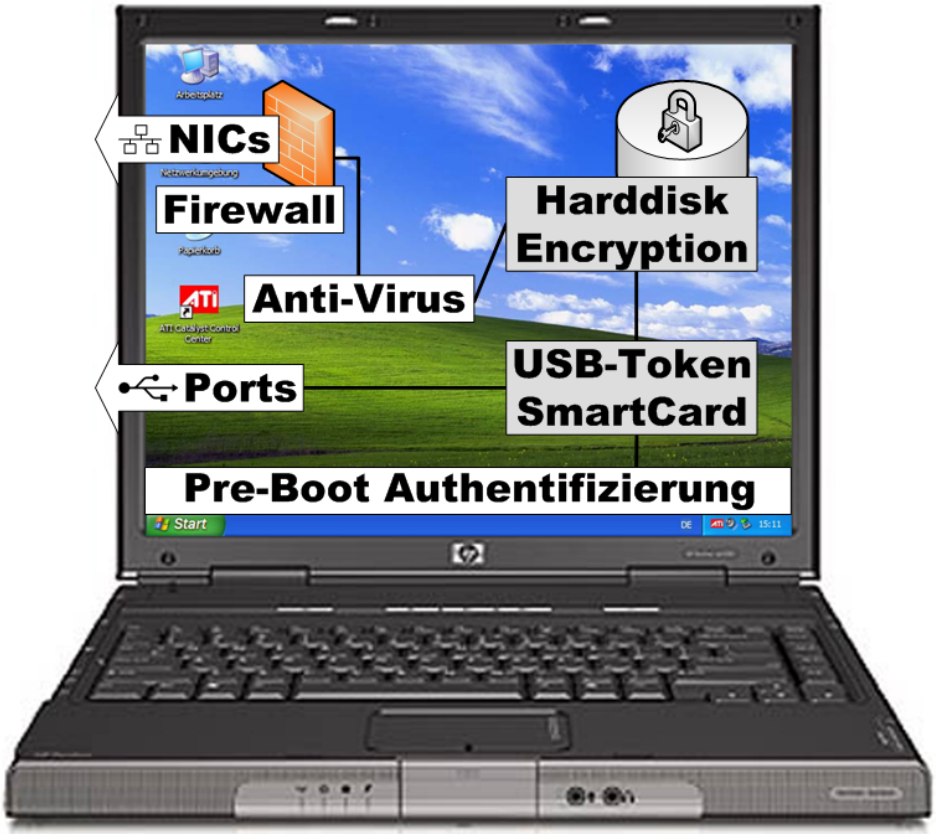

Abbildung 5.1: Teilkomponenten eines minimal abgesicherten mobilen IT-Clients

In diesem Abschnitt der Arbeit wird abschließend beschrieben, wie Unternehmen ihre mobilen IT-Clients vor Angriffen schützen können. Sie sollten eine Sicherheitsrichtlinie besitzen, die beschreibt, wie stark und mit welchen Methoden Clients geschützt werden müssen. Besonders wichtig für einen starken Schutz ist die Einführung von wirksamen Verschlüsselungsverfahren, mit welchen Daten auf Festplatten, sowie während der Übertragung über Netzwerke, verschlüsselt werden können. Jeder mobile Mitarbeiter sollte, auch bei zentra-

ler Verwaltung der Sicherheitsmaßnahmen, eine Schulung für richtiges sicheres Verhalten absolvieren. Es muss auch eine starke Passwortpolitik im Unternehmen umgesetzt werden, die beschreibt, wie lange und wie komplex Benutzerpasswörter sein müssen bzw. wo diese abgespeichert werden dürfen.

Um einen mobilen IT-Client minimal gegen Angriffe abzusichern, bedarf es mehrerer Maßnahmen. Abbildung 5.1 zeigt die wichtigsten Teilkomponenten, die erforderlich sind, um einen mobilen IT-Client minimal gegen Datendiebstahl abzusichern. Bei den grau hinterlegten Teilkomponenten handelt es sich um Maßnahmen, die sich bereits im Grenzbereich zwischen Minimalschutz und erweitertem Schutz von mobilen IT-Clients befinden.

