Diplomarbeit

Security-Framework für mobile Laptop Arbeitsplätze

Ausgeführt zum Zweck der Erlangung des akademischen Grades eines

Dipl.-Ing.(FH) für Telekommunikation und Medien

Am Fachhochschul-Diplomstudiengang Telekommunikation und Medien St.Pölten

unter der Erstbetreuung von

Bakk.rer.soc.oec. Bernhard Fischer

Zweitbegutachtung von

Sven Willner

ausgeführt von

Roland Deinhofer

0210038022

St.Pölten, am 15.August 2006 Unterschrift:

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.

...…… …….

Ort, Datum Unterschrift

Kurzfassung

In den letzten Jahren sind immer mehr Computer-Benutzer zu einem Laptop übergewechselt, sowohl für den privaten Gebrauch, wie auch im Geschäftsleben. Somit sind sie den ständig wechselnden Anforderungen der Wirtschaft besser gewachsen. Allerdings wird durch diesen Umstieg auch ein neuer Zweig der IT-Sicherheit geschaffen. Durch den Umstieg zu mobilen Geräten erhöht sich auch das Risiko von Geräteverlusten und auch Datenverlusten, wenn zum Beispiel ein Notebook verloren geht oder gestohlen wird.

Deswegen wird in dieser Diplomarbeit die Absicherung von mobilen Geräten betrachtet. Dazu gehört zuerst der Schutz des Notebooks selbst, d. h. der physische Schutz vor Diebstahl und auch Verlust.

Danach werden Themen behandelt, die ebenfalls für die Sicherheit relevant sind, aber meist nicht von einer IT-Abteilung vorgegeben werden, sondern einer höheren organisatorischen Schicht.

Auch das am häufigsten eingesetzte Betriebssystem auf Laptops, Microsoft Windows, wird genauer betrachtet, und einige, für die Sicherheit relevante, Funktionen beschrieben und erklärt.

Zu guter Letzt werden noch Anwendungen erklärt, die auf jedem System zum Einsatz kommen sollten, und auch Anwendungen, die bei der täglichen Arbeit verwendet werden.

Dazu werden durch eine umfangreiche Inhaltsanalyse alle Aspekte der Notebook-Sicherheit betrachtet, und wenn nötig durch kleinere Experimente manche Produkte und Einstellungen getestet.

Abstract

In the last years, more computer users change their working device to a laptop, both for private use, as well as in the business life. Thus they were up to the constantly changing requirements of the economy. However, by this transfer also a new branch of IT security appears. By the transfer to theses mobile devices, also the risk of equipment losses and data losses increase, if for example a notebook is lost or stolen.

Therefore this thesis is regarded to the security of mobile devices. In addition the protection of the notebook itself belongs, i.e. the physical protection from theft and also loss.

Afterwards topics are treated, which are also relevant for security, but not usually given by an IT department, but a higher organizational layer.

Also the most common operating system on laptops, Microsoft Windows, is regarded more exactly, and some security relevant functions are described and explained.

As good the latter still applications are explained, which should be used on every system, and also applications are explained, which are used with the daily work.

In addition by an extensive content analysis all aspects of notebook security are regarded, and some products and attitudes are tested by smaller experiments if necessary.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Heutzutage erfordern Geschäftsprozesse immer mehr Flexibilität und Mobilität. Um diesen Anforderungen gerecht werden zu können, wird von überall Zugriff auf wichtige Daten benötigt. Deswegen sind in den letzten Jahren immer mehr Benutzer weg vom festen Arbeitsplatz mit PC hin zum mobilen Laptop gewechselt, und dieser Wechsel ist noch immer in Gange und wird auch noch einige Zeit andauern.

Diese Mobilität bietet aber nicht nur Vorteile. Die Laptops sind auch ein sehr beliebtes Ziel von Angreifern, wobei meistens nicht das Gerät selbst interessant ist, sondern vor allem die darauf gespeicherten Daten. Sehr viele Notebooks werden deshalb unterwegs gestohlen, weil sie um einiges handlicher und auch leichter zugänglich sind als die PCs in einem Bürogebäude. Es besteht aber nicht nur die Gefahr des Diebstahls, sondern auch eine erhöhte Gefahr an Hackerangriffen und Vireninfektionen. Der Grund dafür liegt darin, dass Notebooks oft auch zum privaten Gebrauch verwendet werden, und da sind sie meistens nicht so geschützt, wie in einem Firmennetzwerk hinter einer sicher konfigurierten Firewall. Wenn sich ein Mitarbeiter wieder ins Firmennetz einloggt, können diese infizierten Geräte dann ihre Viren ins Netzwerk einschleusen und andere Geräte infizieren, oder wenn ein Hacker die Kontrolle über ein Gerät übernommen hat, könnte er wichtige Geschäftsdaten auslesen.

Dabei stellt sich die Frage, ob man diese mobilen Datenträger schützen kann. Dazu werden zuerst einige grundlegende Begriffe der IT-Sicherheit erklärt, unter anderem welche Risiken für ein System bestehen, und mit welchen Methoden viele Angreifer arbeiten.

Im nächsten Kapitel wird der physische Schutz von Notebooks betrachtet. Dazu werden einige Methoden gezeigt, wie ein Notebook vor Diebstahl geschützt werden kann. Zusätzlich werden Methoden zur Authentifizierung gezeigt, bei denen die Physis eine große Rolle spielt. Dazu gehören biometrische Authentifizierungsmethoden, wie auch die Authentifizierung mit Hilfe einer Smartcard.

Im vierten Kapitel wird beschrieben, was alles von organisatorischer Seite berücksichtigt werden muss, um ein Unternehmen abzusichern. Dabei sind vor allem die Endgeräte im Unternehmen gemeint. Die wichtigsten Punkte dabei sind die Einhaltung der Sicherheitspolitik und Kennwortrichtlinien. Auch die Vergabe von Benutzerrechten spielt hier eine große Rolle. Weitere wichtige Punkte sind das Patchmanagement und der Einsatz von WLAN (Wireless Local Area Network) in einem Unternehmen. Zu guter Letzt wird auch noch die Absicherung des TCP/IP-Stacks bei Windows gezeigt, da somit viele Angriffsarten eingeschränkt werden können.

Das nächste größere Kapitel beinhaltet einige sicherheitsbezogene Funktionen des Windows Betriebssystem. Dazu erfolgt eine Erklärung des Sicherheitskonzeptes allgemein, und danach werden wichtige Einstellmöglichkeiten bei den Gruppenrichtlinien beschrieben. Als nächster wichtiger Punkt werden die Dienste angeführt, die standardmäßig bei Windows laufen. Allerdings sollten je nach System, nicht benötigte Dienste deaktiviert werden. Danach wird das verschlüsselnde Dateisystem von Windows erklärt und beschrieben, mit dem man wichtige Daten verschlüsseln kann. Weitere Punkte in diesem Kapitel sind die Software Restriktion und der Einsatz von Offlinedateien.

Im sechsten Kapitel werden einige Anwendungen beschrieben, und wie sie sicher konfiguriert werden können. Unter anderem werden dabei Anwendungen betrachtet, die auf jedem Notebook laufen sollten (Antivirus, Personal Firewall), aber auch Anwendungen, die bei der täglichen Arbeit verwendet werden (Webbrowser). Noch dazu werden Alternativen zum verschlüsselnden Dateisystem von Windows gezeigt. Zu guter Letzt werden auch noch Programme erklärt, mit denen man Geräte und Schnittstellen verwalten kann.

Im letzten Kapitel finden sie eine Zusammenfassung der Arbeit, und welche weiterführenden Arbeiten noch interessant wären.

2 Grundlagen

Alle Beziehungen auf das Betriebssystem Windows in der gesamten Diplomarbeit gelten nur für die Versionen ab Windows 2000, das heißt die relevanten Versionen sind Windows 2000 (Server und Professional am Client), Windows 2003 Server und Windows XP Professional. Der Grund dafür ist jener, dass Windows erst ab der Version 2000 ein sicheres Multiuser-Betriebssystem ist, und heutzutage sind eigentlich nur mehr Versionen ab 2000 im Einsatz. Sowohl am Server, als auch am Client.

2.1 Security-Framework

Der Begriff Sicherheit ist ein nicht klar definierbarer Begriff, da dieser zu allgemein ist und erst für den zu untersuchenden Bereich eingeschränkt werden muss. Da diese Arbeit über die Sicherheit von Laptops handelt, beschränke ich mich auf die Sicherheit in der Informationstechnologie, welche oft auch Informationssicherheit genannt wird.

Die Verwaltung der Sicherheit in der Informationstechnologie umfasst eine Kombination aus technischen, geschäftlichen und kommunikativen Fähigkeiten. Eine sehr große Rolle dabei spielt die richtige Einschätzung der Risiken, denn erst wenn ein Unternehmen, oder auch eine Privatperson, weiß, welchen Gefährdungen es ausgesetzt ist, kann es sich dagegen schützen. Daraus ist auch klar ersichtlich, dass die Einschätzung dieser Risiken immer subjektiv ist, da sich ein Unternehmen mit anderen Möglichkeiten befassen muss als eine Privatperson.

Die am weitest verbreiteten Elemente der Informationssicherheit sind dabei die Begriffe Vertraulichkeit, Integrität und Verfügbarkeit. Durch die Übersetzung in die englische Sprache kommt man zu der häufig verwendeten Abkürzung CIA (Confidentiality, Integrity, Availability).

Die Informationssicherheit gehört in den meisten Unternehmen zu den Aufgaben der IT-Abteilung, welche aber immer in Zusammenarbeit mit der Geschäftsleitung oder in größeren Firmen mit dem Sicherheitsbeauftragten zusammenarbeiten sollte.

Diese Abteilung erledigt meistens nur die technische Umsetzung, und nicht die Organisation die dahinter stehen sollte. Meistens stehen Konzepte (Security Policies) dahinter, welche vom Management abgesegnet werden und wofür das Management auch zur Verantwortung gezogen werden kann.

In der Informationstechnologie wird man zwar nie ohne Risiko arbeiten können, weil es keine hundertprozentige Absicherung gibt, da die Angreifer immer einen Schritt voraus sein werden. Allerdings sollten alle Möglichkeiten ausgeschöpft werden, um das Risiko so gering wie möglich zu halten. Deswegen wird in dieser Diplomarbeit dieses Thema der Sicherheit in einem Schalenmodell betrachtet, welches in Abbildung 1 zu sehen ist.

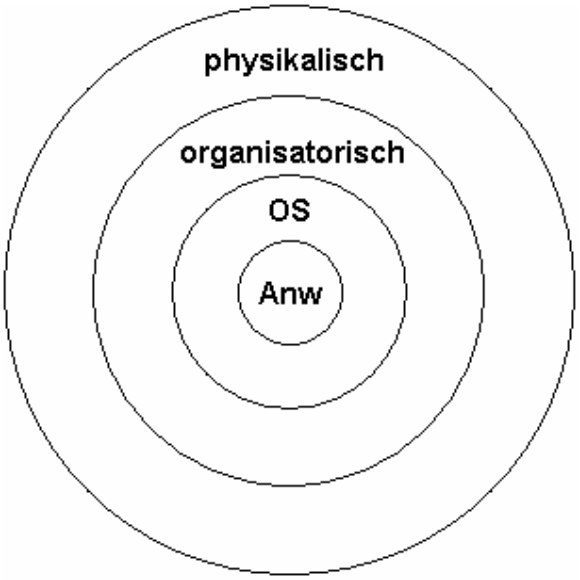

Abbildung 1: Schalenmodell für Security-Framework

In der Abbildung 1 steht OS für operating system, also für das Betriebssystem. In dieser Schicht werden die Sicherheitsaspekte des Betriebssystem Windows betrachtet. Anw. Ist die Abkürzung für Anwendungen, da in dieser Schicht verschiedenste Anwendungen betrachtet werden, und wie sie sicher konfiguriert werden können.

Dabei werden bei allen Schichten Möglichkeiten betrachtet und erklärt, damit in jeder Schicht das Risiko auf ein Minimum reduziert werden kann. Somit bekommt man ein Gesamtpaket, bei welchem das Restrisiko gering ist.

Natürlich muss immer unterschieden werden, wie wichtig die Informationssicherheit im Unternehmen oder privat ist, und wie viel Zeit und Geld man dafür investieren will.

„Ein System wird dann als sicher bezeichnet, wenn der Aufwand für das Eindringen in das System höher ist als der daraus resultierende Nutzen für den Angreifer." (Wikipedia 2006)

2.2 Risikoeinschätzung

Damit Privatpersonen oder Unternehmen ihr System richtig absichern können, müssen sie zuerst das eigene System hundertprozentig kennen und auch wirklich nur Programme und Dienste laufen lassen, die benötigt werden. Somit kann die Angriffsfläche stark reduziert werden, und der Aufwand zur Absicherung des Systems wird auch geringer. In Unternehmen ist auch die Dokumentation für die Nachwelt ein sehr wichtiger Bestandteil. Somit muss nicht jeder neue Mitarbeiter oder Administrator sich alles selbst erarbeiten, sondern es kann auf früheres Wissen zugegriffen werden.

Als nächster Schritt ist es erforderlich, seine Gegner und vor allem deren Möglichkeiten zu kennen. Dazu werden im nächsten Abschnitt häufig eingesetzte Varianten vorgestellt. Danach muss jeder einzelne, ob Privatperson oder Unternehmen, entscheiden, wie relevant die Angriffsmöglichkeiten für das eigene System sind. Noch dazu muss jeder abschätzen wie wichtig die eigenen Daten sind, und wie viel Aufwand betrieben wird um sie zu schützen. Im privaten Bereich ist der Aufwand vergleichsweise gering und das Risiko kann mit ein paar Programmen und Konfigurationen noch verringert werden.

Diesen Ansatz kann man mit einer Strategie von einem früheren chinesischen Kriegsherrn namens Sun Tzu vergleichen. Diese Strategie wurde wie folgt beschrieben:

„Wenn du deinen Gegner und dich selbst kennst, brauchst du das Ergebnis selbst von hundert Schlachten nicht zu fürchten. Wenn du dich selbst, aber nicht den Gegner kennst, wirst du für jeden errungenen Sieg eine Niederlage erleiden. Wenn du weder den Gegner noch dich selbst kennst, wirst du in jeder Schlacht unterliegen." (Schwanfelder 2004, S.73)

2.3 Die Angreifer und deren Möglichkeiten

Zuerst muss eine Einteilung möglicher Angreifer vorgenommen werden. Der Einfachheit halber beschränke ich mich auf externe und interne Angreifer. Umfragen zeigen, dass die Mehrheit aller Angriffe auf ein Netzwerk von intern kommen (siehe AT&T 2004, Seite 8). Diese sind auch um einiges gefährlicher als die Angriffe von außen, weil die Angreifer physischen Zugriff auf Netzwerkressourcen haben und nicht mehr so viele Barrieren zu überwinden haben. Zum Beispiel müssen sie nicht mehr an einer sicher konfigurierten Firewall vorbei. Deswegen sollte ein Administrator nicht zu gutgläubig sein und glauben, dass seine Mitarbeiter niemals die eigene Firma attackieren würden.

Allerdings werden nicht alle internen Angriffe absichtlich vorgenommen. Es kann auch passieren, dass nichts ahnende Benutzer irgendwelche E-Mail Anhänge öffnen und somit die Kontrolle über ihre Geräte verlieren. Dies passiert aber nur dann, wenn die Benutzer von vorn herein zu viele Rechte erhalten haben. Das kann daran liegen, dass eine Firmenpolicy besagt, das manche Benutzer, zum Beispiel Vorstandsmitglieder, Abteilungschefs, usw., wesentlich mehr Rechte besitzen sollen, als sie zur eigentlichen Arbeit benötigen. Aufgrund solcher Firmenvorgaben ist es für einen Administrator sehr schwer, allen Benutzern eingeschränkte Benutzerrechte auszustellen.

Eine weitere Einteilung kann auch noch nach Wissensstand der Angreifer vorgenommen werden. Dabei können unerfahrene Angreifer, von denen es zwar sehr viele gibt, relativ einfach abgehalten werden, wenn grundlegende Regeln der Sicherheit eingehalten werden. Erfahrene Angreifer sind sehr schwer abzuhalten, aber man kann ihnen den Angriff so schwer wie möglich machen, damit sich der Aufwand für sie nicht lohnt und sie somit den Angriff abbrechen. Eines haben die meisten Angreifer gemeinsam. Zum einen verfügen sie über sehr gute Programmierkenntnisse, kennen sich mit Betriebssystemen und wichtigen Anwendungen, und vor allem deren Schwachstellen, aus und kennen sich auch in der Netzwerktechnik sehr gut aus.

Ein weiterer wichtiger Punkt ist die Motivation der Angreifer zu kennen und einzuschätzen. Die unerfahrenen Hacker sehen die Attacken meist als Spiel oder auch um vor Freunden damit zu protzen.

Angreifer, die schon mehr Erfahrung gesammelt haben, üben weitere Angriffe oft nur aus, um sich selbst etwas zu beweisen und noch dazu den Bekanntheitsgrad zu erhöhen. Aber auch unzufriedene oder frühere Mitarbeiter können Angriffe aus Rache ausführen, wenn sich das Unternehmen im Streit mit ihnen getrennt hat.

Es gibt sehr viele verschiedene Angriffsmöglichkeiten, auf die ich hier aber nicht genauer eingehen werde. Stattdessen werde ich folgende Angriffsklassen beschreiben, in die sich laut Russell alle bekannten Angriffsvarianten einteilen lassen (Russell 2002).

2.3.1 Denial of Service

DoS (Denial of Service), zu Deutsch Dienstverweigerung, sind Angriffe gegen einen oder mehrere Dienste. Durch Überlastung dieser Dienste kann zum Beispiel ein Server seinen eigentlichen Clients nicht mehr oder nur verzögert antworten, und diese können möglicherweise nicht mehr arbeiten. Wenn der Angriff nicht von einem Rechner alleine vorgenommen wird, sondern durch eine große Anzahl von Systemen spricht man auch von verteilter Dienstverweigerung oder DDos (Distributed Denial of Service). Mit einem DoS-Angriff kann man zwar nicht in ein System eindringen, aber man kann es lahm legen. Allerdings werden diese Attacken gern als Ablenkung eingesetzt, um den eigentlichen Einbruch in ein System unbemerkbar durchführen zu können. Sehr viele E-Mail Würmer arbeiten auf diese Weise, so auch der bekannte Wurm *W32.Blaster*, der im Jahre 2003 die Update-Site von Microsoft hätte unerreichbar machen sollen (Wikipedia 2003).

2.3.2 Information Leakage

Diese Art des Angriffs wird dazu verwendet, um möglichst viele Informationen über das Zielnetzwerk oder System zu erfahren. Dazu gehören Informationen über Betriebssysteme, Anwendungen und Netzwerkdesign. Dazu genügt es oft missgeglückte Loginversuche genauer zu betrachten. Dabei wird oft das Betriebssystem plus Version und auch die Art des Servers (Webserver, FTP-Server, usw.) verraten. Schuld daran sind oft schlecht, weil nicht sicher genug, gestaltete Protokolle, wie zum Beispiel SNMP (Simple Network Management Protocol). Genauere Informationen zum SNMP-Protokoll zu finden im RFC1173. Die neuere Version SNMPv3 ist im RFC3410 beschrieben.

2.3.3 Zugriff auf normale Dateien

Hierbei handelt es sich um den normalen Arbeitsalltag mit gewöhnlichen Dateien. Um zu verhindern, dass Angreifer Dateien einsehen können, spielt hier die Rechtevergabe eine große Rolle. Es sollten nicht alle Benutzer auf fast alle Daten Zugriff haben, sondern nur diejenigen, die das auch wirklich brauchen. Zum Beispiel sollten alle Mitarbeiter in einer Abteilung einen gemeinsamen Ordner für gemeinsame Dateien haben, aber zusätzlich auch eigene Ordner, um Dateien zu speichern, auf die nur sie selbst Zugriff haben sollen. Das erhöht zwar den Verwaltungsaufwand, aber falls ein Angreifer ein Benutzerkonto knacken kann, kann er somit nicht auf alle Daten zugreifen.

2.3.4 Falschinformation

Dies wird dazu verwendet, um nach einem erfolgreichen Angriff seine Spuren zu verwischen. Dazu gibt es mehrere Möglichkeiten. Zum Beispiel können Logfiles manipuliert werden, um alle Einträge, die vom Angreifer verursacht wurden entweder zu löschen oder zu verstecken. Eine weitere Möglichkeit liegt darin, so genannte Rootkits ins System einzuschleusen. Dabei sind Rootkits fertige Programme, die mit anderen wichtigen Programmen, Treibern oder Einträgen in der Registry ausgetauscht werden, um langzeitigen, unentdeckten Zugang zum System zu haben.

2.3.5 Zugriff auf spezielle Dateien

In diese Klasse fällt die Handhabung von speziellen Dateien, wie unter Windows das *RunAs-Programm (Ausführen als)*. Mit Hilfe dieses Programms kann ein Administrator zum Beispiel Programme installieren, ohne sich mit einem Administratorkonto einzuloggen. Somit muss sich der Benutzer nicht extra ausloggen, wenn ein neues Programm installiert wird oder eine andere administrative Aufgabe ausgeführt wird. Dadurch wird der Zeitaufwand deutlich verringert und die gesamte Prozedur ist auch benutzerfreundlicher. Angreifer versuchen durch Manipulation dieses speziellen Programms zu den Logindaten eines Administratorkontos zu kommen, welche bei der Ausführung des Programms eingegeben werden müssen.

2.3.6 Remote Arbitrary Code Execution

Eine der beliebtesten Angriffsvarianten ist die Ausführung eines beliebigen Codes auf einem fremden System. Da dazu meist keine Authentifizierung erforderlich ist, zumindest auf schlecht abgesicherten Homepages, von denen es genügend gibt, fallen sehr viele Angriffe in diese Klasse. Dazu gibt es einige vorbereitete Tools im Internet, die diesen Angriff automatisch durchführen, und somit müssen die Angreifer selbst nicht mehr allzu erfahren sein, denn das automatische Skript erledigt den Großteil.

2.3.7 Elevation of Privileges

So gut wie jeder Angriff ist auch zu dieser Klasse zu zählen. Genauer gesagt ist jeder Angriff, bei dem ein Hacker Zugriff auf Daten oder Ressourcen erhält, für welche er aber nicht autorisiert ist. Wörtlich gesprochen werden die Rechte, die ein Angreifer beim Einbruch hat versucht zu erhöhen, d.h. ein Angreifer versucht seine Rechte als Gast oder ähnlichem zu erweitern. Entweder möchte er die gleichen Rechte wie ein normaler Benutzer, oder ein noch beliebteres Ziel sind natürlich Administratorrechte.

2.3.8 Zusammenfassung

Dies war eine kurze Beschreibung der verschiedenen Angriffsklassen. Natürlich werden viele Angriffe zu mehreren dieser Klassen gezählt, weil sie oft eine Mischung aus den beschriebenen Punkten sind. Jeder Administrator sollte einen Überblick haben, welche Methoden von Angreifern angewendet werden, denn so kann er sein Netzwerk effizienter schützen.

3 Physisch

In diesem Kapitel werden nicht nur Produkte und Erfindungen beschrieben, die das Notebook selbst physisch schützen, sondern zum Beispiel auch Authentifizierungs-möglichkeiten mit Fingerabdruck oder Produkte zum Aufspüren gestohlener Geräte, da überall die Physis eine große Rolle spielt.

3.1 Kabelschlösser

Eine sehr einfache und vergleichsweise günstige Möglichkeit den Laptop physisch vor Diebstahl zu schützen sind Kabelschlösser. Sie sind Fahrradschlössern sehr ähnlich und können ganz einfach an einen Anschluss am mobilen Datenträger (meist eigener Anschluss, auch Kensington Sicherheitsanschluss genannt) angebracht werden. Ein solch spezieller Kensington Sicherheitsanschluss ist in Abbildung 2 zu sehen.

Abbildung 2: Kensington Sicherheitsanschluss

Ein Nachteil dabei ist aber, dass bei den meisten Notebooks, trotz dieser Schlösser die Festplatten ausgebaut werden können, auf denen sich die wichtigen Daten befinden. Aber für den nicht so erfahrenen Dieb, sind diese Schlösser die richtige Abschreckung, und sollten als erste Verteidigungslinie eingesetzt werden.

Da die Verwendung von Kabelschlössern einen Einschnitt in der Mobilität bedeutet, werden sie eher ungern eingesetzt.

Deswegen muss man in Abstimmung mit den jeweiligen Mitarbeitern über den Einsatz der Schlösser entscheiden und man muss seinen Mitarbeitern auch erklären warum der Einsatz so wichtig ist und was passieren kann, wenn Laptops verloren gehen. Es macht keinen Sinn, für jeden Notebookuser ein Kabelschloss zu besorgen, wenn diese dann nie zum Einsatz kommen.

3.1.1 Varianten

Es gibt mehrere Varianten dieser Schlösser, die hier noch kurz beschrieben werden:

- Stahlkabel plus Schloss für Kensington Sicherheitsanschluss (das Schloss ist entweder mit einem Schlüssel oder einer Zahlenkombination zu öffnen)
- Stahlkabel plus zwei Schlösser für Kensington Sicherheitsanschluss (die Schlösser sind wie oben entweder mit Schlüssel oder mit Zahlenkombination zu öffnen; mit Hilfe des zweiten Schloss kann man zum Beispiel auch einen Beamer sichern)
- Stahlkabel plus Schloss, mit zusätzlichem Alarmauslöser bei Beschädigung des Stahlkabels oder bei Bewegung des Geräts
- Stahlkabel plus Schloss für Videoanschluss (das Schloss ist wie oben entweder mit Schlüssel oder mit Zahlenkombination zu öffnen)

3.2 Methoden zur Verfolgung von Laptops

Eine etwas neuere Erfindung sind Programme, die nach der Installation völlig unsichtbar, zumindest für normale Benutzer (sie sind nicht zu entdecken und ohne Passwort und Installationssoftware auch nicht zu entfernen), auf dem Notebook arbeiten. Sie werden unter anderem für die Nachverfolgung von gestohlenen Geräten verwendet. Dazu senden sie immer wenn sich der Rechner im Internet befindet ein Signal an das Kontrollcenter, mit allen wichtigen Daten um das Gerät aufzuspüren (IP-Adresse, usw.). Dabei werden verschiedenste Verbindungen unterstützt (Modem, DSL, Wireless, usw.). Somit weiß man immer Bescheid, wo sich alle mobilen Geräte befinden. Eine weitere Variante ist die Verfolgung über GPS (Global Positioning System). Falls ein Gerät gestohlen wird, kann man durch einen Eintrag im Kontrollcenter dies vermerken und eine Nachverfolgung einleiten.

