JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Sicherheitsfragen in Zusammenhang mit Data Loss Prevention und Vorschläge zur Erweiterung des Österreichischen Informationssicherheitshandbuchs

MASTERARBEIT

zur Erlangung des akademischen Grades

Diplomingenieur

im Masterstudium

Netzwerke und Sicherheit

Eingereicht von:
Simon Bauer, Bakk. (0555787)

Angefertigt am:
Institut für Informationsverarbeitung und Mikroprozessortechnik

Beurteilung:
Univ.-Prof. Dr. Jörg R. Mühlbacher

Linz, Februar, 2013

Kurzfassung

Diese Masterarbeit beschäftigt sich mit der wissenschaftlichen Beschreibung von Data Loss Prevention, den Gefahrenkanälen für unerlaubten Informationsfluss aus einer Organisation, sowie von potentiellen Erweiterungsmöglichkeiten des Österreichischen Informationssicherheitshandbuchs in Bezug auf Data Loss Prevention.

Nach einer anfänglichen Begriffsbestimmung wird ein Bild der aktuellen Bedrohungslage und im Speziellen der Bedrohung durch „Insider“ gezeichnet. Danach werden die grundlegenden Eigenschaften von Intrusion Detection Systemen/Intrusion Prevention Systemen beschrieben, da sie als eine Teileinheit von Data Loss Prevention gesehen werden können.

Es werden Data Loss Prevention Systeme beschrieben, wie sie nach Kriterien eingeteilt werden können und wie sie arbeiten. Ein wesentlicher Teil der Arbeit ist die Kategorisierung und Beschreibung der Gefahrenkanäle für Informationsdiebstahl in einer Organisation. Die wesentlichsten Gefahrenkanäle werden näher beschrieben.

Anschließend werden gängige Sicherheitsframeworks beschrieben und Eines für eine Analyse ausgewählt. Es werden die Stärken diese Frameworks betrachtet, aber vor allem potentielle Erweiterungsmöglichkeiten damit eine umfassende Informationssicherheit mit Data Loss Prevention gegeben ist.

Abstract

This thesis deals with the scientific description of Data Loss Prevention, the risk channels for illicit flow of information from an organization as well as of potential extensions of the „Österreichisches Informationssicherheitshandbuch“ in respect to Data Loss Prevention.

After an initial definition a picture of the current threat and in particular the threat of „insider“ is drawn. Then the basic characteristics of Intrusion Detection Systems/Intrusion Prevention System are described, as they can be seen as a part of Data Loss Prevention.

Data Loss Prevention systems will be described and criterias given for categorization. A substantial part of this work is the categorization and description of the risk channels for information theft in organizations. The most important risk channels are described in detail.

Then, common security frameworks are described and one is selected for analysis. It's strengths are considered, and potential extensions to provide a comprehensive information security with Data Loss Prevention top.

Danksagung

An dieser Stelle möchte ich mich bei jenen Personen bedanken, die mich beim Verfassen dieser Masterarbeit maßgeblich unterstützt haben.

Ich danke Herrn Institutsvorstand Univ.-Prof. Dr. Jörg R. Mühlbacher für die Betreuung der Masterarbeit. Ein Gleichgewicht an Aufgabenstellung und Themenfreiheit stellte eine strukturierte Arbeit sicher, ließ aber gleichzeitig Raum für mir wichtige Aspekte. Dank gilt auch Herrn Dr. Rudolf Hörmanseder, der immer wieder meine Denkansätze reflektiert und zusätzliche Betrachtungsweisen eingebracht hat.

Mein besonderer Dank gilt meinen Eltern Mag.(FH) Silvia Bauer-Bäck, MSc und DI Thomas Bauer. Sie haben mich zu jeder Zeit des Studiums unterstützt, motiviert und bei Bedarf aufgemuntert. Sie gaben mir die Möglichkeit, mich fachlich und persönlich stark weiterzuentwickeln und während eines Auslandssemesters neue Blickwinkel zu gewinnen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CASES Cyberworld Awareness & Security Enhancement Services

CERT Computer Emergency Response Team

DLP Data Loss Prevention

DPI Deep Packet Inspection

HTTP Hyper Text Transfer Protocol

IDS Intrusion Detection System

IEC International Electrotechnical Commission

IP Internet Protocol

IPS Intrusion Prevention System

ISMS Information Security Management System

ISO International Organisation of Standardization

MELANI Melde- und Analysestelle Informationssicherung

SMTP Simple Mail Transfer Protocol

URL Unified Resource Locator

VPN Virtual Private Network

Kapitel 1

Einleitung

Sergey Aleynikov war bis 2009 Vizepräsident und Programmierer bei Goldman Sachs, einer weltweit tätigen Investment-Bank. An seinem letzten Arbeitstag, bevor er zu einem Unternehmen für Hochfrequenz-Aktienhandel-Programme wechselte, übertrug Aleynikov verschlüsselt einen umfangreichen Teil des Quellcodes der Goldman Sachs Handelsplattform an einen Server in Deutschland. Danach versuchte er die Spuren auf seinem Arbeitsplatzrechner zu verwischen. Zuvor hatte er während seiner Tätigkeit bei Goldman Sachs tausende von Quellcode-Dateien über den Firmen-E-Mailaccount an seine private E-Mailadresse gesendet. Er wurde später angezeigt[Kin12].