Eine Pre-Boot Authentifizierung schützt den Client vor unautorisiertem Starten des Systems. Bei diesem Vorgang ist es möglich, den Benutzer nicht nur über ein Passwort, sondern auch mittels einer SmartCard, eines USB-Token oder eines Fingerabdruckes zu authentifizieren. Die verschlüsselte Festplatte verhindert den Zugriff auf Daten durch unerwünschte Personen und Systeme. Eine aktuelle Anti-Virus Software findet zumeist Viren, die sich bereits auf der Festplatte des mobilen IT-Clients befinden. Die Personal Firewall ermöglicht das Filtern von Netzwerkpaketen. Es kann auch der ungewollter Zugriff von Anwendungen auf das Netzwerk verhindert werden, oder Datenpakete nach IP-Adressen bzw. Ports gefiltert werden.

5.1 Empfohlene lokale Datensicherheitsmechanismen

Einem Angreifer sollte es so schwer wie möglich gemacht werden, auf Daten, die auf dem mobilen Client gespeichert sind, Zugriff zu bekommen.

Das heißt, Sicherheitsmaßnahmen sollten schon während des Bootvorgangs gesetzt werden. Dies kann nicht nur durch die Aktivierung eines Boot- und BIOS-Passwortes umgesetzt werden, sondern auch durch den Einsatz eines Harddisk-Passwortes in Maximum Security Mode. Um diesen Modus aktivieren zu können, muss in vielen Fällen ein erweitertes BIOS auf dem mobilen Gerät installiert werden. Dies kann z.B. mittels ATA Security eXtension BIOS erfolgen.[123] Diese Sicherheitsmechanismen werden trotz bekannter Schwachstellen eingesetzt, da sie den Angreifer langsam machen und damit die Chance erhöhen, dass der Versuch des Datendiebstahls frühzeitig aufgegeben wird.

Beim Einsatz von mobilen IT-Clients muss darauf geachtet werden, dass der Benutzer des Gerätes, bei zentraler Verwaltung, auf keinen Fall lokale Administratorrechte erlangen und dadurch die Konfiguration des Systems ändern kann. Es sollte daher auf diesen Systemen bei zentraler Verwaltung das Konto des Administrators deaktiviert werden. Dies macht nur Sinn, wenn die gesamte Festplatte verschlüsselt wird, damit es nicht möglich ist, von einer

[123] vgl. Abschnitt 3.1.1.3.

CD-ROM zu booten und damit die Registrierung umschreiben zu können.

Solch eine zentrale Verwaltung des Clients hat den Vorteil, dass sie für den mobilen Benutzer transparent geschieht, und die Administratoren damit Sicherheitsrichtlinien zentral steuern können. Diese sollten sorgfältig durchdacht und eventuell mittels Group Policy implementiert werden. Zur Verschlüsselung der Daten auf Notebooks bzw. deren Wechseldatenträgern kann Software wie Safeboot eingesetzt werden, welche eine sehr sichere Lösung und eine zentrale Verwaltung bietet.[124]

Ein sehr wichtiges Thema ist die Authentifizierung der Benutzer des mobilen IT-Clients. Um User sicher authentifizieren zu können, muss mindestens eine Zwei-Faktor Authentifizierung zum Einsatz kommen. Die sichere Authentifizierung der Benutzer kann durch Wissen und Haben erfolgen.

5.2 Empfohlener Schutz gegen Angriffe über Netzwerke

Um den mobilen IT-Client vor Angriffen aus öffentlichen Netzwerken zu schützen, müssen viele Maßnahmen erfolgen. Besonders wichtig ist eine starke Authentifizierung gegenüber Netzwerkservern. Dies kann z.B. ein VPN-Gateway sein. Ein RSA-Token stellt dem mobilen Benutzer ein OTP zur Verfügung, mit dem eine starke Authentifizierung erfolgen kann. Weiters kann auch noch eine Authentifizierung des Gerätes erfolgen, welche mittels TPM geschehen kann.[125] Außerdem ist es nötig, dass sich immer beide Seiten gegenüber ihren Kommunikationspartnern authentifizieren. Unternehmen benötigen für einen gewissen Sicherheitsstandard daher eine PKI in ihrer IT-Infrastruktur, um die Authentifizierung mittels Zertifikaten zu ermöglichen.