Um diese Nachverfolgung muss man sich nicht selbst kümmern, sondern der Verkäufer dieses Produkts hat ein eigenes Team, welches mit zuständigen ISP´s (Internet Service Provider) und auch mit der Polizei zusammenarbeitet.

Zusätzlich können auch Daten auf dem gestohlenen Laptop gelöscht werden. Dazu kann bei dem Programm eingestellt werden, was passieren soll, wenn von vorn herein gesetzte Einstellungen ausgelöst werden. Auslöser können dabei zeitliche Verspätungen oder auch falsch eingegebene Passwörter sein.

3.3 Methoden zur Authentifikation

Die Standardmethode bei der Authentifikation ist mit Benutzername und Passwort. Da aber oft Passwörter in Verwendung sind, die keine große Sicherheit vor Angreifern bieten und damit eine Gefahr für ein System darstellen, werden immer häufiger andere Methoden gesucht, um die Authentifizierung sicherer zu machen. Einige wichtige Merkmale, um ein Passwort sicherer zu machen, werden im Kapitel 4.2 beschrieben.

3.3.1 Smartcard

Eine weitere Stufe der Sicherheit bietet die Authentifizierung mit einer Smartcard. Bei jeder Anmeldung am System werden die Smartcard und ein dazugehöriger Zahlencode, auch PIN (Personal Identification Number, persönliche Identifikationsnummer) genannt, benötigt. Dies wird auch zweistufige Authentifikation genannt, weil der Benutzer die Smartcard benötigt, plus den dazugehörigen Code wissen muss.

Wenn man Smartcards im Einsatz hat, kann man zusätzlich noch einen weiteren Vorteil nutzen. Bei einer Anmeldung an einem System müssen heutzutage sehr oft Benutzernamen plus dazugehörige Passwörter eingegeben werden. Zuerst die Anmeldung am Betriebssystem, dann noch E-Mail, usw. Mit der Smartcard, können diese Anmeldeinformationen auf der Smartcard gespeichert werden, und der Benutzer muss sich nur noch den PIN seiner Smartcard merken. Die restlichen Anmeldevorgänge passieren automatisch. Dieser Vorgang wird Single Sign-On verwendet, und wird immer beliebter und somit auch häufiger eingesetzt.

3.3.2 Biometrische Methoden

In manchen neueren Laptops sind bereits Fingerabdruckleser eingebaut, d.h. ohne den richtigen Fingerabdruck ist kein erfolgreiches Anmelden möglich. Es gibt aber auch Geräte, die nachträglich am Notebook angeschlossen werden können, um solche Authentifizierungsmöglichkeiten zu ermöglichen.

Eine weitere Steigerung dazu wären noch Authentifikation durch Irisscan oder Spracherkennung. Diese beiden Möglichkeiten sind aber eher noch in der Testphase und werden im Gegensatz zum Fingerabdruck noch nicht am Markt eingesetzt, da es noch zu viele Probleme und falsche Erkennungen gibt.

4 Organisation

In diesem Abschnitt wird beschrieben, was alles von organisatorischer Seite berücksichtigt werden sollte, um sein Unternehmen, und dadurch auch die Endgeräte, abzusichern. Die Organisation betrifft nicht nur einen Administrator, sondern auch einen Sicherheitsbeauftragten oder auch die Geschäftsleitung.

4.1 Sicherheitspolitik

Ein allgemein gültiges Rezept für den Aufbau und die Realisierung von Sicherheitsmaßnahmen im Unternehmen gibt es nicht. Doch es existieren Grundsätze, Methoden und Regeln zur planvollen und effektiven Umsetzung. Zudem gibt es auch noch Gesetze und Verordnungen von außen, welche die Geschäftsleitung und die Verantwortlichen zu den notwendigen Aktivitäten zwingen. Es sind so gut wie alle Unternehmen betroffen und das Topmanagement sollte hier eine initiierende und kontrollierende Funktion übernehmen. Deswegen sollte es in jedem Unternehmen eine umfassende Sicherheitspolitik geben. Diese hat letztlich zum Ziel, dass die Schutzmaßnahmen auch die gewünschten Auswirkungen in der Praxis haben. Deswegen sollte es in größeren Unternehmen einen eigenen Sicherheitsbeauftragten geben.

An diese Sicherheitspolitik hat sich dann jeder einzelne Mitarbeiter zu halten, und das nicht nur im EDV-technischen Sinn. Die Einhaltung dieser Regeln muss von den Verantwortlichen auch überprüft werden. Man sollte seinen Mitarbeitern vermitteln, dass die Sicherheit ein sehr wichtiger Punkt ist, und deswegen sollten alle mit ein paar Einschränkungen arbeiten können, wenn dafür als Gegenleistung die Downtime auf ein Minimum reduziert wird. Dabei können unter anderem Schulungen helfen, bei denen den Benutzern gezeigt wird, welche Bedrohungen es gibt, und wie einfach manche abgewendet werden können.

Durch die ständige Weiterentwicklung der IT-Branche, und die dadurch entstehenden neuen Bedrohungen, sollte die Sicherheitspolitik laufend angepasst werden, um auf aktuelle Gefährdungen sofort reagieren zu können.

4.2 Kennwortrichtlinie

Heutzutage werden als erster Schritt der Sicherheit fast überall Passwörter eingesetzt. Diese sind aber auch schon das erste Problem. Benutzer wollen gerne einfache, leicht zu merkende Passwörter. Da diese aber für Angreifer sehr leicht zu knacken sind, werden von Administratoren Passwortrichtlinien eingeführt, die solch einfache Passwörter nicht mehr zulassen. Eine Passwortrichtlinie besteht aus mehreren Einstellmöglichkeiten, welche die Komplexität von Passwörtern beschreiben. Durch solche Richtlinien sind Benutzer gezwungen, sich etwas komplexere Passwörter zu suchen.

Allerdings findet man immer noch viele Benutzer, die sich ihre etwas komplexeren Passwörter auf Post-its aufschreiben und auf den Bildschirm oder die Tastatur kleben. Deswegen muss man seinen Mitarbeitern vermitteln, was passieren kann, wenn ihre Passwörter den falschen Leuten in die Hände fallen, und wenn sie ihre Kennwörter schon aufschreiben müssen, dann sollten sie wenigstens die Post-its gut verstecken.

Laut Microsoft sind unter anderen folgende Kriterien relevant, damit ein Passwort so sicher wie möglich ist. Diese Kriterien sind allgemein gültig, und gelten nicht nur für das Windows Betriebssystem (Microsoft 2006):

- Passwörter oft wechseln
- Passwörter sollten mindestens acht Zeichen enthalten (für normale Benutzer ausreichend, Administratoren sollten noch längere Passwörter verwenden)
- Passwörter sollten alle 4 Zeichenarten enthalten (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen)
- Es sollten keine Wörter aus einem Wörterbuch als Passwort verwendet werden (aber es sollte auch nicht einfach eine Zahl oder ein Sonderzeichen an ein bekanntes Wort angehängt werden)

- Das Passwort muss kein einzelnes Wort sein, sondern es können auch Sätze verwendet werden (dies erhöht die Sicherheit ungemein, und Sätze sind auch leicht zu merken)
- Es sollten keine Geburtsdaten oder Benutzernamen als Passwort verwendet werden
- Das Passwort soll niemals aufgeschrieben werden (sonst gut verstecken)
- Passwörter niemals an andere Personen weitergeben

Den Grund dafür sieht man besser, wenn die Angriffsvarianten der Passwortknacker betrachtet werden. Dabei sind zwei Arten besonders beliebt und kommen immer wieder zum Einsatz.

Zum einen die Wörterbuchattacke, bei dem ein Programm einzelne Wörter aus einem Wörterbuch ausliest, und solange versucht, bis das Passwort geknackt ist, oder das Wörterbuch ohne Erfolg durchlaufen wurde. Im Internet findet man dazu genügend Wörterbücher mit beliebten Passwörtern. Mit einem sehr guten Wörterbuch sind einfache Passwörter leicht und schnell zu knacken.

Zum anderen gibt es noch die Brute-Force-Attacke, bei dem alle möglichen Varianten und Kombinationen aus Zahlen, Sonderzeichen, Klein- und Großbuchstaben ausprobiert werden. Da diese Variante sehr viel Rechenzeit erfordert, ist man gegen längere Passwörter mit dieser Variante chancenlos.

Beim Betriebssystem Windows ist die Passwortrichtlinie ein Teil der Gruppenrichtlinien. Die genauen Einstellmöglichkeiten und auch andere Teile der Gruppenrichtlinien werden im Kapitel „Betriebssystem“ genauer erklärt.

4.3 Benutzerrechte

Eine immer wichtigere Frage ist die Zuteilung der Rechte an die Benutzer. Aus älteren Versionen des Windows Betriebssystem sind es die Benutzer gewohnt, das sie beliebige Programme installieren und ausführen können. Da dies heutzutage, insbesondere beim Surfen im Internet und beim Öffnen von E-Mail-Anhängen, eine große Gefahr darstellt, sollten so gut wie alle Benutzer eingeschränkte Benutzerkonten haben, damit sie keine Programme installieren dürfen.

Somit können viele Viren und Trojaner unschädlich gemacht werden. Im Großen und Ganzen bedeutet dies zwar mehr Arbeit für die IT-Abteilung und Administratoren, aber erhöht die Sicherheit erheblich.

Da man mit dem Administratorkonto alle Sicherheitsmechanismen umgehen kann, ist dieses besonders zu schützen. Dies beginnt schon bei der Einstellung von neuen Mitarbeitern in der IT-Abteilung. Die meisten Mitarbeiter in dieser Abteilung bekommen früher oder später die Rechte eines Administrators, was in einem Unternehmen bedeutet, dass diese Person vollen Zugriff auf alle Server und Clients hat. Deswegen sollten diese neuen Mitarbeiter genauestens geprüft werden, bevor man ihnen diese Rechte erteilt. Zum einen müssen sie die fachliche Qualifikation mitbringen, da ein Administrator sehr viel Verantwortung trägt, und zum anderen muss man sicher sein, das sie das System nicht absichtlich gefährden wollen.

Bei der Vergabe der Rechte darf aber nicht nur auf die Benutzerkonten und deren Rechte selbst geachtet werden, sondern es muss auch die Zugehörigkeit der Benutzerkonten zu gewissen Gruppenkonten genauestens überprüft werden, um durch eine mögliche falsche Gruppenzugehörigkeit dem Benutzer nicht zu viel Rechte zu gewähren.

4.3.1 Wichtige Hinweise

Folgende Tipps sind hilfreich, um alle Aspekte der Rechtevergabe zu beachten:

- Es sollten so wenig Benutzer wie möglich die Rechte eines Administrators bekommen (nur Mitarbeiter der IT-Abteilung und für andere Benutzer nur, wenn es einen wichtigen Grund dafür gibt), auch nicht die eines lokalen Administrators
- Routineaufgaben sollten nicht mit einem Administratorkonto erledigt werden (wird in vielen Betrieben nicht so ernst genommen; eine Abhilfe dafür wird das neue Betriebssystem von Windows namens Vista schaffen, bei dem ein Administrator je nach Aufgabe, automatisch mit den richtigen Rechten arbeitet; man wird aber erst sehen, ob das auch wirklich so funktioniert wie es beschrieben wird), stattdessen sollte der Befehl *RunAs* häufiger eingesetzt werden
- Die Rechte sollten nicht dem Benutzerkonto direkt gewährt werden, sondern nur Benutzergruppen. Dadurch bleibt die Verwaltung übersichtlicher, wenn Benutzerkonten nicht in zu vielen Gruppen Mitglieder sind
- Gastkonto umbenennen und deaktivieren
- Administratorkonto umbenennen und eventuell deaktivieren
- Eventuell ein Konto mit dem Namen Administrator erstellen, aber mit keinen Rechten ausstatten (viele Angreifer wollen das Administratorkonto knacken; somit kann ihnen eine kleine Falle gestellt werden)
- Bei Windows sollte man normalen Benutzern auch keine Rechte als *Hauptbenutzer* gewähren, weil erfahrene Angreifer über solche Konten sehr leicht an höhere Rechte eines *Administrators* oder des *Systems* kommen können

4.4 Patchmanagement

Die Verwaltung der laufenden Softwareaktualisierungen ist ein zeitaufwendiger Prozess, dem aber unbedingt große Aufmerksamkeit geschenkt werden muss. Denn eine Software, egal ob Betriebssystem oder Anwendung, die nicht auf dem neuesten Stand ist, ist ein sehr großes Sicherheitsrisiko. Je länger eine Software ohne Updates in Verwendung ist, desto größer ist die Wahrscheinlichkeit von erfolgreichen Angriffen. Bekannte Sicherheitslücken in Programmen verbreiten sich heutzutage sehr schnell übers Internet, und diese werden dann von Angreifern als Schwachstelle im System ausgenutzt.

Aufgrund verstärkter Aktivitäten von Viren, Würmern und Hackern hat das Patchmanagement eine zentrale Rolle in der Sicherheitsverwaltung eingenommen. Die laufende Aktualisierung des Betriebssystem aber auch der einzelnen Programme, insbesondere des Virenscanner, ist einer der wichtigsten Punkte um die Sicherheit seines Notebooks zu erhöhen. Dazu gibt es bereits bei fast allen Programmen eine automatischen Update Service, welches man unbedingt nutzen sollte.

Dabei sollte der ganze Updatevorgang möglich benutzertransparent stattfinden. Hin und wieder ist zwar ein Neustart nach einem Update erforderlich, aber die halten sich in Grenzen und somit werden die Benutzer nicht eingeschränkt oder gestört.

Für ein erfolgreiches Patchmanagement sind verschiedene Phasen verantwortlich. Als erstes erfolgt die Beurteilung der Hardware und Software (jeweils mit Versionsnummern), einschließlich der Beurteilung der vorhandenen Sicherheitsrisiken und Sicherheitslücken. Dazu muss sich ein Administrator über alle möglichen neuen Sicherheitslücken auf den neuesten Stand halten, damit er weiß, ob seine Software einer Gefährdung ausgesetzt ist oder nicht. Auch ein Administrator muss beurteilen, von welcher Quelle er rasche und qualitativ hochwertige Informationen über neue Sicherheitslücken bekommt.

Zur nächsten Phase gehört die Bestimmung, woher ich neue Softwareupdates bekomme, wie ich auf neue Updates hingewiesen werde (Benachrichtigungen per E-Mail, usw.), ob diese für mein System relevant sind und wie wichtig diese Updates sind.

In der nächsten Phase muss geprüft und geplant werden, ob Updates eingespielt werden. Wenn man sich dazu entschließt ein Update einzuspielen, sollte dies vorher in einer Testumgebung ausprobiert werden (wird etwas vernachlässigt). Nach einem erfolgreichen Test wird die Einspielung des Updates geplant und vorbereitet. Dabei ist wichtig wie und wann Patches eingespielt werden, sodass der normale Produktionsbetrieb nicht oder wenig eingeschränkt ist.

Die letzte Phase ist dann die eigentliche Bereitstellung des Updates. Dazu gehört die erfolgreiche Einspielung eines Updates, mit anschließender Beobachtung des Systems. Denn trotz eines erfolgreichen Tests, muss das System nach der Einspielung genau beobachtet werden, ob nicht doch Einschränkungen oder Änderungen des Systemverhaltens festgestellt werden.

Das große Problem beim Patchmanagement ist jener, das die Angreifer dem Verteidiger immer einen Schritt voraus sind. Es liegt immer eine längere oder kürzere Zeitspanne zwischen der Entdeckung einer Sicherheitslücke und einem dafür entwickelten Patch. Dies kann oft länger dauern, weil vorher getestet werden muss, ob ein Patch, der möglicherweise eine Sicherheitslücke schließt, nicht irgendwelche Nebenwirkungen (andere Sicherheitslücken werden geöffnet, oder manche Systeme funktionieren nicht mehr einwandfrei) hat.

4.5 WLAN

WLAN wird derzeit in Unternehmen noch nicht so häufig eingesetzt, weil es zu Beginn noch zu unsicher war, und viele Administratoren sich zuwenig damit beschäftigen. Die Unsicherheit liegt daran, dass die implementierte WEP (Wired Equivalent Privacy) Verschlüsselung relativ einfach zu knacken ist, oder von den meisten erst gar nicht angewendet wurde. In älteren Versionen wird ein 64bit Schlüssel verwendet, in den neueren schon ein 128bit Schlüssel, aber auch diese sind zu knacken.

Häufig wird auch einfach der Standard Schlüssel des Herstellers verwendet, dieser ist natürlich auch kein wirklicher Schutz vor Eindringlingen, und sollte deshalb öfters geändert werden.

Man sollte auch die Standard SSID (Service Set Identifier) und das Standard Passwort ändern, denn diese Einstellungen werden von möglichen Angreifern zuerst ausprobiert.

Ein weiterer Schritt, um sein drahtloses Netzwerk abzusichern liegt darin, die SSID nicht auszusenden (broadcast unterdrücken), denn so wird man erst für Angreifer sichtbar.

Man sollte auch den Zugang zum Netzwerk nur für die erforderlichen MAC-Adressen (Media Access Control) erlauben, und nicht alle Adressen zulassen.

Abhilfe gegen die Schwächen der WEP Verschlüsselung bietet der Nachfolger WPA (WiFire Protected Access) und mittlerweile auch WPA2. Diese Verschlüsselungsmethode wird aber von älteren Geräten nicht unterstützt. Diese können aber mit einem Softwareupdate auf den neuesten Stand der Technik gebracht werden.

Um die Sicherheit noch weiter zu erhöhen, werden gerne noch weitere EAP-Authentifizierungsmethoden (Extensible Authentication Protocol) eingesetzt. EAP ist nicht die Authentifizierungsmethode selbst, sondern nur ein Transportprotokoll für diese. Dadurch wird die Authentisierung vom Access Point zum Authentication Server verlagert, und dies bringt eine Kostenreduzierung des Access Point mit sich.

Mehr Informationen zu WLAN finden sie im Standard IEEE 802.11.

4.6 TCP/IP-Sicherheit

Da beim Entwurf von den Protokollen TCP (Transmission Control Protocol) und IP (Internet Protocol) nicht sehr viel Wert auf Sicherheit gelegt wurde, stehen standardmäßig nicht sehr viele Sicherheitskomponenten zur Verfügung. Deswegen bietet Microsoft einige Verbesserungen, um die Sicherheit von TCP/IP zu erhöhen. Dazu gehören unter anderem die Absicherung des TCP/IP-Stapels und die Unterstützung des Protokolls IPSec (Internet Protocol Security).

Da Netzwerke ohne Kenntnisse des von TCP/IP nicht ordentlich abgesichert werden können, müssen Administratoren nicht nur über das Betriebssystem genauestens Bescheid wissen, sondern auch über die Netzwerktechnik, da TCP/IP das am häufigsten verwendete Protokoll bei der Netzwerkkommunikation ist. Die meisten Angriffe finden übers Netzwerk statt, da der physische Zugriff auf einen Rechner nicht so leicht zu schaffen ist. Deswegen ist die TCP/IP-Sicherheit von großer Bedeutung. Die bekanntesten Angriffe übers Netzwerk sind Portscans, Spoofing und DoS-Angriffe.

Bei Windows kann man in der Registrierung folgende Einstellungen tätigen (Tabelle 1), damit die Sicherheit des TCP/IP-Stapels erhöht wird.

Tabelle 1: TCP/IP-Sicherheit

Wert	**Daten**	**Beschreibung**
DisableIPSourceRouting	2	deaktiviert
EnableDeadGWDetect	0	deaktiviert
EnableICMPRedirect	0	deaktiviert
EnablePMTUDiscovery	0	deaktiviert
EnableSecurityFilters	0	deaktiviert
KeepAliveTime	300 000	Wert in Millisekunden
NoNameReleaseOnDemand	1	aktiviert
PerformRouterDiscovery	0	deaktiviert

SynAttackProtect	2	unterbricht offene und halboffene Verbindungen
TCPMaxConnectResponseRetransmission	2	Wiederholversuche von nicht beantworteten SYN/ACK-Nachrichten
TCPMaxHalfOpen	500	maximal zulässige halboffene Verbindungen
TCPMaxHalfOpenRetired	400	maximal zulässige halboffene Verbindungen nach erneuter Verbindungsanforderung
TCPMaxPortsExhausted	5	Verbindungen, die abgewiesen werden, bevor der Schutz aktiviert wird
TCPMaxDataRetransmissions	3	erneute Übertragungen eines nicht bestätigten Segments

Zu finden sind diese Einstellmöglichkeiten unter dem Pfad *HKEY_LOCAL_MACHINE* → *System* → *CurrentControlSet* → *Services* → *Tcpip* → *Parameters*. Falls es einige Werte noch nicht gibt, müssen sie hinzugefügt werden.

Zusätzlich gibt es noch die TCP/IP-Filterung, bei der man für jede einzelne Schnittstelle einstellen kann, welche Arten von eingehendem IP-Verkehr verarbeitet werden. Standardmäßig ist sie deaktiviert. Zu finden sind die Einstellmöglichkeiten auch in der Registrierung unter *HKEY_LOCAL_MACHINE* → *System* → *CurrentControlSet* → *Services* → *Tcpip* → *Parameters* → *Interfaces* → *Schnittstellen_GUID*, wobei die Schnittstellen_GUID eine Kombination aus Buchstaben und Zahlen ist. Die einzelnen Einstellmöglichkeiten sind in Tabelle 2 beschrieben.

Tabelle 2: TCP/IP-Filterung

Einstellung	**Typ**	**Beschreibung**
EnableSecurityFilters	DWORD	1 (aktiviert), 0 (deaktiviert)
UdpAllowedPorts	MULTI_SZ	0 (alle), Nullwert (keine), Auflistung der Ports
TCPAllowedPorts	MULTI_SZ	0 (alle), Nullwert (keine), Auflistung der Ports
RawIpAllowedProtocols	MULTI_SZ	0 (alle), Nullwert (keine), Auflistung der Protokolle

Genauere Informationen zur TCP/IP-Sicherheit sind im Buch „Microsoft Windows Sicherheit“ zu finden (Smith 2005).

4.7 Weitere Hinweise

In diesem Abschnitt werden noch einige hilfreiche Einstellungen erwähnt. Als erstes sind hier BIOS-Passwörter (Basic Input/Output System) zu erwähnen. Sie sind einfach zu konfigurieren und bieten Schutz vor nicht so erfahrenen Angreifern, aber auch gegen irrtümliche Änderungen von Benutzern. Damit kann schon das Hochfahren des Rechners verhindert werden, oder zumindest der Zugriff auf das BIOS. Wenn man dazu noch eine sinnvolle Bootreihenfolge (zuerst von Festplatte) angibt, und das booten von CD und Diskette sperrt, sind die meisten Angreifer schon ausgeschaltet. Man kann allerdings das BIOS, und somit auch das Passwort, hardwaremäßig zurücksetzen.

Der nächste Schritt ist der Einsatz des NTFS (New Technology File System) Dateisystems, da es erhebliche Vorteile gegenüber seinem Vorgänger FAT (File Allocation Table) vorzuweisen hat, vor allem was den Punkt Sicherheit angeht. Unter dem veralteten Dateisystem FAT können zwar auch mehrere Benutzer konfiguriert werden, allerdings nur um zum Beispiel unterschiedliche Desktops einrichten zu können. Eine vernünftige Rechteverwaltung ist hier noch nicht implementiert. Ein sehr wichtiger Punkt ist auch die Durchforstung wichtiger Logfiles, um eventuelle Ungewöhnlichkeiten zu erkennen und daraus zu schließen, ob man angegriffen wurde, oder ob Fehler auftreten.

5 Betriebssystem

Durch die sehr weite Verbreitung des Betriebssystem Windows habe ich mich in dieser Diplomarbeit auf Betriebssysteme der Firma Microsoft beschränkt. Genauer gesagt auf die Versionen Windows 2000 und Windows XP Professional. Obwohl frühere Versionen nicht so sicher waren, ist Windows ab der Version 2000, wenn man es richtig konfiguriert, ein sehr sicheres Betriebssystem. Man muss als Administrator immer zwischen einfacher Bedienbarkeit für Endbenutzer und Sicherheit vor Angriffen abwägen. Deswegen sollte man sich genau ansehen, wie man wichtige Einstellungen konfiguriert.

In diesem Kapitel wird zuerst das grundlegende Sicherheitskonzept von Windows beschrieben. Danach werden die Gruppenrichtlinien erklärt und dabei wichtige Einstellungen beschrieben und auch einige Empfehlungen abgegeben. Der nächste wichtige Punkt in diesem Kapitel sind die Dienste. Dabei werden die Dienste gezeigt, die standardmäßig laufen und einige davon erklärt. Zu guter letzt werden noch wichtige Funktionen von Windows gezeigt, die die Sicherheit stark erhöhen. Dazu gehören das verschlüsselnde Dateisystem (EFS – Encryption File System), die Software Restriktion, die Offlinedateien und noch einige andere nützliche Hinweise.

5.1 Windows Sicherheitskonzept

Das zentrale Kernstück der Sicherheit des Betriebssystem Windows bildet ab der Version Windows 2000 der Active Directory Verzeichnisdienst. Dieser Dienst beinhaltet verschiedene Objekte, wie unter anderen Benutzer, Gruppen und Computer. Alle Informationen zu den jeweiligen Objekten sind in einer Datenbank gespeichert, die am Domänencontroller (Windows 2000 oder 2003 Server) gespeichert ist.

Ein sehr wichtiger Bestandteil des Active Directory sind die Gruppenrichtlinien, mit denen lokale Sicherheitsrichtlinien auf die gesamte Domäne verteilt werden können, und somit ist die Verwaltung um einiges einfacher und überschaubarer.

Dabei unterscheidet man die lokalen Sicherheitsrichtlinien und die Active Directory Richtlinien, wobei die sich hierbei nur die Wirkungsweise unterscheidet, nicht aber die Struktur der Richtlinien.

