Data Leakage Prevention

Hannes Kasparick

DIPLOMARBEIT

eingereicht am

Fachhochschul-Masterstudiengang

Sichere Informationssysteme

in Hagenberg

im Mai 2008

Betreuer:
DI Eckehard Hermann

© Copyright 2008 Hannes Kasparick

Alle Rechte vorbehalten

Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die aus anderen Quellen entnommenen Stellen als solche gekennzeichnet habe.

Hagenberg, am 26. Mai 2008

Hannes Kasparick

Inhaltsverzeichnis

Erklärung **iii**

Vorwort **vii**

Kurzfassung **viii**

Abstract **ix**

1 Einleitung **1**

1.1 Vertrauliche Daten schützen 1

1.2 Data Leakage Prevention 4

1.3 Rechtliche Aspekte 5

1.4 Sicherheitsstrategien 7

1.4.1 Zugriffskontrollstrategien 8

1.4.2 Informationsflussstrategien 13

1.5 Firmenpolicies und organisatorische Maßnahmen 14

1.6 Grenzen der Technik 15

2 Wege aus dem Unternehmen **17**

2.1 Interne und Externe Speichermedien 18

2.2 Internetbasierte Wege 18

2.2.1 E-Mail 19

2.2.2 HTTP / HTTPS 20

2.2.3 Instant Messenger 20

2.2.4 Peer to Peer 20
2.2.5 Weitere Protokolle 21
2.3 Drucker 21
2.4 Entsorgung von Speichermedien 21
2.5 Datensicherung 22

3 Klassifizierung von Daten 23
3.1 Vertraulichkeitsklassen 23
3.2 Umgang mit Klassifizierung 24
3.3 Klassifizierung mit DLP-Systemen 25
3.4 Inhaltsbezogene Klassifizierung 26

4 Lösungsansätze 27
4.1 Begleitende Maßnahmen 27
4.1.1 Regeln für DLP-Systeme 28
4.1.2 Extrusion Response 29
4.1.3 Bedrohung durch externe Schnittstellen 29
4.1.4 Entsorgung von Datenträgern 30
4.1.5 Datensicherung 31
4.1.6 Angriffe auf die Netzwerkinfrastruktur 31
4.2 Hostbasierte DLP-Systeme 33
4.3 Netzwerkbasierte DLP-Systeme 33
4.4 Netzwerkbasierte Hilfsmittel 34
4.5 Digital Rights Management 35

5 Der Hostbasierte Lösungsansatz 38
5.1 Der DLP-Agent 39
5.2 Implementierung des Kerneltreibers 43
5.2.1 Manipulation der System-Call-Table (SSDT Hooking) 43
5.2.2 Inline Hooking 45
5.2.3 Manipulation der Prozessliste 45

5.2.4 Interrupt Hooking 46
5.3 Verschlüsselung vertraulicher Daten 47
5.4 Whitelisting von Anwendungen 48
5.5 Netzwerk des Vertrauens 49
5.6 Datenaustausch über die Zwischenablage 50
5.7 Externe Speichermedien 51
5.8 E-Mail 51
5.9 Instant Messenger und Peer-to-Peer 52
5.10 Drucker 52
5.11 Sonstiges 53

6 Musterimplementierung 54
6.1 Voraussetzungen und Ziele 54
6.2 Sicherheitsmanagement 55
6.3 Bestandsaufnahme 56
6.4 Planungsschritte 57
6.5 Installation und begleitende Maßnahmen 60

7 Resümee 62

Literaturverzeichnis 64

Vorwort

Die vorliegende Arbeit entstand im Zuge des Masterstudiums „Sichere Informationssysteme“ (SEC) an der FH Oberösterreich Campus Hagenberg im Sommersemester 2008.

Das Thema „Data Leakage Prevention“ bzw. „Data Loss Prevention“ ist noch relativ neu in der Informationstechnik. Daher gibt es bisher nur wenige Referenzsysteme oder Referenzliteratur, die dieses Thema herstellerunabhängig betrachten. Consultingunternehmen wie z.B. Gartner oder Infowatch sagen der Thematik jedoch eine große Zukunft voraus.

Diese Arbeit richtet sich an alle, die unerwünschte Datenabflüsse aus ihrem Unternehmen verhindern wollen. Es geht darum zu verindern, dass berechtigte Personen unerlaubt Informationen aus dem Unternehmen mitnehmen. Zum Verständnis dieser Arbeit wird vorausgesetzt, dass der Leser Grundkenntnisse der Netzwerktechnik und Erfahrung in der Administration von Betriebssystemen besitzt.

Ich bedanke mich bei meinem Betreuer DI Eckehard Hermann (FH Oberösterreich Campus Hagenberg), für die Unterstützung durch seine fachlichen Ratschläge und für die vielen Stunden, die er zum Lesen und Korrigieren meiner Arbeit aufgebracht hat. Des Weiteren möchte ich Dr. Gunter Bitz (SAP) für die Hilfe bei der Beschaffung und Tony Themelis (Verdasys) für die Unterstützung bei der Implementierung eines Data Leakage Prevention Systems danken.

Kurzfassung

Die Gefahr durch Industriespionage und dem damit verbundenen nicht erwünschten Abfluss von geheimen, firmeninternen Daten wird vielen Unternehmen erst dann bewusst, wenn ein Mitbewerber einen Nachbau des eigenen Produkts nahezu zeitgleich und preisgünstiger am Markt platziert. Bisherige IT-Sicherheitsmaßnahmen beschränkten sich darauf, externe Angreifer aus dem Unternehmen fern zu halten. Seit wenigen Jahren versucht die Sicherheitsbranche mit „Data Loss Prevention-“ bzw. „Data Leakage Prevention-“ oder „Extrusion Prevention Systemen“ Datendiebstahl durch autorisierte Mitarbeiter entgegen zu wirken.

Herkömmliche Firewall- und Zugriffsysteme können Angreifer, die legitimen Zugriff auf vertrauliche Daten besitzen, nicht aufhalten. Data Leakage Prevention Systeme versuchen diese Lücke zu schließen und verhindern, dass eine Person, die legitimen Zugriff auf vertrauliche Daten hat, diese Daten unerlaubt weitergibt. Diese Arbeit zeigt, welche Technologien existieren, um dieses Ziel zu erreichen und in welchem Umfang der Einsatz sinnvoll ist.

Zunächst werden Wege gezeigt, auf welchen Daten ein Unternehmen verlassen können. Die Klassifizierung von Daten ist der zweite Schritt, in dem Daten einer bestimmten Vertraulichkeitsklasse zugeordnet werden. Anschließend wird die technische Umsetzung und Implementierung von Data Leakage Prevention Systemen beschrieben. Daneben werden Sicherheitsmodelle und die rechtlichten Rahmenbedingungen beschrieben. Eine Musterimplementierung gibt praxisnahe Hinweise zur Installation eines Data Leakage Prevention Systems in Unternehmen.

Abstract

Most companies are not aware of industrial espionage and loss of intellectual property until a high quality copy of one of their products is released at a low price by a competitor. Previous IT security measures are limited to protect data from attackers from outside the company. Over the past few years the IT security branch has developed methods to protect data from internal attackers called "Data Loss", "Data Leakage" or "Extrusion Prevention Systems", respectively.

Conventional firewall or access systems cannot protect against attackers who have legitimate access to sensitive data. Data Leakage Prevention systems close this gap and prohibit people who have legitimate access from distributing secret data. This thesis describes the existing technologies to reach this objective and under which circumstances the usage of a Data Leakage Prevention system makes sense. In addition, security models and the judicial environment are described.

In the beginning, the author shows how data can leave a company. The classification of data is the second step to protect data. Afterwards the technical implementation of a Data Leakage System is described. An example implementation of a Data Leakage Prevention System in a fictional company offers practical advice.

Kapitel 1

Einleitung

Immer mehr Unternehmen erkennen den Schutzbedarf ihrer vertraulichen Daten. Dies trifft vor allem auf Unternehmen zu, die Forschung und Entwicklung betreiben und einem starken Konkurrenzdruck unterliegen. Im Bereich Forschung und Entwicklung ist es wichtig, früh mit neuen Technologien und Produkten am Markt präsent zu sein. Um sich einen Wettbewerbsvorteil zu verschaffen, greifen Unternehmen teilweise zu illegalen Methoden wie Industriespionage. Die Daten, die ausspioniert werden, können ganz unterschiedlich sein. Angefangen von Computer Aided Design (CAD)-Bauplänen und Designstudien, über Programmquellcode bis hin zu Strategieplänen eines Unternehmens.

Durch diese Art von Informationen kann sich der Mitbewerb Vorteile verschaffen, die sich negativ auf den Gewinn des eigenen Unternehmens auswirken. Deshalb liegt es im Interesse eines Unternehmens, dass z.B. Daten, die dem Mitbewerb einen Vorteil verschaffen, nicht das Unternehmen verlassen. Diese Arbeit beschäftigt sich mit Möglichkeiten und Vorgehensweisen, um den unerwünschten Datenabfluss über Informationstechnologie (IT)-Systeme zu verhindern oder diesen zumindest aufzudecken. Dabei wird auf Sicherheitsmodelle, technische und organistorische Maßnahmen, sowie deren Auswirkungen eingegangen.

1.1 Vertrauliche Daten schützen

Die Bedrohung kommt dabei immer öfter aus den betroffenen Unternehmen selbst. Laut einer Studie von Infowatch[1] aus dem April 2007 [11] glauben 78 Prozent der Befragten, dass Datendiebstahl durch die eigenen Mitarbeiter die größte Bedrohung für die Datensicherheit darstellt. Diese Bedrohung

[1] http://www.infowatch.com

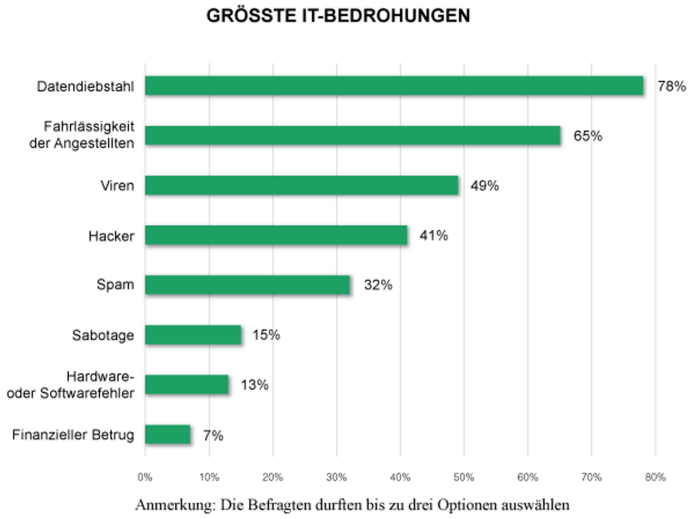

Abbildung 1.1: Umfrage zu IT-Bedrohungen aus [11].

liegt nach Meinung der Befragten weit höher als die durch Hacker (41 %) oder Viren (49 %). Die genauen Ergebnisse der Umfrage stellt Abbildung 1.1 dar.

Die Befragten sehen die internen Bedrohungen mit 55 % zu 45 % größer als externe Bedrohungen. Die weitere Aufschlüsselung der Hauptbedrohungen für die interne Datensicherheit ergibt laut [11], dass „Verlust vertraulicher Daten“ (93 %) und „Verfälschung sensibler Daten“ (85 %) mit großem Abstand führend auf den ersten beiden Plätzen liegen. Auf den Plätzen folgen „Hardwarediebstahl“ (34 %), „Betrug“ (29 %) und „Datenverlust“ (23 %).

Durch den Einsatz von Sicherheitstechnologien, wie beispielsweise Firewall und Anti-Viren Lösungen, sind die Angriffsvektoren für einen externen Angreifer unter Verwendung technischer Mittel kleiner geworden. Aufgrund dessen verlagern Angreifer ihre Hauptaufmerksamkeit auf die menschliche Ebene. Die neuen Angriffsziele sind Menschen, nicht mehr die Technik. Unzufriedene oder schlecht bezahlte Mitarbeiter bieten einen guten Ansatzpunkt. Sie haben arbeitsbedingt die Berechtigungen auf die für den Angreifer interessanten Daten zu zugreifen. Somit ist es nicht nötig technische Zugriffsbeschränkungen, wie Dateisystemrechte oder Verschlüsselung, zu umgehen.

Neben dem Unsicherheitsfaktor Mensch gibt es auch weiterhin ausreichend technische Möglichkeiten an vertrauliche Daten zu gelangen.

In den vergangenen Jahren wurden gezielt Viren und Trojaner[2] für ein bestimmtes Angriffsziel (eine Firma) entwickelt. Durch die geringe Verbreitung (z.B. nur auf Rechnern des angegriffenen Unternehmens) ist eine signaturbasierte Erkennung durch Anti-Virenprogramme nicht möglich. Verhaltensbasierte Anti-Virenprogramme können derartige Viren erkennen, unter der Voraussetzung, dass sie ein für das Anti-Virenprogramm verdächtige Aktionen ausführen.

Verlässliche Aussagen über erfolgreiche und gescheiterte Angriffe sind nicht möglich, da die Aussagen betroffener Unternehmen undurchsichtig und widersprüchlich sind (z.B. [10]). Der Grund dafür ist, dass Unternehmen oder Regierungen erfolgreiche Angriffe aufgrund eines möglichen Imageschadens und Vertrauensverlusts (z.B. Banken, Regierungen) bei Kunden, nicht veröffentlichen.

Neben den genannten Bedrohungen bestehen klassische Angriffsmethoden wie beispielsweise das Abhören unverschlüsselten Netzwerkverkehrs inner- und außerhalb des Unternehmens nach wie vor. Abhängig von den Rahmenbedingungen ist es sinnvoller (kostengünstiger), beim Internetprovider jemanden zu bestechen, damit dieser den Netzwerkverkehr des Opfers speichert, als mit Hilfe von Trojanern zu versuchen vertrauliche Daten zu erlangen. Dies ist beispielsweise dann der Fall, wenn das Risiko, dass ein interner Angriff bemerkt wird, sehr hoch ist. Ein externer Angriff durch Abhören des Netzwerkverkehrs ist nicht feststellbar und ungefährlicher für einen Angreifer. Die Verschlüsselung von Daten, die über unsichere Kanäle übertragen werden, ist somit weiterhin nötig.

Damit vertrauliche Daten nicht unbefugt das Unternehmen verlassen, gibt es seit einiger Zeit den technischen Ansatz des „Data Leakage Prevention Systems“. Diese technischen Systeme sollen die organisatorischen Firmenpolicies (siehe Abschnitt 1.5) zum Schutz der Daten unterstützen.

Der Schutz von Daten vor ungewolltem Export aus dem Unternehmen heraus ist die Aufgabe eines Data Leakge Prevention Systems. Es geht also nicht um den Schutz von Systemen, sondern um den Schutz von Daten! Wenn Unbefugte Zugriff auf geheime Daten erlangen, hat dies verschiedene Folgen, die nicht in absoluten Zahlen messbar sind. Wenn beispielsweise eine Bank oder ein Internetversandhaus Kreditkarteninformationen der Kunden verliert, führt dies bei bekannt werden zu einer Verschlechterung des Rufes. Direkte finanzielle Verluste können beispielsweise dann entstehen, wenn ein Mitbewerber Baupläne für ein Produkt entwendet und dieses Produkt anschließend billiger herstellen kann (weil er keine Entwicklungskosten hat) als der eigentliche Erfinder.

[2]Trojaner werden im Rahmen dieser Arbeit wie üblich als Synonym für Trojanische Pferde verwendet.

1.2 Data Leakage Prevention

Data Leakage Prevention bzw. Data Loss Prevention, kurz DLP, hat das Ziel den unauthorisierten Abfluss von Daten aus dem Unternehmen zu verhindern. Dabei spielen sowohl technische als auch organisatorische Maßnahmen eine Rolle. Da firmeninterne Richtlinien und Vorschriften zum Datenschutz bei bewussten Verstößen der Mitarbeiter wirkungslos sind, gibt es eine Reihe von Herstellern, die den elektronischen Datenabfluss per Software zu verhindern versuchen. Ein Beispiel wäre die Vorschrift, dass Programmquelltexte nicht weiter gegeben werden dürfen. Ohne technische Maßnahmen hindert einen Mitarbeiter nichts daran, den Quelltext trotzdem mit zunehmen und weiter zu geben.

Zum Schutz von geschäftsrelevanten Daten setzen Unternehmen bereits jetzt eine Reihe von Technologien ein. Abbildung 1.2 (ebenfalls aus [11]) stellt die Verteilung der verwendeten Technologien als Balkendiagramm dar. Der Grafik zu Folge, setzt praktisch jedes der befragten Unternehmen Anti-Virensysteme und Firewalls ein. Data Leakage Prevention Systeme kommen nur bei 16 % der Befragten zum Einsatz. Die primären Gründe für diese niedrige Verbreitung sind laut der Studie:

- Mangel an Standards
- Budgetgrenzen
- Mangel an ausgebildeten Spezialisten
- Rechtliche Hindernisse
- Psychologische Hindernisse
- Es gibt keine technischen Lösungen

Fehlende Standards führen zu sogenannten Insellösungen die aufwändig zu warten sind und über wenig Interoperabilität verfügen. Diese Situation gilt es zu vermeiden. Die Installation eines DLP-Systems erzeugt Kosten. Dies sind neben einmaligen Lizenzkosten auch laufende Wartungskosten. Wenn keine Geldmittel für die Anschaffung eines DLP-Systems zur Verfügung stehen, kann es nicht zum Einsatz kommen.

Der Mangel an IT-Spezialisten besteht seit einiger Zeit und diese Situation wird sich kurzfristig nicht ändern [18]. Rechtliche Hindernisse bei der Einführung entstehen aufgrund der länderspezifischen Datenschutzrichtlinien. Je nach Umfang des Einsatzes eines DLP-Systems treten datenschutzrechtliche Fragen in den Vordergrund (siehe Abschnitt 1.3), welche es zu beachten gilt. Zwölf Prozent der Befragten sind der Meinung, dass es keine

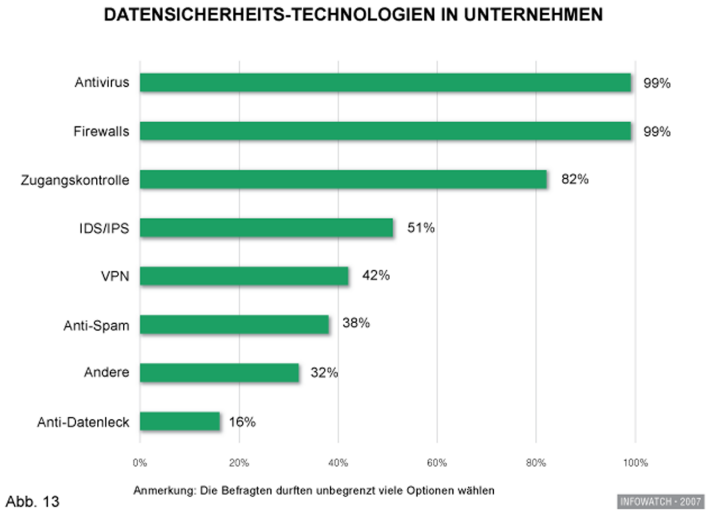

Abbildung 1.2: PGP-Trust Verhältnisse aus [11].

technischen Lösungen für das Problem gibt. Mit diesem Punkt setzen sich insbesondere die Kapitel 4 und 5 auseinander.

Die Idee eines funktionierenden DLP-Systems ist, dass es ungewünschten Datenabfluss auf technischer Ebene unterbinden kann. Dies betrifft sowohl unbekannte Viren und Trojaner, als auch den Mitarbeiter der vertrauliche Daten eigenständig an die Konkurrenz übermittelt. Ein DLP-System macht allerdings eine Anti-Virenlösung deshalb nicht überflüssig. Es verhindert zwar, dass ein Trojaner Daten aus dem Unternehmen entwendet, es hilft jedoch nicht gegen die Installation von Trojanern oder zerstörerischer Viren. Ein Virus, welches Daten löscht oder verschlüsselt, kann seine Tätigkeit unbehelligt vom DLP-System ausführen. Neben der technischen Umsetzung gibt es einige rechtliche Aspekte.