Da besonders mobile Geräte mittels Firewall und HIPS geschützt werden müssen, empfiehlt sich eine zentrale Konfiguration und Überwachung dieser Schutzvorkehrungen. Dies kann z.B. mittels Altiris Endpoint Security Solution umgesetzt werden. Da diese Software kompatibel zu einem Active Directory System ist, kann sie einfach in eine bestehende IT-Infrastruktur eingebunden werden. Natürlich gibt es auch Sicherheitslösungen, welche nicht zentral verwaltet werden müssen. Bei Verwendung dieser Produkte muss der mobile Anwender selbst darauf achten, dass diese richtig konfiguriert sind.

Damit Administratoren den Überblick über installierte Systemupdates auf Clients haben, sollte ein WSUS eingesetzt werden, der Updateprozeduren von Windows Clients sicher abwickelt. Dieser sollte so konfiguriert werden, dass mobile Clients nur bei Verbindung über das eigene Unternehmensnetzwerk eine Verbindung zu diesem Server herstellen und alle

[124] vgl. Abschnitt 4.2.1.2.
[125] vgl. Abschnitt 3.1.2.

wichtigen Updates herunterladen und installieren.

Mobile IT-Client sollte in regelmäßigen Abständen auf Sicherheitslücken überprüft werden. Administratoren können dies mit Securityscannern wie Nessus durchführen, wenn sich die Geräte an dem Standort ihres Unternehmens befinden.

5.3 Vom Basis- zum Komplettschutz für mobile IT-Clients

Für eine komplette Absicherung eines mobilen IT-Clients gegen jegliche Art von Angriffen werden eine Menge an zusätzlicher Soft- bzw. Hardware benötigt. In Abbildung 5.2 wurden Teilkomponenten ergänzt, welche für einen Komplettschutz eines mobilen IT-Clients benötigt werden.