Die lokalen Sicherheitsrichtlinien findet man auf allen Windows Computern, auch wenn sie nicht Mitglied einer Domäne sind. Diese Richtlinien gelten für alle Benutzer, die sich an dem lokalen Rechner anmelden.

Im Gegensatz dazu unterscheidet man bei den Active Directory Richtlinien, die auf einem Domänencontroller konfiguriert werden, computerspezifische (gelten für alle Benutzer, die sich am Rechner anmelden) und benutzerspezifische (gelten nur für den jeweiligen Benutzer) Richtlinien. Diese Richtlinien können dann für alle Computer in der Domäne, oder auch nur für gewisse Standorte oder Organisationseinheiten angewendet werden. Eine Organisationseinheit bildet eine Art Unterordner in der Domäne, um eventuelle Zusammengehörigkeiten besser verwalten zu können (es werden zum Beispiel alle Computer der Marketing-Abteilung in einer eigenen Organisationseinheit zusammengefasst). Die verschiedenen Richtlinien werden in folgender Reihenfolge abgearbeitet:

1) Lokale Sicherheitsrichtlinien
2) Gruppenrichtlinien für Standort-Container
3) Gruppenrichtlinien für Domänen-Container
4) Gruppenrichtlinien für Organisationseinheiten-Container

Wenn es zu Konflikten kommt, gilt immer die Richtlinie, die zuletzt verarbeitet wurde, also haben die lokalen Richtlinien die geringste Priorität und werden bei Konflikten durch eine später verarbeitete Gruppenrichtlinie überschrieben.

5.2 Gruppenrichtlinien

In den nächsten Abschnitten werden die Sicherheitsrichtlinien, die ein Teil der Windows-Einstellungen sind, genauer betrachtet, welche immer computerspezifisch sind, und somit auch auf Rechnern verfügbar sind, die nicht einer Domäne angehören.

Die wichtigsten Einstellmöglichkeiten sind dabei die Kennwortrichtlinie, Kontensperrungsrichtlinie, Kerberos-Richtlinie, Überwachungsrichtlinie, Benutzerrechte, Sicherheitsoptionen und auch die Systemdienste, die allerdings aufgrund ihrer Wichtigkeit in einem eigenen Kapitel (5.3) behandelt werden.

Zu den lokalen Richtlinien kommt man über den Befehl *Start → Ausführen → gpedit.msc*, oder über das MMC-Snap-In (Microsoft Management Console) der Gruppenrichtlinien, wobei man hier noch auswählen kann, von welchen Computer die Richtlinien angezeigt werden sollen. Äquivalent dazu, nur mit höherer Priorität, findet man die Sicherheitseinstellungen der Gruppenrichtlinien in einer Domäne unter *Computerkonfiguration → Windows-Einstellungen* und ist zu erreichen wenn man entweder auf die Domäne oder eine Organisationseinheit einen Rechtsklick mit der Maus macht und danach auf Eigenschaften geht. Dort gibt es dann die Registerkarte Gruppenrichtlinien.

5.2.1 Kennwortrichtlinie

Die Kennwortrichtlinie ist bei den Gruppenrichtlinien im folgenden Ordner zu finden: *Sicherheitseinstellungen → Kontorichtlinien → Kennwortrichtlinien*. Zuerst werden Beispielkonfigurationen gezeigt, und danach die einzelnen Einstellmöglichkeiten der Kennwortrichtlinie erklärt.

Die Benutzer würden am liebsten immer das gleiche Passwort verwenden. Da dies aber ein zu hohes Sicherheitsrisiko ist (durch die Verwendung des gleichen Passworts über einen langen Zeitraum, steigt die Möglichkeit eines erfolgreichen Brute-Force-Angriffs), werden Kennwortrichtlinien konfiguriert, die einfache Passwörter und auch die ständige Beibehaltung desselben Passworts verhindern.

5.2.1.1 Beispielkonfiguration

In der Tabelle 3 findet man die verschiedenen Einstellmöglichkeiten der Kennwortrichtlinie für Clients (lokale Richtlinien) mit den dazugehörigen Standardwerten ohne vorige Änderung. Die Empfehlungswerte sind laut Danseglio dem Windows XP Security Guide entnommen. (Danseglio 2004)

Tabelle 3: Beispielkonfiguration der Kennwortrichtlinien am Client

Richtlinie	**Standard (Windows 2000 und XP)**	**Empfehlung**
Kennwortchronik erzwingen	gespeicherte Kennwörter: 1	gespeicherte Kennwörter: 24
max. Kennwortalter	42 Tage	42 Tage
min. Kennwortalter	0 Tage	2 Tage
min. Kennwortlänge	0 Zeichen	>= 8 Zeichen
Komplexitätsanforderung	deaktiviert	aktiviert
umkehrbare Verschlüsselung	deaktiviert	deaktiviert

Auf einem Server sind die Standardwerte schon um einiges sicherer, wie Tabelle 4 zeigt. Diese Einstellungen am Server können in der gesamten Domäne verbreitet werden. Die Empfehlungswerte sind laut Danseglio dem Windows Server 2003 Security Guide entnommen. (Danseglio 2006)

Tabelle 4: Beispielkonfiguration der Kennwortrichtlinien am Server

Richtlinie	**Standard (Windows Server 2003)**	**Empfehlung**
Kennwortchronik erzwingen	gespeicherte Kennwörter: 24	gespeicherte Kennwörter: 24
max. Kennwortalter	42 Tage	42 Tage
min. Kennwortalter	1 Tag	1 Tag
min. Kennwortlänge	7 Zeichen	12 Zeichen
Komplexitätsanforderung	aktiviert	aktiviert
umkehrbare Verschlüsselung	deaktiviert	deaktiviert

Um wirklich sichere Passwörter zu verwenden, wird von Microsoft empfohlen, besonders für Administratoren, Passwörter ab 15 Zeichen zu verwenden (Technet 2004). Der Grund dafür liegt darin, das Windows für alle Passwörter verschiedene Hashes bildet (LM-Hash, NT-Hash). Da die Verwendung der LM-Authentifizierung (Lan Manager) schon veraltet ist, und der verwendete Algorithmus relativ leicht zu knacken ist, wird dieser nur mehr wegen der Abwärtskompatibilität gebildet. Um die Erzeugung des LM-Hashes zu verhindern kann man in die Option *NoLMHash* in der Registrierung setzen, oder Passwörter ab 15 Zeichen verwenden, weil somit kein LM-Hash mehr gebildet werden kann. Dieser Hash unterstützt auch nicht den gesamten Unicode-Zeichensatz, deswegen wird der zweite Hash, NT-Hash (New Technology), gebildet.

Dieser Hash entsteht bei der Windows-Authentifizierung mit Hilfe von NTLM oder NTLMv2 (New Technology Lan Manager). Aus dem Kennwort wird ein MD4-Hash (Message Digest 4) erzeugt und gespeichert. Aufgrund der unterschiedlichen Algorithmen dauern Angriffe auf NT-Hashes immer länger als Angriffe auf die LM-Hashes desselben Passworts.

Die neueste und sicherste Authentifizierungsmöglichkeit in Windows erfolgt mit dem Kerberos-Protokoll. Dies wird in einer Domäne verwendet.

Für genauere Informationen zu den Authentifizierungsmöglichkeiten und den verschiedenen Hashes in Windows siehe Smith. (Smith 2005, Kapitel 4)

5.2.1.2 Kennwortchronik erzwingen

Wenn man die Kennwortchronik aktiviert, merkt sich das System frühere Passwörter. Somit kann der Benutzer ein Passwort von früher erst wieder verwenden, wenn es aus der Chronik gefallen ist. Die Anzahl entspricht dabei dem eingegebenen Wert, wobei Werte von 0-24 und auch *nicht definiert* möglich sind. Falls also der Maximalwert von 24 eingegeben wird, kann ein Benutzer erst nach dem 25. neuen Passwort wieder sein erstes angeben.

5.2.1.3 Kennwörter müssen den Komplexitätsanforderungen entsprechen

Wenn die Komplexitätsanforderungen aktiviert sind, muss das Benutzerpasswort folgenden Kriterien entsprechen:

- Es darf den Benutzernamen oder Teile davon nicht enthalten
- Es muss Zeichen aus drei der vier Kategorien (Ziffern, Sonderzeichen, Klein- und Großbuchstaben) enthalten
- Es unterliegt den Richtlinien *Minimale Kennwortlänge* und der *Kennwortchronik*

Die Einstellmöglichkeiten für diese Richtlinie sind *Aktiviert, Deaktiviert* und *nicht definiert*.

5.2.1.4 Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern

Durch diese Richtlinie wird die Kompatibilität zu Applikationen gewährleistet, welche ältere Protokolle wie zum Beispiel CHAP (Challenge Handshake Authentication Protocol) verwenden (siehe Technet 2005), die das Benutzerpasswort im Klartext benötigen. Dies ist aber nur in den seltensten Fällen notwendig. Die umkehrbare Verschlüsselung bedeutet nur, dass der Domänencontroller Passwörter schnell entschlüsseln kann. Durch die Aktivierung dieser Richtlinie wird aber die Kennwortsicherheit erheblich geschwächt und sollte somit nie aktiviert werden. Die Einstellmöglichkeiten für diese Richtlinie sind *Aktiviert, Deaktiviert* und *nicht definiert*.

5.2.1.5 Maximales Kennwortalter

Damit ein Benutzer nicht ewig das gleiche Kennwort verwendet, kann er durch diese Richtlinie gezwungen werden, sein Passwort regelmäßig zu ändern. Die Einstellmöglichkeiten für diese Richtlinien reichen von 0-999 Tage und auch *nicht definiert*, wobei 0 bedeutet, dass das Passwort nie abläuft.

5.2.1.6 Minimale Kennwortlänge

Mit dieser Richtlinie können Administratoren kurze, und somit leicht zu knackende Passwörter verhindern. Ein zu hoher Wert ist für ein normales Benutzerkonto auch nicht angemessen, weil sonst viele der Passwörter aufgeschrieben werden. Bei Administrationskonten sollte man aber vor einer längeren Zeichenkette nicht zurückschrecken. Die Einstellmöglichkeiten für diese Richtlinie reichen von 0-14 und auch *nicht definiert*, wobei 0 bedeutet, dass das Benutzerkonto überhaupt kein Passwort erfordert.

5.2.1.7 Minimales Kennwortalter

Diese Richtlinie ist in Verbindung mit der Kennwortchronik sehr sinnvoll, denn somit wird verhindert, dass der Benutzer sein Passwort sofort wieder ändern kann, und somit die Chronik umgeht, indem er eine große Anzahl von neuen Passwörtern solange angibt, bis er wieder seine ursprüngliche Zeichenfolge angeben kann. Die Einstellmöglichkeiten für diese Richtlinie reichen von 0-998 und auch *nicht definiert*, wobei 0 bedeutet, dass der Benutzer sein Passwort sofort wieder ändern kann.

5.2.2 Kontensperrungsrichtlinie

Um gegen mögliche Angriffe effektiver geschützt zu sein, ist es sinnvoll zusätzlich zu den Kennwortrichtlinien auch noch Kontensperrungsrichtlinien zu konfigurieren, welche sich auch wie oben beschrieben in den Kontorichtlinien der Gruppenrichtlinie befinden *(Sicherheitseinstellungen → Kontorichtlinien → Kontensperrungsrichtlinie)*. Dadurch wird zwar die Arbeit für die IT-Abteilung oder einen Helpdesk erhöht, aber dies sollte man in Kauf nehmen, weil die Sicherheit weiter erhöht wird. Auch hier wird zuerst wieder eine Beispielkonfiguration gezeigt, und im Anschluss die einzelnen Richtlinien erklärt.

5.2.2.1 Beispielkonfiguration

Tabelle 5 zeigt die Einstellmöglichkeiten der Kontensperrungsrichtlinie mit den Standardwerten ohne vorige Änderung. Da hier die Standardwerte für Clients und Server die gleichen sind, werden nur die aktuellsten Werte von Windows XP gezeigt. Die Empfehlungswerte wurden wieder laut Danseglio aus dem Windows XP Security Guide entnommen. (Danseglio 2004)

Tabelle 5: Beispielkonfiguration der Kontensperrungsrichtlinien

Richtlinie	**Standard**	**Empfehlung**
Kontosperrungsschwelle	0 (deaktiviert)	50 ungültige Versuche
Kontosperrdauer	nicht definiert	30 Minuten
Kontosperrungszähler zurücksetzen nach	nicht definiert	30 Minuten

5.2.2.2 Kontosperrungsschwelle

Diese Richtlinie legt fest, nach wie vielen falschen Anmeldeversuchen das Benutzerkonto gesperrt wird. Die Einstellmöglichkeiten reichen von 0-999 Versuchen und auch *nicht definiert*, wobei 0 bedeutet, dass diese Richtlinie deaktiviert ist. Hier muss ein Administrator zwischen Sicherheit, Benutzerfreundlichkeit und Arbeitsaufwand für die IT-Abteilung abschätzen. Je kleiner der Wert eingestellt wird, desto öfter werden Anfragen kommen, um ein Benutzerkonto wieder entsperren zu lassen. Falls diese Richtlinie aktiviert wird, werden automatisch die beiden anderen Werte der Kontensperrungsrichtlinie auf 30 Minuten gesetzt und müssen angepasst werden.

Normalerweise werden ungültige Anmeldeversuchen nur beim Windows-Login mitgezählt, nicht aber ungültige Versuche an gesperrten Arbeitsstationen (über *Strg+Alt+Entf* und *Computer sperren* oder durch einen Bildschirmschoner). Wenn diese Versuche auch mitgezählt werden sollen, gibt es bei den Gruppenrichtlinien folgende Einstellung: *Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich.*

5.2.2.3 Kontosperrdauer

Mit Hilfe dieser Richtlinie kann eingestellt werden, wie lange ein Benutzerkonto nach Überschreitung der Kontosperrungsschwelle gesperrt bleibt. Die Einstellmöglichkeiten reichen von 0-99.999 Minuten und auch *nicht definiert*, wobei 0 bedeutet, dass nur der Administrator die Sperrung aufheben kann, und nicht die Sperrung automatisch nach einer gewissen Zeit aufgehoben wird.

5.2.2.4 Kontosperrungszähler zurücksetzen nach

Mit dieser Richtlinie kann der Kontosperrungszähler zurückgesetzt werden, falls sich der Benutzer zum Beispiel nach zwei falschen Anmeldeversuchen richtig einloggt, kann mit diesem Wert angegeben werden, nach welcher Zeit der Zähler wieder zurückgesetzt wird. Die Einstellmöglichkeiten reichen von 1-99.999 Minuten.

5.2.3 Kerberos-Richtlinie

Die neueste und sicherste (im Gegensatz zu seinem Vorgänger LM und NTLM) Authentifizierungsmöglichkeit in Windows erfolgt mit dem Kerberos-Protokoll. Dazu gibt es auch einige Einstellmöglichkeiten, die auch wieder bei den Kontorichtlinien zu finden sind *(Sicherheitseinstellungen → Kontorichtlinien → Kerberos-Richtlinie)*. Diese werden allerdings nur auf Domänencontrollern konfiguriert, nicht auf den Notebooks selbst. Trotzdem werden sie hier kurz erwähnt, da sie die Sicherheit bei der Authentifizierung um einiges erhöhen. Es wird empfohlen die voreingestellten Standardwerte nicht zu ändern. In der Tabelle 6 sieht man die Einstellmöglichkeiten und deren Standardwerte.

Tabelle 6: Standardkonfiguration der Kerberos-Richtlinie

Benutzeranmeldeeinschränkungen erzwingen	Aktiviert
Max. Gültigkeitsdauer des Diensttickets	600 Minuten
Max. Gültigkeitsdauer des Benutzertickets	10 Stunden
Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann	7 Tage
Max. Toleranz für die Synchronisation des Computertakts	5 Minuten

Genauere Informationen zur Kerberos-Authentifizierung finden sie hier (Peikari 2004, S.384ff).

5.2.4 Überwachungsrichtlinie

Mit Hilfe der Überwachungsrichtlinien können die Aktivitäten von Benutzern überwacht werden. Dabei können sowohl fehlgeschlagene wie auch erfolgreiche Ereignisse angezeigt werden, wobei hierbei die fehlgeschlagenen Ereignisse interessanter sind, da sie entweder auf einen Fehler hinweisen, oder sogar auf einen Angriffsversuch. Es gilt bei den Einstellungen darauf zu achten, dass nicht zu viele Ereignisse angezeigt werden, da sonst die Übersicht verloren geht. Außerdem kann bei einer großen Anzahl von zu überwachenden Systemen die Systemleistung gebremst werden. Zu finden sind die Einstellmöglichkeiten wieder bei den Gruppenrichtlinien unter folgendem Punkt:

Sicherheitseinstellungen → Lokale Richtlinien → Überwachungsrichtlinie

Bei jedem Punkt der Überwachungsrichtlinie gibt es die Einstellmöglichkeiten *Erfolgreich, Fehlgeschlagen* und *keine Überwachung.* Es werden nur jene Einstellmöglichkeiten erklärt, bei denen die Aktivierung empfohlen wird. Da die anderen Einstellmöglichkeiten meist nur eine große Anzahl von nichts sagenden Einträgen hinterlässt, wird nicht näher darauf eingegangen.

5.2.4.1 Anmeldeversuche überwachen

Ein sehr wichtiger Punkt bei den Überwachungsrichtlinien ist die Möglichkeit An- und Abmeldeversuche von Benutzern an Computern zu überwachen. Dabei werden alle An- und Abmeldungen überwacht, die entweder lokal oder über das Netzwerk am Computer stattfinden. Zusätzlich werden auch noch An- und Abmeldungen von Dienstkonten überwacht. Bei allen An- und Abmeldungen werden nur jene überwacht, die mit einem Benutzerkonto der Domäne erfolgen. Somit wissen Administratoren Bescheid, auf welchen Systemen, welche Benutzerkonten arbeiten, und ob sie das auch dürfen. Mit Hilfe dieser Einstellung können mögliche Angriffsversuche (falls mit Hilfe eines Programms viele Passwörter ausprobiert werden) auf ein Benutzerkonto erkannt werden.

5.2.4.2 Kontenverwaltung überwachen

Mit Hilfe dieser Einstellung können folgende Aktivitäten eines Benutzerkontos überwacht werden:

- Erstellen, Ändern oder Löschen eines Benutzerkontos oder auch einer Gruppe
- Aktivieren, Deaktivieren oder Umbenennen eines Benutzerkontos
- Kennwortänderungen

5.2.4.3 Anmeldeereignisse überwachen

Zum Unterschied zu der Richtlinie *Anmeldeversuche überwachen*, werden hier alle An- und Abmeldevorgänge überwacht, die mit einem lokalen Benutzerkonto erfolgen. Da es allerdings keine oder zumindest nicht zu viele lokale Benutzerkonten geben sollte (eventuell mit Ausnahme eines lokales Administratorkontos), sollte diese Richtlinie nicht so viele Einträge hinterlassen.

5.2.4.4 Richtlinienänderungen überwachen

Mit Hilfe dieser Einstellung können Änderungen an folgenden Richtlinien überwacht werden, und ins Sicherheitsereignisprotokoll eingetragen werden:

- Zuweisung von Benutzerrechten
- Überwachungsrichtlinien
- Vertrauensrichtlinien

Somit können Administratoren erkennen, wenn sich Gruppenrichtlinien ändern. Dies kann in größeren Netzwerken mit mehreren Administratoren sehr hilfreich sein, falls die Kommunikation der einzelnen Zuständigen ungenügend oder gar nicht vorhanden ist.

5.2.4.5 Systemereignisse überwachen

Bei Aktivierung dieser Überwachungsrichtlinie erhält man eine kleine Anzahl an zusätzlichen Einträgen, die aber von großer Bedeutung sind, da es sich hierbei um alle sicherheitsrelevanten Ereignisse des Systems handelt. Dazu gehören unter anderen auch der Neustart oder das Herunterfahren des Systems.

5.2.5 Zuweisen von Benutzerrechten

Die allgemeinen Richtlinien und Hilfestellungen zu der Vergabe von Benutzerrechten wurden bereits im Kapitel der Organisation beschrieben. In diesem Abschnitt sind nun die genauen Einstellmöglichkeiten des Betriebssystem Windows beschrieben. Dabei wird zwischen Anmelderechten und Berechtigungen unterschieden. Anmelderechte sind jene Rechte, die kontrollieren wer zur Anmeldung an einem System berechtigt ist, und wie diese Anmeldung erfolgt. Berechtigungen hingegen sind für den systemweiten Zugriff auf Ressourcen verantwortlich. Auch dieser Punkt ist ein Teil der Gruppenrichtlinien und ist zu finden unter:

Sicherheitseinstellungen → Lokale Richtlinien → Zuweisen von Benutzerrechten

Die Einstellmöglichkeiten bei allen folgenden Berechtigungen sind *nicht definiert* oder eine Liste von *Benutzerkonten*. Da es eine sehr große Anzahl von Berechtigungen in den Gruppenrichtlinien gibt, werden nicht alle hier erwähnt, sondern nur jene, die meiner Meinung nach wichtig für die Sicherheit von Rechnern sind.

5.2.5.1 Netzwerkzugriff

Es gibt zwei Berechtigungen, die den Netzwerkzugriff steuern. Dabei handelt es sich um *Auf diesen Computer vom Netzwerk aus zugreifen* und auf das Gegenstück *Zugriff vom Netzwerk auf diesem Computer verweigern*. Es wird nur die erste Berechtigung näher beschrieben, da das Gegenstück dann selbst erklärend ist.

Dieses Benutzerrecht wird benötigt, um eine Netzwerkverbindung mit diesem Computer herstellen zu können. Manche Netzwerkprotokolle benötigen dieses Recht. Es kommt immer darauf an um welchen Computer es sich dabei handelt. Deswegen sollte die Liste mit berechtigten Benutzern übersichtlich gehalten werden (durch die Angabe von Benutzergruppen). Auf die meisten Server müssen Administratoren und auch Benutzer zugreifen können (Domänencontroller, Mail-Server, usw.). Wenn sie allen Benutzern den Zugriff auf einen Computer über das Netzwerk gewähren wollen, sollte aber nicht die Gruppe *Jeder* angegeben werden, sondern die Gruppe *Domänen-Benutzer*.

5.2.5.2 Als Teil des Betriebssystem handeln

Mit Hilfe dieses Rechts können Prozesse die Identität von Benutzern annehmen und somit auf Ressourcen zugreifen, auf welche auch Benutzer zugreifen dürfen. Noch dazu kann der aufrufende Prozess weitere Berechtigungen anfordern und auch Zugriffstokens erstellen. Somit kann ein Benutzer die vollständige Steuerung des Systems übernehmen. Deswegen sollte dieses Recht nicht häufig verwendet werden.

5.2.5.3 Hinzufügen von Arbeitsstationen zur Domäne

Wie der Name schon sagt, können Benutzer mit diesem Recht einen Computer zur Domäne hinzufügen, allerdings nur, wenn diese Berechtigung am Domänencontroller für die ganze Domäne konfiguriert wird. Allerdings gibt es eine Einschränkung von maximal zehn Arbeitsstationen, die ein Benutzer der Domäne hinzufügen darf. Diese Berechtigung sollten aber keine normalen Benutzer bekommen, sondern nur Mitglieder der IT-Abteilung.

5.2.5.4 Anpassen von Arbeitsspeicherquoten für einen Prozess

Hiermit kann der maximale Arbeitsspeicher konfiguriert werden, der für einen Prozess verfügbar ist. Die Verwendung dieser Berechtigung wird allerdings nicht empfohlen und sollte ausschließlich Administratoren eingeräumt werden.

5.2.5.5 Anmeldungen

Bei diesem Punkt werden alle Berechtigungen zusammengefasst, die etwas mit einer Anmeldung zu tun haben.

Als erstes werden zwei Berechtigungen zusammengefasst, weil sie sich sehr ähnlich sind. Mit der Berechtigung *Lokal anmelden zulassen* können sich Benutzer lokal an einem Rechner anmelden. Wenn dieses Recht entfernt wird, ist die lokale Anmeldung zwar nicht mehr möglich, allerdings sind weiterhin Remote-Verbindungen möglich, falls die Berechtigung *Anmeldung über Terminaldienste zulassen* gesetzt ist. Auf normalen Rechnern, die einer Domäne angehören, kann sich normalerweise jeder Benutzer der Domäne anmelden (zumindest lokal), auf Servern hingegen meist nur Administratoren oder Mitglieder der IT-Abteilung.

Zusätzlich zu diesen zwei Berechtigungen gibt es noch die jeweiligen Gegenstücke *Lokal anmelden verweigern* und *Anmelden über Terminaldienste verweigern*.

Als nächstes wird die Einstellmöglichkeit *Anmelden als Dienst verweigern* betrachtet. Mit Hilfe dieser Berechtigung kann verhindert werden, dass nicht autorisierte Dienste, wie Trojanische Pferde, fälschlicherweise von Benutzern gestartet werden. Allerdings kann es passieren, dass manche Dienste danach nicht mehr laufen und deswegen wird diese Berechtigung keinem Benutzerkonto zugewiesen. Zusätzlich gibt es auch noch als Gegenstück die Berechtigung *Anmelden als Dienst*.

5.2.5.6 Dateien und Verzeichnisse

Mit Hilfe der Berechtigung *Sichern von Dateien und Verzeichnissen* können die normalen Berechtigungen von Dateien und Verzeichnissen umgangen werden. Dies wird von Backup-Programmen verwendet, wie zum Beispiel *NTBackup.exe*. Dieses Recht sollte wiederum keinen normalen Benutzer erteilt werden, sondern nur Mitglieder der IT-Abteilung, da diese meist für Backups zuständig sind. Um auch bei der Wiederherstellung von gesicherten Dateien und Verzeichnissen die normalen Berechtigungen zu umgehen, gibt es als Gegenstück die Berechtigung *Wiederherstellen von Dateien und Verzeichnissen*. Normalerweise sollten wichtige Daten nicht nur lokal am Laptop gespeichert sein, sondern auch im Netzwerk. Von diesen Daten im Netzwerk sollte auch ein Backup erstellt werden. Somit benötigen nur Administratoren diese Berechtigung. Allerdings kann es sinnvoll sein, wenn Notebook-User längere Zeit unterwegs sind, das sie auch ein Backup erstellen dürfen. Deswegen müssen je nach Unternehmen auch die Notebook-Benutzer diese Berechtigung erhalten.