1.3 Rechtliche Aspekte

Rechtlich gesehen ist die Überwachung des Arbeitsplatzes durch ein DLP-System in Österreich, Deutschland und der Europäischen Union (EU) problematisch. Eine eindeutige Rechtssprechung für die EU, Deutschland und Österreich existiert derzeit jedoch noch nicht [22]. Die Gesetze und Richtlinien Deutschlands und Österreichs gleichen einander sehr stark. Letztendlich ist eine Datenerhebung immer dann möglich, wenn der Betroffene eingewilligt hat. Das österreichische Datenschutzgesetz (DSG) sagt zum Thema Privatsphäre in Paragraph 1:

```
§1. (1) Jedermann hat, insbesondere auch im Hinblick
auf die Achtung seines Privat- und Familienlebens,
Anspruch auf Geheimhaltung der ihn betreffenden
personenbezogenen Daten, soweit ein schutzwürdiges Inter-
esse daran besteht. [...]
```

Um dem gerecht zu werden, könnte der Arbeitgeber beispielsweise einen separaten Personal Computer (PC) bereitstellen (evtl. pro Abteilung), welcher von der Überwachung ausgenommen ist. Dies würde zu einer klaren Trennung von beruflichen und privaten Tätigkeiten führen und sollte einen guten Kompromiss zwischen den Interessen des Arbeitgebers und dem Bedürfnis auf Privatsphäre des Arbeitnehmers schaffen. Auf diese Weise wird der Arbeitgeber auch dem Paragraph 3a des deutschen Bundesdatenschutzgesetzes (BDSG) gerecht, welches fordert

```
[...]keine oder so wenig personenbezogene Daten wie mög-
lich zu erheben, zu verarbeiten oder zu nutzen [...]
```

Da es beim Einsatz eines DLP-Systems nicht darum geht, personenbezogene Daten zu sammeln, sondern Werte und Daten des Unternehmens zu schützen, sollte die Einwilligung des Betroffenen ausreichen. Klarheit kann nur ein Gerichtsurteil schaffen. Zur Einwilligung sagt Paragraph 4a Absatz 1 des deutschen BDSG:

```
(1) Die Einwilligung ist nur wirksam, wenn sie auf der
freien Entscheidung des Betroffenen beruht. Er ist auf
den vorgesehenen Zweck der Erhebung, Verarbeitung oder
Nutzung sowie, soweit nach den Umständen des Einzelfalles
erforderlich oder auf Verlangen, auf die Folgen der Ver-
weigerung der Einwilligung hinzuweisen. Die Einwilligung
bedarf der Schriftform, soweit nicht wegen besonderer Um-
stände eine andere Form angemessen ist. Soll die Einwill-
igung zusammen mit anderen Erklärungen schriftlich
erteilt werden, ist sie besonders hervorzuheben.
```

Problematisch für das Unternehmen ist in diesem Zusammenhang die „freie Entscheidung des Betroffenen“. Durch diese Klausel darf der Arbeitgeber keinen Druck auf den Arbeitnehmer ausüben und es darf dem Arbeitnehmer kein Nachteil entstehen, wenn er einen derartigen Vertrag nicht unterschreibt. Sollten besondere Daten (vgl. deutsches BDSG § 3 Abs. 9) von der Überwachung betroffen sein, wäre eine gesonderte Einwilligung nötig. Dies betrifft z.B. Daten der ethnischen Herkunft, politische oder religiöse Überzeugungen usw. und überschneidet sich nicht mit dem Einsatzzweck eines DLP-Systems.

Um dem Grundsatz zu folgen, möglichst wenige personenbezogene Daten zu speichern (§ 3 dt. BDSG), werden nur Verstöße gegen die unternehmensinternen Richtlinien erfasst. Dies reduziert die durch das DLP-System

zu verarbeitende Datenmenge stark, hat aber zur Folge, dass unerkannte Regelverstöße nicht zurück verfolgbar sind. Dazu ein Beispiel:

> Ein Mitarbeiter kopiert unerlaubt eine Datei auf einen externen Datenträger. Weil der DLP-Administrator einen Fehler bei der Implementierung der Regeln gemacht hat, konnte dies nicht verhindert werden und es wurde auch kein Alarm ausgelöst. Der Datendiebstahl wurde zufällig einige Zeit später bemerkt.

Bei einer vollständigen Erfassung der Benutzeraktionen am Rechner ist es feststellbar, wann die betroffene Datei von wem an welchen Speicherort kopiert wurde. Somit kann herausgefunden werden, wer die Datei zu welchem Zeitpunkt entwendet hat. Dies ist nur dann möglich, wenn eine vollständige Erfassung statt findet. Werden aus Datenschutz- oder anderen Gründen nur Verstöße gegen Vorschriften gespeichert, ist es technisch gesehen nicht möglich diese Art des Datendiebstahls aufzuklären.

Eine Firma, die ein DLP-System einsetzen möchte, kann dies nur mit Einwilligung der betroffenen Mitarbeiter tun. Der kritische Punkt ist die Überwachung persönlicher Daten und die Überwachung der Arbeitsleistung. Wenn es einen Betriebsrat gibt, kann dieser Regelungen für den Bereich der Protokollierungsdaten verlangen und durchsetzen. Der Betriebsrat hat nach dem deutschen Betriebsverfassungsgesetz § 87 Abs.1 Nr. 6 ein Mitspracherecht bei

```
Einführung und Anwendung von technischen Einrichtungen,
die dazu bestimmt sind, das Verhalten oder die Leistung
der Arbeitnehmer zu überwachen.
```

Ein DLP-System überwacht das Verhalten, somit ist der Einsatz eines solchen Systems von dieser Vorgabe betroffen. Das Mitspracherecht für den Betriebsrat gilt solange, bis es ein Gesetz gibt, welches die Überwachung regelt.

1.4 Sicherheitsstrategien

Um Daten zu schützen gibt es zwei Kategorien von Sicherheitsstrategien. Zum Ersten die der Zugriffskontroll- und zum Zweiten die der Informationsflussstrategien.

Zugriffskontrollstrategien haben zwar nicht das primäre Ziel den Datenabfluss zu verhindern, allerdings schränken sie den Zugriff auf Daten ein. Die Zugriffsbeschränkung ist auch im Data-Leakage-Prevention Umfeld wichtig, da es, wie später dargelegt wird, unmöglich ist unerlaubten Datenabfluss

vollständig zu unterbinden. Somit ist es für ein Gesamtkonzept weiterhin wichtig, dass nicht jeder Zugriff auf alle Daten hat. Informationsflussstrategien sind die theoretische Grundlage für DLP-Systeme. Sie beschreiben zulässigen und unzulässigen Informationsfluss zwischen Subjekten[3].

1.4.1 Zugriffskontrollstrategien

Die Zugriffskontrollstrategien untergliedern sich in drei Bereiche (vgl. [5] Abschnitt 6.1.3):

- Discretionay Access Control (DAC)
- Mandatory Access Control (MAC)
- Role based Access Control (RBAC)

Discretionay Access Control (DAC), zu deutsch benutzerbestimmbare Zugriffskontrollstrategien, basieren auf dem Eigentümerprinzip. Das bedeutet, dass jedes Objekt einen Eigentümer hat und dieser für den Schutz dieses Objekts verantwortlich ist. Bei der Vergabe der Rechte in einem DAC-System werden Abhängigkeiten zwischen den Rechten nicht beachtet, sodass es zu widersprüchlichen Zuständen kommen kann. Eine widersprüchliche Rechtevergabe wäre beispielsweise, wenn ein Subjekt durch die Berechtigung zur Ausführung einer Operation implizit die Berechtigung zum Lesen eines Objekts erhält, auf der anderen Seite aber ein explizitites Verbot für den lesenden Zugriff auf das Objekt besteht. Microsoft implementiert in der Windows-NT Linie bis einschließlich zum Server 2003, genauso wie Linux ohne Zusatzerweiterungen (z.B. SELinux), das DAC-Modell.

Mandatory Access Control (MAC), zu deutsch systembestimmte oder regelbasierte Zugriffskontrolle, dominieren über die benutzerbestimmbaren Zugriffsrechte. Wenn es eine systembestimmte Festlegung gibt, die einen Zugriff verbietet, gilt dieser auch dann, wenn der Zugriff auf Benutzerzugriffsebene erlaubt wäre. Im Fall von SELinux ist ein MAC-System ein DAC-System mit einer darüberliegenden Schicht, die Rechte auf System- statt Benutzerebene verwaltet. Die nachfolgenden Sicherheitsmodelle „Bell LaPadula“, „Chinese-Wall“ und „Biba“ gehören in die Kategorie der MAC-Systeme. Das MAC-Modell implementieren unter anderem SELinux, Windows Vista und Solaris mit den Trusted Extensions.

Die dritte Zugriffskontrollstrategie ist die rollenbasierte Zugriffskontrolle (RBAC). Im Gegensatz zu den vorher genannten Kontrollstrategien stehen

[3] Subjekte sind im Rahmen dieser Arbeit natürliche Personen.

nicht die Subjekte im Mittelpunkt, sondern deren Aufgaben. Die Zugriffsrechte sind entsprechend auf bestimmte Aufgaben abgestimmt und ein Subjekt wird einer Aufgabe zugeteilt. Somit hat es alle benötigten Berechtigungen. In Betriebssystemen ohne RBAC-Unterstützung wird eine vergleichbare Funktionalität über Gruppenrechte erreicht. RBAC Implementierungen gibt es unter anderem in Sun Solaris sowie GNU/Linux mit RSBAC-Erweiterung[4].

Das Bell LaPadula Modell

Ein Modell für den Zugriffsschutz auf Daten ist das so genannte „Bell LaPadula Modell“. Es sichert die Vertraulichkeit, nicht aber die Integrität von Daten. Das Bell LaPadula Modell soll sicherstellen, dass es nicht möglich ist, Informationen einer höheren Schutzstufe zu lesen, oder Informationen aus einer höheren Schutzstufe in eine Niedere zu überführen. Vor allem militärische Einrichtungen nutzen das Bell LaPadula Modell zum Schutz ihrer geheimen Daten.

Die Schutzstufen sind horizontal (siehe Abbildung 1.3) ausgerichtet. Eine Verfeinerung dieses Modells ist das „Compartement-“ oder „Lattice-Modell“. Bei diesen Modellen gibt es zusätzlich zu den horizontalen Stufen von Bell LaPadula eine vertikale Segmentierung (z.B. neben der Geheimhaltungsstufe werden Daten einer Abteilung zugeordnet).

Mit Betriebssystemen, die Mandatory Access Control implementiert haben, lässt sich auch das Bell LaPadula Modell realisieren. Beispiele wären Solaris Trusted Extensions, Trusted HP-UX, Trusted IRIX oder auch SELinux. Bell LaPadula unterscheidet zwischen zwei Regeln: der „Simple Security Property“ und der „*-Property“.

Jedes Subjekt (jeder Mitarbeiter), hat eine bestimmte Rolle. Jede Rolle hat Rechte in einer Geheimhaltungsstufe. Die Simple Security Property verhindert, dass jemand Informationen aus einer höheren Geheimhaltungsstufe lesen kann (No-Read-Up Policy). Allerdings ist ein Informationsfluss von einer höheren in eine niedrigere Geheimhaltungsstufe noch möglich.

Mit der Implementierung der *-Property schließt sich diese Lücke. Durch die *-Property ist es nicht mehr möglich, Daten in eine niedere Geheimhaltungsstufe zu überführen (No-Write-Down Policy). Ein Subjekt kann nur noch Objekte (Dokumente) in seiner eigenen oder höheren Geheimhaltungsstufe erstellen.

Problematisch ist die Erstellung und Modifikation von Daten in einer höheren Ebene. Ein Subjekt kann „blind“ in eine höhere Schutzstufe schreiben, aber

[4] http://www.rsbac.org/

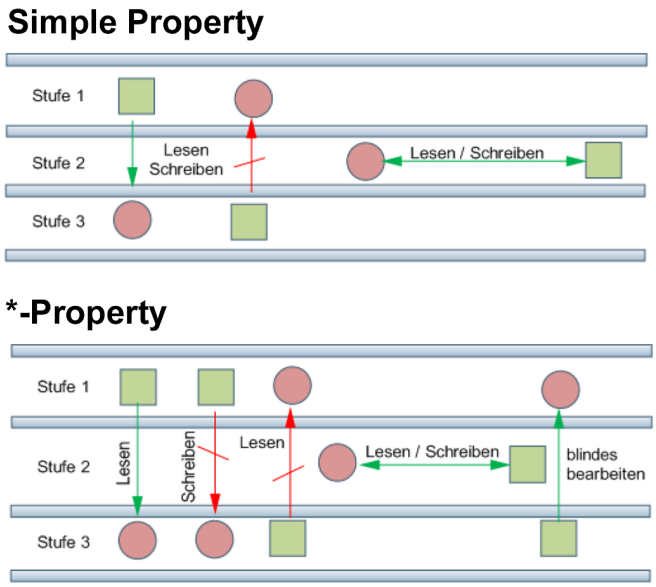

Abbildung 1.3: Simple Property vs. *-Property

die verursachten Änderungen nicht mehr lesen. Das blinde Schreiben ist zur Erfüllung von Integritätsanforderungen kritisch, da ein Subjekt ein Objekt beliebig manipulieren kann. Ein Beispiel:

> Jemand stellt Nachforschungen über etwas an und übergibt die Ergebnisse an seinen Vorgesetzten. Daraufhin hat er keinen lesenden Zugriff mehr auf sein erstelltes Dokument. Es ist aber nach wie vor möglich, dass er das Dokument ohne Leserechte, also blind, ändern kann. So ist es möglich, Falschinformationen auf eine höhere Schutzstufe zu heben.

Die Abbildung 1.3 zeigt die Unterschiede zwischen den beiden Policies. Die Realisierung von Bell LaPadula auf einem einzelnen System ist mit Unterstützung eines der vorher genannten Betriebssysteme möglich. Heutzutage sind Systeme vernetzt, daher muss es zum sinnvollen Einsatz möglich sein, Netzwerkkommunikation in den verschiedenen Stufen umzusetzen. Das Internet Protokoll (IP) bietet für diesen Zweck die „Commercial IP Security Option“ (CIPSO), welche die Vertraulichkeitsstufe eines IP-Pakets „Option“-Feld des IP-Headers codiert.

Durch die Kombination aus Dateisystemberechtigungen und DLP-Klassifizierungen ist es möglich mit einem DLP-System Bell LaPadula zu implementieren. Das verwendete Betriebssystem muss dazu nur Zugriffsrechte

auf Dateisystemebene durchsetzen können. Dies ist allerdings nicht Ziel eines DLP-Systems. Ein DLP-System soll Daten nicht vor unbefugtem Zugriff oder Veränderung schützen, sondern vor der Entwendung von Informationen.

Das Biba-Modell

Das Biba-Modell ist ein Sicherheitsmodell, das die Datenintegrität sicher stellt. Es wurde nicht entwickelt um die Vertraulichkeit der Daten zu garantieren. Das Biba-Modell wurde entwickelt, um die Schwäche des Bell LaPadula Modells zu beheben, dass aus einer niederen Schutzstufe in eine höhere Schutzstufe „blind“ geschrieben werden kann. Mit dem Biba-Modell ist sicher gestellt, dass ein Subjekt keine Daten einer höheren Schutzstufe manipulieren kann. Zum Zweiten ist es nicht möglich, als Mitglied einer höheren Schutzstufe Daten aus einer niederen Schutzstufe zu lesen. Folgendes Szenario wäre denkbar:

> Ein Mönch schreibt ein Gebetsbuch, das von den Bürgern gelesen werden kann, nicht jedoch vom Abt. Umgekehrt kann ein Mönch nur Bücher lesen, die von einem Abt geschrieben wurden, nicht aber den Text eines einfachen Bürgers.

Wie bei Bell LaPadula gibt es auch bei Biba eine Simple- und eine *-Property. Sie sind genau umgekehrt wie in Bell LaPadula.

- Simple Property: Ein Subjekt in einer definierten Integritätsstufe kann keine Objekte aus einer niederen Integritätsstufe lesen (No-Read-Down Policy)
- *-Property: Ein Subjekt in einer definierten Integritätsstufe kann keine Objekte in eine höhere Integritätsstufe schreiben oder manipulieren (No-Write-Up Policy)

Für das Thema Data-Leakage-Prevention ist dieses Modell in der Hinsicht relevant, dass es für einen hochrangigen Mitarbeiter (in einer hohen Schutzstufe) nicht möglich ist die Daten aus den niederen Schutzstufen (in der sich potentiell sehr viele Daten befinden) zu lesen oder weiter zu geben. In Windows Vista hat Microsoft das Biba-Modell implementiert.

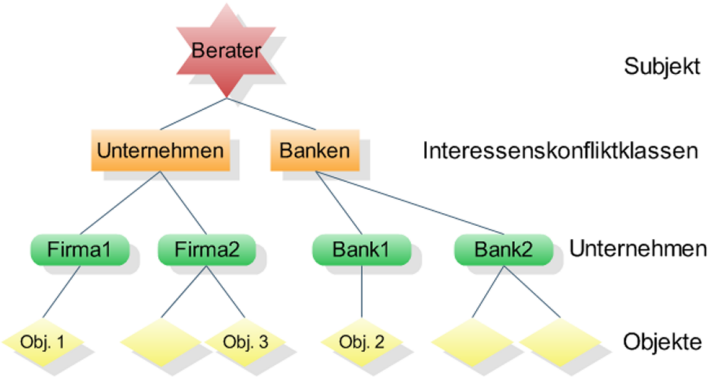

Abbildung 1.4: Objektbaum im Chinese-Wall-Modell

Das Chinese-Wall-Modell

Das Chinese-Wall-Modell (Brewer-Nash Modell) gehört ebenfalls zu den Zugriffskontrollmodellen, bietet aber im Gegensatz zu den beiden vorher beschriebenen Modellen zusätzlich eine Informationsflussbehandlung und ist somit für den Aufbau von DLP-Systemen relevant. Es wurde entwickelt, um die Nutzung von Insiderwissen bei der Abwicklung von Bankgeschäften oder der Beratung unterschiedlicher Unternehmen zu verhindern.

Die grundlegende Idee des Chinese-Wall-Modells basiert darauf, dass die Zugriffsgewährung eines Subjekts auf ein Objekt davon abhängt, auf welche anderen Objekte es in der Vergangenheit bereits zugegriffen hat (vgl. [5] Abschnitt 6.2.3). Die Zugriffshistorie entscheidet, was ein Subjekt darf und was nicht.

Im Chinese-Wall-Modell sind die zu schützenden Objekte in einem Baum strukturiert. Die Blätter des Baumes sind die Objekte, die Unternehmen verwalten. Die Unternehmen stehen somit auf der zweiten Ebene. Die dritte Ebene bilden die Interressenskonfliktklassen. An der Spitze steht der Berater, das Subjekt (siehe Abbildung 1.4).

Die Konfliktklassen in Abbildung 1.4 sind Unternehmen und Banken. Das Objekt Obj. 1 gehört Firma1 und liegt in der Interessenskonfliktklasse aller Unternehmen. Auch Obj. 3 befindet sich in dieser Interessenskonfliktklasse. Das Objekt Obj. 2 steht in keinem Interessenskonflikt zu Obj. 1 und Obj. 3. Ab dem Zeitpunkt in dem der Berater auf das Objekt Obj. 1 zugegriffen hat, darf er nicht mehr auf die Objekte von Firma2 zugreifen, da sie in der gleichen Interessenskonfliktklasse liegen. Er darf aber nach wie vor auf alle Objekte der beiden Banken zugreifen. In dem Moment, in dem er auf Obj. 2 zugreift, ist der Zugriff auf die Objekte von Bank2 gesperrt und ein Informationsaustausch zwischen Bank2 und Firma1 unmöglich.

Bei mehr als einem Subjekt ist der Informationsaustausch unter folgenden Umständen weiterhin möglich: Subjekt1 greift zunächst lesend auf Obj. 1 und anschließend schreibend auf Obj. 2 zu. Daraufhin liest das Subjekt2 die Informationen aus Obj. 2 und schreibt sie in Obj. 3. In diesem Fall findet ein unerwünschter Informationsfluss zwischen Obj. 1 und Obj. 3 innerhalb einer Interessenskonfliktklasse statt.

Deshalb gibt es eine zusätzliche Regel die besagt, dass nach einem Lesezugriff auf ein Objekt aus einer Interessenskonfliktklasse kein schreibender Zugriff auf Objekte einer anderen Interesseskonfliktklasse zulässig ist. Somit ist ein Informationsfluss zwischen verschiedenen Interessenskonfliktklassen nicht möglich.