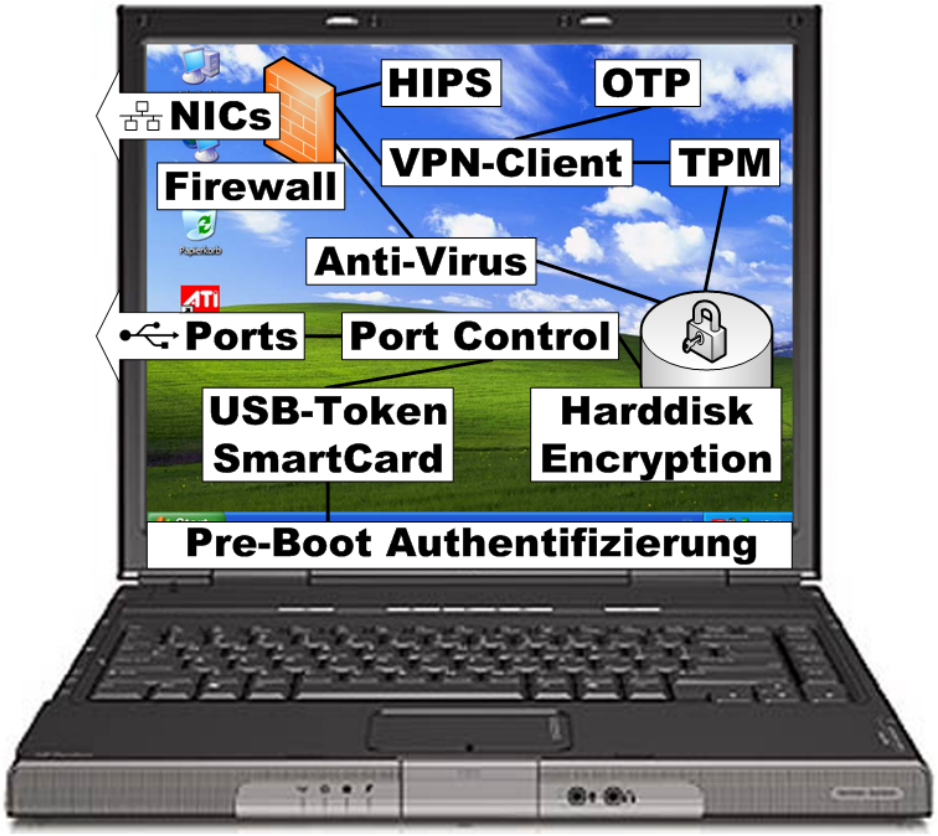

Abbildung 5.2: Teilkomponenten eines komplett abgesicherten mobilen IT-Clients

Die Pre-Boot Authentifizierung sollte für starke Sicherheit auf jeden Fall nicht nur durch ein Passwort sondern auch mittels SmartCard, USB-Token oder biometrischer Merkmale erfolgen. Der Einsatz eines Port Control Mechanismus ermöglicht die sichere Nutzung von Peripheriegeräten. Die Personal Firewall und das HIPS stehen meist in einem noch weitere Sicherheitsfunktionen bietenden Komplettpaket zur Verfügung. Die Installation einer

solchen Software schützt den mobilen IT-Client vor Netzwerkangriffen. Ein VPN-Client ermöglicht die sichere Kommunikation zur IT-Infrastruktur des Unternehmens. Zur Authentifizierung wird ein OTP und ein den Client identifizierendes TPM benutzt. Dieses kann auch dazu verwendet werden, eine sichere Ver- bzw. Entschlüsselung durchzuführen.

Tabelle 5.1 zeigt zuerst grundsätzliche Schutzmechanismen, wovor diese schützen, und durch welche Produkte diese implementiert werden können.

Schutz vor ...	Schutzmechanismus	Implementierungsmöglichkeit
Änderungen der Hardwareansteuerung und Bootreihenfolge	BIOS-Passwort	jedes BIOS bietet Schutz mittels Passwörtern
ungewolltem Booten	Boot-Passwort	jedes BIOS bietet Schutz mit einer Passwortabfrage während dem POST
ungewolltem Zugriff auf die Festplatte	Harddisk-Passwort	ein HD-Passwort kann in jedem BIOS aktiviert werden; mittels ATA Security eXtension BIOS ist es möglich, auch Maximum Security Mode zu aktivieren
Diebstahl von kryptographischen Schlüsseln	Speicherung in einem sicheren Bereich, kein Auslesen der Schlüssel möglich	ein TPM speichert Schlüssel, wobei diese nicht ausgelesen werden können; zur Ver- und Entschlüsselung wird das TPM benötigt

Tabelle 5.1: Grundlegende Absicherung eines mobilen IT-Clients

Um Schutzmechanismen zu implementieren gibt es zwei Möglichkeiten. Entweder der Benutzer des mobilen IT-Client ist selbst darauf angewiesen, dass er die richtige Konfiguration einsetzt, oder die Sicherheitsmechanismen werden zentral verwaltet.

Bei lokaler Konfiguration der Sicherheitsmechanismen benötigt der mobile Benutzer Rechte, um diese dementsprechend nach seinen Wünschen anzupassen. In den meisten Fällen wird dies über das Administratorkonto durchgeführt. Wenn der mobile Benutzer selbst für die Sicherheit seiner Daten verantwortlich ist, muss er auch dementsprechend geschult sein, um mit den Sicherheitsmechanismen richtig umgehen zu können. In Tabelle 5.2 werden Implementierungsmöglichkeiten für lokale Sicherheitskonfiguration aufgelistet. Außerdem zeigt sie welche Schutzmechanismen vor welchen Angriffsarten schützen.

Eine zentrale Verwaltung der Schutzmechanismen von mobilen IT-Clients kommt meist in großen Unternehmen zum Einsatz. Administratoren können dadurch unternehmensweite Sicherheitsrichtlinien, auch auf mobilen Geräten, umsetzen und verwalten.