5.2.5.7 Herunterfahren

Hier werden zwei Berechtigungen betrachtet. Zum einem die Berechtigung *System herunterfahren*. Mit Hilfe dieser Einstellmöglichkeit können Benutzer den Rechner herunterfahren. Auf normalen PC´s sollten alle Benutzer (Mitglieder der Domäne) diese Berechtigung erhalten, auf Servern hingegen nur Administratoren. Eine ähnliche Berechtigung ist *Herunterfahren von einem Remotesystem aus*. Hiermit kann ein Rechner auch von remote über das Netzwerk heruntergefahren werden. Dieses Recht sollte allerdings nur für Administratoren gewährt werden, denn normale Benutzer müssen keine Computer von remote herunterfahren, sondern nur ihren eigenen lokalen Rechner.

5.2.5.8 Ändern der Systemzeit

Wie der Name schon sagt, können Benutzer mit dieser Berechtigung die Uhrzeit des lokalen Systems ändern, allerdings nicht die Zeitzone. Dieses Recht sollte nur Administratoren gewährt werden, da viele Protokolle mit Zeitstempeln arbeiten, und durch die Änderung der lokalen Zeit kann es zu Problemen kommen. In einer Domäne kommuniziert ein Client mit dem Domänencontroller bei der Anmeldung mit Hilfe des Kerberos-Protokolls, welches maximal fünf Minuten Zeitunterschied zulässt, sonst kann sich der Benutzer nicht mehr anmelden. Deswegen sollten sich alle Computer mit dem Domänencontroller zeitsynchronisieren.

Mit einer Änderung der lokalen Zeit eines Computers können auch die Einträge in einem Ereignisprotokoll verfälscht werden, da hier die am Computer eingestellte Zeit angezeigt wird.

5.2.5.9 Sicherheitsüberwachungen generieren

Mit dieser Einstellung können Überwachungseinträge im Sicherheitsprotokoll generiert werden. Diese Berechtigung sollte aber keinem Benutzerkonto zugewiesen werden, sondern ausschließlich von den Gruppen *Lokaler Dienst* und *Netzwerkdienst* verwendet werden, da sonst Angreifer das Sicherheitsprotokoll mit falschen Einträgen befüllen könnten.

5.2.5.10 Zeitplanungspriorität anheben

Hiermit können die Prioritäten von Prozessen verändert werden. Da Benutzer somit aber das System lahm legen können (durch eine sehr hohe Priorität für einen falschen Prozess), sollten nur Administratoren dieses Recht erhalten.

5.2.6 Sicherheitsoptionen

Zu den Sicherheitsoptionen für Computer gehören unter anderem spezielle Benutzerkonten (Administrator, Gast, usw.), Datensignatur und Laufwerkzugriffe und sind auch ein Teil der Gruppenrichtlinien, zu finden unter:

Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen

Auch hier gibt es wieder eine sehr große Anzahl von Sicherheitsoptionen, und auch hier werden wieder nur die wichtigsten beschrieben.

5.2.6.1 Konten

Mit Hilfe der Option *Administratorkontostatus* kann das Administratorkonto für den normalen Betrieb aktiviert oder deaktiviert werden. Unabhängig davon ist ein Start des Systems im abgesicherten Modus, wo das Administratorkonto immer aktiviert ist. Häufig wird das lokale Administratorkonto umbenannt (mit der Option *Administratorkonto umbenennen* der Sicherheitsoptionen oder auch manuell), und viele glauben, dass sie sich so vor möglichen Angriffen schützen. Viele Angriffstools arbeiten aber nicht mit dem Kontonamen sondern mit der allgemein bekannten SID (Security Identifier, siehe Microsoft Knowledgebase 2005) dieses Kontos, und somit erreicht man mit einer Umbenennung des Kontos nicht viel. Allerdings können nicht so erfahrene Angreifer damit schon blockiert werden. Es sollte aber auch die Standardbeschreibung des Kontos (Vordefiniertes Konto für die Verwaltung des Computers bzw. der Domäne) geändert werden. Wenn das Konto nicht allzu häufig benötigt wird, sollte es deaktiviert werden.

Mit Hilfe der Option *Gastkontenstatus* kann das Gastkonto aktiviert oder deaktiviert werden, unabhängig vom Systemstart (abgesicherter Modus oder normaler Modus). Dieses Konto sollte immer deaktiviert werden, denn sonst könnten sich Benutzer ohne Passwort anmelden und auf alle Ressourcen zugreifen, bei denen die Gruppe *Jeder* Zugriff hat.

Standardmäßig ist es bereits deaktiviert, also sollte hier nichts verändert werden. Zusätzlich sollte auch der Name des Gastkontos noch mit der Hilfe der Sicherheitsoption *Gastkonto umbenennen* verändert werden.

5.2.6.2 Interaktive Anmeldung

Die Option *Letzten Benutzernamen nicht anzeigen* ist sehr sinnvoll und kann gegen Angriffe auf Benutzerkonten schützen. Der Grund dafür ist jener, das Windows normalerweise den Benutzernamen des zuletzt erfolgreich eingeloggten Benutzers in der Anmeldeoberfläche anzeigt, und somit wissen Angreifer schon einen Teil der Anmeldeinformationen, und können eventuell mit einem Brute-Force-Angriff auf das Passwort in das System eindringen. Wenn sie allerdings den Benutzernamen und das Passwort nicht wissen, ist es so gut wie unmöglich in einer sinnvollen Zeit in das System einzudringen. Allerdings ist dies für die Benutzer wieder ein Wort mehr, welches sie sich merken müssen, und dieses wird dann oft auch aufgeschrieben. Wenn der Benutzername angezeigt wird, und man fragt einen Benutzer nach seinem Anmeldenamen wissen ihn die meisten nicht, weil sie nicht darauf achten, sondern immer nur ihr Passwort eingeben.

Zusätzlich kann noch mit der Option *Kein STRG+ALT+ENTF erforderlich* festgelegt werden, das beim Systemstart sofort das Anmeldefenster kommt, ohne das der Benutzer vorher die Tastenkombination STRG+ALT+ENTF drücken muss. Wenn die Benutzer diese Option nicht kennen, werden sie sie auch nicht vermissen.

Zusätzlich könnten auch noch Nachrichten mit den Optionen *Nachricht für Benutzer, die sich anmelden* wollen und *Nachrichtentitel für Benutzer, die sich anmelden wollen* angezeigt werden. Mit Hilfe solcher Nachrichten werden manchmal Warnungen angezeigt, um nicht autorisierte Personen abzuschrecken, wenn sie sich Zugang zum Computer verschaffen wollen. Diese Option wird aber nicht sehr oft verwendet.

Mit der Option *Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)* kann verhindert werden, dass die Anmeldeinformationen lokal zwischengespeichert werden (genauer gesagt kann die Anzahl der lokal gespeicherten Anmeldeinformationen eingestellt werden).

Dies ist aber für Notebook-Benutzer nicht sinnvoll, weil diese oft in das System einsteigen, ohne eine Netzwerkverbindung zu haben, und dies ist ohne den lokalen Anmeldeinformationen dann nicht mehr möglich, außer es gibt eigene lokale Benutzerkonten, die verwendet werden, wenn der Benutzer nicht im Netz ist. Dies ist aber zu umständlich und wird nicht empfohlen.

Sehr ähnlich ist die Einstellung *Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich*, welche für Notebook-Benutzer wiederum nicht sinnvoll ist, da sie ohne Netzwerkverbindung ihren Computer nicht mehr entsperren können. Da aber jeder Benutzer immer und überall seinen Computer sperren sollte, wenn er nicht davor sitzt, würde sich ein Benutzer ohne Verbindung zu einem Domänencontroller selbst aus seinem System sperren.

Durch die Kennwortrichtlinien können Passwörter ablaufen und ungültig werden. Damit der Benutzer rechtzeitig vor dem Ablaufen seines Kennworts informiert wird, gibt es die Einstellung *Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern*. Damit werden Benutzer bei jeder Anmeldung an die Domäne erinnert, das ihr Kennwort in einigen Tagen abläuft, und ob sie das Passwort jetzt sofort ändern wollen. Somit haben die Benutzer mehr Zeit, um sich ein neues, sicheres Kennwort zu überlegen.

Um die Anmeldung sicherer zu gestalten als die übliche Anmeldung mit Benutzername und Passwort, werden immer häufiger Smartcards verwendet. Dazu gibt es auch eine Einstellung, um die Anmeldung mit der Smartcard zu erzwingen, und zwar ist dies die Einstellmöglichkeit *Smartcard erforderlich*. Dazu gibt es auch noch eine weitere Einstellmöglichkeit, mit der man das Verhalten des Systems festlegen kann, wenn die Smartcard aus dem Lesegerät entfernt wird (*Verhalten beim Entfernen von Smartcards*). Die Möglichkeiten sind *keine Aktion, Arbeitsstation sperren, Abmeldung erzwingen* oder auch *nicht definiert*.

5.2.6.3 Netzwerkzugriff

Eine sehr wichtige Einstellung ist *Anonyme SID-/Namensübersetzung zulassen*. Damit kann ein anonymer Benutzer mit Hilfe einer SID (zum Beispiel der allgemein bekannten SID des Administratorkontos) den Benutzernamen erfahren. Wenn also in einem Unternehmen das Administratorkonto umbenannt wurde, könnten Benutzer über die SID auf den aktuellen Namen des Administratorkontos kommen, und danach einen Angriffsversuch starten. Deswegen sollte diese Einstellung immer *deaktiviert* sein. Dies ist auch die Standardeinstellung bei Domänenmitgliedern.

Des Weiteren gibt es noch einige andere Einstellungen, die mit anonymen Benutzern zu tun haben. Grundsätzlich sollten aber anonymen Benutzern nichts erlaubt werden, und sie sollten auch auf keine Freigaben oder ähnliches zugreifen können, oder besser noch, sie sollten die Freigaben auch nicht sehen.

5.2.6.4 Netzwerksicherheit

Wie bereits weiter oben im Kapitel 5.2.1.1 erklärt gibt es in Windows verschiedene Authentifizierungsmöglichkeiten. Die älteste davon ist die LM-Authentifizierung. Es werden aber für alle Passwörter noch immer die LM-Hashes gebildet und gespeichert, um die Kompatibilität zu älteren Systemen zu gewährleisten. Wenn allerdings keine alten Systeme (Windows 95, Windows 98 und Windows ME) und Anwendungen mehr im Einsatz sind, sollte mit Hilfe der Einstellmöglichkeit *Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern*, die Bildung des LM-Hashes verhindert werden, da bei diese Hashes ein schwächerer kryptografischer Algorithmus verwendet wird. Allerdings müssen nach der Aktivierung dieser Option alle Benutzer ihre Kennwörter ändern.

5.2.6.5 Wiederherstellungskonsole

Falls Probleme mit dem Rechner auftreten, und dieser nicht mehr normal gestartet werden kann, gibt es die Möglichkeit den Computer mit der Wiederherstellungskonsole zu starten. Dazu gibt es auch eine Einstellung, mit der man die Wiederherstellungskonsole starten kann, ohne ein Passwort für das Administratorkonto angeben zu müssen (*Automatische administrative Anmeldungen zulassen*). Da dies aber auch sehr gefährlich ist, wird davon abgeraten. Somit könnten nicht berechtigte Benutzer Vollzugriff auf ein System erhalten, wenn sie es mit der Wiederherstellungskonsole neu starten.

Zusätzlich gibt es noch die Option *Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen*. Mit Hilfe dieser Option hat man mehr Möglichkeiten bei der Wiederherstellung, und sie sollte auch immer aktiviert sein. Ansonsten würde man einem Wiederherstellungs-Techniker oder einem Administrator die Arbeit unnötig schwerer machen.

5.2.6.6 Systemkryptografie

Wie im Kapitel 5.4 beschrieben gibt es in Windows die Möglichkeit, Daten zu verschlüsseln. Um einen sicheren Verschlüsselungsalgorithmus verwenden zu können, gibt es die Einstellmöglichkeit *FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden*. Damit wird nicht mehr der veraltete DESX-Algorithmus (Data Encryption Standard Extended) verwendet, sondern 3DES (Triple Data Encryption Standard). Dies sollte aktiviert werden, wenn man die Verschlüsselung mit Hilfe von EFS verwendet, allerdings wird die Systemleistung verlangsamt. Deswegen nur aktivieren, wenn EFS verwendet wird.

5.2.6.7 Ereignisprotokoll

Zu guter letzt gibt es noch einige Sicherheitseinstellungen für das Ereignisprotokoll, die unter *Computerkonfiguration* → *Windows-Einstellungen* → *Sicherheitseinstellungen* → *Ereignisprotokoll* zu finden sind.

Mit Hilfe dieser Einstellungen kann unter anderem die maximale Größe der verschiedenen Protokolle festgelegt werden, und wie lange die Protokolle aufbewahrt werden. Zusätzlich kann auch eingestellt werden, wer Zugriff auf die Protokolle hat (zum Beispiel ob auch das Gastkonto Zugriff haben soll).

5.3 Dienste

Dienste, genauer gesagt Dienststeuerungsprogramme sind Programme, die unabhängig von irgendwelchen Benutzerkonten ausgeführt werden, egal ob ein Benutzer am System angemeldet ist oder nicht. Sie sind eigentlich auch ein Bestandteil der Gruppenrichtlinien, und somit können sie auch über die gesamte Domäne verteilt werden, damit auf jedem Computer dieselben Dienste laufen. Da sie aber von besonderer Bedeutung sind, werden sie in einem eigenen Kapitel behandelt. Dienste sind die Hauptangriffspunkte eines Systems, und deswegen muss ihnen besondere Aufmerksamkeit geschenkt werden. Durch die Deaktivierung nicht benötigter Dienste wird die Angriffsfläche ihres Systems mit ein paar kleinen Schritten stark reduziert. Im folgenden Abschnitt werden die Dienste gezeigt, welche es standardmäßig in Windows gibt, und davon werden die wichtigsten erklärt.

5.3.1 Standard

Nach einer Installation eines Betriebssystems werden laut Microsoft standardmäßig die Dienste, die in Tabelle 7 gezeigt werden, erstellt und konfiguriert (Microsoft, Default Settings for Services). Dieser Link zeigt die Dienste einer englischen Version von Windows XP. Diese wurden von mir ins Deutsche übernommen, und alphabetisch geordnet.

Tabelle 7: Standarddienste in Windows XP

Vollständiger Dienstname	**Dienstname**	**Starttyp**	**Konto**
Ablagemappe	ClipSrv	Manuell	LS
Anmeldedienst	Netlogon	Automatisch	LS
Anwendungsverwaltung	AppMgmt	Manuell	LS
Arbeitsstation	lanmanworkstation	Automatisch	LS
Automatische Updates	wuauserv	Automatisch	LS
COM+-Ereignissystem	EventSystem	Manuell	LS

COM+ Systemanwendung *		Manuell	LS
Computerbrowser	Browser	Automatisch	LS
Designs *	Themes	Automatisch	LS
DHCP-Client	Dhcp	Automatisch	LS
Distributed Transaction Coordinator	MSDTC	Manuell	ND
DNS-Client	Dnscache	Automatisch	ND
Drahtloskonfiguration *	WZCSVC	Automatisch	LS
Druckwarteschlange	Spooler	Automatisch	LS
Eingabegerätezugang *	HidServ	Deaktiviert	LS
Ereignisprotokoll	Eventlog	Automatisch	LS
Fehlerberichterstattungsdienst *	ERSvc	Automatisch	LS
Gatewaydienst auf Anwendungsebene *	ALG	Manuell	LD
Geschützter Speicher	ProtectedStorage	Automatisch	LS
Hilfe und Support	helpsvc	Automatisch	LS
IMAPI-CD-Brenn-COM-Dienste *	ImapiService	Manuell	LS
Indexdienst	cisvc	Manuell	LS
Intelligenter Hintergrund-übertragungsdienst	BITS	Manuell	ND
IPSec-Dienste	PolicyAgent	Automatisch	LS
Kryptografiedienste *	CryptSvc	Automatisch	LS
Leistungsprotokolle und Warnungen	SysmonLog	Manuell	ND
Microsoft Software Shadow Copy Provider *	SwPrv	Manuell	LS
Nachrichtendienst	Messenger	Automatisch	LD

NetMeeting-Remotedesktop-Freigabe	mnmsrvc	Manuell	LS
Network Location Awareness *	NLA	Manuell	LS
Netzwerk-DDE-Dienst	NetDDE	Manuell	LS
Netzwerk-DDE-Serverdienst	NetDDEdsdm	Manuell	LS
Netzwerkverbindungen	Netman	Manuell	LS
NT-LM-Sicherheitsdienst	NtLmSsp	Manuell	LS
Plug & Play	PlugPlay	Automatisch	LS
QoS RSVP		Manuell	LS
RAS-Verbindungsverwaltung	RasMan	Manuell	LS
Remoteprozeduraufruf (RPC)	RpcSs	Automatisch	LS
Remoteregistrierung	RemoteRegistry	Automatisch	LD
Routing und RAS	RemoteAccess	Manuell	LS
RPC-Locator	RpcLocator	Manuell	ND
Schnelle Benutzerumschaltung *	FastUserSwitching Compatibility	Manuell	LS
Sekundäre Anmeldung *	seclogon	Automatisch	LS
Seriennummer der tragbaren Medien *	WmdmPmSN	Automatisch	LS
Server	lanmanserver	Automatisch	LS
Shellhardwareerkennung *	ShellHWDetection	Automatisch	LS
Sicherheitskontenverwaltung	SamSs	Automatisch	LS
Sitzungs-Manager für Remotedesktophilfe *	RDSessMgr	Manuell	LS
Smartcard	SCardSvr	Manuell	LD
Smartcard Hilfsprogramm		Manuell	LD

SSDP Suchdienst *		Manuell	LD
Systemereignisbenachrichtigung	SENS	Automatisch	LS
Systemwiederherstellungsdienst *		Automatisch	LS
Taskplaner	Schedule	Automatisch	LS
TCP/IP NetBIOS-Hilfsprogramm	LMHosts	Automatisch	LD
Telefonie	TapiSrv	Manuell	LS
Telnet	TlntSvr	Manuell	LS
Terminaldienste *	TermService	Manuell	LS
Überwachung verteilter Verknüpfungen (Client)	TrkWks	Automatisch	LS
Universal Plug & Play Geräte-Host *		Manuell	LS
Unterbrechungsfreie Stromversorgung	UPS	Manuell	LD
Upload Manager *	Uploadmgr	Automatisch	LS
Utility Manager *		Manuell	LS
Verwaltung für automatische RAS-Verbindung	RasAuto	Manuell	LS
Verwaltung logischer Datenträger	dmserver	Automatisch	LS
Verwaltungsdienst für die Verwaltung logischer Datenträger	dmadmin	Manuell	LS
Volumeschattenkopie *	VSS	Manuell	LS
Warndienst	Alerter	Manuell	LD
Webclient *	WebClient	Automatisch	LD
Wechselmedien	NtmsSvc	Manuell	LS
Windows Audio*	AudioSrv	Automatisch	LS

Windows Bilderfassung (WIA) *	StiSvc	Manuell	LS
Windows Firewall/Gemeinsame Nutzung der Internetverbindung		Automatisch	LS
Windows Installer	MSIServer	Manuell	LS
Windows Verwaltungsinstrumentation	winmgmt	Automatisch	LS
Windows Zeitgeber	W32Time	Automatisch	LS
WMI-Leistungsadapter *	WmiApSrv	Manuell	LS

Dabei sind die Dienste, die mit einem Stern versehen sind, erst ab Windows XP implementiert und somit in Windows 2000 standardmäßig nicht vorhanden.

Ein Dienst wird immer über ein Konto angemeldet, damit er auf alle nötigen Ressourcen zugreifen kann. Dabei werden drei verschiedene Benutzerkonten (letzte Spalte in der Tabelle 7; Lokales System LS, Lokaler Dienst LD und Netzwerkdienst ND) verwendet, wobei das erstgenannte die meisten Rechte hat und auch am häufigsten zum Einsatz kommt.

Dienste können entweder automatisch oder manuell gestartet werden oder auch deaktiviert sein. Zusätzlich gibt es noch die Starttypen *Bootstart* und *Systemstart*, die aber nur in der Registrierung eingestellt werden können. Die normalen Einstellungen kann man allerdings in der Computerverwaltung oder bei den Gruppenrichtlinien unter *Computerkonfiguration* → *Windows-Einstellungen* → *Sicherheitseinstellungen* → *Systemdienste* einrichten. Allerdings kann nicht pauschal gesagt werden, welche Dienste laufen sollen und welche deaktiviert werden sollen, weil dies immer systemabhängig ist. Es sollten aber keine Dienste laufen, von denen man sicher weiß, dass sie nicht benötigt werden, und die auch kein anderer Dienst benötigt.

Gespeichert werden die Konfigurationseinstellungen in der Registrierung, und zwar im Ordner *HKEY_LOCAL_MACHINE* → *System* → *CurrentControlSet* → *Services*.

5.3.1.1 Anmeldedienst

Dieser Dienst ist für die sichere Authentifizierung zwischen Computer einer Domäne und dem Domänencontroller verantwortlich. Er wird automatisch gestartet, wenn der Computer Mitglied einer Domäne ist und sollte dann auch nicht deaktiviert werden. Zusätzlich wird dieser Dienst auch bei der Replizierung zwischen zwei Domänencontrollern verwendet. Wenn der Dienst deaktiviert wird, erkennt der Computer den Domänencontroller nicht, und somit kann er sich nicht authentifizieren und funktioniert nicht ordnungsgemäß. Wenn der Laptop kein Mitglied in einer Domäne ist, kann dieser Dienst deaktiviert werden, oder eventuell auf Manuell, wenn er doch in Zukunft einer Domäne beitritt.

5.3.1.2 Arbeitsstation

Mit Hilfe dieses Dienstes werden Netzwerkverbindungen von Clients erstellt und verwaltet. Ausgeschlossen sind davon Verbindungen ins Internet (http-Verbindungen; Hypertext Transfer Protocol). Falls dieser Dienst gestoppt wird, sind keine Verbindungen von Clients zu Servern (z.B. Fileserver, Printserver, usw.) möglich, deswegen sollte dieser Dienst immer laufen.

5.3.1.3 Automatische Updates und Intelligenter Hintergrundübertragungsdienst

Dies ist ein sehr wichtiger Dienst, denn dieser ist für die automatischen Windows Updates zuständig. Wenn dieser Dienst läuft, überprüft das Betriebssystem automatisch das Internet nach wichtigen Updates. Je nach Einstellung werden diese Updates entweder ohne Benachrichtigung heruntergeladen und installiert, oder man wird vor dem Download und der Installation benachrichtigt, und es können auch nur jene Updates heruntergeladen werden und installiert werden, die vom jeweiligen System benötigt werden.

Falls die automatischen Updates deaktiviert sind, und dieser Dienst nicht läuft, können die Updates manuell von der Windows-Update Homepage heruntergeladen und installiert werden (Microsoft Update). Allerdings wird dazu der Internet Explorer ab Version 5.0 benötigt.

Alternativ dazu kann auch ein Server im eigenen Netz auf Updates überprüft werden, wenn WSuS (Windows Server Update Service, siehe Aguiluz 2005) implementiert wurde.

Damit das Betriebssystem allerdings im Hintergrund nach Aktualisierungen suchen kann, muss zusätzlich auch noch der Dienst namens *Intelligenter Hintergrundübertragungsdienst* aktiviert sein. Dabei muss er nicht automatisch gestartet werden, sondern es genügt die Einstellung *manuell*. Hierbei wird bei einer Anforderung (Windows Update wird nach Zeitplan gestartet) der Dienst gestartet, und nach Fertigstellung wieder beendet.

5.3.1.4 DHCP-Client und DNS-Client

Dieser Dienst muss laufen, wenn der Computer seine IP-Adresse automatisch von einem DHCP-Server (Dynamic Host Configuration Protocol) erhalten soll. In einem großen Netzwerk hat das einige Vorteile, unter anderem können keine IP-Adressenskonflikte auftreten, da der Server jede IP-Adresse nur einmal vergibt. Der DHCP-Server kann auch dem Client die IP-Adresse eines DNS-Servers (Domain Name System) mitteilen, wenn am Client dies so konfiguriert ist (*DNS-Serveradresse automatisch beziehen*). Dadurch werden dynamische DNS-Server mit Updates versorgt.

Zusätzlich können DNS-Namen aufgelöst und zwischengespeichert werden, wenn am Client der Dienst DNS-Client läuft. Diese Fähigkeit ist in einer Active-Directory-Umgebung von großer Bedeutung, da somit die Domänencontroller und andere Geräte gefunden und identifiziert werden können.

Um eine IP-Adresse an einen Computer zu binden, ist es sinnvoll Reservierungen vorzunehmen. Dabei erkennt der Server die MAC-Adresse des Clients, sieht in seiner Reservierungstabelle nach, und der Client bekommt immer seine IP-Adresse. Wenn der Dienst deaktiviert wird, muss man die IP-Adresse statisch konfigurieren, und auch das DNS wird nicht mehr automatisch aktualisiert.

5.3.1.5 Drahtloskonfiguration

Dieser Dienst ist für die automatische Konfiguration von unterstützten WLAN-Adaptern zuständig. Heutzutage ist dies ein sehr wichtiger Dienst, weil immer mehr Notebooks mit Hilfe von WLAN arbeiten. Dieser Dienst sollte automatisch gestartet werden, wenn sie eine drahtlose Kommunikation mit WLAN verwenden wollen. Wenn sie WLAN nicht verwenden, kann er auch deaktiviert werden. Genauere Informationen zu WLAN finden sie im Kapitel 4.5.

5.3.1.6 Druckerwarteschlange & Faxdienst

Dieser Dienst wird benötigt, wenn von diesem Rechner aus gedruckt werden soll. Egal ob es sich dabei um einen lokal angeschlossenen Drucker handelt, oder aber um einen Drucker, der über das Netzwerk erreichbar ist. Dieser Dienst sollte automatisch gestartet werden, da ansonsten nicht gedruckt werden kann. Falls ein Notebook allerdings keinen Drucker benötigt, kann dieser Dienst deaktiviert werden.