1.4.2 Informationsflussstrategien

Im Gegensatz zu den bisher beschriebenen Zugriffskontrollstrategien, steht bei den Informationsflussstrategien, wie auch bei DLP-Systemen, die Informationssicherheit im Mittelpunkt. Die Strategien beschreiben zulässige und unzulässige Informationskanäle zwischen verschiedenen Subjekten (vgl. [5] Abschnitt. 6.3).

Das Verbandsmodell

Das Verbandsmodell ist ein Informationsflussmodell. Es verallgemeinert den Bell LaPadula Ansatz und beschreibt Informationsflüsse zwischen Datenvariablen eines Programms. Das charakteristische am Verbandsmodell ist, dass Beschränkungen für den Informationsfluss unabhängig von den Objekten, die die Informationen repräsentieren, festgelegt sind. Das bedeutet, dass es Vorschriften für zulässige und unzulässige Informationskanäle gibt, die den Umgang mit Informationen reglementieren. Informationen dürfen nur innerhalb von Sicherheitsstufen oder gemäß einer festgelegten Ordnung fließen.

Analog zum Bell LaPadula Modell besitzt jedes Objekt und jedes Subjekt eine Sicherheitsmarke. Im Verbandsmodell dürfen Informationen nur innerhalb einer Sicherheitsstufe oder aufwärts fließen. Ein abwärts gerichteter Informationsfluss sowie der Fluss zwischen Sicherheitsstufen, die in keiner Beziehung zueinander stehen, ist in diesem Modell nicht erlaubt.

Mit dem Verbandsmodell ist es möglich, Informationsflüsse zu definieren. Nachteile ergeben sich daraus, dass für jede Sicherheitsstufe die erlaubten Informationsflüsse definiert sein müssen. Für eine detaillierte Definition sind daher entsprechend viele Sicherheitsstufen festzulegen. Dies hat sehr

aufwändige und schlecht skalierende Verwaltungsmaßnahmen bei der Realisierung solcher Systeme zur Folge.

Ein weiterer Nachteil des Modells liegt in der unflexiblen Sicherheitsklassifikation. Im Wesentlichen findet eine statische Zuordnung von Objekten zu einer Sicherheitsstufe statt. Das hat zur Folge, dass zu niedrig eingestufte Subjekte so wenige Rechte erhalten, dass sie ihre Tätigkeiten nicht mehr ausführen können. Um dies zu vermeiden werden in der Praxis die Subjekte häufig zu hoch eingestuft, mit der Konsequenz, dass die Benutzer mehr Rechte haben, als benötigt (vgl. [5] Abschnitt 6.3). Somit haben sie Zugang zu mehr Informationen, als erlaubt.

Neben dem beschriebenen Verbandsmodell, gibt es weitere Informationsflussmodelle, wie z.B. das Modell von Sutherland [20] oder das Restrictiveness-Modell von Mc-Cullough [14].

1.5 Firmenpolicies und organisatorische Maßnahmen

Die beschriebenen Sicherheitsmodelle technisch zu implementieren ist ein Weg, um Informationssicherheit zu gewährleisten. Neben technischen Maßnahmen werden Firmenpolicies definiert, die den Umgang mit Daten regeln. Firmenpolices sind Richtlinien oder Vorschriften, die für Mitarbeiter im Unternehmen gelten. Sie sind eine notwendige Maßnahme dem Datendiebstahl entgegen zu wirken, da sie definieren was erlaubt und verboten ist.

Solche Vorschriften können z.B. ein Verbot von bestimmten Gegenständen (Kameras und Mobiltelefonen), oder Richtlinien im Umgang mit unbekannten Dateien enthalten. Neben der Einführung von Policies hat es sich in der Praxis als sinnvoll erwiesen, Awareness-Schulungen zum Thema Datenschutz und Datensicherheit durchzuführen, um den Mitarbeitern die Auswirkungen ihres Handels zu verdeutlichen.

Zur Erstellung und Durchsetzung von Firmen- bzw. Sicherheitspolicies ist ein IT-Sicherheitsmanagement nötig. Dies einzuführen ist der erste Schritt um einen effektiven Datenschutz zu implementieren. Anschließend können die Maßnahmen, die im weiteren Verlauf beschrieben werden, umgesetzt werden. Nach einer persönlichen Mitteilung von Klaus Hecht [9], würde „ohne IT-Sicherheitsmanagement die Einführung einer effektiven DLP-Strategie fehlschlagen, da die Einführung eines DLP-Systems organistorisch nicht durchführbar ist“.

In Fällen, in denen Unternehmen externen Compliancerichtlinien (z.B. Sarbanes Oxley, HIPAA) unterliegen, müssen diese Firmen Policies zum Datenschutz haben. DLP-Systeme können die Richtlinien auf effiziente Weise

unterstützen und dem Benutzer Arbeitsschritte abnehmen. Hierzu ein Beispiel:

> Die Firmenpolicy besagt, dass vertrauliche Daten zwischen den Unternehmensstandorten nur dann per E-Mail versendet werden dürfen, wenn sie sicher verschlüsselt sind. Ein DLP-System kann die Aufgabe der automatischen Ver- und Entschlüsselung von E-Mails übernehmen, ohne dass der Benutzer sich um die Eingabe von Passwörtern kümmern muss.

Outsourcing verschiedener Bereiche der IT ist heutzutage nicht unüblich, wie beispielsweise die „Gartner Outsourcing & Vendor Management Summit“[5] zeigt. Um zu verhindern, dass vertauliche Kundeninformationen vom Outsourcing-Partner ungewollt verwertet werden, sind Regelungen nötig. In diesen muss definiert sein, wie mit Daten und externen Partnern umzugehen ist und wie sichergestellt werden kann, dass der Outsourcing-Partner die Daten nicht weiter gibt. Eine Möglichkeit besteht beispielsweise darin, das DLP-System auf den externen Systemen ebenfalls zu installieren, um die Datensicherheit zu gewährleisten.

Neben technischen Maßnahmen muss es eine eindeutige Zuordnung der Verantwortung für die Daten geben. Eine klare Abgrenzung der Verantwortungsbereiche ist z.B. nötig, um im Fall einer Datenschutzverletzung jemanden zur Rechenschaft ziehen zu können. Die Verantwortungen zu definieren ist Aufgabe des IT-Sicherheitsmanagements. Um die Zuordnung von Daten umsetzen zu können, ist eine Klassifizierung der Daten nötig (siehe Kapitel 3).

1.6 Grenzen der Technik

Technische Maßnahmen bzw. DLP-Systeme haben Grenzen, da sie nur Computer überwachen können, nicht aber ihr physisches Umfeld. Daher gibt es, abhängig von Art und Menge der zu schützenden Daten, Möglichkeiten ein DLP-System zu umgehen. Mehrere Szenarien sind denkbar, wie die nachfolgenden Beispiele zeigen.

Wenn ein Mitarbeiter einen geheimen Bauplan vom Monitor abfotografiert, kann eine Software dies nicht unterbinden. Unmöglich ist es ebenfalls, die im Gehirn des Angestellten gespeicherten Informationen am Ausgang zu löschen. Ein Mitarbeiter kann interessante Daten auch mit einem Stift zu Papier bringen und somit alle Systeme umgehen. Eine weitere Möglichkeit

[5] http://www.gartner.com/it/page.jsp?id=597509

besteht darin, die Daten in ein nicht kontrollierbares Format umzuwandeln, z.B. in dem er sie in eine fremde Sprache übersetzt. Dies kommt einer manuellen Verschlüsselung gleich.

Allerdings ergibt sich für den Datendieb das Problem, dass der Aufwand der schriftlichen Datenspeicherung schnell an einen Punkt gerät, wo dies aufgrund der Menge nicht mehr möglich ist. Sollte die Datenmenge jedoch klein genug sein, um sie auf Papier zu bringen, ist der Einsatz eines DLP-Systems ohne Nutzen. Problematisch ist es ebenfalls, wenn die Administratoren des DLP-Systems selbst versuchen Daten zu stehlen. Sie können die Einstellungen der Software nach ihren Wünschen anpassen und Hinweise auf Manipulationen verschleiern.

Somit ist festzustellen, dass DLP-Systeme nur dann sinnvoll einsetzbar sind, wenn die zu schützenden Datenmengen so umfangreich sind, dass sie nicht ohne Hilfe der IT-Infrastruktur aus dem Unternehmen entwendet werden können.

Kapitel 2

Wege aus dem Unternehmen

Daten aus einem Unternehmen heraus zu schmuggeln oder zu stehlen ist das Ziel eines Angreifers. Um dieses Ziel zu erreichen, stehen ihm viele Mittel und Wege offen, wie dieses Kapitel zeigen wird. Aufgabe der IT-Sicherheitsverantwortlichen ist es, diese Kanäle abzusichern und den Abfluss von vertraulichen Daten zu verhindern. Eine Übersicht über mögliche Kanäle zeigt Abbildung 2.1.

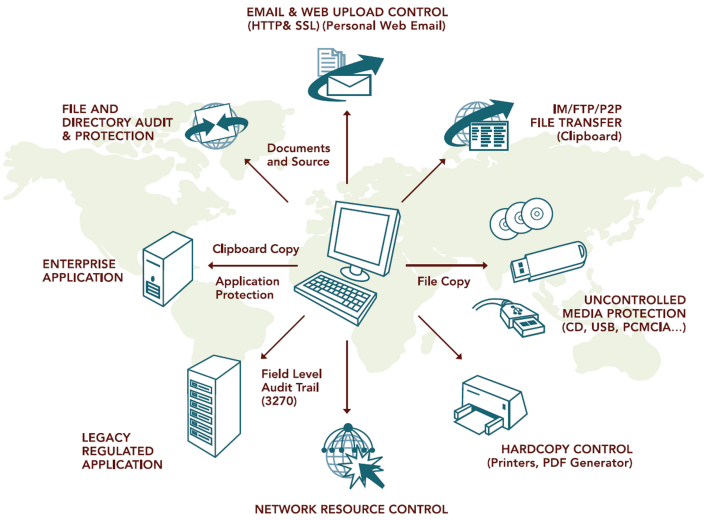

Abbildung 2.1: Datenkanäle aus dem Unternehmen [21]

2.1 Interne und Externe Speichermedien

Eine einfache Möglichkeit Daten unerlaubt aus dem Unternehmen zu befördern sind externe Speichermedien. Nachfolgend eine Liste der gängigen Datenträger:

- USB-Stick
- beschreibbare CD und DVD
- USB-Festplatten
- Firewire-Festplatten
- Musik-Player (mp3-Player, iPod)
- Digitalkamera
- Mobiltelefon (Bluetooth, Infrarot, USB)
- Wechselfestplatten
- Speicherkarten (SD, MemoryStick)
- Diskette
- Bandlaufwerke

Die Fähigkeit eines DLP-Systems mit externen Speichermedien umgehen zu können ist unter dem Begriff „Endpoint-Security“ bekannt. Die Gefahr des Datenverlusts durch externe Speichermedien ist als sehr hoch anzusehen, da sie einfach zu verwenden sind und gleichzeitig sehr hohe Speicherkapazitäten bieten. Im Gegensatz zu E-Mail lassen sich so auch große Datenmengen (mehrere Gigabyte) aus dem Unternehmen heraus transferieren.

Die Gefahr, dass interne Datenträger als Medium für Datendiebstahl genutzt werden ist etwas geringer, da hierfür das Gehäuse des Computers geöffnet werden muss. Dies ist im Vergleich zur Verwendung externer Speichermedien aufwändiger, aber ohne weitere Schutzmaßnahmen (siehe Kapitel 4) nicht schwierig.

2.2 Internetbasierte Wege

Neben internen und externen Datenträgern stellen internetbasierte Kanäle ebenfalls eine hohe Gefahr dar. Aufgrund der geringeren Übertragungsrate

im Vergleich zu internen und externen Datenträgern, ist die Möglichkeit große Datenmengen zu transportieren eingeschränkt. Dies spielt aber nur bei sehr großen Datenmengen und beschränktem Zeitfenster eine Rolle. Die folgende Aufzählung gibt einen Überblick über die internetbasierten Kanäle:

- E-Mail
- Instant Messenger
- Peer to Peer Netzwerke
- HTTP / HTTPS[1]
- FTP[2], SCP[3] und andere Uploadprotokolle

Neben dem firmeneigenen Internetanschluss kann ein Mitarbeiter, vorausgesetzt ihm steht ein technisch entsprechend ausgerüstetes Telefon zur Verfügung, eine eigene Internetverbindung aufbauen. Die Bandbreite, die z.B. das Universal Mobile Telecommunications System (UMTS) zur Verfügung stellt, ist ausreichend, um größere Datenmengen aus dem Unternehmen zu transferieren. Mit UMTS lassen sich bei einer Uploadbandbreite von 384kbit/s in einer Stunde etwa 165 Megabyte Daten übertragen.

2.2.1 E-Mail

Bei den internetbasierten Kanälen ist E-Mail eine sehr weit verbreitete Art, Daten aus dem internen Netz heraus zu senden. Die Datenmengen, die sich per E-Mail verschicken lassen, sind im Vergleich mit externen Datenträgern zwar gering, allerdings ist die Gefahr, dass Daten auf diesem Weg das Unternehmen verlassen totzdem hoch. E-Mail wird in vielen Bereichen verwendet und ist somit grundsätzlich eine Anwendung, die vielen Mitarbeitern zur Verfügung steht. E-Mail komplett zu verbieten ist daher nur selten möglich.

Der Versand von E-Mails vom Client aus kann über verschiedene Protokolle erfolgen. Verbreitet sind SMTP(S)[4], MAPI[5] und HTTPS, es gibt allerdings einige weitere proprietäre Protokolle, die zur Datenübertragung zwischen Client und Mailserver genutzt werden. E-Mail-Provider bieten teilweise sehr große IMAP[6] Postfächer an (z.B. GMX, Google im Gigabyte-Bereich). Über IMAP und seine verschlüsselte Variante sind ebenfalls Uploads möglich.

[1] Hyper Text Transport Protocol / Secure
[2] File Transfer Protocol
[3] Secure Copy
[4] Simple Mail Transport Protocol (Secure)
[5] Messaging Application Programming Interface
[6] Internet Message Access Protocol

Neben lokal installierten Mailprogrammen existieren eine Vielzahl von Webmailanbietern, die es ermöglichen E-Mails zu versenden. Der Upload der Daten erfolgt dabei sowohl über unverschlüsseltes HTTP als auch über verschlüsseltes HTTPS.

2.2.2 HTTP / HTTPS

Das HTTP-Protokoll dient hauptsächlich dem Download von Webseiten aus dem Internet. Neben dem Download bietet es jedoch auch die Möglichkeit, Daten zu versenden. Dass die Uploadmöglichkeit über HTTP allgemein bekannt ist und genutzt wird, zeigen große Dateihoster wie Rapidshare[7] oder Megaupload[8]. Das Geschäftsmodell dieser Dateihoster ist die Speicherung von Daten, die die Kunden über HTTP auf die Server laden.

Da die Verwendung von HTTP, genau wie SMTP für die meisten Mitarbeiter erlaubt sein muss, damit sie arbeiten können, besteht nicht die Möglichkeit HTTP generell zu sperren. Gleiches gilt für die verschlüsselte Variante HTTPS. Die Gefahr, die durch HTTP(S) besteht ist somit ebenfalls als hoch zu bewerten.

2.2.3 Instant Messenger

Neben E-Mail ist Instant Messaging zu einem beliebten Kommunikationsmittel geworden. Es gibt eine Vielzahl Protokolle und Anwendungen. Die Meisten von ihnen erlauben den Dateiversand und stellen somit eine Gefahr für die Datensicherheit dar. Viele Protokolle sind unverschlüsselt, allerdings bieten modernere Protokolle oft starke Verschlüsselung an. Zu den bekanntesten Vertretern gehören AIM, Jabber, ICQ, IRC, MSN und Skype. Skype und Jabber gehören zu den jüngeren Protokollen und arbeiten mit starker Verschlüsselung.

Instant Messenger sind leicht zu bedienen und eignen sich daher gut, um geheime Daten aus dem Unternehmen zu senden. Ist die Verwendung von Instant Messengern erlaubt, so ist die Gefahr eines unerwünschten Datenversands genauso hoch, wie bei den bisher beschriebenen internetbasierten Kanälen.

2.2.4 Peer to Peer

Tauschbörsen haben einen hohen Anteil am globalen Datenaufkommen im Internet. Populäre Protokolle sind derzeit BitTorrent, eDonkey, Gnutella

[7] http://www.rapidshare.com
[8] http://www.megaupload.com

und DirectConnect. Tauschbörsen eignen sich ebenfalls um Daten aus dem Unternehmen zu schleusen, allerdings ist die Anwendung unkomfortabler als beim Instant Messaging, E-Mail oder Webupload per HTTP(S).

2.2.5 Weitere Protokolle

Neben den bereits beschriebenen Protokollen, die sich zum Upload von Daten eignen, gibt es eine Reihe weiterer Protokolle die, wenn sie erlaubt sind, eine Gefahr darstellen. Das Webdav Protokoll sollte nicht unerwähnt bleiben, da es HTTP erweitert und somit in vielen Fällen über die Firewall hinaus erlaubt ist. Neben HTTP sind FTP sowie SCP geeignet und weit verbreitet um Daten auf ein externes System zu übertragen. Neben bekannten Protokollen kann ein Angreifer auch ein eigenes Protokoll verwenden, oder die Daten über Tunneltechnologien (z.B. SSH-Tunnel) oder Virtuelle Private Netzwerke (VPN) versenden.

2.3 Drucker

Sind die Möglichkeiten, Daten über das Internet oder elektronische Datenträger zu entwenden blockiert, bleibt einem Angreifer die Möglichkeit, die gewünschten Daten auszudrucken. Die Gefährdung, die dadurch entsteht ist abhängig davon, wie umfangreich die schützenswerte Datenmenge ist. Bewegt sie sich in Größenordnungen, die nicht druckbar sind, ist sie vernachlässigbar. Neben physischen Druckern lassen sich auch virtuelle Drucker (z.B. FreePDF) nutzen um Daten umzuwandeln und zu entwenden (siehe Abschnitt 5.10).

2.4 Entsorgung von Speichermedien

An einem gewissen Zeitpunkt sind Datenträger zu entsorgen. Die Dauer bis dieser Zeitpunkt erreicht ist, variiert zwischen verschiedenen Datenträgern und kann je nach Verwendungszweck und Medium zwischen wenigen Tagen (z.B. CD-R für Datentransport) und Jahrzehnten (Langzeitspeichermedien) liegen. Falls Daten, die zum Entsorgungszeitpunkt auf dem Datenträger gespeichert sind, noch immer relevant sind, besteht bei unsachgemäßer Entsorgung die Gefahr, dass diese Daten ungewollt in die falschen Hände geraten.

Unter unsachgemäßer Entsorgung eines Datenträgers ist alles zu verstehen, was es einem Angreifer ermöglicht, Daten vom zu entsorgenden Medium zu lesen bzw. zu rekonstruieren. Beispiele hierfür wären die Entsorgung von Datenträgern im Elektronikmüll, Restmüll oder bei einem Elektronikhändler.

2.5 Datensicherung

Eine Datensicherung der relevanten Daten findet heute in vielen Unternehmen statt. Die Datensicherung kann auf verschiedenen Medien erfolgen. Üblich sind heute Magnetbänder, optische Medien oder Festplatten. Wenn die gesicherten Daten auf den Sicherungsmedien unverschlüsselt aufbewahrt werden, ist die Gefahr hoch, dass die Daten von Unbefugten ausgelesen werden. Ein Angreifer braucht beispielsweise nur das Sicherungsmedium stehlen und bekommt so Zugriff auf die Daten.

Die Gefahr des Datendiebstahls von Datensicherungsmedien wächst mit der externen Lagerung von Datensicherungen. Sie lagern im Idealfall örtlich getrennt vom Ort der Erstellung, um im Katastrophenfall (Brand, Überschwemmung, Erdbeben usw.) nicht zerstört zu werden. Somit ist auch der Transportweg zum externen Datensicherungsort eine Gefahr für die Daten. Ein Angreifer kann die Daten während des Transports stehlen und hat im Fall, dass die Daten nicht verschlüsselt sind, Zugriff auf diese.

Kapitel 3

Klassifizierung von Daten

Um Daten durch ein Data Leakage Prevention System zu schützen, müssen diese klassifiziert werden. Klassifizierung bedeutet, dass die Daten einer Vertraulichkeitsklasse zugeordnet werden. Anhand der Klassifizierung und den damit verbundenen Bestimmungen entscheidet ein DLP-System, welche Nutzung bestimmter Daten unter den gegebenen Umständen erlaubt bzw. nicht erlaubt ist.