Schutz vor ...	Schutzmechanismus	Implementierungsmöglichkeit
Einsicht in Daten bei Verlust oder Diebstahl	Verschlüsselung von Daten auf der Festplatte	Software wie TrueCrypt und das Systemwerkzeug EFS ermöglichen es, sensible Daten sicher zu verschlüsseln
Fälschung von Identitäten	verbesserte Authentifizierungsmechanismen	SmartCards und USB-Token (z.B. von Aladdin), bzw. Fingerabdruckscanner, wie dies Lenovo in ihre Notebooks integriert
Datendiebstahl über Wechselmedien	Datentransfer zu Wechselmedien unterbinden	manuelles Deaktivieren bzw. Aktivieren der Ports
Angriffen über unsichere Netzwerke	Benutzung einer Firewall und eines HIPS	Software wie Kaspersky Internet Security bieten Schutz mittels Firewall, HIPS und anderen Mechanismen
Viren und Trojanern	Installation eines Virenscanners	Software wie AVG Anti-Virus stellt gute Virenscanner zur Verfügung
Mitlauschen und Änderungen der Netzwerkdatenpakete sowie Vortäuschen falscher Identitäten	Verschlüsselung der Datenpakete und Integritätsprüfung beim Empfänger	Benutzung von SSL, welches von den gängigsten Webbrowsern unterstützt wird, sowie Kommunikation über VPN über IPSec mittels RSA-Token und Authentifizierung über digitale Zertifikate

Tabelle 5.2: Absicherung eines mobilen IT-Clients mit lokaler Verwaltung

Da der Anwender in diesem Fall nicht mehr für die sichere Verwendung des Notebooks verantwortlich ist, muss sichergestellt sein, dass er nicht die Möglichkeit hat, das System in irgendeiner Form unsicher zu machen. Das heißt, es müssen seine Benutzerrechte so eingestellt werden, dass er das System uneingeschränkt für seine Bedürfnisse verwenden kann, er jedoch nicht in der Lage ist, es durch Änderung der Konfiguration unsicher zu machen. Bei zentralen Konfigurationsänderungen durch einen Administrator werden diese erst bei der nächsten Verbindung mit der IT-Infrastruktur des Unternehmens auf dem mobilen IT-Client aktualisiert.

In Tabelle 5.3 werden Lösungsmöglichkeiten aufgelistet, mit welchen mobile IT-Clients abgesichert und zentral verwaltet werden können.

Schutz vor ...	Schutzmechanismus	Implementierungsmöglichkeit
Einsicht in Daten bei Verlust oder Diebstahl	Verschlüsselung von Daten auf der Festplatte	z.B. Safeboot bietet Encryption Lösungen, welche zentral verwaltet werden können
Fälschung von Identitäten	Verbesserte Authentifizierungsmechanismen	Fingerabdruckscanner wie dies Lenovo in ihren Notebooks integriert hat, SmartCards und USB-Token (z.B. von Aladdin) können Zertifikate der PKI des Unternehmens enthalten
Datendiebstahl über Wechselmedien	Benutzung von Wechseldatenträgern nur eingeschränkt zulassen	z.B. Safeboot bietet Port Control Lösungen, welche zentral verwaltet werden können
Angriffen über unsichere Netzwerke	Benutzung einer Firewall und eines HIPS	z.B. Altiris Endpoint Security Solution bietet eine zentrale Konfiguration von Firewall, HIPS und anderen Mechanismen
Viren und Trojanern	Installation eines Virenscanners	Software wie AVG Anti-Virus stellt gute Virenscanner zur Verfügung, welche eine automatische Virenprüfung durchführen können
Mitlauschen und Änderungen der Netzwerkdatenpakete	Verschlüsselung der Datenpakete und Integritätsprüfung beim Empfänger	Benutzung einer VPN-Verbindung über IPSec mittels Authentifizierung via RSA-Token und Zertifikaten
Fehlern des mobilen Benutzers, welche das System unsicher machen	User kann keine sicherheitsgefährdenden Änderungen durchführen	z.B. Altiris Endpoint Security bietet die zentrale Verwaltung von Benutzerrechten mittels Group Policy

Tabelle 5.3: Absicherung eines mobilen IT-Clients mit zentraler Verwaltung

Leider gibt es momentan noch keine Lösung, die es ermöglicht, einen mobilen IT-Client mit nur einem Softwareprodukt komplett abzusichern. Es müssen daher mehrere Produkte

kombiniert werden. Durch die Kombination unterschiedlicher Sicherheitssoftware kann es zu Inkompatibilität zwischen diesen kommen. Damit Unternehmen ihre mobilen IT-Clients trotzdem gut absichern können, sollten diese vor dem Einsatz der kombinierten Sicherheitsprodukte, auf deren einwandfreies funktionieren ausführlich getestet werden. Wenn dies berücksichtigt wird, können mobile IT-Clients sicher in der Öffentlichkeit eingesetzt werden.