Allerdings ist der Faxdienst, der standardmäßig nicht installiert wird, von diesem Dienst abhängig. Deswegen muss vorher überprüft werden, ob man die Faxfunktionalität auch nicht benötigt, bevor dieser Dienst deaktiviert wird. Falls der Faxdienst benötigt wird, kann er über die *Systemsteuerung* → *Software* → *Windows Komponenten hinzufügen oder entfernen* → *Faxdienst* installiert werden.

5.3.1.7 Ereignisprotokoll & Systemereignisbenachrichtigung

Auch dieser Dienst sollte laufen, denn er ist für die Ereignismeldungen vom Betriebssystem, von Anwendungen und von Diensten, und deren Einträge in Protokolldateien (Anwendungen, Sicherheit und System) verantwortlich. Da bei einer Problembehandlung ein Durchforsten dieser Protokolldateien sehr sinnvoll ist, sollten auch die wichtigen Einträge darin enthalten sein. Falls dieser Dienst deaktiviert wird, werden wichtige Meldungen vom Betriebssystem nicht mehr in die Protokolldateien geschrieben. Dieser Dienst kann nicht angehalten werden.

Die Systemereignisbenachrichtigung ist für die Überwachung und Weitergabe von Systemereignissen zuständig. Dazu gehören unter anderem auch Benutzeran- und abmeldevorgänge und auch Stromversorgungsereignisse.

5.3.1.8 Fehlerberichterstattungsdienst

Wenn dieser Dienst läuft können Fehlermeldungen vom Betriebssystem oder von anderen Microsoft-Anwendungen übers Internet an Microsoft gesendet werden. Durch diese Informationen kann die Firma Microsoft, wenn nötig Patches entwickeln. Diese können dann wieder mit Hilfe der Updatefunktion am System installiert werden. Dadurch wird die Qualität laufend erhöht.

Unter *Systemsteuerung* → *System* → *Erweitert* → *Fehlerberichterstattung* kann noch genauer eingestellt werden, ob dieser Dienst nur für das Betriebssystem aktiviert wird, oder auch für Programme (eine Liste von Programmen kann angegeben werden). Wenn keine Informationen an Microsoft gesendet werden sollen, muss der Dienst deaktiviert werden.

5.3.1.9 Geschützter Speicher

Dies ist ein sehr wichtiger Dienst und deswegen sollte er immer laufen. Er dient dem Schutz von jenem Speicher, in dem wichtigen Daten, wie zum Beispiel private Schlüssel, abgelegt werden. Damit wird verhindert, dass nicht autorisierte Dienste, Prozesse oder Benutzer an diese Informationen gelangen. Dieser Speicher verwendet HMAC (Hash-Based Message Authentication Code) und die SHA1-Hashfunktion (Secure Hash Algorithm), um den Hauptschlüssel des Benutzers zu verschlüsseln.

5.3.1.10 Infrarotmonitor

Falls ein Notebook einen Infrarotanschluss besitzt, und dieser bei der Installation des Betriebssystems auch erkannt wird, wird dieser Dienst standardmäßig installiert und aktiviert. Mit Hilfe der Infrarotschnittstelle können Daten sehr einfach kopiert werden. Allerdings birgt das auch ein Sicherheitsrisiko. Deswegen sollte genau überlegt werden, welche Schnittstellen zum Datenaustausch verwendet werden dürfen, und alle anderen nicht benötigten Schnittstellen sollten deaktiviert werden.

5.3.1.11 IPSec-Dienste

Mit Hilfe dieses Dienstes kann die Kommunikation zwischen Client und Server geschützt und verschlüsselt werden. Dies ist vor allem dann sehr wichtig, wenn Clients über ein öffentliches Netz wie das Internet auf einen Firmenserver zugreifen (VPN-Verbindung; Virtual Private Network). Genauere Informationen zu IPSec finden sie im RFC 2401.

5.3.1.12 Netzwerkverbindungen & RAS-Verbindungsverwaltung

Der erste Dienst ist für die Konfiguration der Netzwerkverbindungen (LAN-Verbindung, DFÜ-Verbindungen und VPN-Verbindungen) am Client verantwortlich, und muss laufen, wenn über diese Verbindungen kommuniziert werden soll. Zusätzlich zeigt er auch den Status der Verbindung in der Taskleiste an.

Der zweite Dienst hingegen erstellt Netzwerkverbindungen und verwaltet diese auch. Dabei werden DFÜ- und VPN-Verbindungen zwischen einem Computer und einem Remotenetzwerk unterstützt. Wenn keine Verbindungen zu Remotenetzwerken verwendet werden, kann dieser Dienst deaktiviert werden, ansonsten sollte er auf manuell gesetzt werden. Somit wird er bei einer Anforderung gestartet.

5.3.1.13 Plug & Play

Dies ist nicht nur für mobile Computer ein wichtiger Dienst. Mit Hilfe dieses Dienstes können Hardwareänderungen automatisch erkannt und der Benutzer muss dabei wenig oder überhaupt nicht eingreifen. Dadurch wird ein schnelles Hinzufügen und Entfernen von Geräten (z.B. USB-Sticks, usw.) ermöglicht. Dieser Dienst darf nicht deaktiviert werden, weil ansonsten der Computer nicht mehr starten kann.

5.3.1.14 Remoteprozeduraufruf

Dies ist ein sehr wichtiger Dienst, da sehr viele andere Dienste von ihm abhängig sind, und somit muss er immer laufen, denn ohne ihn, könnte nicht einmal das Betriebssystem geladen werden. Er dient auch der sicheren Kommunikation zwischen Prozessen (entweder im LAN oder auch im Internet).

5.3.1.15 Sekundäre Anmeldung

Dieser Dienst ist ebenfalls sehr wichtig und sollte auch laufen. Mit Hilfe dieses Dienstes können Benutzer manche Anwendungen unter einem anderen Benutzerkonto ausführen. Wenn dieser Dienst deaktiviert wird, kann der Befehl *RunAs* (nähere Informationen im Kapitel 2.3.5) nicht mehr ausgeführt werden.

5.3.1.16 Sicherheitskontenverwaltung

Dieser Dienst ist auch als SAM (Security Accounts Manager) bekannt. Er ist für die Verwaltung von Benutzer- und Gruppenkonteninformationen zuständig. Diese Informationen werden in der Registry gespeichert. Dieser Dienst sollte nicht deaktiviert werden, weil somit andere Dienste möglicherweise nicht richtig gestartet werden.

5.3.1.17 Smartcard & Smartcard Hilfsprogramm

Dieser Dienst wird immer bedeutender, da mittlerweile schon viele Notebooks die Authentifizierung mit einer Smartcard unterstützen, und die Benutzer setzen diese Möglichkeit immer häufiger ein. Er verwaltet und steuert den Zugriff auf Smartcards. Wenn keine Smartcards verwendet werden, kann er deaktiviert werden.

Falls ältere Smartcard-Lesegeräte im Einsatz sind, sollte auch der Dienst *Smartcard Hilfsprogramm* gestartet werden. Somit werden auch Geräte unterstützt, die nicht Plug & Play-fähig sind.

5.3.1.18 Telefonie

Mittlerweile wird die IP-Telefonie sehr häufig eingesetzt. Dazu muss dieser Dienst laufen. Aber nicht nur für die IP-Telefonie muss dieser Dienst gestartet sein, auch wenn das Notebook Modemverbindungen benötigt, muss dieser Dienst laufen. Falls keine Modemverbindung benötigt wird, und auch kein Telefoniedienst eingesetzt wird, kann dieser Dienst deaktiviert werden.

5.3.1.19 Windows Firewall/Gemeinsame Nutzung der Internetverbindung

Dieser Dienst wird benötigt, falls man die interne Personal Firewall des Windows Betriebssystem verwenden will. Allerdings gibt es die in Windows 2000 und Windows XP Home nicht. Eine genauere Beschreibung der Windows Firewall finden sie im Kapitel 6.2.1. Mit Hilfe der gemeinsamen Nutzung der Internetverbindung kann der Laptop als eine Art Gateway für andere Computer verwendet werden. Dies wird allerdings nicht sehr oft eingesetzt.

Falls die Windows Firewall verwendet wird, muss auch der Dienst *Gatewaydienst auf Anwendungsebene* laufen, da dieser für die Unterstützung von Plug-Ins von Drittanbietern für die Windows Firewall zuständig ist.

Auch der Dienst *Network Location Awareness* ist erforderlich, wenn die Windows Firewall funktionieren soll. Er sammelt Informationen über die Netzwerkumgebung und gibt diese an Anwendungen weiter.

5.3.1.20 Windows Installer

Dieser Dienst ist für die Verwaltung von Anwendungen zuständig. Dazu gehören die Installation, Deinstallation, Änderungen und Reparaturen. Dabei führt er Anweisungen aus, die in einer *.msi-Datei enthalten sind. Zusätzlich überwacht er auch den Dateizustand und kann bei kleineren Problemen Wiederherstellungen durchführen. Da sehr viele Installationsprogramme den Windows Installer verwenden, sollte dieser Dienst nicht deaktiviert werden.

5.3.1.21 Windows-Verwaltungsinstrumentation

Mit Hilfe dieses Dienstes werden das Betriebssystem, Geräte, Anwendungen und Dienste verwaltet. Ohne ihn könnten viele Anwendungen des Betriebssystems nicht richtig ausgeführt werden und auch die Gruppenrichtlinien werden möglicherweise nicht korrekt angewendet.

5.3.2 Zusätzliche Dienste

Hier werden noch einige zusätzliche Dienste erwähnt, die auf jedem Notebook laufen sollten. Als erstes ist hier der Dienst des Antivirenprogramms zu erwähnen. Dieser Dienst ist für den Echtzeitschutz des Systems verantwortlich. Je nach Programm wird dieser Dienst einen anderen Namen haben, allerdings sollte der Start immer automatisch erfolgen.

Dann sollte auch noch ein Dienst der Personal Firewall am Laptop laufen. Auch hier ist je nach Programm der Name unterschiedlich, jedoch auch hier sollte der Start immer automatisch erfolgen.

5.3.2.1 SNMP-Dienst & SNMP-Trap-Dienst

Falls in einem Unternehmen SNMP verwendet wird (auch für die Überwachung von Laptops, was meiner Meinung nach nicht so sinnvoll ist), muss dieser Dienst laufen, damit eingehende Anforderungen verarbeitet werden können.

5.4 Encryption File System

Um die Sicherheit noch weiter zu erhöhen, sollte man vertrauliche Daten auf seinem Notebook verschlüsseln. Damit kann man auch einen Verlust oder Diebstahl seines Notebooks besser verkraften, da zumindest die Daten geschützt sind, und von Unbefugten normalerweise auch nicht wieder entschlüsselt werden können.

Seit der Version 2000 unterstützt auch Windows die Verschlüsselung von Dateien und Ordnern, allerdings nur, wenn man NTFS (ab Version 5.0) als Dateisystem verwendet. Ausnahme dabei ist die Windows XP Home Edition. EFS ist sehr einfach zu handhaben, weil alles über dir Eigenschaftsseite einer Datei oder eines Ordners konfiguriert werden kann. Und so einfach funktioniert es: Im *Explorer* bei der gewünschten *Datei/Ordner* mit der *rechten Maustaste* auf *Eigenschaften*. Bei den *Dateiattributen* auf *Erweitert*, und dann auf *Inhalt verschlüsseln, um Daten zu schützen* (Abbildung 3).

Abbildung 3: EFS Aktivierung

Unter Windows XP kann man nach einer kleinen Änderung in der Registry dem Auswahlmenü (nach Betätigung der rechten Maustaste) auch direkt den Punkt *Verschlüsseln* hinzufügen, und somit muss nicht mehr der Weg über die Eigenschaftsseite gegangen werden. Dazu ist folgendes zu machen: Unter *Start* → *Ausführen* einfach den Befehl *regedit* eingeben. Dann zum Ordner *HKEY_LOCAL_MACHINE* → *SOFTWARE* → *Microsoft* → *Windows* → *CurrentVersion* → *Explorer* → *Advanced* wechseln und einen *DWORD-Wert* mit dem Namen *EncryptionContextMenu* und dem Wert 1 hinzufügen. Es besteht kein Unterschied, ob der Weg über die Eigenschaftsseite gegangen wird, oder ob direkt der Befehl Verschlüsseln gewählt wird.

Es besteht auch noch die Möglichkeit, die Verschlüsselung über die Eingabeaufforderung zu verwirklichen. Dazu gibt es den Befehl *cipher*. Um mehr Informationen zu diesen Befehl zu erhalten können sie in einer Eingabeaufforderung *cipher /?* Eingeben. Somit kommt man auf die Hilfe-Seite dieses Befehls. Dabei sind die Optionen des Befehls in Windows 2000 und Windows XP unterschiedlich. In der Diplomarbeit wird aber nicht näher darauf eingegangen, weil dieser Weg etwas umständlicher und nicht so benutzerfreundlich ist, und deswegen sehr selten verwendet wird.

Wenn man eine einzelne Datei verschlüsseln will, kommt eine Warnung (siehe Abbildung 4) vom Betriebssystem.

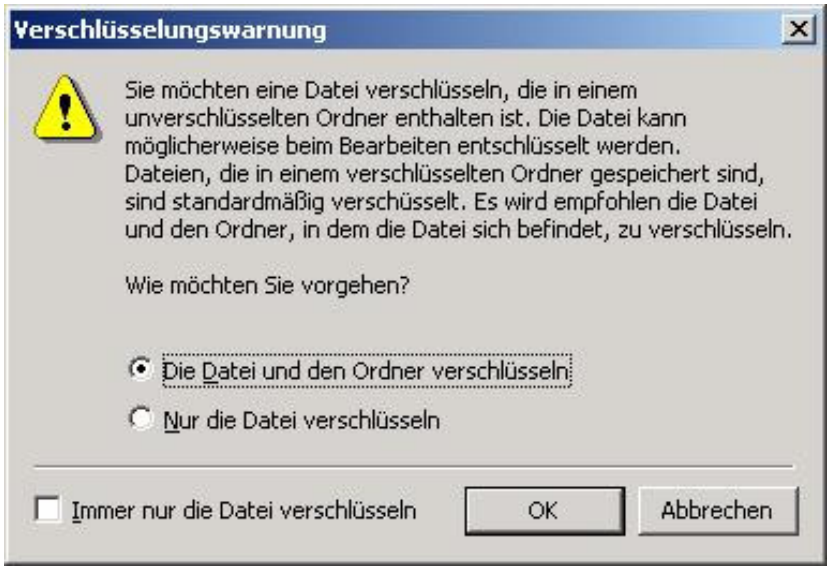

Abbildung 4: Verschlüsselung einer Datei

Die Gefahr, wenn nur die Datei verschlüsselt wird, besteht darin, dass viele Programme bei der Bearbeitung von Dateien temporäre Dateien anlegen, die bei einer nicht ordnungsgemäßen Beendigung des Programms weiterhin bestehen bleiben und möglicherweise entschlüsselt werden können. Da diese Programme die temporären Dateien im selben Ordner erstellt, in dem die Original-Datei liegt, kann dieses Problem umgangen werden, indem der ganze Ordner verschlüsselt wird.

Falls ein Ordner zur Verschlüsselung gewählt wird, kommt noch ein Auswahlmenü (siehe Abbildung 5), bei dem entschieden werden kann, ob auch Dateien in diesem Ordner und Unterordner verschlüsselt werden sollen. Tabelle 8 zeigt die Auswirkungen, wenn nur der Ordner selbst verschlüsselt wird, und Tabelle 9 zeigt die Auswirkungen, falls auch die Dateien und Unterordner verschlüsselt werden.

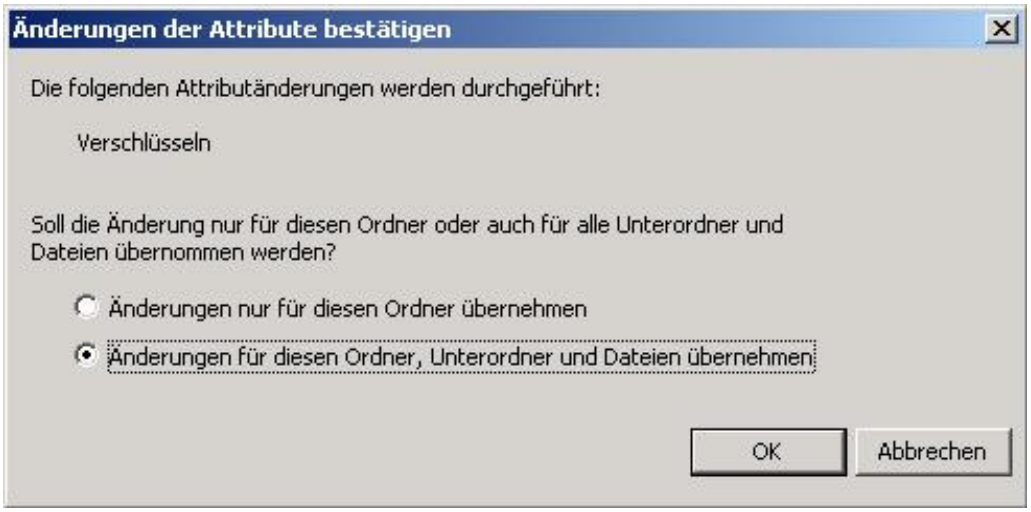

Abbildung 5: Verschlüsselung eines Ordners

Tabelle 8: Auswahl 1 (nur der Ordner wird verschlüsselt)

Beschreibung der Datei	**Status**
Bereits in diesem Ordner oder Unterordner gespeicherte Dateien	Bleiben unverändert, d.h. sie bleiben entweder ver- oder entschlüsselt, je nachdem wie der Status vorher war
Wenn Dateien erst später in diesen Ordner erzeugt oder kopiert werden	Verschlüsselt mit dem FEK (File Encryption Key) des jeweiligen Benutzers
Wenn Dateien erst später in einem Unterordner erzeugt oder kopiert werden	Unverändert
Wenn Dateien erst später in diesen Ordner oder einem Unterordner verschoben werden	Unverändert

Tabelle 9: Auswahl 2 (auch Dateien und Unterordner werden verschlüsselt)

Beschreibung der Datei	**Status**
Bereits in diesem Ordner oder Unterordner gespeicherte Dateien	Wenn man Schreibrechte hat, werden die Dateien mit dem FEK verschlüsselt, wenn nicht, dann bleiben sie unverändert
Wenn Dateien erst später in diesen Ordner oder einem Unterordner erzeugt oder kopiert werden	Verschlüsselt mit dem FEK des jeweiligen Benutzers
Wenn Dateien erst später in diesen Ordner oder einem Unterordner verschoben werden	Unverändert

5.4.1 Technologie

EFS verwendet Public-Key-Verschlüsselung (unterschiedlicher Schlüssel für die Ver- und Entschlüsselung) in Verbindung mit symmetrischer Verschlüsselung (gleicher Schlüssel für die Ver- und Entschlüsselung). Public-Key-Verschlüsselung ist eine asymmetrische Verschlüsselung und dadurch um einiges langsamer als die symmetrische Verschlüsselung. Die Datei wird mit dem FEK ver- und entschlüsselt (symmetrisch). Dieser FEK wird dann selbst mit dem öffentlichen Schlüssel des Benutzerzertifikats verschlüsselt, und an die verschlüsselte Datei angehängt. Zusätzlich werden auch die FEK´s aller Recovery Agenten an das File angehängt. Für die Entschlüsselung des FEK wird der private Schlüssel des Benutzerzertifikats verwendet (asymmetrisch). Dieser private Schlüssel liegt an einem sehr sicheren Ort auf der Festplatte.

5.4.2 Funktionsweise

Falls die Verschlüsselung aktiviert ist, kann der Benutzer trotzdem ganz normal mit den Dateien arbeiten, d.h. die Datei wird automatisch entschlüsselt wenn ich damit arbeite, und danach wieder automatisch verschlüsselt. Es ist keine zusätzliche Passworteingabe erforderlich, weil nach der Anmeldung am System auch die erforderlichen Schlüssel und Zertifikate zur Verfügung stehen. Man benötigt dazu keine Administratorrechte, d.h. jeder Benutzer kann Dateien verschlüsseln, sobald er Schreibrecht darauf hat.

Grundsätzlich darf nur der Benutzer auf die verschlüsselte Datei zugreifen, der sie auch verschlüsselt hat. Noch dazu gibt es einen oder mehrere Recovery Agenten, die ebenfalls Zugriff auf die verschlüsselte Datei haben. Ab Windows XP kann man auch andere Benutzer auf eine verschlüsselte Datei zugreifen lassen. Eine weitere Abhilfe, falls ein anderer Benutzer auf eine verschlüsselte Datei zugreifen will, ist jene, das der Benutzer, der die Datei verschlüsselt hat, seine Schlüssel und Zertifikate anderen Benutzern zur Verfügung stellt. Sollte man aber grundsätzlich vermeiden, denn somit geht ein gutes Stück an Sicherheit verloren.

Unter Windows 2000 wird als Absicherung EFS automatisch deaktiviert, wenn es keinen Recovery Agenten gibt. Dieser wird allerdings normalerweise automatisch erstellt. Bei Windows XP ist das leider nicht mehr der Fall. Hier muss man den Recovery Agent manuell einrichten, und zwar bevor ein User Daten verschlüsselt, weil ein nachträglich erstellter Recovery Agent diese Daten nicht mehr entschlüsseln kann.

Wenn man eine mit EFS verschlüsselte Datei auf ein anderes Dateisystem als NTFS kopiert, geht das Attribut der Verschlüsselung verloren, deswegen sollte man hier sehr vorsichtig sein. Eine Ausnahme sind dabei Backups, hier bleiben die Dateien verschlüsselt.

Eine weitere Absicherung ist folgende. Falls es beim Ver- oder Entschlüsseln zu einem Fehler oder Absturz kommt, gibt es eine Absicherung. Es wird vorher eine Backup Datei erstellt, die nach der erfolgreichen Ver- oder Entschlüsselung wieder gelöscht wird.

Alle anderen Rechte bleiben trotz der Verschlüsselung aber bestehen, d.h. zum Beispiel ein Administrator kann weiterhin Benutzerdateien löschen, auch wenn sie verschlüsselt sind.

5.4.3 Initialverschlüsselung

Die Initialverschlüsselung kann sehr lang dauern, weil beim ersten Mal auch überprüft wird, ob der Benutzer ein gültiges EFS Zertifikat mit dem öffentlichen Schlüssel des Benutzers hat. Wenn er noch kein gültiges Zertifikat hat, fordert EFS eines von einer CA (Certification Authority) an, wenn eine im Netzwerk verfügbar ist, sonst wird eines vom EFS selbst ausgestellt. Solange dann das Zertifikat gültig ist, arbeitet EFS wesentlich schneller, weil dieser Vorgang nicht mehr wiederholt werden muss. Beim normalen Arbeiten mit verschlüsselten Dateien merkt man fast keinen Geschwindigkeitsunterschied und deswegen merkt der Benutzer eigentlich keine Änderungen.

5.4.4 Verschlüsselungsalgorithmen

Windows 2000 verwendet den DESX-Algorithmus für die symmetrische Verschlüsselung und den RSA-Algorithmus für die asymmetrische Verschlüsselung, und konnte aufgrund des schwachen DESX-Algorithmus rasch geknackt werden, worauf die Verwendung eines externen Tools zur Verschlüsselung seiner vertraulichen Daten empfohlen wurde.

Windows XP unterstützt neben DESX auch noch den Algorithmus 3DES. Mit diesem wird die Sicherheit erheblich erhöht, auch wenn die Performance von 3DES nicht gerade die beste ist.

Deswegen wird ab späteren Windows Versionen (Windows Server 2003 und Windows XP ab Service Pack 1) auch noch zusätzlich der Algorithmus AES (Advanced Encryption Standard) unterstützt. Dadurch ist EFS mit AES sehr sicher, und auch die Geschwindigkeit ist besser als bei der früheren Version mit 3DES.

Damit 3DES oder AES verwendet wird, gibt es bei den Gruppenrichtlinien folgenden Eintrag.

Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden.

Alle verwendeten symmetrischen Verschlüsselungs-Algorithmen sind Block-Cipher, d.h. sie teilen die zu verschlüsselnden Daten in Blöcke fester Größe, verschlüsseln diese Blöcke und bringen sie dann wieder in Verbindung miteinander. Wie diese Blöcke genau miteinander verbunden werden wird als *mode of operation* bezeichnet. Bei diesen Algorithmen wird wie fast überall der CBC (Cipher Block Chaining) Modus als Verbindung der einzelnen Blöcke verwendet. Eine nähere Erklärung zu den einzelnen Algorithmen und Operationsmodi findet sie im Anhang.

5.4.5 Verwaltung der Schlüssel

Wenn man eine Datei verschlüsselt, wird dies mit dem FEK erledigt. Dieser wird ebenfalls verschlüsselt und dem File als Header angehängt. Der FEK wird mit dem public key des Benutzerzertifikats und dem public key aus dem Zertifikat des Recovery Agenten verschlüsselt. Diese Schlüssel, und auch die Zertifikate, werden bei den anderen Zertifikaten abgelegt (zu finden unter Internetoptionen → Inhalte → Zertifikate oder auch über das mmc Snap-In Zertifikate).

Zusätzlich sollte man, wenn man das erste Mal eine Verschlüsselung durchgeführt hat, sofort die Schlüssel (vor allem den privaten Schlüssel) des Benutzers und des Recovery Agenten auf Diskette oder einem anderen Speicher sichern, und diese gut verwahren. Der Recovery Agent sollte danach auch seine Schlüssel von der Festplatte löschen, damit keine unbefugten Zugriffe damit vollzogen werden können.

Der Export der Schlüssel erfolgt ganz einfach im Zertifikatsbereich. Dort ein Zertifikat auswählen und auf exportieren. Eine genauere Beschreibung findet man auf der Microsoft Knowledgebase.