3.1 Vertraulichkeitsklassen

Bevor Daten klassifiziert werden können, müssen Vertraulichkeitsklassen definiert werden. Dies ist Aufgabe des IT-Sicherheitsmanagements. Das österreichische Informationssicherheitsgesetz schlägt in Paragraph 2 Absatz 2 die Klassen „eingeschränkt“, „vertraulich“, „geheim“ und „streng geheim“ vor. Das österreichische Datenschutzgesetz unterscheidet in Artikel 2 Paragraph 4 zwischen „nur indirekt personenbezogen“, „personenbezogen“ und „sensibel“. Die Definition der Klassen kann individuell angepasst werden. Für ein Unternehmen könnten die Vertraulichkeitsklassen beispielsweise wie folgt aussehen:

- nicht klassifiziert
- vertraulich
- geheim
- streng geheim

Hierbei handelt es sich um eine Halbordnung, die in diesem Beispiel ansteigend ist:

nicht klassifiziert < vertraulich < geheim < streng geheim

Daten die „nicht klassifiziert“ sind, sind für die Veröffentlichung freigegeben. Dies sind beispielsweise Pressetexte oder Produktwerbungen. Vertrauliche Daten sind nicht für die Öffentlichkeit gedacht. Darunter fallen alle firmeninternen Arbeitsdokumente. Daten die als „geheim“ klassifiziert sind, würden bei Veröffentlichung einen erheblichen Schaden anrichten. Die höchstmögliche Klassifikation in diesem Beispiel wäre „streng geheim“. Informationen dieser Vertraulichkeitsklasse sind geheim und bei Veröffentlichung würde ein schwerer Schaden entstehen.

Die Kriterien, die für eine Klassifizierung nötig sind müssen definiert sein, bevor mit der Klassifizierung begonnen werden kann. Diese Kriterien müssen präzise sein und wenig Interpretationsspielraum bieten.

3.2 Umgang mit Klassifizierung

Als Nächstes ist zu bestimmen, wer für die Klassifizierung verantwortlich ist. Beim Einsatz eines Sicherheitsmodells (siehe Abschnitt 1.4) ergibt sich die Zuständigkeit aus dem verwendeten Modell. Kommt kein Sicherheitsmodell zum Einsatz, so ist die Verantwortung für die Klassifizierung über eine Policy zu regeln, die der IT-Sicherheitsverantwortliche erstellt. Die Policies müssen durch das Firmenmanagement akzeptiert und durchgesetzt werden, damit Verstöße geahndet werden können.

Die Zuständigkeit könnte beispielsweise derjenige übernehmen, der die Daten erstellt. Es könnte aber auch eine übergeordnete Instanz sein, die entscheidet, welche Daten welchen Vertraulichkeitsgrad bekommen sollen. Derjenige der zuständig ist, trägt die Verantwortung für die korrekte Klassifizierung.

Daten, die einmal klassifiziert wurden verlieren diese Klassifizierung nicht mehr (eine Änderung der Klassifizierung ist weiterhin möglich). Diese Eigenschaft ist vom Sicherheitsstandpunkt aus betrachtet zwar nützlich, aber nicht immer erwünscht. Ein mögliches Szenario wäre, dass alle Dokumente spätestens fünf Jahre nach ihrer Erstellung die Vertraulichkeitsstufe „nicht klassifiziert“ bekommen sollen. Dies ist z.B. bei gesperrten österreichischen Diplomarbeiten der Fall. Falls ein vergleichbares Szenario gegeben ist, müssen Deklassifizierungsrichtlinien existieren, die ebenfalls vom IT-Sicherheitsbeauftragten erstellt werden.

3.3 Klassifizierung mit DLP-Systemen

Abhängig davon welche Mechanismen das DLP-System unterstützt, kann die Klassifizierung manuell oder automatisiert erfolgen. Die automatische Klassifizierung erfordert kein Eingreifen des Endbenutzers und erfolgt somit für ihn transparent. In diesem Fall legt der IT-Sicherheitsverantwortliche die Regeln für die Klassifikation fest. Der Benutzer hat zu keinem Zeitpunkt die Möglichkeit selbst zu entscheiden, welche Daten das System klassifiziert. Alternativ zur automatischen Klassifizierung kann der Benutzer die Dokumente selbstständig klassifizieren und deklassifizieren.

Beide Arten der Klassifizierung haben Vor- und Nachteile. Der Vorteil der automatischen Klassifizierung ist, dass sie Daten im Vergleich zur manuellen Methode sehr zeiteffizient klassifiziert. Der Nachteil ist, dass der Eigentümer, der die Daten am besten kennt, nicht in den Klassifizierungsprozess eingreifen kann. Die automatische Methode verhindert allerdings auch, dass ein Benutzer vertrauliche Daten absichtlich nicht klassifiziert.

Vorteil bei der manuellen Klassifizierung ist, dass die Daten individuell und genauer klassifizierbar sind. Im Rahmen dieser Arbeit wurde festgestellt, dass in der Praxis die automatische Klassifizierung nicht so feingranular konfigurierbar ist, dass sie vergleichbare Ergebnisse erzielt wie die manuelle Methode. Nachteilig ist wiederum, dass bei der Einführung eines DLP-Systems alle relevanten Daten manuell klassifiziert werden müssen, was einen zeitlichen und personellen Aufwand mit sich bringt und zusätzliche Kosten verursacht.

Die Klassifizierung, die das DLP-System durchführt, ist entweder kontext- oder inhaltsbezogen. Kontextbezogen bedeutet, dass die Entscheidung zur Klassifizierung auf dem Dateityp, Speicherort, einer Dateioperation, dem Kommunikationskanal oder Vergleichbarem basiert. Ein Beispiel wäre der Kopiervorgang von einem Dateiserver auf einen USB-Stick. Alternativ dazu kann ein DLP-System nach dem Inhalt einer Datei (inhaltsbezogen) klassifizieren (siehe auch Abschnitt 3.4). Beispielsweise kann das System alle Dokumente, die die Wörter „Top Secret“ und „Studie“ als geheim klassifizieren.

Auf der technischen Seite muss ein DLP-System dafür sorgen, dass die Klassifizierung nicht durch Unberechtigte aufgehoben werden kann. In dem Moment, wo keine Klassifizierung mehr gegeben ist, kann das DLP-System die Daten nicht mehr schützen.

3.4 Inhaltsbezogene Klassifizierung

Die inhaltsbezogene Klassifizierung wird auch als „Content Inspection“ bezeichnet. Diese erspart dem Benutzer die händische Klassifizierung, bzw. ermöglicht ihm diese erst gar nicht, da das DLP-System sie selbstständig durchführt. Diese Vorgehensweise setzt voraus, dass das DLP-System alle Dateiformate die verwendet werden, verarbeiten kann. Andernfalls kann es den Inhalt nicht lesen und somit nicht entscheiden, ob der Inhalt einer Datei die Voraussetzungen für eine Klassifizierung erfüllt.

Ein mögliches Kriterium kann beispielsweise das Vorkommen von mehr als fünf Kreditkartennummern innerhalb eines Dokuments sein. Dazu muss das DLP-System nur wissen, wie eine Kreditkartennummer aufgebaut ist und das Dokumentenformat interpretieren können. Die Umsetzung geschied über die Verwendung von Regular Expressions, die das DLP-System überprüft. Die Regular Expression für eine MasterCard Kredikartennummer sieht beispielsweise wie folgt aus:

```
(3[47][0-9]{2}(-|\s)?[0-9]{6}(-|\s)?[0-9]{5})
```

Die Bedingung, ein Dokument mit mehr als fünf MasterCard Kreditkartennummern zu klassifizieren, kann beispielsweise so aussehen:

```
<greaterThan>
        <evtBufferEntityFrequency name="cc_mastercard"/>
        <int value="5"/>
</greaterThan>
```

Die DLP-Administratoren müssen bei der Content Inspection allerdings genau wissen, wie vertrauliche Daten aussehen und welches Format sie haben, um entsprechende Regeln für das DLP-System zu erstellen.

Kapitel 4

Lösungsansätze

Nachdem die vorangegangenen Kapitel die theoretischen Grundlagen erklärt und Bedrohungen für die Datensicherheit aufgezeigt haben, analysiert dieses Kapitel die technischen Lösungsansätze, wie sie in der Praxis zum Einsatz kommen. Es gibt mehrere Lösungsansätze, die je nach Einsatzumfeld besser oder schlechter geeignet sind. Eine Lehrmeinung oder ein anerkanntes Referenzmodell für Data Leakage Prevention Systeme existiert bisher nicht. Daher lehnen sich die nachfolgenden Ausführungen daran an, was verschiedene Hersteller unter Data Leakage Prevention (DLP) verstehen.

Nachfolgend werden begleitende Maßnahmen, host- und netzwerkbasierte DLP-Systeme, sowie die Möglichkeiten von Digital Rights Management beschrieben, um unautorisierten Abfluss von Daten aus dem Unternehmen zu verhindern. Grundlegende Voraussetzung für den Einsatz eines DLP-Systems ist, dass definiert wurde welche Daten zu schützen sind. Die nachfolgenden Ausführungen setzen voraus, dass die schützenswerten Daten bereits klassifiziert sind (siehe Kapitel 3), so dass ein DLP-System mit ihnen umgehen kann.

4.1 Begleitende Maßnahmen

Neben den technischen Maßnahmen sind begleitende, organisatorische Maßnahmen nötig, da eine Software alleine nicht die Möglichkeit hat, Daten effektiv vor unbefugter Verwendung zu schützen. Die Konfiguration eines DLP-Systems setzt unter anderem Regeln voraus, die im Vorfeld definiert werden.

4.1.1 Regeln für DLP-Systeme

Der Umgang eines DLP-Systems mit klassifizierten Daten ist durch Regeln bestimmt. Die Regeln für ein DLP-System definiert der IT-Sicherheitsverantwortliche. Die Implementierung der Regeln erfolgt durch den DLP-Administrator. Die Trennung ist deshalb sinnvoll, weil der IT-Sicherheitsverantwortliche einen ganzheitlichen Blick über die IT-Infrastruktur und die Sicherheitsanforderungen hat, der (DLP-)Administrator jedoch nur die technischen Gegebenheiten in seinem Aufgabengebiet kennt. Die DLP-Software setzt die Regeln letztendlich auf den Systemen des Unternehmens durch.

Die Regelerstellung kann nach dem White- oder Blacklistingansatz erfolgen. Whitelisting bedeutet, dass grundsätzlich alles verboten ist und jede Ausnahme einzeln definiert wird. Der Blacklistingansatz geht genau umgekehrt vor. Hier ist grundsätzlich alles erlaubt und Verbote sind separat definiert. Die konfigurierten Regeln für das DLP-System besagen, was mit bestimmten Daten passieren darf und was nicht.

Wie die Regeln letztendlich aussehen, ist vom Hersteller des DLP-Systems abhängig. Sie können beispielsweise im XML-Format vorliegen. Je nach System gibt es Unterschiede, wie detailliert sich Regeln definieren lassen. Das nachfolgende Beispiel ist eine Regel, die den Druck von Dokumenten erkennt, welche die Endung .doc, .pdf, .xls oder .ppt besitzen.

```
<and>
        <in>
        <evtSrcFileExt/>
                <list>
                        <string value="doc"/>
                        <string value="pdf"/>
                        <string value="xls"/>
                        <string value="ppt"/>
                </list>
        </in>
        <equal>
                <evtOperationType/>
                <constOpPrint/>
        </equal>
</and>
```

Das Erkennen eines relevanten Vorgangs durch Regeln ist nur ein Teilaspekt von DLP-Systemen. Auf einen Regelverstoß sollte eine Reaktion (Response) erfolgen.

4.1.2 Extrusion Response

Unabhängig davon, welche der nachfolgenden Technologien zum Einsatz kommt, muss feststehen welche Reaktion auf einen Regelverstoß erfolgen soll. Folgende Reaktionen sind in der Praxis üblich und je nach Hersteller individuell konfigurierbar:

- Logging / Speicherung
- Warnung senden
- Alarm auslösen
- Dialogfeld beim Anwender einblenden
- Blockierung

Nicht jedes DLP-System bietet alle genannten Möglichkeiten. Logging bzw. Speicherung bedeutet, dass eine Information über einen Regelverstoß im System abgelegt wird, so dass zeitlich nachvollziehbar ist, wann ein Regelverstoß stattgefunden hat. Die nächstmögliche Steigerung zur einfachen Speicherung ist die Warnung. Eine Warnung ist beispielsweise ein Eintrag im DLP-Managementsystem. Häufen sich Warnungen, oder liegt ein starker Regelverstoß vor, so kann das DLP-System einen Alarm auslösen, der ein sofortiges Handeln eines IT-Sicherheitsverantwortlichen zu Folge hat. Ein Alarm kann beispielsweise eine E-Mail oder eine SMS sein. Soll der Anwender über seinen Regelverstoß informiert werden, kann eine Warnmeldung am Bildschirm eingeblendet werden. Die wichtigste Maßnahme, die jedes DLP-System beherrschen muss, ist die Blockierung eines Datentransfers, der gegen die Regeln verstößt.

4.1.3 Bedrohung durch externe Schnittstellen

Die Gefahr durch externe Datenträger lässt sich nicht nur durch DLP-Systeme lösen, sondern auch durch Veränderungen an der verwendeten Hardware. Externe Datenträger werden über physikalische Schnittstellen wie z.B. USB, Firewire oder E-SATA angesprochen (siehe Abschnitt 2.1).

Ohne physikalische Schnittstellen ist die Verwendung von externen Datenträgern unmöglich und der potentielle Informationsfluss gestoppt. Gleiches gilt für Wechseldatenträger, wie beispielsweise CDs/DVDs, Disketten oder Magnetbänder. Die Entfernung der potentiell gefährlichen Hardware schränkt die Anzahl der ausgehenden Kanäle ein.

Ein denkbares Szenario ist die Verwendung von ThinClients, die nur zwei PS2 Schnittstellen zum Anschluss von Maus und Tastatur besitzen. Der Vorteil besteht darin, dass der Anschluss weiterer Datenträger in diesem Fall nicht möglich ist. Der Nachteil beim Einsatz von ThinClients besteht darin, dass die Grafikleistung im Vergleich zu Standardcomputern sehr gering ist.

4.1.4 Entsorgung von Datenträgern

Die sichere Entsorgung von Datenträgern auf denen unverschlüsselte Daten gespeichert sind, ist nötig, damit Unbefugte die Daten nicht auslesen und verwerten können. Bei einer vollständigen und sicheren Verschlüsselung aller schützenswerten Daten spielt die sichere Entsorgung keine Rolle, da die Daten durch die Verschlüsselung geschützt sind. Zu den betroffenen Datenträgern gehören nicht nur Festplatten, sondern auch Medien der Datensicherung, USB-Sticks, CD-ROMs und alle weiteren Datenspeicher auf denen vertrauliche Daten gespeichert sind.

Das US „Department of Defense“ (DoD) hat Standards zum Thema sichere Datenträgerlöschung veröffentlicht. Zu nennen sind in diesem Zusammenhang die Standards DOD 5220.22-M (E) [4] und DoD 5220.22-M (ECE). Der 5220.22-M (E) Standard besagt, dass „Rigid Disks“ (u.A. Festplatten) zur sicheren Löschung dreimal nach folgender Vorschrift überschrieben werden müssen:

1. Durchgang: Beschreiben mit fest vorgegebenem Wert
2. Durchgang: Überschreiben mit Zufallswerten
3. Durchgang: Überschreiben mit dem Komplementwert des ersten Durchlaufs

Diese Art der Löschung ist für streng geheime und kritische Daten allerdings nicht ausreichend. Für kritischere Daten gilt die DoD 5220.22-M (ECE) Spezifikation. Sie ist eine Variante des DoD 5220.22-M (E) mit sieben Durchläufen, wobei die Daten zunächst mit den drei Durchläufen des DoD 5220.22-M (E) Standards, anschließend mit einem Zufallswert, danach erneut mit den drei Durchläufen des DoD 5220.22-M (E) überschrieben werden.

Peter Gutmann von der Universität Auckland (Neuseeland) schlägt zur sicheren Löschung 35-maliges Überschreiben mit bestimmten Mustern vor [8]. Vom BSI[1] gibt es zu diesem Themenbereich die technische Leitlinie BSI - TL

[1] Bundesamt für Sicherheit in der Informationstechnik

03420, die Richtlinien für das „Löschen und Vernichten von schutzbedürftigen Informationen auf analogen und digitalen Datenträgern“ bereitstellt.

Neben dem Überschreiben von Daten empfiehlt das DoD das Schreddern, Schmelzen, Pulverisiern oder Verbrennen. Bei magnetischen Datenträgern ist der Einsatz von Degaussern ebenfalls empfohlen. Ein Degausser entmagnetisiert den Datenträger durch ein starkes Magnetfeld. Somit lassen sich auch Festplatten löschen, die aufgrund von Hardwaredefekten nicht mehr überschreibbar sind. Die vom BSI nach DIN 33858 zertifizierten Geräte sind als sichere Methode zur Löschung anerkannt.

Ein einfaches Löschen der Daten oder die Formatierung eines Datenträgers ist nicht ausreichend. Dabei werden nicht die Daten gelöscht, sondern nur die Verzeichniseinträge. Somit bleiben die Daten auf dem Datenträger lesbar und können mit Hilfe von Datenwiederherstellungstools rekonstruiert werden.

4.1.5 Datensicherung

Dass der Diebstahl von Datensicherungen eine Gefahr für die Informationssicherheit ist legt Abschnitt 2.5 dar. Beheben lässt sich die genannte Problematik mit Hilfe starker Kryptographie. Sollten verschlüsselte Datensicherungen gestohlen werden, kann der Dieb die Informationen nicht auslesen, da sie nur in verschlüsselter Form vorliegen.

Unverschlüsselte Datensicherungen sind nur dann als sicherer Speicherort anzusehen, wenn garantiert werden kann, dass die Daten nicht unerlaubt ausgelesen werden können. Die Realisierung eines solchen Zugriffsschutz ist nicht Thema dieser Arbeit.

4.1.6 Angriffe auf die Netzwerkinfrastruktur

Die Netzwerkinfrastruktur ist ein Angriffspunkt, der durch DLP-Systeme nicht geschützt wird, aber die Gefahr des ungewollten Informationsabflusses durch Abhören beinhaltet. Hierbei ist in Local Area Network (LAN)- und Wide Area Network (WAN)-Bereich zu unterscheiden.

Im LAN-Bereich ist folgendes Szenario denkbar, bei dem ein Angreifer Daten, die auf seinem Arbeitsplatz gespeichert sind, kopieren möchte:

> Den DLP-Agent deaktivieren oder von einem Livesystem booten führt nicht zum Erfolg, da die Daten verschlüsselt sind, sobald der DLP-Agent deaktiviert ist (siehe Abschnitt 5.3). Deshalb hängt der Angreifer einen Hub in das Netzwerk ein um die

> vollständige Netzwerkkommunikation seines Computers mitzuschneiden. Anschließend überträgt er die gewünschten Daten auf einen Dateiserver (legitimer Vorgang), um an die unverschlüsselten Daten zu gelangen. Anschließend extrahiert er die Nutzdaten aus den Netzwerkdaten und erhält so die gewünschten Informationen.

Im WAN-Bereich kann ein Angreifer ebenfalls den Netzwerkverkehr abhören, indem er beispielsweise die Daten beim Internet Service Provider abfängt (z.B. über einen Mirrorport am Switch des Providers).

Im LAN- und im WAN-Bereich ist Verschlüsselung eine sichere Lösung. VPN stellen eine bewährte und leistungsfähige Technologie zur Verfügung, um Daten in Weitverkehrsnetzen vor unbefugtem Zugriff zu schützen. Im lokalen Netz ist der Einsatz von VPN-Technologien kritisch zu betrachten, da der Administrationsaufwand bei vielen Clients erheblich ist.

Im LAN richtet sich die Strategie gegen Geräte ohne DLP-Agent (siehe Abschnitt 4.2). Somit wird verhindert, dass ein Angreifer mit einem eigenen Gerät Daten sniffen kann (das Sniffen am eigenen Computer verhindert der Whitelistingansatz für Software, siehe Abschnitt 5.4). Für diesen Zweck gibt es unter anderem das standardisierte 802.1x Protokoll, welches eine Methode für die Authentifizierung und Authorisierung im Ethernet bietet. Jedes Netzwerkgerät, dass Zugriff auf ein mit 802.1x gesichertes Netzwerk erlangen will, muss sich erfolgreich authorisieren lassen. Somit sind unauthorisierte Zugriffe von Fremdgeräten ausgeschlossen.