Literaturverzeichnis

[Ahl06] Ernst Ahlers. Heise Website: *http://www.heise.de/newsticker/meldung/69598*, 2006.

[AS07] Thomas Kunz Alexander Sennhauser. LASEC Website: *http://www.epfl.ch/courses/sp07/HDEnc_report.pdf*, 2007.

[Baj02] Sundeep Bajikar. Intel Corp. Website: *http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf*, 2002.

[Bec07] Becrypt. Becrypt Website: *www.becrypt.com*, 2007.

[Ber04] Datenschutz Berlin. Datenschutz Berlin Website: *http://www.datenschutz-berlin.de/to/begriffe.htm*, 2004.

[Cor04] Microsoft Corp. Microsoft Website: *http://technet.microsoft.com/en-us/library/bb457146.aspx*, 2004.

[Cor07] Microsoft Corp. Microsoft Website: *http://www.microsoft.com/germany/kleinunternehmen/aufgaben/sicherheit/artikel/warum-sicherheit-so-wichtig-ist.mspx*, 2007.

[Det06] Evren Eren Kai-Oliver Detken. *Mobile Security*. Hanser, 2006.

[Dor07] FTK Dortmund. FTK Dortmund Website: *http://www.ecin.de/mobilebusinesscenter/unternehmenskommunikation/index.html?rcol*, 2007.

[dsn07] dsniff. dsniff Website: *www.monkey.org/~dugsong/dsniff*, 2007.

[Fil04] FileStorm. FileStorm Website: *http://www.filestorm.de/workshop/bios2.html*, 2004.

[Fit05] Arne Fitzenreiter. Fitzenreiter Website: *http://www.fitzenreiter.de/ata/ata.htm*, 2005.

[FS03] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. Wiley, 2003.

[fSidI07a] Bundesamt für Sicherheit in der Informationstechnik. BSI Website: *http://www.bsi.de/sichere_plattformen/trustcomp/infos/tpm_report/tpm_grundlagen.htm*, 2007.

[fSidI07b] Bundesamt für Sicherheit in der Informationstechnik. BSI Website: *http://www.bsi.bund.de/gshb/deutsch/m/m04147.htm*, 2007.

[Ger03] Markus Gerstner. Universität Erlangen Website: *http://www4.informatik.uni-erlangen.de/Lehre/SS03/PS_KVBK/talks/Ausarbeitung-NTFS_EFS.pdf*, 2003.

[Ger06] Heinz Gerwing. BSI Website: *http://www.bsi.de/literat/doc/drahtkom/drahtkom.pdf*, 2006.

[Gmb07a] Aladdin GmbH. Aladdin Website: *http://www.aladdin.de/produkte/usbtoken_esecurity/etoken_etokens_smcards.html*, 2007.

[Gmb07b] Hama GmbH. Hama Website: *http://www.hama.de/portal/pageId*3179/catId*12433/action*3499/searchMode*1/bySearch*u3*, 2007.

[Hac06] USB Hacks. USB Hacks Website: *http://www.usbhacks.com/2006/10*, 2006.

[Hei05] Peter Heinzmann. cnlab Website: *http://www.cnlab.ch/referate/SSL-verstehen.pdf*, 2005.

[Inc06] McAfee Inc. McAfee Website: *http://www.mcafee.com/us/local_content/white_papers/wp_phishing_pharming.pdf*, 2006.

[Inc07a] Altiris Inc. Altiris Website: *www.altiris.com*, 2007.

[Inc07b] RSA Security Inc. RSA Security Website: *http://www.rsa.com/worldwide/pdfs/Authenticators_DEUTSCH.pdf*, 2007.