5.4.6 Vorteile

- keine Installation notwendig, weil es im Betriebssystem implementiert ist
- gratis
- benutzerfreundlich
- ab Windows XP mit SP sehr sicher aufgrund des Algorithmus AES
- einfaches Erkennen der verschlüsselten Dateien, mittels Attribut E oder ab Windows XP sogar in Farbe gehalten
- ab Windows XP:
    - können auch offline Dateien verschlüsselt werden
    - kann man auch anderen Benutzern den Zugriff erlauben (bei file sharing)

5.4.7 Nachteile

- unter Windows 2000 noch zu unsicher, aufgrund des schwachen Algorithmus DESX
- Verschlüsselung auf Dateiebene, d.h. man muss bei jeder Datei/Ordner einzeln angeben, ob ich verschlüsseln will oder nicht
- Es kann nicht die ganze Festplatte/Partition verschlüsselt werden, weil es einige Ausnahmen gibt (Systemdateien, komprimierte Dateien, usw.)
- Es können auch Dateien verschlüsselt werden, von denen man nicht Besitzer ist. Es reichen folgende Rechte aus (Write Attributes, Create Files/Write Data, und List Folder/Read Data permissions). Wenn man solche Dateien verschlüsselt, kann sie allerdings der Besitzer nicht mehr entschlüsseln, wenn ich ihm nicht meinen private key zukommen lasse. Deswegen Vorsicht wenn man mehrere Ordner, Unterordner und Dateien verschlüsselt (wer ist Besitzer?)
- Es können nur Daten auf einer NTFS Partition verschlüsselt werden, auch von Remote, aber man kann nicht die Daten verschlüsseln, die übers Netzwerk übertragen werden, und man kann auch keine Daten auf Disketten, usw. verschlüsseln

5.4.8 Weitere Produkte

Es gibt auch noch einige andere Produkte zum Thema Festplattenverschlüsselung. Davon werden zwei im Kapitel 6.4 genauer betrachtet und erklärt.

5.5 Software Restriktion

Diese Möglichkeit zur Absicherung von PCs und Notebooks ist erst ab Windows XP und Windows 2003 Server implementiert und fungiert als Teil der Gruppenrichtlinie. Die Software Restriktion ist eine Richtlinie, die Administratoren hilft, jede Software zu identifizieren, beliebig einzuschränken und zu kontrollieren welche Software auf welchen PC laufen darf. Das Positive an dieser Richtlinie ist, das sie vollständig in eine vorhandene Active Directory Struktur eingebunden werden kann (ab Version 2003), aber auch auf Stand-alone Rechnern eingesetzt werden kann. Noch dazu kann man eine feinere Abstimmung auf Benutzerbasis durchführen. Eine nicht bekannte Software, wie zum Beispiel ein Virus, darf nicht installiert und ausgeführt werden.

Dabei gibt es zwei verschiedene Ansätze, die folgendermaßen arbeiten. Entweder man lässt von vorn herein jede Software zu, und schränkt danach mit Regeln ein paar Programme ein (Unrestricted), oder man lässt von vorn herein gar keine Software zu, und erlaubt nachträglich ein paar Programme (Disallowed). Der zweite Weg ist natürlich der zu empfehlende, wenn man auf Sicherheit einen Wert legt.

Es gibt folgende 4 Arten von Regeln:

- Hash (es muss eine ausführbare Datei angeben werden)
- Path (es muss ein Pfad angegeben werden, z.B. Ordner, in dem alle Programme nicht mehr ausgeführt werden dürfen)
- Certificate (ähnlich Hash, aber mit Zertifikaten)
- Zone (je nachdem, wo das Programm heruntergeladen wurde, bis jetzt aber nur für Windows Installer packages *.msi)

5.6 Offlinedateien

Ein sehr wichtiger Punkt bei Notebooks ist die Speicherung der Daten. Normalerweise sollten keine Daten lokal gespeichert werden, oder zumindest keine wichtigen Geschäftsdaten. Der große Vorteil von Notebooks ist aber die Mobilität, und somit wollen die Mitarbeiter von überall auf ihre Daten zugreifen und somit werden viele Daten lokal abgespeichert. Der beste Weg, damit nicht mehrere verschiedene Versionen von Dateien (lokal und am Server) entstehen, bietet das Betriebssystem Windows mit den Offlinedateien. Hier kann von allen beliebigen Daten am Server eine lokale Kopie erstellt werden, welche sich bei der nächsten An- bzw. Abmeldung im Netzwerk mit den Daten am Server synchronisieren. Somit hat man ein sicheres Backup, da die Daten am Server ja gesichert werden, und es entstehen auch keine verschiedenen Versionen. Der einzige Nachteil dabei ist, dass die Daten am Notebook nicht immer verschlüsselt sind und somit bei Diebstahl des Notebooks einigermaßen leicht ausgelesen werden können. Erst ab Windows XP können diese Offlinedateien auch mit Hilfe von EFS verschlüsselt werden.

5.7 Weitere Hinweise

In diesem Abschnitt werden wieder andere wichtige Hinweise erwähnt, um ein Windows System noch weiter abzusichern.

Wichtig ist es auch, hin und wieder die Registry zu säubern (dazu gibt es genügend Tools, da die manuelle Säuberung zu gefährlich und unübersichtlich ist), oder das System auch einmal neu aufzusetzen, wenn häufig Software installiert und deinstalliert wird.

Es sollten auch nicht benötigte Ports gesperrt werden, da diese wieder einen Angriffspunkt bilden.

Weiters sollten nicht zu viele Freigaben vorhanden sein, vor allem wenn man nicht genau weiß, wer darauf zugreifen soll und darf.

Bei Windows ist die Anmeldung mit dem Domänenkonto auch dann möglich, wenn keine Netzwerkverbindung besteht, und somit kein Domänencontroller erreichbar ist.

Der Grund dafür ist jener, dass Windows die Anmeldeinformationen (in einer nicht umkehrbar verschlüsselten Form) lokal abspeichert, nachdem der Benutzer sich einmal erfolgreich am Domänencontroller authentifiziert hat. Dies ist für Notebook-Benutzer sehr sinnvoll, weil sie sich überall mit dem Domänenkonto anmelden können, und es muss kein eigener lokaler Benutzer angelegt werden.

5.8 Zusammenfassung

In diesem Kapitel wurde zuerst das grundlegende Sicherheitskonzept von aktuellen Windows Betriebssystemen beschrieben und erklärt. Danach wurde auf die wichtigsten Einstellmöglichkeiten der Gruppenrichtlinien näher eingegangen. Hierbei wurden auch einige Empfehlungen abgegeben, wobei aber jeder Administrator selbst entscheiden muss, welche Punkte er für sein System beachten muss.

Ein weiterer sehr wichtiger Punkt in diesem Kapitel waren die Dienste, die normalerweise auf einem Windows-System laufen. Auch hier muss wieder jeder Administrator selbst entscheiden, welche Dienste er wirklich benötigt. Alle Dienste die nicht benötigt werden, sollten deinstalliert oder zumindest deaktiviert werden.

Ab der Version 2000 bietet Windows auch die Möglichkeit die Daten auf dem System zu verschlüsseln. Dazu ist EFS im Betriebssystem implementiert, und sollte auch verwendet werden, falls man nicht andere Methoden zur Verschlüsselung der Dateien auf dem System verwendet. Da EFS einige Nachteile hat, werden andere Alternativen im Kapitel 6.4 beschrieben.

Zum Schluss wurden noch die Punkte der Software Restriktion und die Verwendung von Offlinedateien erklärt, die ebenfalls ein wichtiger Schritt für die Notebook-Benutzer sind.

6 Anwendungen

Bei den Anwendungen gibt es eine Vielzahl die dabei helfen, sein Notebook besser zu schützen. Die wichtigsten werden in den nachfolgenden Punkten erwähnt.

6.1 Anitivirus

Die größte Gefahr geht derzeit von Viren, Trojanern (genauer Trojanische Pferde) und Würmern aus. Deshalb sollte auf jedem Rechner ein Antivirusprogramm installiert sein, und das System ständig zu kontrollieren. Dazu gehören auch die laufende Untersuchung von Internetdownloads, E-Mail-Anhänge aber auch Dateien auf CD-ROMs oder Disketten nach Viren. Dabei kann ein Antivirusprogramm Viren, Trojaner und Computerwürmer aufspüren, blockieren und eventuell auch beseitigen.

Dabei werden heute oft die Begriffe Viren, Trojaner und Würmer nicht mehr unterschieden, obwohl sie von der Infektionsweise sehr unterschiedlich sind. Dazu kurz eine Erklärung der Begriffe (siehe Wikipedia 2006).

6.1.1 Virus

Ein Virus kopiert sich immer in nicht infizierte Dateien, welche ihm als Wirt dienen, wie auch ein Virus in der Medizin. Der Virus verwendet dabei die Ressourcen des Wirtes und schadet ihm dabei. Die Vermehrung ist meistens unkontrolliert, und kann nur mit Hilfe des Wirtes erfolgen. Alleine hat ein Virus keine Schadfunktion und kann sich auch nicht verbreiten, er kann sich nur in eine nicht infizierte Datei kopieren Je nach Virus wird beim Aufruf des infizierten Programms entweder sofort oder später eine Schadfunktion ausgeführt. Die Verbreitung des Virus erfolgt durch das Kopieren der infizierten Datei auf andere Systeme. Viren sind aber heutzutage nicht mehr so verbreitet. Die Vorherrschaft der Schädling liegt derzeit eindeutig bei den Würmern, der sich durch die Vernetzung sehr rasch auf eine große Anzahl von Systemen verbreiten kann.

6.1.2 Trojaner

Trojaner sind Computerprogramme, die sich hinter einer nützlichen Funktion oder einen bekannten Dateinamen verstecken. Im Gegensatz zu Viren, die dem System Schaden zufügen und somit entdeckt werden, ist die Absicht eines Trojaners unerkannt zu bleiben. Ein Trojaner muss keine Schadensfunktion haben, es genügt schon, wenn ein Programm eine versteckte Funktion besitzt, die nicht öffentlich bekannt ist. Viele Trojaner installieren aber ein eigenständiges schädliches Programm auf dem Rechner, wie zum Beispiel Backdoor-Programme oder auch Programme, die die Tastatureingaben mitprotokollieren. Da hilft auch ein nachträgliches Entfernen des Trojaners nichts, weil das schädliche Programm trotzdem noch installiert ist, und eigenständig entfernt werden muss. Die Verbreitung der Trojaner erfolgt gewissermaßen durch die Bekanntheit der nützlichen Funktion oder Dateinamens hinter dem sich der Trojaner versteckt. Viele Benutzer laden sich diese Programme selbst aus dem Internet runter, ohne zu ahnen, was sie hier eigentlich herunter geladen haben. Trojaner können sich aber auch mit Hilfe von Computerwürmern verbreiten.

6.1.3 Wurm

Ein Computerwurm ist ein Programm, welches sich über Netzwerke wie das Internet verbreitet. Meistens ist er in E-Mail-Anhängen versteckt, und versendet sich nach Infektion eines Systems selbst weiter. Mittlerweile gibt es auch schon Handywürmer (siehe Wikipedia 2006, Computerwurm), die sich über MMS (Multimedia Messaging Service) oder auch über Bluetooth verbreiten. Ein Computerwurm muss zwar am System selbst keinen Schaden anrichten, aber durch die sehr rasche Verbreitung kann er Netzwerke, vor allem Engpässe an Routern oder Firewalls, lahm legen.

6.1.4 Funktionsweise von Antivirus-Programmen

Jeder Virusscanner hat eine Virendefinitionsliste, in der bekannte Virenmuster und auch Muster anderer schädlicher Software gespeichert sind. Die Virenscanner vergleichen dann diese Muster mit den zu untersuchenden Dateien. Dadurch können neue Viren nicht erkannt werden, da das Virenprogramm das neue Muster noch nicht kennt. Deswegen ist es erforderlich, die Virendefinitionsliste immer auf dem neuesten Stand zu halten.

Die meisten Antivirenprogramme bieten die Möglichkeit des Echtzeitscan, bei welchem der Virenwächter ständig im Hintergrund als Dienst läuft, und laufend alle Dateien untersucht, die auf die Festplatte geschrieben werden oder auch von dort gelesen werden. Durch diese Funktion konnte es früher zur Verlangsamung des Systems kommen, ist aber heutzutage nicht mehr relevant und bemerkbar. Um das System nicht zu bremsen wird beim Echtzeitscan nicht so genau gescannt, wie bei einer vollständigen Systemprüfung.

Eine vollständige Systemprüfung arbeitet wesentlich genauer, und dauert dementsprechend auch einiges an Zeit. Allerdings sollten vollständige Scan des Öfteren durchgeführt werden, und man sollte sich nicht nur auf den Echtzeitscan verlassen. Diese müssen aber manuell vom Benutzer gestartet werden.

So gut wie jeder Virenscanner bietet eine automatische Updatefunktion, die auch in einen meist vorhandenen Zeitplan eingebaut werden sollte, damit der Virenscanner alle Updates von Virendefinitionen und auch des Programms selbst schnellstmöglich erhält. Wenn ein Antivirusprogramm nicht laufend aktualisiert wird, bietet es nicht wesentlich mehr Schutz als wenn gar kein Virenprogramm installiert ist.

6.2 Firewall

Zu unterscheiden sind hier Hardware-Firewalls, wie sie zum Beispiel in Unternehmen zum Einsatz kommen, und Software-Firewalls, die eher im privaten Bereich zum Einsatz kommen und auch Personal Firewalls genannt werden. Mit Hilfe von Firewalls kann der Internetverkehr eingeschränkt und genau kontrolliert werden. Da für Notebooks nur Software-Firewalls relevant sind, wird hier auf die Beschreibung von Hardware-Firewalls verzichtet. Als Prinzip jeder Firewall, auch der Hardware-Firewall, sollte gelten: „Was nicht ausdrücklich erlaubt wird, ist verboten."

Wenn eine Firewall auf einem Notebook installiert wird, und danach verbindet sich das Notebook zum ersten Mal mit dem Internet, kommen sehr viele Anfragen ob gewisse Programme und Prozesse sich mit dem Internet verbinden dürfen. Nach einer Prüfung, können diese Anfragen permanent erlaubt werden. Somit entfällt der ständige Verwaltungsaufwand, und nach einiger Zeit läuft die Firewall ohne sich zu melden. Dies ist zumindest der Idealfall, denn somit finden keine unerlaubten Angriffe statt, oder zumindest werden sie nicht bemerkt, was wiederum nicht so gut wäre.

6.2.1 Windows Firewall

Ab Windows XP ist bereits in das Betriebssystem eine Firewall, namens Internetverbindungsfirewall (ICF, Internet Connection Firewall), implementiert, die ab Service Pack 2 auch für viele Anwender ausreichend ist. Allerdings hat man als erfahrener Benutzer zu wenige Einstellmöglichkeiten und deswegen werden häufig noch andere Programme verwendet und die Windows Firewall deaktiviert. Ein Nachteil davon ist, dass der ausgehende Verkehr nicht gefiltert werden kann. Noch dazu können die eingestellten Regeln nicht mit Hilfe von Skripts oder Gruppenrichtlinien auf mehrere PCs verteilt werden.

Allerdings gibt es ein eigenes Profil für PCs, welche sich in einer Domäne befinden. Dieses Profil ist nicht ganz so restriktiv wie das normale Profil, und kann in kleineren Unternehmen ausreichen. Aber auch dies ist mit Vorsicht zu genießen.

6.3 Webbrowser

Damit die Benutzer im Internet surfen können, benötigen sie einen Webbrowser. In sehr vielen Unternehmen wird der im Betriebssystem implementierte Microsoft Internet Explorer verwendet. Im privaten Bereich ist der Firefox von Mozilla sehr beliebt. Ein Browser sollte benutzerfreundlich sein, möglichst schnell arbeiten und auch auf die Sicherheit sollte großer Wert gelegt werden. Denn heutzutage geht die meiste Gefahr vom Internet aus. Ob es nun beim täglichen surfen ist, oder auch beim Öffnen von E-Mail-Anhängen.

6.3.1 Microsoft Internet Explorer

Der von Microsoft entwickelte Internet Explorer ist seit Windows 98 im Betriebssystem implementiert und erreicht dadurch sehr hohe Marktanteile. Allein die Tatsache, dass er ohne Installation und gratis auf sehr vielen Rechnern verbreitet ist, genügt schon, dass er so häufig verwendet wird. Deswegen sollten die Möglichkeiten zur Absicherung genau betrachtet werden. Ich beziehe mich in meiner Arbeit auf die Version 6 des Internet Explorer, weil die neueste Version 7 erst als Betaversion erhältlich ist.

Um zu den relevanten Konfigurationsmöglichkeiten zu kommen muss im Internet Explorer unter dem Menü *Extras* → *Internetoptionen* gewählt werden.

Unter der Registerkarte *Allgemein* findet man bereits die ersten Einstellmöglichkeiten, die für die Sicherheit relevant sind. Und zwar sind dies die *temporären Internetdateien*. Mit Hilfe dieser Dateien werden Webinhalte, wie Bilder, lokal gespeichert, damit beim nächsten Besuch der gleichen Seite, diese schneller geladen wird. Bei den *Einstellungen* kann man die Cachegröße definieren, das heißt wie viel Platz auf der Festplatte für die temporären Internetdateien verwendet wird. Früher, bei langsamen Internetverbindungen, war es sinnvoll, große Werte zu wählen, damit möglichst viel lokal gespeichert wird. Dies ist bei den schnellen Internetverbindungen von heute nicht mehr nötig, denn durch die temporären Dateien kann das Surfverhalten der Benutzer ausspioniert werden.

Eine weitere Möglichkeit, das Surfverhalten von Benutzern zu kontrollieren bietet der so genannte *Verlauf*. Hier werden alle Webseiten angezeigt, die in den letzten „x“ Tagen, je nach Einstellung, besucht wurden. Falls ein Benutzer verhindern möchte, das andere Personen, die Zugriff auf sein Benutzerkonto haben, sein Surfverhalten einsehen können, sollte er von Zeit zu Zeit die temporären Internetdateien und auch den Verlauf löschen.

Die nächste interessante Registerkarte ist die *Sicherheit*. Hier gibt es vier vordefinierte Zonen, und zwar *Internet, Lokales Intranet, Vertrauenswürdige und Eingeschränkte Sites*. Beim normalen Surfen befindet man sich in der Internetzone, welche durch einen Schieberegler, oder auch manuell über *Stufe anpassen*, sicher konfiguriert werden kann. Hier sind vor allem die ActiveX-Steuerelemente mit Vorsicht zu genießen, und deswegen sollten sie auch deaktiviert werden (nur in Ausnahmefällen zulassen). Wenn gewünscht können einzelne Webseiten als vertrauenswürdig oder eingeschränkt eingestuft werden, und für diese Seiten kann die Sicherheitsstufe angepasst werden, ohne die Einstellungen der anderen Stufen zu ändern. Die Zone *lokales Intranet* ist zuständig für lokal gespeicherte Webseiten und für Zugriff auf Rechner im eigenen Netzwerk.

Unter der Registerkarte *Datenschutz* gibt es noch einen Popup-Blocker, der sie heutzutage vor lästigen Popups, wie zum Beispiel Werbefenster, usw., schützt. Falls Seiten geblockt werden, die sie aber sehen möchten, können Ausnahmeregelungen konfiguriert werden.

Für den Internet Explorer gibt es zusätzlich auch die Möglichkeit über die Gruppenrichtlinien einige wichtige Einstellungen vorzunehmen, damit sie auf allen Computern in einer Domäne identisch sind. Zu finden sind diese Einstellungen unter *Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Internet Explorer.* Zusätzlich gibt es auch noch benutzerspezifische Einstellungen, die unter *Benutzerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Internet Explorer* zu finden sind. Genauere Informationen dazu unter im Windows XP Sicherheitshandbuch (Microsoft 2004).

6.3.2 Mozilla Firefox

Mozilla Firefox wird im privaten Bereich immer häufiger eingesetzt. Vor allem die benutzerfreundliche Oberfläche, und die Tatsache, dass er auf verschiedensten Betriebssystemen (Windows, Linux, Solaris, MacOS) läuft, machen ihm zu einer sehr guten Alternative zum Internet Explorer von Microsoft. Dieser Open-Source-Browser kann kostenlos aus dem Internet heruntergeladen werden, und ist auch in mehreren Sprachen erhältlich. Durch die ständige Weiterentwicklung gibt es häufige Updates, die jeder Benutzer auch regelmäßig installieren sollte. Dazu gibt es natürlich ein automatisches Update-Service.

Ähnlich wie beim Internet Explorer die Internetoptionen gibt es auch beim Firefox einen Menüpunk, wo alle sicherheitsrelevanten Aspekte konfiguriert werden können. Dazu geht man im Menü auf *Extras* → *Einstellungen*.

Unter *Datenschutz* gibt es die erste Registerkarte *Chronik*, die wie der Verlauf beim Internet Explorer, eine Auflistung von früher besuchten Webseiten ist. Auch hier können wieder die Tage angegeben werden, wie lange die Seiten in der Chronik hinterlegt werden. Beim Firefox gibt es zusätzlich auch noch eine Download-Chronik, um Dateien zu sehen, die kürzlich heruntergeladen wurden, je nachdem welche Einstellung getroffen wird.

Als nächstes gibt es die Registerkarte *Gespeicherte Formulardaten*. Bei Aktivierung dieses Punktes werden die Daten gespeichert, die sie in irgendwelche Felder auf Internetseiten eingegeben haben. Wenn sie zum Beispiel bei Google nach gewissen Suchbegriffen suchen, merkt sich der Browser diese Daten, und wenn sie wieder einmal nach denselben Begriffen suchen möchten, können sie diese schnell auswählen.

Die Registerkarte *Passwörter* ist mit Vorsicht zu genießen. Hier könnten bei Aktivierung verschiedenste Passwörter gespeichert werden, um nicht bei jedem Besuch gewisser Seiten immer Benutzername und Passwort eingegeben werden müssen. Allerdings sollten Passwörter nie lokal gespeichert werden, außer diese gespeicherten Passwörter sind selbst auch noch einmal geschützt. Firefox bietet dazu das so genannte *Master-Passwort*, mit dem genau dieser Zweck erfüllt wird.Damit muss pro Internetsitzung nur mehr ein Passwort, und zwar das Master-Passwort, eingegeben werden. Alle anderen Passwörter liegen verschlüsselt auf der Festplatte, und müssen nicht immer eingegeben werden.

Die nächste wichtige Registerkarte ist der *Cache*. Der Cache ist das Gegenstück zu den temporären Dateien beim Internet Explorer. Auch hier kann wieder die Größe des Speichers angegeben werden, der für die Daten reserviert wird.

Nach dem *Datenschutz* gibt es noch *Inhalt*. Hier gibt es auch einen Popup-Blocker, bei dem natürlich auch wieder Webseiten ausgenommen werden können, denn auf manchen Seiten werden die Popups benötigt.

6.4 Verschlüsselung

Um die Sicherheit noch weiter zu erhöhen, sollte man vertrauliche Daten auf seinem Notebook verschlüsseln. Damit kann man auch einen Verlust oder Diebstahl seines Notebooks besser verkraften, da zumindest die Daten geschützt sind, und von Unbefugten normalerweise auch nicht wieder entschlüsselt werden können. Die Verschlüsselung wird ein immer wichtigeres Thema, und im nächsten Abschnitt wird eine Alternative zum EFS von Windows vorgestellt.

6.4.1 Truecrypt

Die Verschlüsselungssoftware Truecrypt ging Anfang 2004 aus dem Projekt E4M (Encryption for the masses) hervor und gilt als sehr gute Alternative zum EFS von Windows 2000. Es wurde seitdem stetig weiter entwickelt und gilt als sehr sicher. Unter anderem wird es auch von der Computerzeitschrift c´t empfohlen (siehe Beier 2005).

6.4.1.1 Installation

Im Gegensatz zum EFS von Windows ist hier eine Installation notwendig, die allerdings sehr einfach durchzuführen ist. Am besten lädt man sich die aktuelle Version des Programms von der Download-Rubrik der Homepage des Herstellers (siehe Truecrypt). Hier erhält man eine ZIP-Datei die entpackt werden muss, und danach kann man das Setup-Programm ausführen. Auf der Startseite findet man die üblichen Einstellmöglichkeiten bei einer Installation eines Programms. Danach dauert die Installation nicht sehr lange.

Zusätzlich findet man in der ZIP-Datei ein Benutzerhandbuch, in dem alle wichtigen Einstellungen beinhaltet sind, und welches man sich vor der ersten Benützung des Programms durchlesen sollte.

6.4.1.2 Einrichtung

Nach der Installation muss erstmal die Arbeitsumgebung eingerichtet werden. Dazu muss im ersten Fenster (Abbildung 6) der Befehl *Create Volume* ausgewählt werden.

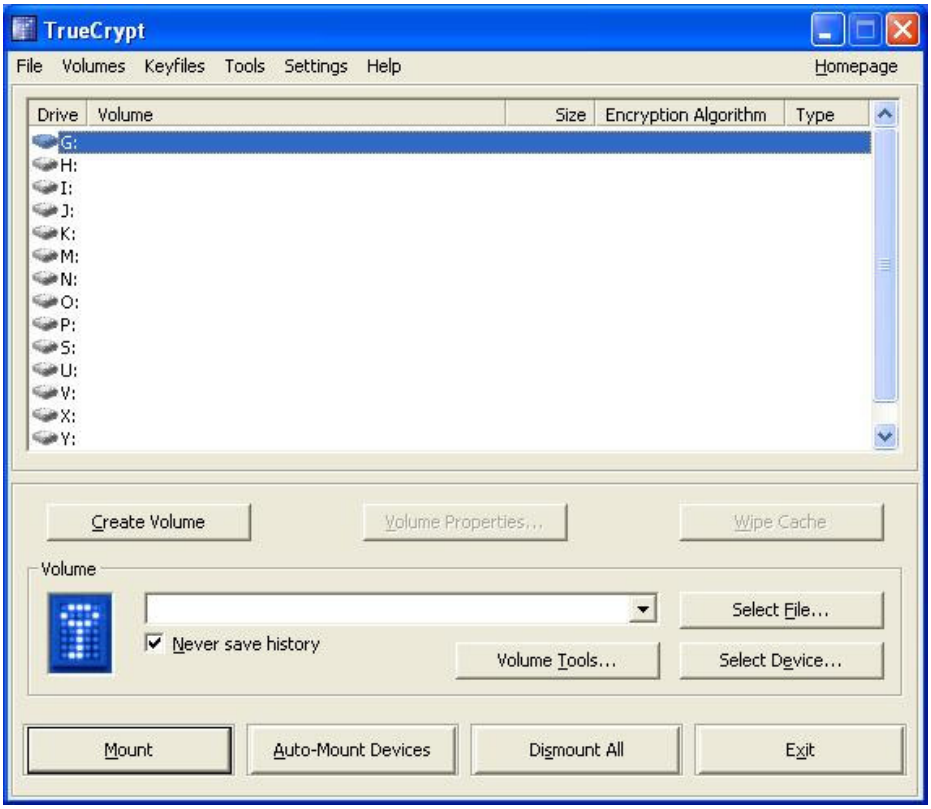

Abbildung 6: Truecrypt Hauptfenster

Danach hat man die Möglichkeit ein Standard Volume oder ein Hidden Volume zu erzeugen. Normalerweise genügt es, wenn man hier Standard wählt, aber die grundsätzliche Möglichkeit, ein Volume auch zu verstecken ist eine feine Einstellmöglichkeit. Das Hidden Volume wird dabei im freien Speicher eines Standard Volumes versteckt. Allerdings funktioniert das nur, wenn man es in einem FAT Standard Volume versteckt, da man hier den freien Speicher besser reservieren kann als beim NTFS. Eine genauere Beschreibung des Hidden Volume findet man im Benutzerhandbuch.