Neben 802.1x gibt es eine Reihe weiterer Protokolle bzw. Systeme zur Netzwerkauthentifizierung, die allerdings nicht offen standardisiert sind. Diese Systeme (z.B. Cisco NAC, Microsoft NAP) bieten mehr Möglichkeiten als reines 802.1x. Dies wären beispielsweise die Überprüfung des Patchlevel eines Clients oder die automatische Installation eines Anti-Virenprogramms, falls keines vorhanden ist.

Heutige Switches bieten die Funktion, die Anzahl der zulässigen Geräte pro Switchport zu regeln. Dies geschieht über die Media Access Control (MAC)-Adressen der Netzwerkkarten. Ist nur eine MAC-Adresse pro physikalischem Switchport erlaubt, blockiert der Switch den Port, sobald er mehr als eine MAC-Adresse (z.B. durch anschließen eines zweiten Geräts über einen HUB oder Switch) erkennt.

Trotz 802.1x und dieser Maßnahmen bleibt dem Angreifer ein Weg um den Netzwerkverkehr im LAN abzuhören, der mit technischen Mitteln nicht zu verhindern ist:

> Der Angreifer verwendet hierfür einen HUB, den er zwischen die abzuhörenden Kommunikationspartner in das Netzwerk einfügt.

> Anschließend ändert er seine MAC-Adresse auf eine am Switchport gültige. Somit erkennt der Switch kein neues Gerät. Der Angreifer kann zwar nicht im Netzwerk kommunizieren, aber passives Abhören der Kommunikation ist möglich.

Voraussetzung für diesen nicht abwehrbaren Angriff ist, dass der verwendete Hub keine BPDU-Pakete[2] versendet. Anhand der BPDU-Pakete erkennt der Switch den HUB und blockiert den Switchport. Einfache (preiswerte, nicht managebare) Hubs versenden keine BPDU-Pakete und sind daher für einen Angreifer geeignet.

4.2 Hostbasierte DLP-Systeme

Eine Maßnahme um unerwünschten Informationsabfluss zu verhindern, ist der Einsatz eines hostbasierenden Data Leakage Prevention Systems. Bei einem hostbasierten DLP-System ist auf jedem Client (PC, Notebook oder anderes Gerät) einen Softwareagent (nachfolgend DLP-Agent genannt) des DLP-Systems aktiv, der bestimmte Regeln im Umgang mit Daten überwacht und durchsetzt.

Die Regeln bezieht der DLP-Agent von einem Managementserver, wo zentral festgelegt wird, was erlaubt ist und was nicht. Das System kann direkt mit dem Endanwender interagieren und beispielsweise Dialogboxen einblenden, falls der Anwender eine unerlaubte Aktion ausführen möchte.

Der Softwareagent eines hostbasierten DLP-Systems greift über eigene Kernelmodule in das Betriebssystem ein und kann so alle Aktivitäten des Systems überwachen. Somit kann der DLP-Agent auch sehen, welche Aktionen der Benutzer ausführt. Dies beeinhaltet ebenfalls die bereits erwähnte Endpoint Security, also die Überwachung aller am Computer angeschlossenen Datenträger. Hostbasierte DLP-Systeme sind in den meisten Einsatzgebieten das Mittel der Wahl, da sie mehr Kanäle als netzwerkbasierte DLP-Systeme überwachen können (siehe Kapitel 5).

4.3 Netzwerkbasierte DLP-Systeme

Netzwerkbasierte DLP-Systeme sind aus technischer Sicht Intrusion-Detection- bzw. Intrusion-Prevention-Systemen (IDS / IPS) sehr ähnlich. Sie haben allerdings die genau gegenteilige Aufgabe. Während ein IDS / IPS versucht von außen kommende Angriffe abzuwehren, hat ein DLP-System

[2] Bridge Protokoll Data Unit

die Aufgabe Angreifer von Innen aufzuhalten. Beide Systeme durchsuchen ausschließlich den Netzwerkverkehr nach auffälligen Mustern und können somit nur das Netzwerk als Informationsflusskanal überwachen. Alle anderen Kanäle sind einem netzwerkbasierten System verborgen. Hierin liegt die größte Schwäche des Systems, denn im Netzwerk ist nur ein Bruchteil der Datendiebstahlsversuche zu erkennen (vgl. Kapitel 2).

Das Ziel, unerwünschten Informationsabfluss zu unterbinden, erreichen netzwerkbasierte Systeme nur dann, wenn die Datenübertragung unverschlüsselt im Netzwerk erfolgt. Die Überwachung von verschlüsselten Inhalten ist nicht möglich. Somit bleibt der Nutzen des netzwerkbasierten Systems gering, da alle verschlüsselten Netzwerkprotokolle (z.B. HTTPS) das DLP-System ungehindert passieren.

Im Gegensatz zur hostbasierten Variante ist fast ausschließlich der inhaltsbezogene Ansatz zum Auffinden von Regelverstößen möglich. Somit müssen die Suchmuster für unerlaubte Aktivitäten immer im Vorfeld bekannt sein. Dies lässt den Administrationsaufwand ansteigen, da die Erstellung von inhaltsbasierten Regeln aufwändiger ist, als die Erstellung kontextbasierter Regeln. Die einzige Ausnahme vom inhaltsbezogenen Ansatz bietet die kontextbezogene Filterung nach der Absenderadresse eines IP-Pakets.

Die Integration eines netzwerkbasierten DLP-Systems in das Netzwerk ist nicht trivial, da eine Reihe von DLP-Sensoren notwendig sind, um das Netzwerk ausreichend zu überwachen. Zwar bieten moderne Switches die Möglichkeit, den Datenverkehr auf definierte Ports (sog. Monitoring-Ports) zu kopieren, allerdings kann es bei diesem Ansatz zur Überlastung des Monitoring-Ports kommen. Über Monitoring-Ports ist es zudem nicht möglich einen Datenabfluss zu verhindern, da er nur die Beobachtung, aber kein Eingreifen, ermöglicht.

Zusammenfassend ist festzustellen, dass rein netzwerkbasierte DLP-Systeme keinen nennenswerten Schutz bieten, da sie ausschließlich das Netzwerk als Datenabflusskanal überwachen können und auch dies nur dann, wenn die Daten nicht verschlüsselt wurden. Ein rein netzwerkbasiertes DLP-System ist für einen Angreifer daher sehr leicht zu umgehen. Der Vorteil netzwerkbasierter DLP-Systeme besteht darin, dass nicht auf jedem Client eine DLP-Software installiert werden muss, wie dies bei hostbasierten DLP-Systemen der Fall ist.

4.4 Netzwerkbasierte Hilfsmittel

Firewalls auf Open Systems Interconnection (OSI) Layer 3, 4 und 7 sind keine Data Leakage Prevention Systeme, allerdings sind sie zur Unterstüt-

zung eines DLP-Systems hilfreich. Firewalls können keine inhaltsbezogenen Regeln verarbeiten und grenzen sich somit von DLP-Systemen ab. Sie vereinfachen allerdings die Regelerstellung für ein DLP-System, indem sie netzwerkbasierte Kanäle vollständig blockieren. Insbesondere der für DLP-Systeme relevante ausgehende Netzwerkverkehr lässt sich reglementieren.

Auf OSI Layer 3 lassen sich IP-Adressen oder komplette Subnetze sperren, um für bestimmte Arbeitsrechner wenige, klar definierte Kommunikationspartner zu definieren. Die in Kapitel 2 erwähnten Instant Messenger sind auf Layer 3 ebenfalls blockierbar, indem die Firewall die Verbindung zu den Loginservern verbietet.

Auf Layer 4 lassen sich die erlaubten und verbotenen Ports definieren. Die ausschließliche Filterung auf Layer 4 ist für einen Angreifer allerdings leicht zu umgehen, da er seine Kommunikation auf die erlaubten Ports verlagern kann. Abhilfe schaffen Proxies oder Firewalls die auf Anwendungsebene arbeiten.

Diese Firewalls verstehen die Syntax bzw. Semantik eines Protokolls und können somit feststellen, ob ein Protokoll erwünscht oder unerwünscht ist. Alle erlaubten Protokolle müssen somit von der Firewall unterstützt werden. Auch anwendungsbasierte Firewalls können nicht ohne weiteres in verschlüsselte Protokolle hinein sehen. Eine Echtzeitentschlüsselung von Secure Socket Layer (SSL)-gesicherten Verbindungen ist zwar möglich, aber aufwändig (siehe [1]).

Hilfreich zur Beweissicherung und zur Entdeckung von unbekannten Netzwerkkanälen ist Netflow. Router senden Informationen über den IP-Verkehr an einen Netflow-Kollektor, der dann eine Auswertung erstellt. In der Auswertung sind unter anderem Informationen über Zeit, Quell- und Zieladresse sowie Quell- und Zielport enthalten. Somit ist jede einzelne Verbindung nachvollziehbar und aus der Korrelierung der gespeicherten Datensätze lassen sich verdächtige Zugriffe erkennen.

Zusammenfassend ist festzustellen, dass Firewalls und Netflow hilfreich im DLP-Bereich sind. Sie bieten alleine jedoch keinen Schutz gegen unerwünschten Informationsabfluss. Zudem besteht die Gefahr, dass die Unternehmensfirewall durch andere Netzwerkkanäle (z.B. UMTS-USB-Modemverbindung) umgangen wird.

4.5 Digital Rights Management

Digital Rights Management (DRM) wurde entwickelt, um urheberrechtlich geschützte Daten vor unerlaubter Nutzung zu schützen. Meist geht es dabei um Audio- oder Videodaten, aber auch andere Formate wie eBooks und

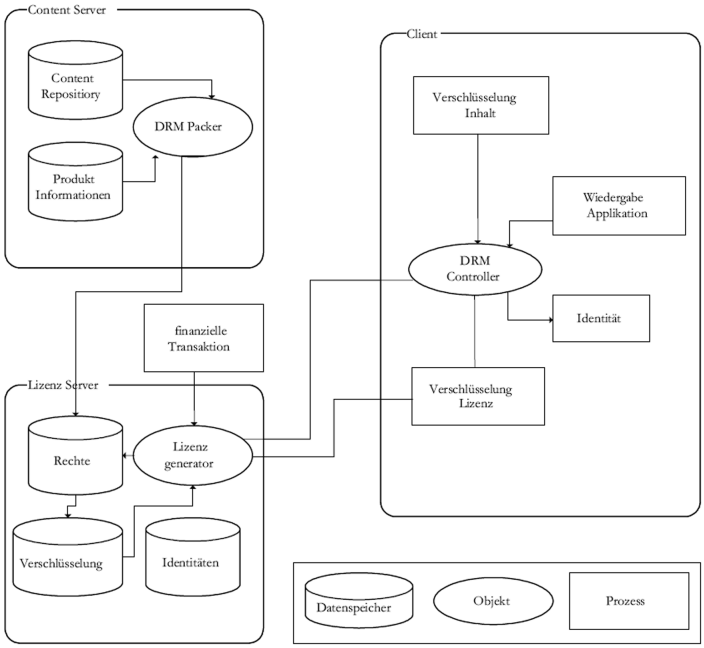

Abbildung 4.1: Architektur eines DRMs aus [17].

Officedokumente können mit DRM geschützt werden. DRM schränkt die Nutzung von Daten ein. Folgende Szenarien sind beispielsweise möglich:

- Ein DRM System beschränkt das Abspielen eines Videos auf drei Male (Anwendung: Onlinevideothek).
- In PDF-Dokumenten sorgt DRM dafür, dass ein digitales Dokument nicht druckbar und der Inhalt nicht kopierbar ist.

DRM bietet demjenigen, der es anwendet eine Nutzungskontrolle über seine Daten. Genau dies versuchen DLP-Systeme ebenfalls.

Die technische Umsetzung eines DRM-Systems stellt Abbildung 4.1 schematisch dar. Die Zugriffskontrolle wird über kryptografische Verfahren abgesichert. Der Content Server verwaltet die zu schützenden Inhalte. Er kann sie mit Hilfe des DRM-Packers verschlüsseln. Der Lizenzserver erzeugt die Lizenzen mit den gewünschten Attributen. Die Lizenzen enthalten die Schlüssel zum Entschlüsseln der Inhalte. Soll ein Zugriff auf DRM-geschützten Inhalt erfolgen, fordert der DRM-Controller vom Lizenzserver die passende Lizenz an.

Der Einsatz von DRM bringt einige Vor- und Nachteile mit sich. DRM ist an eine Anwendung oder beschränkte Anzahl an Anwendungen gebun-

den. Das bedeutet, dass für alle schützenswerten Daten DRM-fähige Anwendungen zum Einsatz kommen müssen. Die Komplexität dieser Vorgehensweise steigt mit der Anzahl der verwendeten Formate. Daneben sind DRM-Systeme nicht in der Lage die bereits genannten Abflusskanäle zu sichern. DRM verhindert nicht den Abfluss von Daten, sondern nur die unautorisierte Nutzung.

Einer der Vorteile von DRM ist, dass die geschützten Inhalte nur auf Systemen verwendet werden können, die DRM einsetzen und aktiviert haben. Mit DRM ist es möglich die Nutzung der Daten genau festzulegen und Inhalte vor der Verwendung durch Dritte zu schützen.

Abschließend ist festzuhalten, dass DRM-Systeme in den meisten Fällen nicht zum Unterbinden von Datenabflüssen geeignet sind. Der Lösungsansatz ist zwar gut, aber die Komplexität ist in der Praxis zu hoch. Dies liegt darin begründet, dass DRM-Systeme nicht dafür entwickelt wurden, Informationsabflüsse zu verhindern, sondern um die unerwünschte Verwendung von Informationen zu verhindern.

Kapitel 5

Der Hostbasierte Lösungsansatz

Wie in Kapitel 4 beschrieben, gibt es host- und netzwerkbasierte Data Leakage Prevention Systeme. Nachdem dort festgestellt wurde, dass netzwerkbasierte Systeme nicht geeignet sind um ungewünschten Datenabfluss wirkungsvoll zu verhindern, erläutert dieses Kapitel den hostbasierten Ansatz. Falls nicht anders gekennzeichnet, wird von einer Microsoft Windows Umgebung ausgegangen.

Den schematischen Aufbau einer hostbasierten Lösung zeigt Abbildung 5.1. Der DLP-Managementserver verteilt die Regeln (vgl. Abschnitt 4.1.1) an die Clients. Clients sind alle Geräte, die auf vertrauliche Daten zugreifen wie beispielsweise Arbeitsplatzrechner, Laptops und PDAs oder Datei- und Terminalserver. Auf jedem der Clients ist ein DLP-Agent installiert, welcher die Regeln vom DLP-Managementserver bezieht. Schützenswerte Daten dürfen nie auf Geräte ohne DLP-Agenten gelangen.

Die Sicherheit hostbasierter Systeme beruht darauf, dass immer ein DLP-Agent vorhanden ist, der die Einhaltung der Vorgaben überwacht. In dem Moment, wo der DLP-Agent nicht vorhanden ist, kann ein Angreifer die Daten entwenden. Im weiteren Verlauf wird davon ausgegangen, dass ein Angreifer Administrator- bzw. Rootrechte auf seinem System besitzt. Diese kann er entweder legal (Firmenpolitik erlaubt jedem Benutzer als Administrator zu arbeiten) oder illegal (Livesystem, Privilege Escalation Bugs) erlangt haben.

Abbildung 5.1: Hostbasiertes DLP schematisch

5.1 Der DLP-Agent

Der DLP-Agent ist ein elementarer Bestandteil einer hostbasierten Data Leakage Prevention Lösung. Er muss die Einhaltung der Regeln und Überwachung der Benutzeraktionen gewährleisten. Unter Windows sind Teile des DLP-Agents als Kerneltreiber implementiert, damit eine Überwachung des Betriebssystems möglich ist. Unter GNU/Linux kommen Kernelmodule zum Einsatz, alternativ kann der Code auch direkt in den Kernel einkompiliert werden. Durch das Einkompilieren des DLP-Agent-Codes ist eine Deaktivierung des DLP-Agents durch etwaiges Entladen des Kernelmoduls nicht möglich.

Unter Windows verwenden DLP-Agents klassische Rootkit-Technologien (siehe Abschnitt 5.2). Damit versuchen einige Hersteller ihre DLP-Agents zu verstecken, um eine geringere Angriffsfläche zu bieten (Security by Obscurity). Sie verbergen die Prozesse und Dateien vor dem Benutzer. Auch mit Administratorrechten und Standardtools (z.B. Sysinternals Suite[1]) sind DLP-Agenten oft nicht zu entdecken. Mit speziellen Anti-Rootkit-Tools lassen sich hingegen eine Reihe von versteckten Prozessen, Dateien und

[1] http://www.microsoft.com/germany/technet/sysinternals/utilitiesindex.mspx

Diensten im System finden, da sie nicht die Windows-API, sondern eigene Funktionen verwenden. Die Ausführung von Anti-Rootkit-Tools auf einem Windows-System erfordert Administratorrechte.

Der DLP-Agent hat folgende Aufgaben:

- Regeln vom Managementserver beziehen
- Regeln durchsetzen
- Daten klassifizieren
- Verschlüsselung schutzbedürftiger Daten
- Überwachung / Logging
- Zugriffsrechte regeln

Bevor der DLP-Agent Daten schützen kann, muss er genaue Regeldefinitionen erhalten, welche Aktionen erlaubt und welche nicht erlaubt sind. Die Regeln erhält er über das Netzwerk vom DLP-Managementserver. Die Integrität der Datenübertratung muss hierbei sicher gestellt sein. Andernfalls besteht die Gefahr, dass eine Manipulation der Regeln bei der Übertragung vom DLP-Managementserver zum Client erfolgt. Die Integrität der Daten kann beispielsweise durch digitale Signaturen gesichert werden.

Auch wenn die Regeln grundsätzlich nicht geheim sind (sie sind als Firmenpolicy veröffentlicht), bietet sich eine verschlüsselte Übertragung zum Schutz der Regeln an. Verschlüsselung ist dann erwünscht, wenn nicht alle Regelinhalte bekannt sein sollen. Einige Verschlüsselungsverfahren (z.B. TLS[2]) sichern zusätzlich die Integrität der Daten. Bei der Verwendung von TLS ist weder das Auslesen im Klartext noch eine Veränderung der Regeln während der Übertragung möglich.

Neben der Datenintegrität und optionaler Verschlüsselung muss sichergestellt sein, dass der Managementserver wirklich der ist, für den er sich ausgibt und dass es sich nicht um einen Nachbau des Angreifers handelt. Eine Möglichkeit diesen Anforderungen zu begegnen ist beispielsweise die Übertragung per HTTPS oder eines anderen durch TLS gesicherten Protokolls. Durch das verwendete Zertifikat kann der Client feststellen, ob er mit dem echten Managementserver kommuniziert.

Die Regeln speichert der DLP-Agent lokal ab und schützt sie gegen unbefugte Veränderungen. Die lokale Speicherung ist nötig, damit dem DLP-Agent auch ohne Netzwerkverbindung ein Regelwerk zur Verfügung steht.

[2] Transport Layer Security

Dies ist insbesondere für Laptops, ohne permanente Verbindung in das Firmennetzwerk nötig. Der Schutz der lokal auf der Festplatte gespeicherten Regeln gegen Veränderung ist wichtig, da die Gefahr besteht, dass ein Angreifer die Regeln manipuliert und so das DLP-System umgeht. Die Veränderung der Regeln ist beispielsweise möglich, indem er von einem Livesystem (z.B. Linux Live-CD mit NTFS Unterstützung oder WindowsPE Live-CD) bootet und die Regeldaten manipuliert. Auch hier helfen, wie bei der Übertragung der Regeln im Netzwerk, Verschlüsselung, Prüfsummen und digitale Signaturen.

Die vom Managementserver bezogenen Regeln muss der DLP-Agent gegenüber dem Benutzer durchsetzen. Bei einem Regelverstoß kann der DLP-Agent die Aktion einfach blockieren (vgl. Abschnitt 4.1.2). Er kann dem Benutzer auch ein Dialogfenster einblenden und bestätigen lassen, ob er den Regelverstoß akzeptiert. Parallel dazu protokolliert der DLP-Agent Verstöße und sendet Nachrichten über diese an den DLP-Managementserver. Somit ist eine zentrale Korrelierung der Ereignisse möglich. Ist der Logserver (meist gleichzeitig der DLP-Managementserver) nicht erreichbar, führt der DLP-Agent eine Zwischenspeicherung durch und sendet die Daten sobald der Logserver wieder verfügbar ist.