[Inc07c] Tripwire Inc. Tripwire Website: *www.tripwire.com*, 2007.

[Jüp01] Olaf Jüptner. *IT-Sicherheit für den Mittelstand*. Hessisches Ministerium für Wirtschaft Website: *http://www.hessen-it.de/data/download/broschueren/IT-Sicherheit.pdf*, 2001.

[Kei07] Gregg Keizer. ComputerworldUK Website: *http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=2982*, 2007.

[Kra06] Michael Krauß. Universität Mannheim Website: *http://www.ra.informatik.uni-mannheim.de/lsra/student_work/seminar/hws06/Michael_Krauss/praesentation.pdf*, 2006.

[Kri06] Markus Krieger. *Sicherheit allgemein*. Rechenzentrum Uni Würzburg Website: *http://www.rz.uni-wuerzburg.de/fileadmin/rzuw/docs/infos/sicherheit/secday06_allgemein.pdf*, 2006.

[Len07] Lenovo. Lenovo Website: *http://www.pc.ibm.com*, 2007.

[Lor00] Silvia Lori. Networkworld Website: *http://www.networkworld.com/news/tech/2000/0828tech.html*, 2000.

[NH04] Petter Nordahl-Hagen. Petter Nordahl-Hagen Website: *http://home.eunet.no/~pnordahl/ntpasswd*, 2004.

[Onl06] Heise Online. Heise Website: *http://www.heise.de/newsticker/meldung/69598*, 2006.

[Oph07] Ophcrack. Ophcrack Website: *http://ophcrack.sourceforge.net*, 2007.

[PCD04] PCDirekt. PCDirekt Website: *http://www.tippsblog.de/2004/11/ibm_verzeichnet.html*, 2004.

[Roc03] RockBox. RockBox Website: *http://www.rockbox.org/lock.html*, 2003.

[Saf07] Safeboot. Safeboot Website: *www.safeboot.com*, 2007.

[sal07] *Salzburger Nachrichten*, 8. Mai, 2007.

[Sch06] Philipp Schaumann. Sicherheitskultur Website: *http://sicherheitskultur.at/man_in_the-middle.htm*, 2006.

[Sec06] McGrew Security. McGrew Security Website: *http://www.mcgrewsecurity.com/research/hackingU3*, 2006.

[Sla05] Slazenger. Slazenger Website: *http://www.slazenger.de/pb/detail/AVG_AntiVirus_Update_70322_verfuegbar.html*, 2005.

[Sny01] Joel M. Snyder. Opus One Website: *http://www.opus1.com/www/whitepapers/vpn-auth-methods.pdf*, 2001.

[Tec07] Microsoft TechNet. Microsoft TechNet Website: *http://technet2.microsoft.com/windowsserver/en/library/ac90c1de-9e04-46fd-b8ab-0bb4ab8515461033.mspx?mfr=true*, 2007.

[Tod04] Markus Todt. Bacher Systems Website: *http://www.bacher.at/download/loesungen/bacher.at_intrusion-detection-&-prevention.pdf*, 2004.

[Tru07] TrueCrypt. TrueCrypt Website: *http://www.truecrypt.org*, 2007.

[Vid05] Arne Vidström. *Computer Forensics and the ATA Interface*. Swedish Defence Research Agency Website: *http://www.foa.se/upload/rapporter/foi-computer-forensics.pdf*, 2005.

[VM97] Klaus Weidner Viktor Mraz. Heise Website: *http://www.heise.de/kiosk/archiv/ct/1997/10/286*, 1997.

[Vog07] Vogon. Vogon International Website: *http://www.vogon-international.com/literature/en/pwdcrackerpod.pdf*, 2007.

[Waa05] Thomas Waas. Christian Grafe Website: *http://social.christian-grafe.de/Social%20Engineering%20-%20Christian%20Grafe.doc*, 2005.

[wie07] wienweb.at. wienweb.at Website: *http://www.wienweb.at/content.aspx?id=84152&channel=2&cat=6*, 2007.

[Wir05] Business Wire. Findarticles Website: *http://findarticles.com/p/articles/mi_m0EIN/is_2005_April_13/ai_n13606192*, 2005.