Jetzt wird noch der Speicherort, der Verschlüsselungs- und auch Hash-Algorithmus, und die Größe die für das Volume reserviert wird, ausgewählt.

Zu guter letzt wird noch ein Passwort angegeben, mit welchen das Volume geschützt wird, und welches Dateisystem verwendet werden soll. Dann wird noch ein Random-Pool durch Bewegungen des Mauszeigers erzeugt, mit dem Pool wird unter anderem der freie Speicher des Volumes aufgefüllt, damit kein Angreifer weiß, ob und wie viele Daten sich im Volume befinden. Somit ist das Volume fertig gestellt und man kann damit arbeiten.

Im Fenster der Abbildung 6 wird nun ein beliebiger Laufwerksbuchstabe ausgewählt (es werden alle freien Laufwerksbuchstaben angezeigt), und danach der Befehl *Select File* ausgewählt. Hier wird das zuvor erstellte Volume ausgewählt. Nach Eingabe des Passworts geht man auf *Mount*, und das Laufwerk kann verwendet werden.

Jetzt hat man das Volume mit einem Laufwerksbuchstaben in Verbindung gebracht, und man kann jetzt auf dieses Laufwerk zugreifen, als wenn es ein lokales Laufwerk wäre. Es wird alles verschlüsselt, was in diesem Laufwerk abgelegt wird. Der Benutzer, der diese Verknüpfung eingetragen hat, kann ganz normal mit dem Laufwerk arbeiten, andere Benutzer sehen das Laufwerk nicht. Dabei arbeitet alles völlig benutzertransparent, denn alle Daten werden automatisch ver- oder entschlüsselt, je nachdem ob sie gespeichert oder geöffnet werden. Es können sogar Programme in diesem Laufwerk installiert werden, und es funktioniert alles so, als wäre es eine normale Partition, nur ist eben alles verschlüsselt. Die Ver- und Entschlüsselung findet dabei immer im RAM statt.

6.4.1.3 Volumes

Es gibt zwei verschiedene Arten von Volumes, die in den nächsten Abschnitten genauer erklärt werden. Bei beiden Arten kann man Standard Volumes oder Hidden Volumes erstellen. In einem Standard Volume können, nachdem es gemountet wurde, Daten gespeichert werden, Programme installiert werden, usw. Es arbeitet wie eine normale Partition. Ein Hidden Volume kann man in einem Standard Volume verstecken, und je nachdem, welches Passwort ich beim mounten eingebe, dieses Volume (Standard oder Hidden) wird dann gemountet.

- File-hosted

  Ein File-hosted Volume ist eine normale Datei, die auf allen möglichen Speichermöglichkeiten (Festplatte, USB-Stick, usw.) liegen kann. Diese Datei beinhaltet eine vollständig verschlüsselte virtuelle Partition.

- Partition/Device hosted

  Dies ist eine richtige Partition, die ebenfalls vollständig verschlüsselt werden kann. Man kann auch ganze Festplatten, USB-Sticks, Disketten, usw. vollständig verschlüsseln. Allerdings sollten sich davor keine Daten auf der Partition befinden, da diese verloren gehen. Für diese Art von Volumes benötigt man allerdings Administrator Rechte.

6.4.1.4 Verschlüsselungsalgorithmen

Folgende Algorithmen werden unterstützt. Wenn man auf Geschwindigkeit einen großen Wert legt, kann ein Benchmark-Test durchgeführt werden. Je nach Ergebnis des Tests kann dann ein Algorithmus gewählt werden. Allerdings sollte nicht die Geschwindigkeit das ausschlaggebende Kriterium sein, sondern die Bekanntheit des Algorithmus, und die Schlüssellänge.

Verschlüsselungsalgorithmen:

- AES (256bit Schlüssel, 128bit Block)
- Blowfish (448bit Schlüssel, 64bit Block)
- CAST5 (128bit Schlüssel, 64bit Block)
- Serpent (256bit Schlüssel, 128bit Block)
- 3DES (3*56 = 168bit Schlüssel, 64bit Block)
- Twofish (256bit Schlüssel, 128bit Block)
- Mischformen aus den obigen Algorithmen

Auch bei diesem Programm wird bei jedem Algorithmus der CBC-Modus verwendet.

Hash-Algorithmen:

- RIPEMD-160
- SHA-1
- Whirlpool

6.4.1.5 Vorteile

- Gratis
- benutzerfreundlich (einfache Installation, und nach der Einrichtung, die sehr schön im Benutzerhandbuch beschrieben ist, auch völlig benutzertransparent)
- es werden sehr viele Betriebssysteme unterstützt (Windows 2000, 2003, XP und auch einige Linux Varianten)
- man kann auch externe Geräte wie USB-Sticks, Disketten, usw. verschlüsseln
- sehr gute Auswahl von Verschlüsselungsalgorithmen
- Möglichkeit eines Hidden Volume (kann auch geschützt werden, vor überschreiben von outer/standard Volume)
- im normalen Betrieb benötigt man keine Administratorrechte, nur bei der Installation und bei manch anderen Funktionen (Partition hosted volumes)
- auch per command line verfügbar, allerdings nicht so einfach wie bei der graphischen Oberfläche (sehr nützlich zum erstellen von kleinen Skripts für das Mounten von Laufwerken bei der Benutzeranmeldung)
- es gibt auch einen Traveller Modus, bei dem keine Installation notwendig ist, allerdings erfordert dieser Administratorrechte

6.4.1.6 Nachteile

- Installation notwendig, aber nicht kompliziert
- keine Verschlüsselung einer bereits vorhandenen Partition ohne Datenverlust (kann man aber vorher wegsichern, und danach in die verschlüsselte Partition verschieben)
- keine Verschlüsselung der Windows Partition (normalerweise C)
- Nach jeder Anmeldung muss man sein Volume erneut mounten, damit man damit arbeiten kann (man kann aber ein Skript schreiben, welches bei der Anmeldung läuft und automatisch die Volumes mountet, oder die gemounteten Volumes als Favoriten speichern, und diese beim nächsten mal mounten

6.4.2 Secure Notebook

Secure Notebook ist ein weiteres Produkt zur Verschlüsselung von Festplatten (Partitionen), und wird in Österreich von der Firma mki Technologie und Dienstleistungs GmbH vertrieben (mkitech 2006). Es können nicht nur Festplatten verschlüsselt werden, sondern auch andere Medien, wie zum Beispiel USB-Sticks oder PCMCIA Geräte. Dieses Produkt ist kostenpflichtig, allerdings gibt es Testversionen, die einem von der oben genannten Firma zur Verfügung gestellt werden.

6.4.2.1 Installation

Auch bei diesem Programm ist zuerst eine Installation notwendig, die allerdings relativ einfach und benutzerfreundlich ist. Bei der Installation muss eine Partition angegeben werden, von der das Programm ca. 100MB verwendet (siehe Abbildung 7). Darin wird ein neuer MBR (Master Boot Record) erstellt, und ein eigenes SBS (Secure Boot System) wird erstellt, welches später vor dem Betriebssystem geladen wird. Beim Laden des SBS wird ein Passwort abgefragt, welches eingegeben werden muss, oder auf einer Smartcard gespeichert ist.

Abbildung 7: Secure Notebook Installation

Danach wird ein Passwort vergeben, welches bei der Konfiguration des Programms benötigt wird. Nach der Installation befindet sich in der Systemsteuerung ein eigener Punkt namens *SECUDE Secure Notebook*. Ohne das Passwort kann nicht auf diesen Punkt zugegriffen werden.

Bei der Installation sollte auch eine ERD (Emergency Recovery Disc) erstellt werden, die im Falle des Falles verwendet werden kann, um auf die verschlüsselte Festplatte zugreifen zu können.

6.4.2.2 Funktionsweise

Wenn nach der Installation der Punkt *SECUDE Secure Notebook* in der Systemsteuerung aufgerufen wird, gelangt man zu den in Abbildung 8 gezeigten Kontrollcenter des Programms.

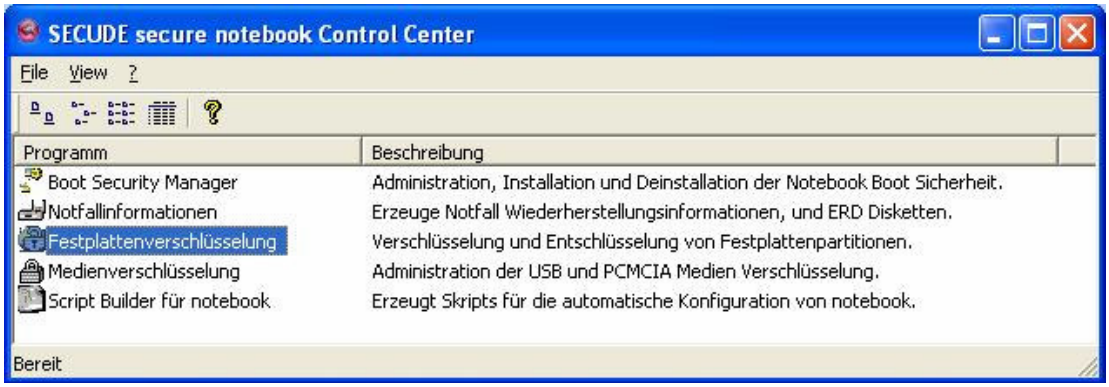

Abbildung 8: Secure Notebook Kontrollcenter

Der wichtigste Punkt hier ist die *Festplattenverschlüsselung*. Hierzu wird das bei der Installation vergebene Passwort benötigt. Danach wird die zu verschlüsselnde Partition ausgewählt. Allerdings können nur NTFS-Partitionen verschlüsselt werden. Dann kann noch eingestellt werden, ob die gesamte Partition verschlüsselt werden soll (Empfehlung), oder ob nur die verwendeten Bereiche verschlüsselt werden sollen. Anschließend werden noch der zu verwendende Verschlüsselungsalgorithmus und die Schlüssellänge ausgewählt. Jetzt kann noch ein Passwort vergeben werden, welches vor der Entschlüsselung wieder eingegeben werden muss.

Es handelt sich um einen offline Schutz, d.h. falls das System nicht über das SBS geladen wird, sind die Daten verschlüsselt, und können somit nicht eingesehen werden. Wenn das System normal übers SBS geladen wird, merken die Benutzer keinen Unterschied.

Zusätzlich zu der Festplattenverschlüsselung werden von der Firma noch weitere Produkte angeboten (z.B. Single SignOn), welche nachträglich implementiert werden können. Die einzelnen Produkte sind modular aufgebaut und arbeiten sehr gut zusammen. Man könnte zum Beispiel den Schlüssel für das SBS auf einer Smartcard speichern, die dann bei jedem Systemstart benötigt wird. Zusätzlich könnten auf dieser Smartcard alle erforderlichen Daten fürs Single SignOn gespeichert werden.

6.4.2.3 Verschlüsselungsalgorithmen

Dieses Programm unterstützt folgende Verschlüsselungsalgorithmen, wobei jeder Algorithmus im CBC Modus arbeitet.

- AES
- Blowfish
- DES
- DESX
- XOR

Je nach Verschlüsselungsalgorithmus kann man eine Schlüssellänge angeben, und je nachdem beansprucht die Ver- und Entschlüsselung auch einige Zeit. Eine genauere Beschreibung der einzelnen Algorithmen findet man im Anhang A.

6.4.2.4 Medienverschlüsselung

Mit diesem Programm können auch externe Medien (USB und PCMCIA) verschlüsselt werden. Dazu gibt es einen eigenen Punkt im Secure Notebook Kontrollcenter. Danach wieder eine sehr einfache Benutzeroberfläche mit Auswahl des Algorithmus, Schlüssellänge, usw. Man kann zusätzlich auch angeben, ob ein Benutzer die Initialverschlüsselung durchführen darf, und was mit unverschlüsselten Medien gemacht werden soll. Dazu gibt es folgende Möglichkeiten.

- Zugriff verweigert
- Schreibschutz
- Zugriff erlaubt, mit Warnung
- Zugriff erlaubt

6.4.2.5 Vorteil

- gesamte Festplatte kann verschlüsselt werden
- gute Auswahl von Verschlüsselungsalgorithmen
- man kann auch externe Geräte wie USB-Sticks und auch PCMCIA-Geräte verschlüsseln

6.4.2.6 Nachteil

- es ist eine Installation notwendig, aber danach einfach zu handhaben
- Recovery mit Hilfe der ERD etwas umständlich
- kostenpflichtig

6.5 Device Control

Für den Schutz und die Administration eines Netzwerkes ist es wichtig, die Einbringung ungeeigneter und gefährlicher Software, sowie auch Daten, zu verhindern. Dazu hat man früher zum Beispiel Verriegelungen an Diskettenlaufwerken angebracht. Heutzutage gibt es da weit elegantere Lösungen, die aber auch einen erheblichen Einschnitt an der Arbeit der Benutzer vornehmen. Mit folgenden Programmen können einige Schnittstellen und Geräte kontrolliert werden, wie z.B. die USB Schnittstelle oder auch Disketten- oder CD-Laufwerke.

Dazu wurden zwei gängige Programme getestet und miteinander verglichen.

6.5.1 Smartline Devicelock

SmartLine Devicelock ist ein Programm zur Verwaltung der Computer Schnittstellen mit der Außenwelt. Dieses Programm unterstützt dabei die Geräte und Schnittstellen, die in Abbildung 9 gezeigt werden.

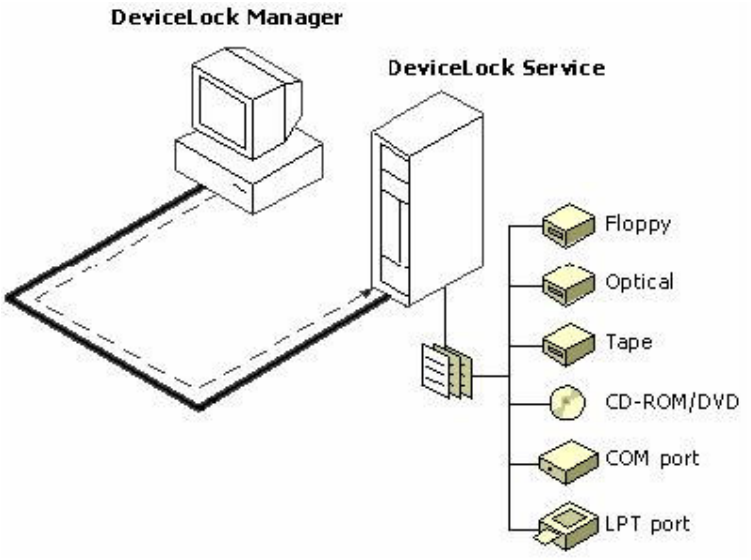

Abbildung 9: Aufbau von Devicelock

6.5.1.1 Installation

Bei der Installation sind zu Beginn wieder die bekannten Einstellmöglichkeiten wie bei jeder anderen Installation auch. Zusätzlich kann ausgewählt werden, welche Schnittstellen automatisch gesperrt werden (siehe Abbildung 10). Am Schluss wird noch ein Zertifikat mit einem öffentlichen und einen privaten Schlüssel erstellt.

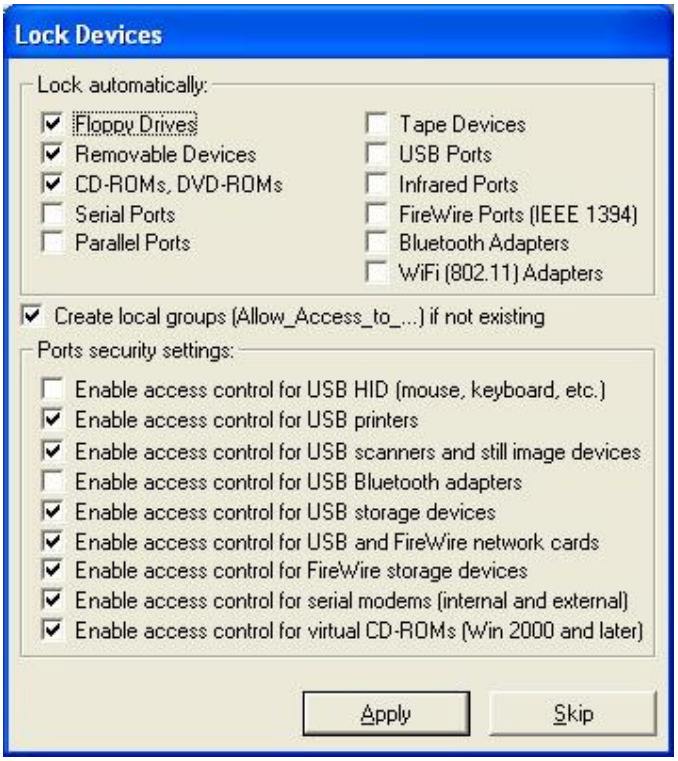

Abbildung 10: Devicelock Installation

6.5.1.2 Allgemeines

Grundsätzlich besteht das Programm aus zwei Teilen. Das zentrale Herzstück, dem Devicelock Manager, mit dem man die einzelnen Computer und deren Schnittstellen verwaltet. Es gibt auch noch den Devicelock Enterprise Manager, der einige zusätzliche Funktionen unterstützt. Unter anderem kann man mit Hilfe des Enterprise Manager das Devicelock Service über das Netzwerk auf anderen Computern installieren.

Für die normale Verwaltung genügt aber der Devicelock Manager völlig. Der zweite Teil ist das oben genannte Devicelock Service, das auf allen zu verwaltenden PC´s installiert werden muss (kann mit Hilfe des Enterprise Manager erledigt werden). Dieser Dienst muss laufen, wird aber normalerweise automatisch gestartet.

Die Benutzeroberfläche des Programms ist sehr einfach und man findet sich sehr schnell zurecht, und kann auch sehr effizient arbeiten.

6.5.1.3 Funktionsweise

Bei diesem Programm gelten immer die eingestellten Rechte, welche man über die Zeitplansteuerung auswählt. Dies gilt immer, wenn der Client mit dem Server in Verbindung steht. Falls der Client offline ist, oder keine Verbindung zum Server herstellen kann, gelten die zuletzt gültigen Rechte. Wenn man aber mit seinem Notebook unterwegs ist, und temporär Zugriff auf eine gesperrte Schnittstelle benötigt, findet man in der Systemsteuerung einen Punkt, mit dem man solche temporäre Änderungen vornehmen kann. Dazu muss man bei der Installation die benötigten Zertifikate am Server und Client installieren und zusätzlich einen Code über das Telefon austauschen. Ist zwar etwas umständlich, aber kann in vielen Fällen sehr hilfreich sein.

6.5.1.4 Wichtige Einstellmöglichkeiten

- Zugriffskontrolle nach Zeitplan möglich
- Überprüfung mittels ACL (Access Control List)
- Zugriffskontrolle auf 2 Ebenen (Schnittstelle oder Typ oder beides)
- Man kann auch Einstellungen vornehmen, um ganze Geräteklassen (z.B. Drucker) aber auch einzelne Geräte (die auf der White-List stehen) von der Überprüfung auszunehmen
- Geräte können auch in read-only mode gesetzt werden
- Einbindung in eine Active Directory Umgebung
- Kontrolle der Inputdaten auf Größe und Typ (→ kein Pufferüberlauf)
- Protokollierung von Benutzeraktivität auf den diversen Geräten
- läuft nur auf Windows Betriebssystemen (NT, 2000, XP und 2003 Server)

6.5.2 Sanctuary Device Control

Sanctuary Device Control ist das umfangreichste und komplizierteste Programm. Allein die Installation beinhaltet schon am Server 3 Programme plus einen Dienst am Client. Dafür sind nette Zusatzdienste, wie z.B. die Möglichkeit zur Verschlüsselung einzelner Geräte beinhaltet. Für die Verschlüsselung benötigt man aber einen eigenen Certificate Server in der Active Directory Umgebung. Ein weiterer Zusatzdienst ist die Shadowing Funktion, mit dieser können Kopien von Dateien, die Benutzer auf Geräte schreiben, eingesehen werden. Man kann auch mit der Auditing Funktion die Administratortätigkeiten überwachen. Falls erforderlich kann man auch ein eigenes Schlüsselpaar erstellen, mit denen sichergestellt wird, das die Datenintegrität zwischen Application Server und Client gegeben ist.

Folgende Geräte und Schnittstellen können kontrolliert werden:

- Diskettenlaufwerke
- CD-ROM, DVD
- Serielle, parallele und USB- Schnittstellen
- Bandlaufwerke
- Palm
- Modems
- Scanner
- Smartcard Lesegeräte
- Firewire
- Bluetooth
- WiFi
- IrDA
- PCMCIA

Am Server muss zuerst eine SQL Datenbank installiert werden, danach der Application Server und zu guter letzt noch eine Konsole, mit der man alles verwalten kann. Zusätzlich muss auf jeden Client ein Dienst installiert werden.

6.5.2.1 Funktionsweise

Dieses Programm sperrt von vornherein ein paar Schnittstellen, wenn man sie nicht ausdrücklich freigibt. Wenn man keine Netzwerkverbindung zum Verwaltungs-PC hat, bleiben die zuletzt eingestellten Rechte bestehen. Vorteil von diesem Programm ist, das man auch zusätzlich die Geräte verschlüsseln kann, allerdings nur wenn ein Certificate Server vorhanden ist.

6.5.2.2 Wichtige Einstellmöglichkeiten

- Für jedes Gerät eine Access Control List
- Standardmäßig kein Zugriff für Benutzer auf irgendein Gerät (Ausnahme Administrator)
- Analysemöglichkeiten von versuchten Zugriffen
- Alle Daten, die auf autorisierte Geräte übertragen werden, können vollständig protokolliert und eingesehen werden
- Änderung der Berechtigungen ohne Computerneustart
- Berechtigungen können benutzer-, gruppen- und rechnerspezifisch verwaltet werden
- Es kann auch ein Zeitplan für den erlaubten Zugriff erstellt werden
- Einbindung in Active Directory möglich
- Definition von online bzw. offline Berechtigungen
- Copy Limits sind einstellbar
- Lokale Kopie der letzten Zugriffsrechte (somit auch weiterhin Schutz für Rechner, die nicht mit dem Netzwerk verbunden sind)
- Agent am Client (Kerneltreiber) ohne Benutzeroberfläche
- Verschlüsselung der Daten auf removable Devices möglich

6.6 Zusammenfassung

In diesem Kapitel wurden einige wichtige Anwendungen betrachtet, die auf jedem System laufen sollten, um es zu schützen, aber auch die sichere Konfiguration von Standardanwendungen, die Benutzer zum Arbeiten benötigen.

An erster Stelle wurden hier Antivirusprogramme und Personal Firewalls und deren Arbeitsweise erwähnt, da sie ein unbedingtes Muss auf jedem System sind, um vernünftig und sicher arbeiten zu können. Dazu wurden auch die gängigsten Angriffsarten (Viren, Trojaner und Würmer) kurz erklärt. Noch dazu wurde die im Betriebssystem Windows implementierte Internetverbindungsfirewall kurz vorgestellt.

Als nächster Schritt wurden die gängigsten Webbrowser und deren sichere Konfiguration betrachtet, weil diese Art von Programmen jeden Tag von Mitarbeitern sehr häufig verwendet werden, und schlecht konfigurierte Browser eine Sicherheitslücke darstellen.

Ein weiterer sehr wichtiger Punkt sind Programme zur Verschlüsselung der Festplatte. Hier wurden zwei Alternativen zum EFS von Windows genauer betrachtet und getestet. Da es bei jedem Produkt Vor- und Nachteile gibt, hier noch mal eine kurze Übersicht und meine persönliche Meinung zu den verschiedenen Produkten. Ich empfehle das Produkt Secure Notebook, weil es wirklich die gesamte Festplatte verschlüsseln kann, und außerdem völlig benutzertransparent arbeitet. Der Benutzer merkt fast keinen Unterschied, wenn man die Software einmal installiert hat, und die Festplatte verschlüsselt. Es entsteht zwar eine kleine Performanceverschlechterung, die aber normalerweise kein Benutzer merken wird. Durch den modularen Aufbau der Produkte dieser Firma, kann man auch nachträglich Erweiterungen vornehmen (z.B. Single Signon). Bei den anderen Produkten kann man leider nicht die gesamte Festplatte verschlüsseln, und auch sonst gibt es Nachteile. Zum Beispiel ist EFS in der Version Windows 2000 noch zu unsicher und auch die Verwaltung der Benutzerzertifikate ist relativ umständlich. Man muss auch aufpassen, falls mehrere Benutzer auf die gleichen Daten Zugriff haben. Sobald ein Benutzer diese Daten verschlüsselt, können die anderen nicht mehr darauf zugreifen. Truecrypt hat den Nachteil, dass die Einrichtung der Umgebung relativ umständlich ist (eigenes Volume erstellen und danach mounten) und, dass die Mountinformationen bei jedem neuen Anmeldevorgang neu eingestellt werden müssen.