Neben der Durchsetzung der Regeln zum Schutz der Daten, kann der DLP-Agent auch die Klassifizierung von Dateien vornehmen. Erstellt ein Benutzer eine neue Datei mit bestimmten Eigenschaften, so klassifiziert er diese. Die zu schützende Datei selbst darf der DLP-Agent dafür nicht verändern. Eine Veränderung der zu schützenden Datei bedeutet einen unerwünschten Integritätsverlust der Datei.

Die Klassifizierungsinformationen kann der DLP-Agent auf verschiedene Art und Weise speichern. Auf NTFS-Datenträgern bieten sich beispielsweise NTFS Alternative-Data-Streams (Beschreibung in [13]) an. Werden ausschließlich diese genutzt, muss der DLP-Agent sicher stellen, dass der Benutzer die Datei auf keinem Nicht-NTFS-Datenträger speichern kann, da ansonsten die Klassifizierungsinformationen verloren gehen. Alternative Möglichkeiten zur Speicherung der Klassifizierungsinformationen gibt es ebenfalls. Der DLP-Agent kann Zusatzinformationen direkt als zusätzliche Dateien im Dateisystem ablegen. Da der DLP-Agent als Kernelmodul realisiert ist, kann er diese Dateien vor dem Benutzer verbergen und bei Dateisystemoperationen (kopieren, verschieben) automatisch mitschicken. Eine dritte Möglichkeit besteht darin, dass er eine Datenbank mit Informationen über die klassifizierten Dateien führt. Bei Kopiervorgängen auf andere Rechner sendet er die Klassifizierungsinformationen immer mit.

Die Abbildung 5.2 zeigt den schematischen Aufbau eines clientbasierten DLP-Systems am Endgerät. Das System besteht aus zwei Teilen, dem DLP-Agent und dem DLP-Treiber. Der DLP-Treiber arbeitet im Kernel-Mode

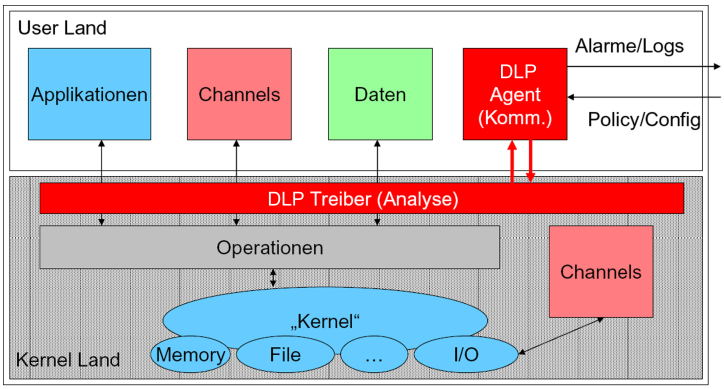

Abbildung 5.2: Schematische Darstellung eines DLP-Agent aus [7]

und kann so jegliche relevanten Operationen überwachen. Diese Operationen können Dateisystemzugriffe, Netzwerkkommunikation oder andere Formen von I/O sein. Der DLP-Agent überwacht die Einhaltung der vorgegebenen Regeln durch die Kommunikation mit dem DLP-Treiber. Welche Techniken bei der Implementierung des Treibers zum Einsatz kommen beschreibt Abschnitt 5.2.

In dem Moment, wo der DLP-Agent nicht aktiv ist, kann der Benutzer alle vom DLP-System gesetzten Restriktionen umgehen. Es bleiben dann nur noch Schutzmaßnahmen wie Dateisystemrechte oder Firewalls. Ein Angreifer mit Administratorrechten kann den DLP-Agent deaktivieren. Deshalb ist es notwendig, dass alle kritischen Daten nur dann lesbar sind, wenn der DLP-Agent gestartet ist. Dieser Anforderung werden DLP-Systeme gerecht, indem sie die vertraulichen Daten verschlüsseln (siehe Abschnitt 5.3). Es ist aber nicht immer nötig den DLP-Agent zu deaktivieren, um an die Daten zu gelangen.

Im einfachsten Fall genügt ein Live-System, das der Angreifer von einer CD-ROM startet. Dann kann er die für ihn relevanten Daten selektiv kopieren oder die gesamte Festplatte spiegeln. Neben optischen Medien können heutige Rechner auch von USB-Datenträgern oder dem Netzwerk booten. Um derartige Zugriffsversuche zu verhindern muss sicher gestellt sein, dass ein Angreifer das Gehäuse des Computers nicht öffnen kann. Dies ist nötig, damit ein Angreifer nicht die Bootreihenfolge im BIOS beeinflussen kann. Ein BIOS Passwort bietet keinen ausreichenden Schutz, da es durch Entnahme der Mainboardbatterie leicht zu deaktivieren ist. Das verschlossene Gehäuse schützt vor der Entnahme der Mainboardbatterie.

Diese Problematik lässt sich beispielsweise durch abschließbare Gehäuse lösen. Diese Maßnahme verhindert auch einen Ausbau der Festplatte, wodurch die Daten auf einem Zweitgerät lesbar wären. Eine (zusätzliche) Ver-

siegelung des Gehäuses ermöglicht es eine unbefugte Öffnung des Gehäuses im Nachhinein zu erkennen.

5.2 Implementierung des Kerneltreibers

Der DLP-Agent besteht aus zwei Teilen. Einem User-Land-Teil und einem Kernel-Teil. Durch den Kernel-Teil ist der Zugriff auf alle relevanten Betriebssystemressourcen (vgl. vorheriges Kapitel) gegeben. Die Implementierung des Kerneltreibers für ein DLP-System gleicht der eines Kernel-Rootkits. Dieses Kapitel beschreibt wie die technische Realisierung erfolgt.

Die Umsetzung dieser Anforderung erfolgt unter Windows über einen Systemtreiber, unter Linux können nachladbare Kernelmodule oder in den Kernel einkompilierte Treiber verwendet werden. Nachladbare Kernelmodule werden zur Laufzeit in das Betriebssystem eingebunden. Sobald das Modul bzw. der Treiber geladen ist, kann der DLP-Agent Kerneldatenstrukturen wie z.B. die System-Call-Table oder die Prozessliste modifizieren. Nachfolgende Rootkit-Technologien werden von DLP-Systemen verwendet:

- Manipulation der System-Call-Table (unter Windows SSDT Hooking genannt)
- Inline Hooking
- Manipulation der Prozessliste
- Interrupt Hooking

Abhängig vom verwendeten Produkt gibt es weitere Verfahren, welche nicht Thema dieser Arbeit sind. Nicht jeder Hersteller implementiert die vier genannten Möglichkeiten.

5.2.1 Manipulation der System-Call-Table (SSDT Hooking)

In heutigen Betriebssystemen gibt es üblicherweise zwei Arten wie ein Prozess ausgeführt werden kann. Im User-Mode oder im Kernel-Mode. Ein Prozess, der im User-Mode läuft kann keine priviligierten Befehle ausführen und hat keinen direkten Zugriff auf Kerneldaten oder Hardware. Privilegierte Befehle sind für das Betriebssystem reservierte Befehle, z.B. lesen von der Festplatte oder starten eines neuen Prozesses. Prozesse, die im Kernel-Mode laufen, haben alle Privilegien und können direkt auf den gesamten Adressraum des Arbeitsspeichers zugreifen.

Wenn ein Prozess im User-Mode eine Kernel-Operation ausführen will, so ruft er das entsprechende System-Service[3] (z.B. NtCreateThread) über die jeweilige API-Funktion auf. Durch Aufruf der API-Funktion wird ein sogenannter System-Call (unter Windows eingeleitet durch den Software Interrupt SYSENTER oder INT 0x2E), durchgeführt. Über diesen wird der Interrupt Service Routine (KiSystemService) mitgeteilt, welches System-Service ausgeführt werden soll. Dabei wechselt auch die Central Processing Unit (CPU) in den Kernel-Mode, um auf alle Ressourcen (z.B. Adressraum des Kernels im Arbeitsspeicher) des Kernels zugreifen zu können. Daraufhin sucht KiSystemService in der System-Call-Table nach dem gewünschten System-Service und führt den Code an der angegebenen Adresse im Kernel-Mode aus. Nach Ausführung des System-Services werden die Ergebnisse an den User-Mode-Prozess übergeben und die CPU wechselt wieder zurück in den User-Mode (siehe [6]).

Ein Beispiel für einen System-Service unter Windows Server 2003 ist „NtCreateThread“ zum Erstellen eines neuen Threads. Wie in Abbildung 5.3 in der Zeile 5 zu erkennen ist, hat dieser die Nummer 0x37 (Spalte 1). Bevor der Interrupt SYSENTER oder 0x2E an die CPU gesendet wird, wird der Wert 0x37 in das EAX Register geschrieben. Durch den Inhalt des EAX Registers ist der Interrupt Service Routine KiSystemService bekannt, welches System-Service aufgerufen werden soll. Auf der Metasploit Homepage[4] gibt es eine Übersicht über alle System-Call-Nummern unter Windows. Die Ausführung von System-Services kann auf zwei Wegen abgefangen bzw. verändert werden.

Die erste Möglichkeit besteht darin, die Startadresse des System-Service, den das Betriebssystem ausführt, in der System-Call-Table zu ändern. Die System-Call-Table beinhaltet die Adressen für jeden System-Service bzw. die Pointer auf jeden System-Service (vgl. mit C oder C++). Der DLP-Treiber kann die Adressen in der Tabelle so umschreiben, dass der Code des DLP-Systems anstatt des echten System-Service ausgeführt wird. Unter Windows heißt die System-Call-Table „System-Service-Descriptor-Table“ (SSDT). Ausschnitte einer manipulierten SSDT zeigt Abbildung 5.3.

Die rot markierten Zeilen zeigen manipulierte Einträge (eine Unkenntlichmachung der Prozessnamen ist aus Datenschutzgründen nötig). In der Abbildung ist zu erkennen, dass bestimmte Adressen bzw. die Pointer für bestimmte System-Services (z.B. NtCreateSection) nicht in den Adressraum der `ntkrnlpa.exe` (der Windows Kernel), sondern in den Adressraum eines anderen Programms zeigen (Spalte 3). Die Manipulation der Adressen ist

[3] System-Services sind Dienste (z.B. Schreib- oder Lesezugriff auf die Festplatte), welche Teil des Kernels sind und von User-Mode-Prozessen über die entsprechende API-Funktion aufgerufen werden können.

[4] http://www.metasploit.com/users/opcode/syscalls.html

1	0x33	0x8098AD12	\WINDOWS\system32\ntkrnlpa.exe	0x8098AD12	NtCreateProfile
2	0x34	0xBAEDF82C	\??\C:\WINDOWS\System32\Drivers\[illegible].SYS	0x8091EB70	NtCreateSection
3	0x35	0x809884DE	\WINDOWS\system32\ntkrnlpa.exe	0x809884DE	NtCreateSemaphore
4	0x36	0x809343BC	\WINDOWS\system32\ntkrnlpa.exe	0x809343BC	NtCreateSymbolicLinkObject
5	0x37	0xBAEDF8D4	\??\C:\WINDOWS\System32\Drivers\[illegible].SYS	0x80941B1A	NtCreateThread
6	0x38	0x8098A20E	\WINDOWS\system32\ntkrnlpa.exe	0x8098A20E	NtCreateTimer
7	0x39	0x8096B152	\WINDOWS\system32\ntkrnlpa.exe	0x8096B152	NtCreateToken

Abbildung 5.3: Manipulierte System Service Descriptor Table

in den Spalten 2 und 4 zu erkennen. Spalte 2 enthält die aktuelle Adresse, während der Wert in Spalte 4 den Originalwert enthält. Veränderte Werte weisen auf ein Rootkit hin. In diesem konkreten Fall sind es Spuren des DLP-Treibers.

Die zweite Möglichkeit eigenen Code anstelle der echten System-Services auszuführen besteht darin, den Programmcode des System-Services zu manipulieren. Dies wird als „Inline Hooking“ bezeichnet.

5.2.2 Inline Hooking

Inline Hooking ist eine Technik, die bei einem Rootkit bzw. einem DLP-Treiber verwendet wird, um Funktionsaufrufe zu manipulieren. Dies kann sowohl im User-Mode als auch im Kernel-Mode geschehen. Inline Hooking basiert darauf, den Programmcode von Funktionen direkt im Speicher zu verändern. Manipulationen im User-Mode können nur im eigenen Speicher des Prozesses stattfinden. Im Kernel-Mode kann auf alle Speicherbereiche zugegriffen werden. Da der DLP-Treiber im Kernel-Mode läuft, kann er den Speicher aller Prozesse verändern.

Das Inline Hooking funktioniert wie folgt: Zu Beginn eines System-Service führt der DLP-Treiber eine Sprunganweisung zum eigenen Code (den des DLP-Systems) durch. Nach Ausführung des DLP-System Codes springt das Programm zurück in die Originalfunktion. Durch den DLP-System-eigenen Code kann es beliebige Manipulationen vornehmen.

5.2.3 Manipulation der Prozessliste

Um den DLP-Agent vor dem Benutzer zu verbergen, manipuliert das DLP-System die Prozessliste. Durch die Manipulation erreicht es, dass es für normale Programme (z.B. Taskmanager) nicht mehr auffindbar ist.

Betriebssysteme speichern Accountinginformationen im Speicher, meistens in Form von Strukturen oder Objekten. Wenn ein User-Mode-Prozess vom Betriebssystem Informationen anfordert, z.B. welche Prozesse laufen oder welche Treiber vorhanden sind, gibt das Betriebssystem diese Objekte zurück. Da sich diese Objekte im Speicher befinden, kann der DLP-Treiber sie direkt

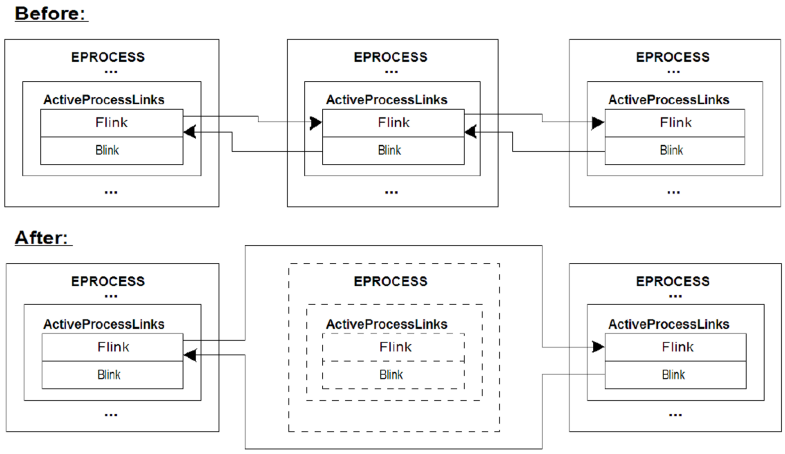

Abbildung 5.4: Manipulation d. Prozessliste aus [12].

ändern. Es ist nicht nötig API-Calls zu verändern, um die Antworten zu filtern.

Windows speichert die Prozessliste in einer doppelt verketteten Liste aus EPROCESS Strukturen. Jede EPROCESS Struktur enthält eine LIST_ENTRY Struktur, die wiederum die Pointer FLINK und BLINK beinhaltet. Sie zeigen auf den vorhergehenden bzw. nachfolgenden Prozess in der Liste.

Um einen Prozess zu verstecken, verändert der DLP-Treiber FLINK und BLINK der vorhergehenden und nachfolgenden Struktur, so dass die zu versteckende Struktur nicht mehr in der Liste auftaucht. Das Entfernen aus der Liste hat keine Nebeneffekte für den versteckten Prozess. Der Scheduler ruft ihn weiterhin auf (siehe Abbildung 5.4).

5.2.4 Interrupt Hooking

Eine weitere Möglichkeit zur Implementierung bietet das Interrupt Hooking. Immer wenn durch Software oder Hardware ein Interrupt ausgelöst wird, wird eine Interrupt Service Routine aufgerufen und vom Betriebssystem ausgeführt. Für jeden Interrupt existiert eine eigene Interrupt Service Routine.

Die Speicheradresse der jeweiligen Routine ist in der Interrupt Descriptor Table (IDT) gespeichert. Jeder Prozessor hat seine eigene IDT, was heutzutage aufgrund der weiten Verbreitungen von Multi-Core Prozessoren relevant ist. Manipulationen müssen demzufolge in allen IDTs stattfinden. Die IDT ist ein Array, das 256 Einträge enthält, einen für jeden Interrupt (siehe [6] Kapitel 3).

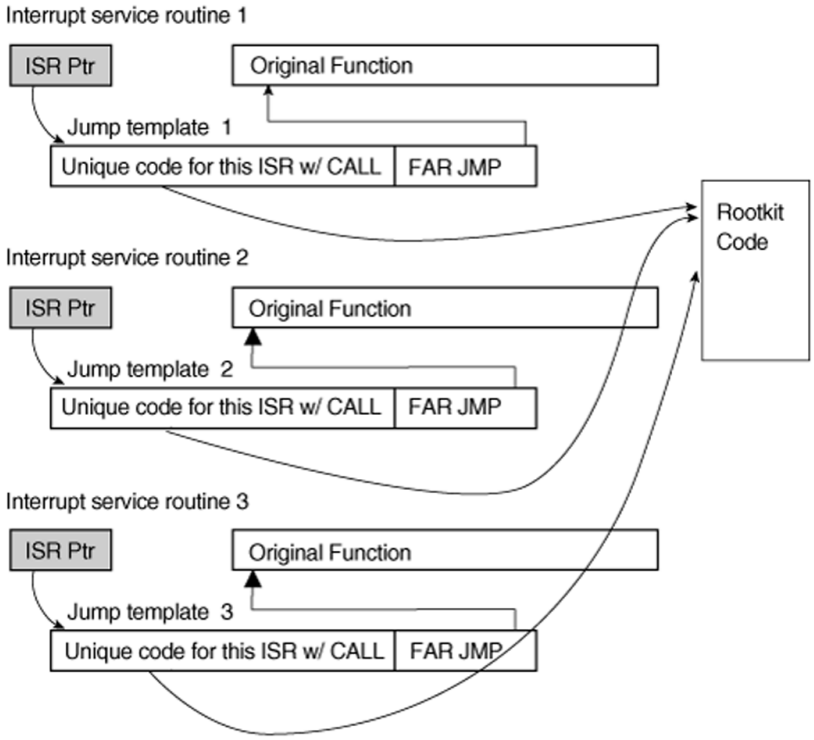

Abbildung 5.5: IDT Hooking mit Jump Templates aus [6]

Die Abbildung 5.5 zeigt die IDT-Manipulation durch „Jump Templates“. Jedes Template ruft den gleichen Rootkit-Code auf, der in diesem Fall wie eine normale Funktion behandelt wird. Eine Funktion hat die Eigenschaft, dass sie nach ihrer Ausführung immer zum Punkt des Aufrufs zurück kehrt bzw. einen Befehl nach dem Aufruftspunkt. Diese Eigenschaft erlaubt es, jedem Interrupt Handler zusätzlichen Code hinzuzufügen und somit den Programmablauf zu ändern. Die „FAR JMP“ Adresse enthält den Rücksprung auf den Originalcode der Interrupt Service Routine.

5.3 Verschlüsselung vertraulicher Daten

Verschlüsselung ist die einzig sichere Möglichkeit vertrauliche Daten zu schützen, wenn der DLP-Agent nicht aktiv ist. Andernfalls liegen die Daten offen. Unter der Voraussetzung, dass vertrauliche Daten auf Datenträgern gespeichert wurden, die für einen Angreifer erreichbar sind (z.B. Festplatte im Arbeitsplatzcomputer oder Laptop), muss ein DLP-System die Funktion bieten, alle Daten, die als vertraulich klassifiziert wurden, automatisch und transparent zu verschlüsseln. Die Entschlüsselung erfolgt wiederum transparent auf Computern mit aktivem DLP-Agent. Ohne aktiven DLP-Agent

ist eine Entschlüsselung nicht möglich.