[Wis07] Roland Wismüller. Universität Siegen Website: *http://www.bs.informatik.uni-siegen.de/web/wismueller/vl/ss07/rn1/v12a_2.pdf*, 2007.

Anhang A

Abkürzungsverzeichnis

3DES 3 Data Encryption Standard

AES Advanced Encryption Standard

AP Access Point

API Application Programming Interface

ARP Address Resolution Protocol

ASIC Application Specific Integrated Circuit

BIOS Basic Input Output System

BITS Background Intelligent Transfer Service

BSI Bundesamt für Sicherheit in der Informationstechnik

CA Certificate Authority

CCMP Counter Mode with Cipher Block Chainig Message Authentication Code Protocol

CD-ROM Compact Disk-Read Only Memory

CERT/CC Computer Emergency Response Team/Coordination Center

DDF Data Decryption Field

DES Data Encryption Standard

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DoS Denial of Service

DRF Data Recovery Field

EAP-TLS Extensible Authentication Protocol-Transport Layer Security

EAP Extensible Authentication Protocol

EAPOL Extensible Authentication Protocol over LAN

EFS Encrypting File System

eID electronic Identity Card

EK Endorsment Key

ESP Encapsulating Security Payload

FEK File Encryption Key

FSTRL File System Run Time Library

GP Group Policy

GPL General Public License

GPMC Group Policy Management Console

GPO Group Policy Object

HD Harddisk

HTTP Hypertext Transfer Protocol

IEEE Institute of Electrical and Electronics Engineers

ID Identity

IKE Internet Key Exchange

IPSec Internet Protocol Security

LPC Low Pin Count

MD4 Message Digest Algorithm 4

MITM Man In The Middle

NDIS Network Device Interface Specification

NIC Network Interface Card

NIST National Institute of Standards and Technology

NTFS New Technology File System

PCR Platform Configuration Register

PKI Public Key Infrastructure

POST Power On Self Test

PSK Pre-Shared Key

QID Query Identifier

RADIUS Remote Authentication Dial-In User Service

RAM Random Access Memory

RC4 Rivest Cipher 4

RID Relative Identifier

RPC Remote Procedure Call

RSA Rivest Shamir Adleman

SA Security Association

SID Security Identifier

SMB Server Message Block

SP Service Pack

SSL Secure Sockets Layer

TCG Trusted Computing Group

TCPA Trusted Computed Platform Alliance

TPM Trusted Platform Module

TSS Trusted Software Stack

UDP User Datagram Protocol

URL Uniform Resource Locator

USB Universal Serial Bus

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WLAN Wireless Local Area Network

WPA Wi-Fi Protected Access

WSUS Windows Server Update Services

Anhang B

Inhalt der beigelegten CD-ROM

Software

- Aircrack 0.9.1
- Altiris Endpoint Security Solution Evaluation Version
- ATA Security eXtension BIOS 2.11
- AVG Anti-Virus Free Edition 7.5
- Ethereal 0.9.9
- Kaspersky Internet Security 7.0
- Nessus Client 1.0.2
- Nessus Server 3.0.5
- Nmap 7.20
- Norton Internet Security 2007
- Offline NT Password & Registry Editor release 060213
- Ophcrack 2.4.1
- TrueCrypt 4.3
- WEPCrack 0.1.0
- WSUS 2.0

Nessus Reporte

- aktivierte Windows Firewall, SMB erlaubt, Updates installiert
- deaktivierte Windows Firewall

Listings

- arpspoof zur Vergiftung des ARP-Caches
- dnsspoof für das Weiterleiten der DNS-Responses
- dnsspoof.hosts für falsche DNS-Replies
- Listing für einen Portscan, auf ein mit Kaspersky Internet Security 7.0 geschütztes System
- Listing für einen Portscan ohne HIPS
- Log Eintrag eines erkannten Angriffs durch einen Portscan
- Snifferdaten bei automatischem Windows Update
- Snifferdaten bei nicht mehr erkanntem Portscan von den meisten HIPS
- webmitm für Debuginformstionen bei einem MITM-Angriff