Kann zwar über ein Skript automatisch erledigt werden, ist aber trotzdem relativ umständlich. Jedes Produkt hat seine Vor- und Nachteile, deswegen sollte jeder selbst entscheiden, mit welchen Möglichkeiten er besser zu Recht kommt, oder eventuell ein anderes Produkt zur Festplattenverschlüsselung verwenden.

Zu guter Letzt wurden noch zwei Produkte zur Geräte- und Schnittstellenkontrolle genauer betrachtet und getestet. Auch hier wieder eine kurze Zusammenfassung plus eine persönliche Meinung zu den Produkten. Ich empfehle das Produkt Smartline Devicelock, da es sehr einfach zu installieren und auch zu benutzen ist. Es gibt einen Manager, mit dem kann man alle PC´s verwalten, auf denen der Devicelock Dienst installiert ist und läuft (wird automatisch gestartet). Diesen Dienst kann man vom Verwaltungs-PC aus installieren. Wenn man keine Netzwerkverbindung zum Verwaltungs-PC hat, bleiben die zuletzt eingestellten Rechte bestehen. Allerdings findet man in der Systemsteuerung einen Punkt, bei dem man temporär Zugriffe erlauben kann (leider nur für USB Geräte), wenn man die benötigten Zertifikate installiert hat (zusätzlicher telefonischer Codeaustausch mit dem Administrator notwendig, aber grundsätzlich eine sehr gute Idee).

Ein etwas umfangreicheres, aber auch komplizierteres Programm ist Sanctuary Device Control. Dies beginnt bereits bei der Installation. Zuerst muss man eine SQL-Datenbank installieren, danach den Application Server, dann noch eine Konsole zur administrativen Verwaltung und auf jeden Client, den man verwalten möchte, auch noch einen eigenen Dienst. Ein Nachteil besteht auch darin, dass dieses Programm von Haus aus ein paar Schnittstellen sperrt, wenn man sie nicht ausdrücklich freigibt. Dies hat mich am Anfang ziemlich beschäftigt. Wenn man keine Netzwerkverbindung zum Verwaltungs-PC hat, bleiben die zuletzt eingestellten Rechte bestehen. Vorteil von diesem Programm ist, das man auch zusätzlich die Geräte verschlüsseln kann, allerdings nur wenn ein Certificate Server vorhanden ist. Es gibt noch weitere Funktionen, die allerdings nicht benötigt werden (Auditing, Shadowing, usw.).

Im Großen und Ganzen ist Device Control aber ein grober Einschnitt für die meisten Benutzer und somit sehr gut zu überlegen, ob und wie es eingesetzt werden soll.

7 Zusammenfassung und zukünftige Arbeit

Die Sicherheit spielt in der Informationstechnologie eine sehr große Rolle, und deswegen sollte ihr große Aufmerksamkeit geschenkt werden. Es kann zwar niemals eine hundertprozentig sichere Arbeitsumgebung geschaffen werden, aber durch eine Vielzahl von Einstellungen und Konfiguration kann ein sehr sicheres System geschaffen werden.

Durch die Absicherung eines Systems an verschiedenen Grenzen zur Außenwelt kann das Risiko eines Angriffs deutlich vermindert werden. Deswegen wurde in dieser Diplomarbeit ein Schalenmodell betrachtet, welches dabei helfen soll, alle möglichen Sicherheitsaspekte für Notebooks besser einteilen zu können. Somit hat man einen besseren Überblick über sein System. Wenn das Risiko in allen einzelnen Schichten minimiert wird, erhält man ein sehr sicheres Gesamtsystem.

Eine wesentliche Erkenntnis aus dieser Arbeit ist jene, das es kein perfektes System gibt, und auch alle Empfehlungen in dieser Diplomarbeit sind eben nur Empfehlungen und keine hundertprozentig richtige oder falsche Einstellung. Es kommt immer auf das jeweilige System an, und in welcher Umgebung es zum Einsatz kommt.

Die wichtigsten Punkte dieser Arbeit sind die verschiedenen getesteten Produkte, die verwendet werden um Daten zu verschlüsseln und auch um Geräte und Schnittstellen zu verwalten. Da es allerdings bei allen Produkten Vor- und Nachteile gibt, kristallisiert sich kein perfektes Produkt heraus, das verwendet werden sollte. Deswegen könnten in einer weiterführenden Arbeit noch weitere Produkte getestet werden.

Noch dazu könnten andere Betriebssysteme genauer erforscht werden, um deren Sicherheitsaspekte kennen zu lernen. In erster Linie wird hier das neue Betriebssystem von Microsoft, Windows Vista, zu begutachten sein. Außerdem sollten auch andere Betriebssysteme, als die von Microsoft, untersucht werden. Die meisten Unternehmen verwenden zwar auf Benutzerseite Windows Betriebssysteme, aber vielleicht kann zum Beispiel Linux in den nächsten Jahren seinen Marktanteil erhöhen.

A Verschlüsselungsalgorithmen

Die wichtigsten Kriterien für Verschlüsselungsalgorithmen sind vor allem die Sicherheit (Schlüssellänge), die Performance (Geschwindigkeit beim Ver- und Entschlüsseln) und die Art des Cipher Modus. Heutzutage werden vor allem Block Cipher mit symmetrischen Schlüsseln verwendet. Ein Block Cipher nimmt immer einen Block unverschlüsselter Nachricht (plaintext) und verschlüsselt den in einen Block gleicher Größe (ciphertext). Bei größeren Daten, ist die Verbindung dieser einzelnen Blöcke entscheidend für die Sicherheit. Dies nennt man den mode of operation. Dieser legt fest, ob und wie die einzelnen Blöcke miteinander in Verbindung gebracht werden.

Bei den nachfolgenden Algorithmen handelt es sich um symmetrische Verschlüsselungsalgorithmen, d.h. zur Ver- und Entschlüsselung wird der gleiche Schlüssel verwendet. Die Blockgröße ist dabei fix und die Schlüssellänge kann bei den meisten Algorithmen variiert werden.

A.1 DES & 3DES

DES und auch die Erweiterung 3DES sind etwas ältere Algorithmen und werden schön langsam von AES verdrängt. 3DES ist zwar sicherer als DES, aber sehr langsam im Gegensatz zu neueren Algorithmen. DES wurde 1975 erstmals veröffentlicht und 1977 standardisiert. Der Algorithmus wurde von IBM und der US Regierung entwickelt.

DES arbeitet mit einem 56bit Schlüssel und mit einer Blockgröße von 64bit. Aufgrund der kleinen Blockgröße und der geringen Schlüssellänge ist DES nicht mehr sicher (kann mit einer brute force Attacke innerhalb angemessener Zeit geknackt werden) und wird deshalb durch neuere Algorithmen ersetzt.

A.2 DESX

DESX ist eine Variante des DES Algorithmus, der die Komplexität etwas erhöht. Es werden einfach vor und nach der eigentlichen DES Operation zusätzliche Schlüssel (64bit) mit dem plaintext XOR-verknüpft. Dadurch ist die resultierende Schlüssellänge 184bit, wobei davon nur 118bit effektiv sind, und somit die Sicherheit nicht so hoch ist, wie gewünscht. Deswegen ist dieser Algorithmus eher mit Vorsicht zu genießen, weil er trotz der Erhöhung der Sicherheit nicht mit aktuellen Algorithmen wie AES oder Blowfish mithalten kann.

A.3 AES

AES ist einer der sichersten Algorithmen derzeit, und wird als Nachfolger von DES und 3DES sehr häufig eingesetzt. Dieser Algorithmus wird auch Rijndael-Algorithmus, nach seinen Erfindern Joan Daemen und Vincent Rijmen, genannt. Er wurde 1998 erstmals veröffentlicht und 2001 standardisiert. AES ist ein schneller Algorithmus, leicht zu implementieren und er braucht wenig Speicher.

AES unterstützt verschiedene Schlüssellängen (128, 192 und 256 bit) und arbeitet mit einer fixen Blockgröße von 128 bit. Es werden mehr Blockgrößen und Schlüssellängen unterstützt, aber im Standard sind nur die oben genannten definiert.

Ein weiterer Vorteil von AES ist, das es ein frei verfügbarer Algorithmus ist und derzeit praktisch nicht zu knacken ist.

A.4 Blowfish

Blowfish ist ein sehr schneller Algorithmus, und er sollte DES und IDEA ersetzen. Er wurde von Bruce Schneier entwickelt, 1993 erstmals veröffentlicht aber nie standardisiert. Blowfish unterstützt verschiedene Schlüssellängen (32 – 448 bit in 8 bit Schritten, Standard 128 bit) und arbeitet mit einer fixen Blockgröße (64 bit). Auch Blowfish ist ein frei verfügbarer Algorithmus, und mit einer richtig gewählten Schlüssellänge auch sehr sicher, obwohl die Blockgröße von 64bit mittlerweile als zu gering eingestuft wird.

A.5 Twofish

Twofish ist ebenfalls ein sehr sicherer Algorithmus, der auch bei der Endausscheidung um der AES Standard dabei war. Er ist ähnlich dem Blowfish Algorithmus, und wurde auch unter anderem von Bruce Schneier mitentwickelt. Dieser Algorithmus kommt von der Geschwindigkeit dem AES Algorithmus sehr nahe, aber an Blowfish kommt auch er nicht vorbei. Twofish arbeitet mit einer Blockgröße von 128bit und unterstützt Schlüssellängen bis 256bit. Aufgrund der Blockgröße ist er ein sehr sicherer Algorithmus.

A.6 XOR

XOR ist zwar rein akademisch betrachtet ein Verschlüsselungsalgorithmus, aber trotzdem sollte man die Finger davon lassen, weil er sehr leicht zu knacken ist. Der einzige Vorteil ist, dass er ziemlich schnell ist.

Aufgrund der Funktionsweise dieser logischen Operation kann man aber Daten leicht ver- und entschlüsseln.

Bsp.:	Daten	⊕	Schlüssel	=	verschlüsselte Nachricht
	verschlüsselte Nachricht	⊕	Schlüssel	=	Daten

Das ⊕ -Zeichen steht für die Operation XOR.

B Modes of operation

Bei den einzelnen Algorithmen ist nicht nur die Schlüssellänge entscheidend, sondern vor allem auch der Modus, wie die einzelnen Blöcke miteinander in Verbindung gebracht werden. Daraus kann man ungefähr erkennen, wie sicher manche Algorithmen sind, und wie schnell sie arbeiten.

B.1 ECB

ECB (Electronic Codebook) ist der einfachste Modus. Es wird kein Zusammenhang zwischen den verschiedenen Blöcken hergestellt, d. h. das die gleichen Blöcke plaintext zu gleichen Blöcken ciphertext verschlüsselt werden (siehe Abbildung 11). Dies ist allerdings ein sehr großer Nachteil. Bei der Entschlüsselung funktioniert es genau umgekehrt, also besteht auch kein Zusammenhang zwischen den einzelnen Blöcken.

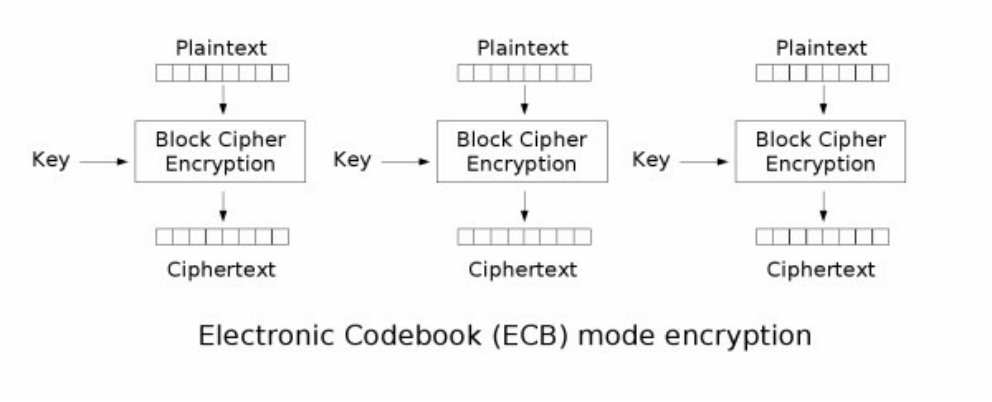

Abbildung 11: ECB Verschlüsselung

B.2 CBC

Bei diesem Modus wird jeder Block plaintext vor der Verschlüsselung mit dem ciphertext des vorigen Blocks XOR-verknüpft (⊕ - Zeichen in der Abbildung 12). Damit jede Nachricht einzigartig ist, wird der erste Block mit einem Initialisierungsvektor XOR-verknüpft. Dieser Modus wird sehr häufig verwendet, obwohl er den kleinen Nachteil hat, dass er alles sequentiell abarbeitet und deswegen etwas langsam ist.

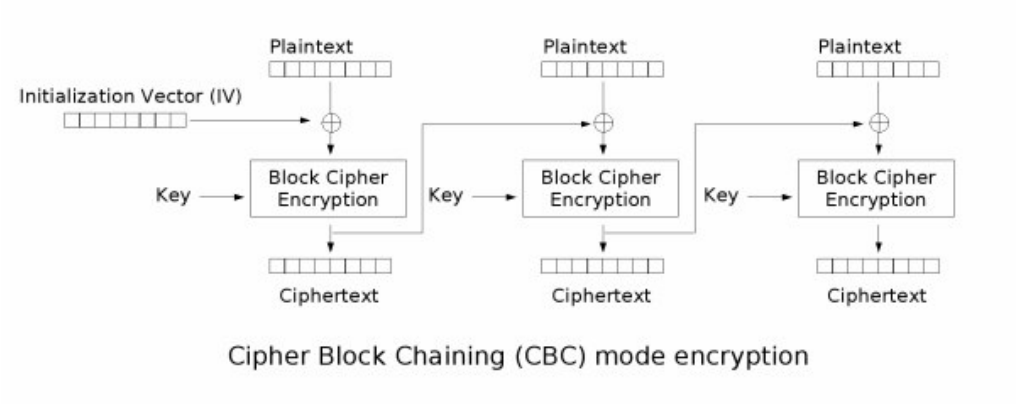

Abbildung 12: CBC Verschlüsselung

Es gibt auch noch eine Erweiterung der CBC Modus, und zwar den PCBC Modus. Dieser ist allerdings kein Standard und wird nicht sehr häufig verwendet, außer bei Kerberos 4. Die Erweiterung besteht darin, dass dieser Modus Fehler beim Verschlüsselungsvorgang erkennen sollte und die gelieferten Ergebnisse nicht angenommen werden sollten.

B.3 CFB und OFB

Die Modi CFB (Cipher Feedback) und OFB (Output Feedback) sind sich sehr ähnlich. Beide machen aus dem Block Cipher einen Stream Cipher, und sind dadurch um einiges schneller. Die Funktionsweise sieht man am besten in den nachfolgenden Abbildungen (Abbildung 13 und Abbildung 14).

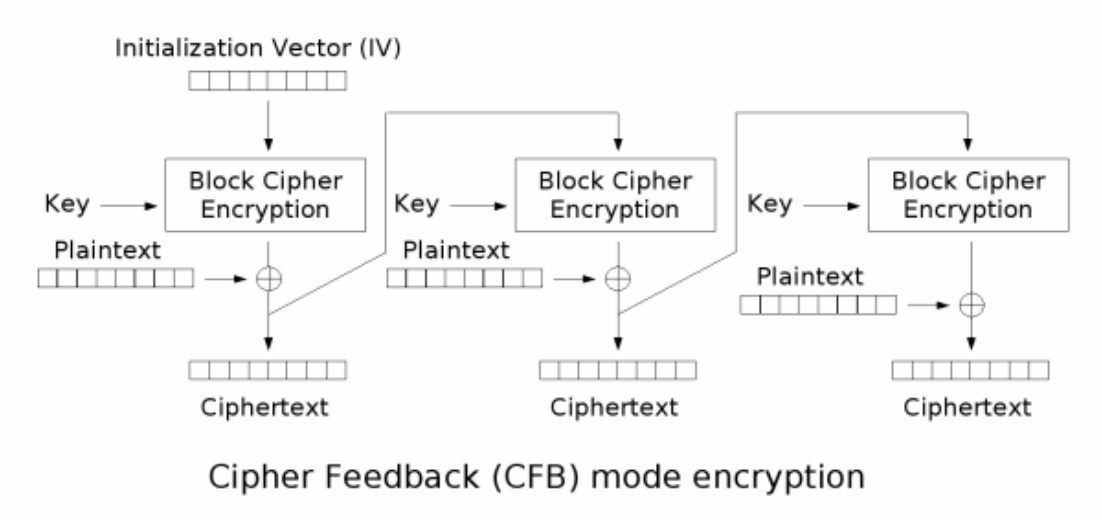

Abbildung 13: CFB Verschlüsselung

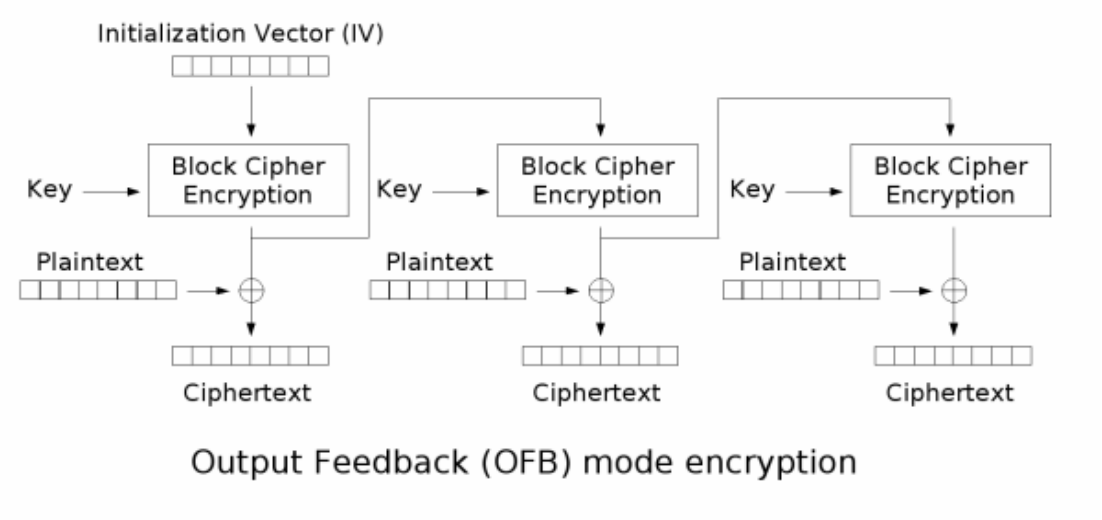

Abbildung 14: OFB Verschlüsselung

B.4 CTR

Auch der CTR-Modus (Counter) macht aus einem Block Cipher einen Stream Cipher, und ist dadurch auch sehr schnell. Der Counter kann eine beliebige Funktion sein, welche eine Folge liefert, welche lange Zeit nicht wieder auftritt. In der Abbildung 15 sieht man die genaue Funktionsweise, wobei Nonce ähnlich dem IV (Initialization Vector) der anderen Abbildungen ist.

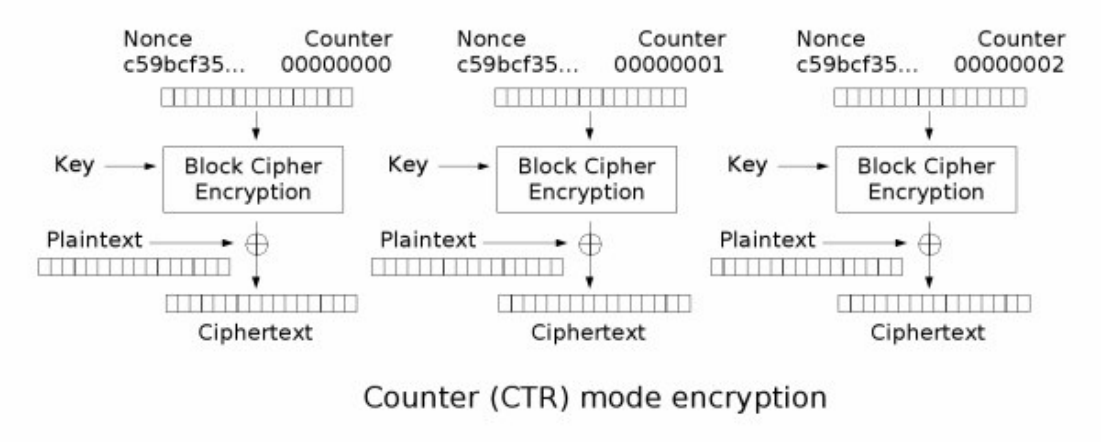

Abbildung 15: CTR Verschlüsselung

Abkürzungsverzeichnis oder Glossar

3DES	3-maliger DES
AES	Advanced Encryption Standard
BIOS	Basic Input/Output System
CA	Certification Authority
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol
CTR	Counter
DES	Data Encryption Standard
DESX	Data Encryption Standard Extended (eine Variante von DES)
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EBC	Electronic Codebook
EFS	Encryption File System
FAT	File Allocation Table
FEK	File Encryption Key
FTP	File Transfer Protocol
GPS	Global Positioning System
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol

ICF	Internet Connection Firewall
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LM	Lan Manager
MAC	Media Access Control
MBR	Master Boot Record
MD4	Message Digest 4
MMC	Microsoft Management Console
MMS	Multimedia Messaging Service
NLA	Network Location Awareness
NT	New Technology
NTFS	New Technology File System
NTLM	New Technology Lan Manager
OFB	Output Feedback
PIN	Personal Identification Number
SAM	Security Accounts Manager
SBS	Secure Boot System
SHA1	Secure Hash Algorithm
SID	Security Identifier
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SUS	Software Update Service
TCP	Transmission Control Protocol
VPN	Virtual Private Network

WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi (Wireless Fidelity) Protected Access

Literaturverzeichnis

Aguilut, B. (2005): Windows Server Update Services.
http://download.microsoft.com/download/d/1/c/d1c00a2d-b384-4ee4-b350-969ef39a6120/WSUSOverview.doc. (Datum des Zugriffs: 29. Juni 2006)

AT&T (2004): Netzwerksicherheit: Management von Chance und Risiko.
http://www.att.com/emea_de/docs/wp/network_security_de.pdf.
(Datum des Zugriffs: 19. Juni 2006).

Beier, A. (2005): Sicher aufbewahrt: Datenverschlüsselung unter Windows 2000 und XP Home nachgerüstet.
http://www.heise.de/mobil/artikel/58723/0. (Datum des Zugriffs: 20. Juni 2006)

Danseglio, M. (2004): Windows XP Security Guide.
http://go.microsoft.com/fwlink/?linkid=14840. (Datum des Zugriffs: 6. Juni 2006).

Danseglio, M. (2006): Windows Server 2003 Security Guide.
http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en&hash=T8CTX4G.
(Datum des Zugriffs: 8. Juni 2006).

IEEE802.11 (2006): LAN/MAN Wireless LANS
http://standrards.ieee.org/getieee802/802.11.html. (Datum des Zugriffs: 29. Juni 2006)

Microsoft: Default Settings for Services
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sys_srv_default_settings.mspx. (Datum des Zugriff: 30. Juni 2006)

Microsoft (2004): Windows XP Sicherheitshandbuch
http://www.microsoft.com/germany/sicherheit/guidance/modules/winxp.asp.
(Datum des Zugriffs: 20. Juni 2006)

Microsoft (2006): Schützen sie ihre persönlichen Daten mit sicheren Kennwörtern.
http://www.microsoft.com/germany/athome/security/privacy/password.mspx
(Datum des Zugriffs: 6. Juni 2006).

Microsoft Knowledgebase (2005): Bekannte Sicherheits-IDs in Windows-Betriebs-systemen.
http://support.microsoft.com/kb/243330. (Datum des Zugriff: 20. Juni 2006)

Microsoft Knowledgebase (2006): How to back up the recovery agent EFS private key in Windows Server 2003, in Windows 2000, and in Windows XP.
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q241201. (Datum des Zugriffs: 28. Juni 2006)

Microsoft Update: http://windowsupdate.microsoft.com/

Mkitech (2006): mki Technologie und Dienstleistungs GmbH
www.mkitech.at (Datum des Zugriffs: 3. August 2006).

Peikari (2004): Kenne deinen Feind: Fortgeschrittene Sicherheitstechniken
O´Reilly Verlag.

RFC1157 (1990): A Simple Network Management Protocol.
www.ietf.org/rfc/rfc1157.txt (Datum des Zugriffs: 31. Mai 2006).

RFC2401 (1998): Security Architecture for the Internet Protocol
www.ietf.org/rfc/rfc2401.txt (Datum des Zugriffs: 29. Juni2006)

RFC3410 (2002): Introduction and Applicability Statements for Internet Standard Management Framework.
www.ietf.org/rfc/rfc3410.txt (Datum des Zugriffs: 31. Mai 2006).

Russell, R. (2002): Hack Proofing Your Network, Second Edition.
Syngress Publishing.

Smith, B. (2005): Microsoft Windows Sicherheit – Die technische Referenz. Zweite Auflage. Microsoft Press

Schwanfelder, W. (2004): Sun Tzu für Manager: Die 13 ewigen Gebote der Strategie. Campus Verlag.

Technet (2004): Windows 2000 Sicherheitshandbuch: Sichere Installation von Windows 2000. http://www.microsoft.com/germany/technet/datenbank/articles/900225.mspx. (Datum des Zugriffs: 11. August 2006).

Technet (2005): Bedrohungen und Gegenmaßnahmen. Kapitel 2: Richtlinie auf Domänenebene. http://www.microsoft.com/germany/technet/sicherheit/topics/serversecurity/tcg/tcgch02n.mspx. (Datum des Zugriffs: 28. Juli 2006).

Truecrypt: http://www.truecrypt.org/downloads.php.

Wikipedia (2003): W32.Blaster www.wikipedia.de (Datum des Zugriffs: 19. Juli 2006).

Wikipedia (2006): Computersicherheit www.wikipedia.de (Datum des Zugriffs: 29. Mai 2006).

Wikipedia (2006): Computervirus www.wikipedia.de (Datum des Zugriffs: 2. August 2006).

Wikipedia (2006): Computerwurm www.wikipedia.de (Datum des Zugriffs: 2. August 2006).

Wikipedia (2006): Trojanisches Pferd www.wikipedia.de (Datum des Zugriffs: 2. August 2006).