Alternativen zur Verschlüsselung seitens des DLP-Agents gibt es auch, allerdings sind diese weniger sicher. Eine Alternative ist das in Windows integrierte Encryption File System (EFS), welches starke Verschlüsselung bietet. Falls schützenswerte Daten nur in verschlüsselten Ordnern gespeichert werden, sind Angriffe über ein Livesystem oder den Umbau der Festplatte in einen anderen Computer erfolglos. Diese Art der Verschlüsselung bietet jedoch keinen Schutz, für den Fall, dass der Angreifer den DLP-Agent im laufenden Betrieb beendet. Gleiches gilt auch für alle anderen Verschlüsselungsprogramme, die verschlüsselte Ordner oder Festplatten bereit stellen.

Zusammenfassend bleibt festzuhalten, dass ein DLP-System in der Lage sein muss, alle kritischen Daten automatisch zu verschlüsseln. Wenn dies nicht der Fall ist, muss über organisatorische Maßnahmen sicher gestellt werden, dass kein Zugriff auf die Daten erfolgen kann, wenn der DLP-Agent deaktiviert ist. Insbesondere bei Laptops ist dies nicht zu garantieren. Ein Beispiel für die erwähnten organisatorischen Maßnahmen sind Benutzer, die auf ThinClients arbeiten und sich als unpriviligierte Benutzer auf einen Terminal Server verbinden.

5.4 Whitelisting von Anwendungen

Die Sicherheit des Gesamtsystems lässt sich durch die Verwendung von Whitelisting für Anwendungen erhöhen. Das bedeutet, dass keine Anwendung ausgeführt werden kann, wenn sie nicht auf einer Whitelist steht. Dies hat den Effekt, dass sich die Anzahl der Programme, die zum unerwünschten Informationstransfer genutzt werden, auf die erlaubten Anwendungen reduziert.

Es gibt mehrere Whitelistingmechanismen. Sichere Mechanismen verwenden sichere kryptografische Prüfsummen zur Identifikation erlaubter Anwendungen. Ein unsicherer Mechanismus ist die Filterung nach Dateinamen, da eine Umbenennung des betroffenen Programms zur Umgehung der Whitelist führt. Nach heutiger Lehrmeinung sind SHA256 und bessere sowie Ripemd-160 geeignete Prüfsummenalgorithmen [2]. Im Optimalfall kommen gleichzeitig zwei verschiedene Prüfsummen zum Einsatz.

Nach heutigem Wissensstand ist die Verwendung von MD5 unsicher [19]. Es ist problemlos möglich zwei ausführbare Dateien mit gleicher MD5-Summe zu erzeugen. Tests (Aufbau siehe [19]) im Rahmen dieser Arbeit ergaben, dass es auf einem einfachen PC (Athlon X2 3800+) weniger als 20 Minuten dauert, zwei Programme mit identischer MD5-Summe zu erstellen.

Microsoft bietet in seinen Versionen von Windows XP und Windows Server 2003 die Funktionalität, Whitelisten für Programme zu verwenden. Windows bietet vier Wege Sofware zu identifizieren[5]:

- Hash - Ein kryptografischer Fingerabdruck einer Datei.
- Zertifikat - Ein Zertifikat, mit der die Datei digital signiert wurde.
- Pfad - Ein lokaler Pfad oder UNC-Pfad (Universal Naming Convention), unter dem die Datei gespeichert ist.
- Zone - Eine Internetzone.

Die in der Liste genannten Einstellungen verteilen Gruppenrichtlinien des Active Directory an die Client PCs. Whitelisting von Programmen hat einen Sicherheitsgewinn zur Folge. Zum einen können Anwender keine unzulässigen Programme mehr starten, die unter Umständen die Systemstabilität beeinträchtigen, zum anderen kann Schadsoftware ausgeschlossen werden. Aufgrund der Tatsache, dass nur autorisierte Anwendungen starten, kann auch kein Malware-Prozess starten. Skriptbasierte Viren lassen sich durch Deaktivierung der Skriptinterpreter ebenfalls beseitigen.

Diese Maßnahmen lassen sich jedoch nicht in jedem Umfeld durchsetzen. Ein Bespiel sind Programmierumgebungen:

> Ein Programmierer, der regelmäßig seine Quelltexte kompiliert erhält sehr oft neue ausführbare Dateien, die er dann nicht starten darf.

Der Whitelistingansatz ist nicht nur bei der reinen Ausführung von Programmen anwendbar, sondern auch bei der Verwendung von TCP- und UDP-Ports. Diese Funktion bieten einige DLP-Systeme. Dort ist definiert, welche Programme welche Ports verwenden dürfen (gleiches Prinzip wie bei Personal Firewalls). Dies schränkt die Möglichkeiten eines Angreifers stark ein, da er nur noch vom Administrator freigegebene Netzwerkprogramme verwenden kann.

5.5 Netzwerk des Vertrauens

Das so genannte „Netzwerk des Vertrauens“ (engl. Community of Trust) ist eine Möglichkeit, Zugriffe auf vertrauliche Daten einzuschränken. Es ist

[5] http://technet.microsoft.com/de-de/library/bb457006(en-us).aspx

keine direkte Maßnahme um einen Informationsabfluss zu verhindern, aber durch die Einschränkung des Zugriffs verringert sich die Gefahr, dass jemand unberechtigt Daten kopiert.

Im Netzwerk des Vertrauens kommunizieren nur Computer mit aktiviertem DLP-Agent miteinander. Jede Aktivität, ob erlaubt oder unerlaubt, wird von DLP-Agents überwacht. So ist sicher gestellt, dass schützenswerte Daten nicht nach außen gelangen.

Versucht beispielsweise ein Client ohne DLP-Agent sich mit einem Server, der sich im Netzwerk des Vertrauens befindet, zu verbinden, erlaubt der Server den Verbindungsaufbau nicht. Dies hat den Nebeneffekt, dass der Server Verbindungsversuche bei einem Angriff über das Netzwerk ebenfalls beendet. Das Netzwerk des Vertrauens lässt sich sowohl im lokalen Netz, als auch über das Internet oder VPN verwenden.

5.6 Datenaustausch über die Zwischenablage

Über die Zwischenablage können Daten zwischen verschiedenen Programmen ausgetauscht werden (kopieren & einfügen). Somit besteht die Gefahr, dass Daten aus einem als vertraulich klassifizierten Dokument heraus, in ein anderes, nicht klassifiziertes Dokument, kopiert und so Informationen aus dem Unternehmen heraus transferiert werden. Das bedeutet, dass der DLP-Agent auch die Zwischenablage überwachen muss.

Bei einem DLP-System, dass Dateien nach deren Inhalt klassifiziert (Content Inspection) ist die Gefahr, dass ein solcher Versuch Daten zu entwenden gelingt, als eher gering einzuschätzen. Das System klassifiziert die neue Datei sofort als vertraulich und verhindert somit unbefugten Datenabfluss. Davon nicht betroffen sind Kopiervorgänge in eine Anwendung, die die Daten nicht in einer Datei speichert, sondern über das Netzwerk verschickt (z.B. Instant Messenger, E-Mail).

Daher ist eine Überwachung der Zwischenablage nötig. Der DLP-Agent entscheidet dann aufgrund verschiedener Kriterien, ob eine (Kopier)Aktion erlaubt ist oder nicht. Nachfolgend einige Beispiele für solche Kriterien:

- Quellanwendung
- Zielanwendung
- Inhalt - Überprüfung durch reguläre Ausdrücke
- Klassifikation des Quelldokuments

USB Parameters	VID	4 digit hex number obtained from USB forum to identify the vendor of the USB device. 0x0000 is prohibited! This setting is not recommend to touch!
	PID	4 digit hex number assign by vendor to identify the product. This setting is not recommend to touch!
	Vendor String	Variable length character string. Not recommend to touch!
	Product String	Variable length character string. Not recommend to touch!

Abbildung 5.6: Aus Produktbeschreibung iCreate

Ist die Quellanwendung ein Kriterium (beispielsweise ein ERP-System), stellt der DLP-Agent sicher, dass kein Kopieren aus dieser Anwendung heraus möglich ist. Bei der Überprüfung nach dem Inhalt der zu kopierenden Daten besteht die in Abschnitt 3.4 beschriebene Problematik, dass die Erstellung der Filterkriterien sehr komplex ist. Einfacher ist es, Kopieraktionen abhängig davon zu erlauben, ob das Quelldokument einer bestimmten Klassifikationsstufe zugeordnet ist oder nicht.

5.7 Externe Speichermedien

Hostbasierte DLP-Systeme sind im Gegensatz zu netzwerkbasierten DLP-Systemen in der Lage, die Verwendung von externen Speichermedien am Endgerät zu überwachen. Einige Hersteller bezeichnen dies als „Endpoint Security“. Der DLP-Agent verhindert, dass vertrauliche Daten auf externe Datenträger geschrieben werden.

Sollen externe Datenträger verwendet werden, stellt der DLP-Agent sicher, dass die Daten dort nicht unverschlüsselt gespeichert werden (siehe Abschnitt 5.3). Einige DLP-Systeme bieten die Funktion die Verwendung von USB-Sticks mit bestimmter Vendor- und Product-ID zu erlauben. Die Verwendung nicht autorisierter USB-Sticks unterbindet das System.

Die Sicherheit, einen USB-Stick anhand der Vendor- und Product-ID 100%ig zu identifizieren ist nicht gegeben. Ein Thema im Debianforum (siehe [16]) behauptet, dass die IDs manipulierbar sind. Die dort erwähnten Tools ermöglichen die Veränderung der Vendor- und Product-ID. Die Produktbeschreibung von iCreate besagt, dass eine Änderung von Product- und Vendor-ID möglich, aber nicht empfohlen ist (siehe Abbildung 5.6). In einem Funktionstest im Rahmen dieser Arbeit konnte die Funktionsfähigkeit von iCreate nicht nachvollzogen werden.

5.8 E-Mail

Wie bereits in Abschnitt 2.2.1 beschrieben, ist E-Mail eine Anwendung, die nicht immer verboten werden kann. Ein DLP-System hat daher die Aufgabe, unerwünschten Informationsabfluss über E-Mail zu verhindern.

Dies versuchen einige Unternehmen auch ohne DLP-Systeme, indem sie Personal einsetzen, das ausgehende E-Mails liest [15] und unerlaubte Nachrichten filtert. Dies ist allerdings nur bei unverschlüsselten E-Mails möglich. Wenn eine E-Mail mit PGP oder ähnlichen Verfahren geschützt ist, oder die Daten in einem verschlüsselten Archiv angehängt sind, besteht keine Möglichkeit der Kontrolle.

Verschlüsselte Daten kann ein DLP-System ebenfalls nicht kontrollieren, es kann nur die Umwandlung in ein verschlüsseltes Format verhindern (siehe Abschnitt 5.11). Bei unverschlüsselten E-Mails überprüft der DLP-Agent entweder den Inhalt der E-Mail oder die Klassifizierung der angehängten Dokumente. Anhand der Klassifizierung erlaubt oder blockiert das DLP-System den Versand. Dies erfolgt unabhängig vom verwendeten E-Mail-Client.

5.9 Instant Messenger und Peer-to-Peer

Instant Messenger und Peer-to-Peer-Anwendungen sind durch Layer-7-Firewalls blockierbar. Das Skype-Protokoll war für einige Zeit nur schwer zu blockieren, wird aber von modernen Firewalls zuverlässig erkannt [3]. Da einige Instant Messenging Protokolle die Verschlüsselung der Daten unterstützen, kann der Datenstrom im Netzwerk nicht immer mitgelesen werden. Somit ist eine Filterung durch netzwerkbasierte DLP-Systeme nicht möglich.

Hostbasierte DLP-Systeme begegnen dem Datenabfluss über Instant Messenger und Peer-to-Peer-Programme auf dem gleichen Weg wie dies bei E-Mail der Fall ist. Anhand des Inhalts oder der Klassifizierung einer zu verschickenden Datei wird entschieden, ob die Kommunikation erlaubt ist oder nicht. Der in Abschnitt 5.4 beschriebene Whitelistingansatz bietet neben Firewalls eine zweite Variante, unerwünschte Instant Messenger und Peer-to-Peer-Programme zu blockieren.

5.10 Drucker

Informationen lassen sich nicht nur über Internet oder externe Datenträger aus dem Unternehmen transferieren, sondern auch in gedruckter Form. Der DLP-Agent eines hostbasierten DLP-Systems überwacht daher, welche Daten auf welchen Druckern gedruckt werden. Die Entscheidung ob ein Druckauftrag legitim ist oder nicht, entscheidet das System ebenfalls aufgrund des Inhalts oder der Klassifizierung der Daten.

Neben physischen Druckern gibt es virtuelle Drucker. Ein Beispiel wären PDF-Drucker. Sie installieren einen Treiber und sind im „Drucken“-Dialog als Drucker vorhanden. PDF-Drucker erlauben es, aus beliebigen Anwendungen mit Druckfunktion, Daten im PDF-Format zu erstellen. Virtuelle Drucker müssen vom DLP-System somit auch überwacht werden. Andernfalls ist eine Umwandlung klassifizierter Daten in unklassifizierte Daten möglich. Da ein DLP-System unklassifizierte Daten nicht schützt, kann ein Angreifer diese Daten entwenden.

5.11 Sonstiges

Die Umwandlung klassifizierter Dateien in unklassifizierte Dateien ist ein Risiko für die Datensicherheit, da DLP-Systeme nur klassifizierte Daten überwachen. Ein Beispiel für eine Umwandlung sind Packprogramme oder Verschlüsselungssoftware. Ein hostbasiertes DLP-System setzt vor der Umwandlung an. Da es als Kernelmodul Zugriff auf das Betriebssystem hat, überprüft es die Daten, bevor sie in ein anderes Format umgewandelt oder verschlüsselt werden.

Um an Daten zu gelangen, kann ein Angreifer den Umweg über Screenshots gehen und alle relevanten Daten als Bild speichern. Diese Bilder sind nicht klassifiziert, enthalten aber vertrauliche Daten. Windows stellt standardmäßig eine Screenshotfunktion zur Verfügung, es existieren auch Drittanbieterprogramme, die diese Funktionalität besitzen. Ein hostbasiertes DLP-System blockiert die Screenshotfunktionen, bzw. lässt sie nur für Bildschirmbereiche zu, die keine klassifizierte Daten enthalten.

Kapitel 6

Musterimplementierung

Dieses Kapitel beschreibt die Implementierung eines DLP-Systems in einer fiktiven Firma. Es stellt am praktischen Beispiel dar, welche Voraussetzungen erfüllt sein müssen, wie die einzelnen Schritte der Planung und die Implementierung ablaufen. Dieses Kapitel beschränkt sich dabei auf die für die Einführung eines DLP-Systems wesentlichen Schritte.

6.1 Voraussetzungen und Ziele

Die nachfolgend betrachtete Musterfirma ist ein mittelständischer Anlagenbauer, der Maschinen neu entwickelt und selbst produziert. Die Steuerungssoftware für die Anlagen lässt die Firma intern programmieren. Das Unternehmen beschäftigt etwa 2.000 Mitarbeiter und besitzt ca. 500 PC-Arbeitsplätze und weitere 50 Laptops.

In der Vergangenheit hat ein Mitbewerber aus dem fernen Osten eine Neuentwicklung der Firma zeitgleich, allerdings wesentlich preisgünstiger, auf den Markt gebracht. Dies führte zu Absatzverlusten bei der Firma. Die Betriebsleitung vermutet, dass der Mitbewerber Zugriff auf die Entwicklungsunterlagen bzw. Baupläne und den Quellcode der Steuerungssoftware hatte. Um derartige Situationen in der Zukunft zu vermeiden, möchte die Firma ein DLP-System einsetzen. Vor der Implementierung soll der Nutzen überprüft werden.

Das Ziel der Implementierung ist es, dass Baupläne und Quellcode das Unternehmensnetzwerk nicht mehr verlassen können. Da es keine Partnerfirmen in den Entwicklungsbereichen gibt, brauchen kritische Daten nicht weiter gegeben werden und externe Partner spielen bei den Sicherheitsbetrachtungen für das DLP-System keine Rolle. Die Voruntersuchungen ergeben, dass Daten der Buchhaltung ebenfalls schützenswert sind, die Mengen

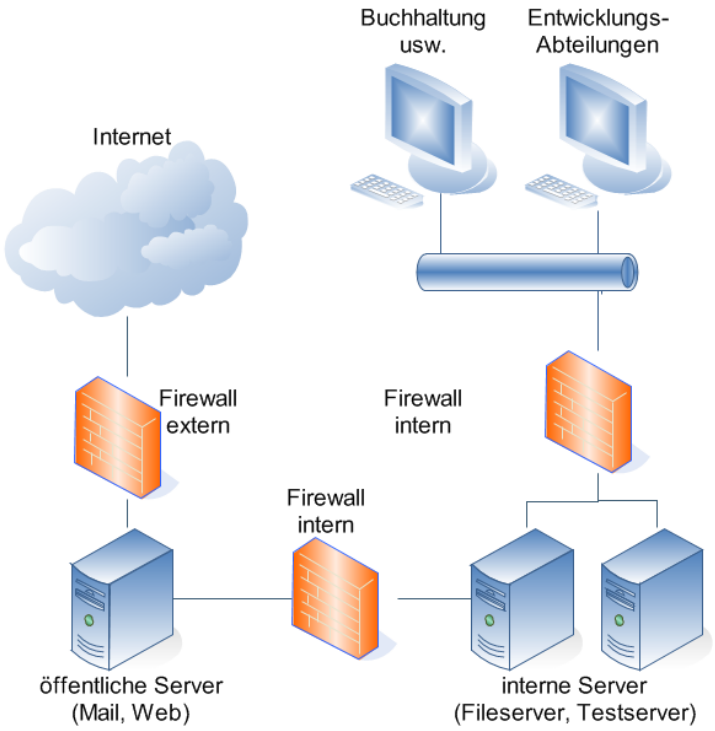

Abbildung 6.1: Vereinfachter Netzwerkplan der Musterfirma

kritischer Daten allerdings so gering ist, dass sie durch Aufschreiben auf Papier entwendet werden könnten. In der Buchhaltung ist daher kein Einsatz eines DLP-Systems geplant. Das Unternehmen möchte zuerst praktische Erfahrungen mit dem DLP-System sammeln, um später zu entscheiden, ob der Einsatz auch in der Buchhaltung eventuell doch sinnvoll ist.

6.2 Sicherheitsmanagement

Für die IT-Sicherheit im Unternehmen ist bisher die IT-Abteilung zuständig. Es gibt keinen dedizierten IT-Sicherheitsverantwortlichen. Nachdem festgestellt wird, dass die Aufgaben zur erfolgreichen Einführung eines DLP-Systems mit der derzeitigen Aufgabenverteilung nicht möglich ist, wird ein IT-Sicherheitsbeauftragter bestimmt. Er ist für die Aufgaben des IT-Sicherheitsmanagements verantwortlich und erarbeitet die Vorgaben, die die IT-Abteilung anschließend umsetzt.

Zu den Aufgaben des IT-Sicherheitsverantwortlichen im Rahmen der Einführung des DLP-Systems gehören die Bestandsaufnahme der aktuellen Situation, eine Risikoanalyse, die Erstellung von Klassifizierungsrichtlinien und

die Erstellung eines Planes zur Installation des DLP-Systems. Die Umsetzung erfolgt durch die IT-Abteilung. Die Risikoanalyse ergab, dass die zu erwartenden Kosten durch die Folgen von Industriespionage höher sind als die zu erwartenden Ausgaben für ein hostbasiertes DLP-System, welches die Daten in den kritischen Abteilungen schützt.

Die Entscheidung für ein hostbasiertes DLP-System ist darin begründet, dass bisher keine Überwachung der Endgeräte (z.B. USB-Sperren) stattfindet und netzwerkbasierte DLP-Systeme wichtige Datenkanäle (z.B. USB-Datenträger) nicht überwachen können. Zudem sind netzwerkbasierte Systeme durch Verschlüsselung der Netzwerkdaten leichter umgehbar als hostbasierte DLP-Systeme (siehe Abschnitt 4.3). Ein hostbasiertes DLP-System erfasst wesentlich mehr Kanäle und die Installation einer zweiten Software zur Überwachung lokaler Schnittstellen hat sich als umständlich und ineffizient herausgestellt.

Nach der Festlegung auf ein hostbasiertes DLP-System erstellt der IT-Sicherheitsverantwortliche Vertraulichkeitsklassen für alle Daten der betroffenen Abteilungen. Dabei verwendet er die in Abschnitt 3.1 angeführte Halbordnung:

- nicht klassifiziert
- vertraulich
- geheim
- streng geheim

Als nicht klassifiziert gelten alle Daten, die für die Öffentlichkeitsarbeit (z.B. Werbung, öffentliche Berichte) bestimmt sind. Alle firmeninternen Daten sollen mindestens der Stufe „vertraulich“ angehören. Alle Quelltexte für die Programme zur Steuerung der Maschinen werden der Vertraulichkeitsstufe „geheim“ zugeordnet. Die höchste Vertraulichkeitsstufe (streng geheim) sollen alle Konstruktionszeichnungen und Baupläne der Maschinen erhalten.

6.3 Bestandsaufnahme

Unabhängig davon, ob ein DLP-System implementiert wird oder nicht, ist es für den IT-Sicherheitsbeauftragten wichtig, dass er weiß, aus welchen Bestandteilen sich die IT-Infrastruktur des Unternehmens zusammensetzt. Aus der Bestandsaufnahme ergibt sich der in Abbildung 6.1 gezeigte vereinfachte Netzwerkplan.

Neben der Analyse der Netzwerkumgebung sind weitere Daten über die verwendeten Systeme nötig, um den Einsatz eines hostbasierten DLP-Systems planen zu können. Zu diesen Daten gehören:

- Gerätetyp
- Betriebssystem (Version)
- Hardwareausstattung
- IP-Adresse / Subnetz.

Der Gerätetyp sagt aus, ob es sich um einen PC, Server oder einen Laptop handelt. Informationen über die Version des Betriebssystems werden benötigt, um Aussagen zur Kompatibilität der DLP-Software mit dem Betriebssystem zu treffen. Die Hardwareausstattung spielt eine untergeordnete Rolle, ist aber zum Testen möglicher Performanceprobleme relevant.

Die IP-Adresse des Endgerätes spielt bei der Verwendung eines hostbasierten DLP-Systems ebenfalls eine untergeordnete Rolle, ist aber für Einstellungen auf der Firewall relevant. Die Firewall schränkt den Zugriff bestimmter IP-Adressen und Subnetze auf wenige Protokolle ein und verringert somit die Anzahl der Möglichkeiten Daten aus dem Unternehmen heraus zu transferieren. Regeln des DLP-Systems können ebenfalls IP-Adressen beinhalten. Nachdem der IT-Sicherheitsverantwortliche durch die Bestandsaufnahme einen Überblick erlangt hat, kann er mit der Planung zur Installation des DLP-Systems beginnen.

6.4 Planungsschritte

Die Planung umfasst vier große Teilbereiche. Der erste Teilbereich beschäftigt sich mit den Abflusskanälen für Daten aus dem Unternehmen. In den von der Einführung des DLP-Systems betroffenen Abteilungen der Musterfirma werden folgende Kanäle gefunden:

- USB-Datenträger
- HTTP(S), FTP(S)
- E-Mail
- Drucker
- Datensicherungen

- interne Festplatten

Weitere internetbasierte Kanäle, wie beispielsweise Instant Messaging, blockiert die bereits vorhandene Layer-7-Firewall. Diese Firewall erlaubt nur die Protokolle HTTP(S) und FTP als Verbindung zum Internet. E-Mails können die betroffenen Abteilungen nur über einen firmeninternen Mailserver senden und empfangen. Von jeder gesendeten E-Mail erstellt der Mailserver eine Kopie (BCC[1]), um im Verdachtsfall den E-Mail-Verkehr überprüfen zu können. Das DLP-System überwacht die Übermittlung von Daten per E-Mail und blockiert den Sendevorgang gegebenenfalls.

USB-Sticks werden in der Musterfirma häufig verwendet, so dass ein Verbot nicht in Frage kommt und der Whitelistingansatz für USB-Sticks (siehe Abschnitt 5.7) zu aufwändig ist. Der Gefahr durch USB-Datenträger will der IT-Sicherheitsverantwortliche durch Verschlüsselung aller Daten ab der Sicherheitsstufe „vertraulich“ durch das DLP-System begegnen. Somit ist eine Entschlüsselung der kritischen Daten nur noch innerhalb der durch das DLP-System geschützten Bereiche möglich. Die Verschlüsselung vertraulicher Daten soll nicht nur für USB-Datenträger gelten, sondern auch auf lokalen Datenträgern aktiv sein. Damit vereinfacht sich die Entsorgung der Festplatten und selbst bei einem möglichen Diebstahl der Datenträger (z.B. gestohlener Laptop) ergibt sich keine Gefahr für die zu schützenden Daten.

Die Gefahr, dass vertrauliche Daten ausgedruckt und aus dem Unternehmen heraus getragen werden ist mittel. Die Gefahr wird als mittel einschätzt, da die Datenmenge der Quelltexte zu umfangreich für eine sinnvolle Weiterverarbeitung ist. Der Ausdruck von Bauplänen birgt hingegen ein höheres Gefahrenpotential. Diesem Umstand soll begegnet werden, indem Ausdrucke nur noch über einen definierten Printserver möglich sind, der, genau wie der Mailserver, Kopien der Druckaufträge speichert um im Verdachtsfall eine Kontrollmöglichkeit zu haben. Der Ausdruck von geheimen und streng geheimen Daten überwacht das DLP-System, es blockiert den Ausdruck jedoch nicht. Es blendet ein Dialogfenster ein, dass den Anwender darauf hinweist, die Ausdrucke nicht unbeaufsichtigt zu lassen und sie nach Gebrauch im Aktenvernichter zu entsorgen.

Um im Katastrophenfall nicht die Datensicherungen zu verlieren, lagert die Firma eine Kopie der Datensicherung in einer 20 Kilometer entfernten Zweigstelle in einem Tresor. Bisher sind die Datensicherungen unverschlüsselt aufbewahrt worden. Mit Einführung des DLP-Systems sollen auch diese verschlüsselt werden, um eine Gefahr für die Daten durch Diebstahl auszuschließen. Die Verschlüsselung der Backups erfolgt nicht durch das DLP-System, sondern durch die Backupsoftware. Dadurch ist gewährleistet, dass

[1] Blind Carbon Copy

auch bei einem Totalausfall des DLP-Systems und einem damit verbundenen Schlüsselverlust die Daten wieder herstellbar sind.

Der zweite große Teilbereich der Planungsphase ist die Abstimmung mit dem Betriebsrat über die geplanten Maßnahmen. Dies ist nötig, da durch die Installation des DLP-Systems ein Eingriff in die Privatsphäre der Mitarbeiter geschieht (siehe Abschnitt 1.3). Da es sowohl im Interesse der Unternehmensführung, als auch des Betriebsrates ist, die unternehmenskritischen Daten zu schützen, gestalten sich die Verhandlungen unkompliziert. Die Beteiligten einigen sich darauf, dass in jeder der betroffenen Abteilungen ein öffentlicher PC installiert wird, der von der Entwicklungsumgebung getrennt ist und nicht vom DLP-System überwacht wird. Die Mitarbeiter sollen Ergänzungen zu den Arbeitsverträgen erhalten, die die Neuerungen durch das DLP-System beinhalten. Mitarbeiter, die unter den neuen Bedingungen nicht arbeiten wollen (die Ergänzungen zum Arbeitsvertrag nicht unterschreiben), sollen in eine andere Abteilung versetzt werden.

Die Erstellung von Firmenpolicies zum Umgang mit Daten und die Planung der Schulung der Mitarbeiter umfasst den dritten Teilbereich der Planungsphase. In der Musterfirma werden die bestehenden Datenschutzrichtlinien dahingehend erweitert, dass die Vertraulichkeitsklassen erklärt und der Umgang mit klassifizierten Daten reguliert wird. Eine Schulung der Mitarbeiter wird die Erklärung der erweiterten Firmenpolicies sowie den Umgang mit dem DLP-System beinhalten. Zu den Policies gehören beispielsweise das Verbot von Kameras in Produktions- und Entwicklungsbereichen der Firma.

Der vierte und letzte Teilbereich der Planung umfasst die Evaluierung möglicher DLP-Syteme und der anschließenden Erstellung eines Installationsplanes. Dazu gehören auch die Planung begleitender Maßnahmen, wie die beispielsweise Änderung von Firewallregeln zur Minimierung der Datenabflusskanäle. Die Evaluierung der DLP-Software findet aufgrund folgender Hauptkriterien statt:

- Klassifizierungsfeatures
- transparente Verschlüsselung
- Bedienung
- Kosten
- Sicherheitsüberprüfung
- USB-Port Überwachung

Das zu installierende DLP-System muss die automatische und inhaltsbasierte Klassifizierung unterstützen, genauso wie die transparente Verschlüsselung klassifizierter Daten. Eine gute Bedienbarkeit ist Wunsch der zukünftigen Administratoren. Die Systeme, die in die engere Auswahl kommen, werden einer Sicherheitsprüfung unterzogen, ob sie sich umgehen lassen. Nicht zuletzt spielen auch die Kosten des Systems eine Rolle. Die USB-Port Überwachung bezieht sich darauf, USB-UMTS-Modems zu erkennen und zu blockieren.

Um die Verwendung unautorisierter Endgeräte im Netzwerk der Entwicklungsabteilungen zu verhindern, soll das standardisierte 802.1x Protokoll zum Einsatz kommen. Der IEEE[2] 802.1x Standard ist eine Methode zur Authentifizierung und Autorisierung im Ethernet. Die Authentifizierung eines Clients erfolgt durch einen Authentifizierungsserver (Radius[3]). Mit dieser Maßnahme und zusätzlichen Firewallregeln, sollen Zugriffe von Systemen ohne DLP-Software auf vertrauliche Daten verhindert werden. Die Alternativmöglichkeit des „Netzwerk des Vertrauens“ (siehe Abschnitt 5.5) wird abgelehnt, da mit 802.1x und der Änderung der Firewallregeln eine kostengünstigere Variante existiert.

6.5 Installation und begleitende Maßnahmen

Im Anschluss an die Evaluierungsphase wird das gewählte DLP-System auf den PCs und Laptops gemäß den Planungen in den Entwicklungsabteilungen installiert. Als Erstes wird das DLP-Managementssystem installiert. Anschließend werden die DLP-Agents, zentral gesteuert durch das DLP-Managementsystem, auf den Systemen der technischen Zeichner installiert. Nachdem es hier zu keinen größeren Komplikationen kommt, werden auch die Systeme der Softwareentwickler umgestellt. Das Management des gesamten DLP-Systems erfolgt über einen zentralen DLP-Managementserver.

Der DLP-Managementserver ist eine virtuelle Maschine, die täglich per Snapshot gesichert wird. Somit ist kein aufwändiges Clustern nötig. Die Hochverfügbarkeit der Hardware garantiert die darunter liegende, bereits existierende, Virtualisierungslösung. Sollte das Managementsystem abstürzen, kann es innerhalb weniger Minuten wieder hergestellt werden. Für den Betrieb des DLP-Systems ergibt sich daraus ein vertretbarer Nachteil, dass in der Zeit eines möglichen Ausfalls kein Zugriff auf aktuelle Alarmmeldungen möglich ist bzw. maximal die Einstellungen und Meldungen der letzten 24 Stunden verlorgen gehen.

[2] Institute of Electrical and Electronics Engineers
[3] Remote Authentication Dial-In User Service

Die in Abschnitt 5.4 beschriebene Funktion des Whitelistings von Anwendungen wird nicht implementiert. Gründe dafür sind, dass der Arbeitsablauf der Programmierer gestört würde und dass die Gefahr durch unerlaubte Programme für gering gehalten wird, da nur HTTP(S) und FTP durch die Firewalls zugelassen ist und diese Protokolle und vom DLP-System überwacht werden.

Um Systeme ohne DLP-Agent aus den Entwicklungsnetzwerken fernzuhalten wird 802.1x implementiert. Den Zugriff anderer Abteilungen auf zu schützenden Entwicklungsbereiche verhindern VLANs und Access Control Lists (ACLs) der Router. ThinClients kommen nicht zum Einsatz, da die Grafikleistung nicht ausreichend ist.

Die Klassifizierung der Daten erfolgt über die DLP-Agents, welche contentbasiert arbeiten. Die vom IT-Sicherheitsbeauftragten erstellten Regeln zur Klassifizierung werden über den zentralen DLP-Managementserver verwaltet. Mobiltelefone und andere Geräte die einen unkontrollierten Kanal in das Internet öffnen (z.B. USB-UMTS-Modems) sind in den geschützten Abteilungen verboten. Die Kontrolle der USB-Ports übernimmt ebenfalls das DLP-System.

Kapitel 7

Resümee

Der Schutzbedarf vertraulicher Informationen in Unternehmen wird in Zeiten der Globalisierung immer wichtiger. Neuentwicklungen sind teuer und benötigen hohe Entwicklungsbudgets. Ein Mitbewerber, der Zugriff auf die Entwicklungsergebnisse hat, besitzt einen Vorteil, der es ihm ermögtlicht, preisgünstiger zu produzieren.

Traditionelle Sicherheitstechniken wie Firewalls, Zugriffsrechte, Verschlüsselung oder Anti-Virenprogramme können die unerwünschte Verwendung der Daten durch Berechtigte nicht verhindern. Die Aufgabe von Data Leakage Prevention Systemen ist es vertrauliche Daten zu schützen und einen unerwünschten Informationsabfluss zu verhindern. Wie dies geschieht und in welchem Unfang hängt vom Einsatzumfeld des Systems ab.

Netzwerkbasierte DLP-Systeme können nur einen kleinen Teilbereich der Abflusskanäle überwachen und sind von einem Angreifer leicht zu umgehen. Hostbasierte DLP-Systeme setzen einen DLP-Agent auf jedem System voraus, welcher alle Aktivitäten überwacht. Beim Einsatz eines hostbasierten Systems muss sicher gestellt werden, dass vertrauliche Daten nie auf einem System gespeichert werden können, dass nicht von einem DLP-Agent überwacht wird.

Damit das DLP-System die Daten schützen kann, gibt es Vertraulichkeitsstufen, nach denen die Daten klassifiziert werden. Die Richtlinien für die Klassifizierung legt das IT-Sicherheitsmanagement fest. Ein funktionierendes IT-Sicherheitsmanagement ist für den effektiven Betrieb eines DLP-Systems Voraussetzung.

DLP-Systeme sind trotzdem kein „Wundermittel“ gegen Industriespionage. Ihr Einsatzumfeld ist auf Bereiche beschränkt, bei denen die Datenmengen so groß sind, dass sie nicht manuell (z.B. mit Stift und Papier) kopierbar sind und das menschliche Gehirn sie nicht speichern kann. DLP-Systeme

haben ein weiteres Manko: Sie können ihr physisches Umfeld nicht beeinflussen und sind somit externen Angriffen schutzlos ausgeliefert. Als einfache Beispiele können Digitalkameras zum Abfotografieren des Bildschirminhalts oder das Abfangen „kompromittierender Abstrahlung“ von EDV-Systemen (Tempest) gelten.

Daher müssen zum Schutz der Informationen verschiedene Sicherheitsmechanismen ineinander greifen. Die Installation eines DLP-Systems ist sinnlos, wenn der Vorgesetzte aus Bequemlichkeitsgründen weiterhin unternehmenskritische Daten unverschlüsselt auf seinem privaten Laptop mit sich führt. Genauso führen unverschlüsselte Netzwerkverbindungen durch unkontrollierbare Netze die Bemühungen zum Datenschutz ad absurdum. Ein DLP-System muss die Funktionalität haben, sämtliche schützenswerte Daten zu verschlüsseln. Andernfalls kann ein Angreifer Wege finden, um an die unverschlüsselten Daten zu gelangen.

Es ist zwar wissenschaftlich nicht beweisbar, aber die Vermutung liegt nahe, dass das Wissen um die Überwachung vertraulicher Daten einige Angreifer davon abhält, Daten zu stehlen. Die Wahrscheinlichkeit, dass der Angreifer entdeckt wird ist sehr hoch. Auch wenn DLP-Systeme von IT-Sicherheitsexperten zumindest in Teilen umgangen werden können, so ist doch zu beachten, dass die wenigsten Mitarbeiter in den betroffenen Bereichen über derartiges Fachwissen verfügen. Anders sieht die Situation jedoch aus, wenn geziehlt IT-Sicherheitsexperten in Unternehmen geschleust werden um Daten zu stehlen.

Abschließend ist festzuhalten, dass Data Leakage Prevention Systeme, die Informationssicherheit signifikant erhöhen und zum Schutz von Unternehmenswerten beitragen.

Literaturverzeichnis

[1] BlueCoat: *Open, Manage and Accelerate SSL Encrypted Applications*. http://www.bluecoat.de/downloads/whitepapers/BCS_wp_SSL_Accel.pdf. Kopie auf CD-ROM (BCS_wp_SSL_Accel.pdf).

[2] BSI: *M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens*. http://www.bsi.bund.de/gshb/deutsch/m/m02164.htm. Kopie auf CD-ROM (BSI M 2.164.pdf).

[3] Checkpoint: *Check Point Offers Superior Protection for Enterprise Exposure to Consumer Applications*. http://www.checkpoint.com/press/2007/skype092107.html. Kopie auf CD-ROM (checkpoint_skype.pdf).

[4] DoD: *National Industrial Security Program Operating Manual, 1995*. http://www.usaid.gov/policy/ads/500/d522022m.pdf. Kopie auf CD-ROM (d522022m.pdf).

[5] Eckert, C.: *IT-Sicherheit*. Oldenbourg Wissenschaftsverlag, 2006.

[6] G. Hoglund / J. Butler: *Rootkits: Subverting the Windows Kernel*. Addison Wesley Professional, 2005.

[7] Götz, C.: *Extrusion Prevention*. http://www.securityforum.at/sf07/pdf/folien/06-goetz-extrusion_prevention.pdf. Kopie auf CD-ROM (06-goetz-extrusion_prevention.pdf).

[8] Gutmann, P.: *Secure Deletion of Data from Magnetic and Solid-State Memory*. http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html. Kopie auf CD-ROM (gutmann.pdf).

[9] Hecht, K.: *Mündliche Unterhaltung zum Thema „Data Leakage Prevention“*.

[10] Heise: *China späht angeblich PCs des Bundeskanzleramtes aus*. http://www.heise.de/newsticker/meldung/94899. Kopie auf CD-ROM (heise online - China spaeht angeblich PCs des Bundeskanzleramtes aus.pdf).

[11] INFOWATCH: *Managing Internal Threats*. http://www.infowatch.com/de/threats?chapter=162971949&id=26. Kopie auf CD-ROM (Infowatch - Interne IT-Bedrohungen in Europa 2006.pdf).

[12] KASSLIN, STAHLBERG, LARVALA, TIKKANEN: *Hide 'n Seek revisited - full stealth is back*. http://www.f-secure.com/weblog/archives/KimmoKasslin_VB2005_proceedings.pdf. Kopie auf CD-ROM (KimmoKasslin_VB2005_proceedings.pdf).

[13] M. RUSSINOVICH / D. SOLOMON : *Microsoft Windows Internals (4th Ed*. Microsoft Press, 2005.

[14] MCCULLOUGH, D.: *A Hookup Theorem for Multilevel Security*. IEEE Transactions on Software Engineering, 1990.

[15] PROOFPOINT: *Outbound Email and Content Security in Todays Enterprise, 2007*. http://www.proofpoint.com/id/outbound/. Kopie auf CD-ROM (Proofpoint-Outbound-Email-and-Content-Security-2007.pdf).

[16] RENDEGAST: *USB-Stick, USB-ID geändert*. http://www.debianforum.de/forum/viewtopic.php?p=586037. Kopie auf CD-ROM (usbstick - debianforum.de.pdf).

[17] ROSENBLATT W., TRIPPE W., M. S.: *Digital Rights Management: Business and Technology*. Wiley & Sons, 2001.

[18] SELBACH, D.: *Massenhaft Jobs - Informations- und Telekommunikationstechnik*. hochschulanzeiger, 94:20, 2008.

[19] SELINGER, P.: *MD5 Collision Demo*. http://www.mscs.dal.ca/~selinger/md5collision/. Kopie auf CD-ROM (Peter Selinger MD5 Collision Demo.pdf).

[20] SUTHERLAND, D.: *A model of Information*. 9th National Computer Security Conference, Sept. 1986.

[21] VERDASYS: *Digital Guardian Data Sheet*. http://verdasys.com/pdf/Digital_Guardian_DS.pdf. Kopie auf CD-ROM (Digital_Guardian_Datasheet.pdf).

[22] WEDDE, P.: *Protokollierung und Arbeitnehmerdatenschutz*. Datenschutz und Datensicherheit, 10(10):752–755, 2007.