Data Loss Prevention (DLP) Systeme hätten in diesem Fall möglicherweise die unberechtigte Übertragung der firmeninternen Quellcode-Dateien verhindern können beziehungsweise Alarmmeldungen an die IT-Sicherheitsabteilung absetzen können. DLP ist sowohl ein altes, als auch neues Thema in der Welt der IT-Sicherheit. Seitdem die Menschheit Informationen und Wissen sammelt wird auch versucht diese vor der unberechtigten Weitergabe zu schützen. Heutzutage erleiden immer mehr Unternehmen Informationssicherheitsverletzungen durch bösartige Insider oder Angreifer von außen. Viel Geld wird verloren durch Diebstahl oder Betrug, der Weitergabe von Unternehmensgeheimnissen, Verlust von personenbezogenen Daten oder durch einen Vertrauens-

oder Imageverlust bei den Kunden – unabhängig von möglichen juristischen Nachwirkungen.

1.1 Aufgabenstellung

Im Rahmen einer Masterarbeit am Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM) soll die Thematik rund um „Data Loss Prevention (DLP)“ sowohl theoretisch als auch praktisch betrachtet werden.

Der theoretische Teil soll unter anderem umfassen:

- Wie arbeiten DLP Systeme?
- Was ist der Unterschied zu Intrusion Detection Systemen?
- Welche Gefahrenkanäle für Informationsdiebstahl können identifiziert werden?
- Ist eine Kategorisierung dieser Gefahrenkanäle möglich?

Als praktischer Teil soll ein nationales oder internationales Sicherheitsframework (z.B.: IT-Grundschutz) ausgewählt und analysiert werden, ob Erweiterungsmöglichkeiten zu Vorgehensweisen und Maßnahmen von Data Loss Prevention gegeben sind.

1.2 Begriffsbestimmungen

1.2.1 Data Loss Prevention/Data Leakage Prevention

Es gibt keine standardisierte oder wissenschaftliche Definition für den Begriff „Data Loss Prevention“. Vielmehr ist es eines von vielen Modewörtern der IT-Sicherheitsindustrie um die Verhinderung von Datendiebstahl in Unternehmen zu adressieren. [Lay07] spricht

von „data leakage prevention, information leak prevention, content monitoring, extrusion prevention systems and privacy compliance systems“, Gartner[OM11] nennt es „Data Loss Prevention“, [WL10] verwendet es als „preventing Data Exfiltration“.

Obwohl die Bezeichnung „Data Leakage Prevention“ eher die Bedeutung trifft, wird in dieser Masterarbeit die Abkürzung „DLP“ für „Data Loss Prevention“ verwendet. Zum einen ist es eine häufige Verwendung in der Literatur, zum anderen verwenden zahlreiche DLP-Software-Hersteller, siehe Unterabschnitt 3.2.2, die Bezeichnung „Data Loss Protection“ für ihre Produkte. Bei weiterer Recherche zu diesem Thema oder bei Produkten ist immer darauf zu achten, was unter der verwendeten Begrifflichkeiten verstanden wird.

1.2.2 Authentisierung und Authentifikation

Im Sprachgebrauch beziehungsweise in der Literatur kommt es immer wieder zu einer vermischten Anwendung der Wörter „authentisieren/Authentisierung“ und „authentifizieren/Authentifikation“. Da in der englischsprachigen Literatur meist nur „to authenticate/authentication“ vorkommt, wird die Übersetzung „authentifizieren/Authentifikation“ verwendet.

Richtigerweise, wenn man die Bedeutungen im Duden nachschlägt, findet man den Unterschied von „authentisieren“ (glaubwürdig, rechtsgültig machen)[1] und „authentifizieren“ (beglaubigen, die Echtheit von etwas bezeugen)[2]. Wie [SSP08] beschreibt, befindet sich eine Person beim *Authentisieren* in einer beweisenden Rolle, macht also gegenüber einem System seine Identität glaubhaft, zum Beispiel mittels eines Passwortes. Dieses System hingegen ist durch das *Authentifizieren* in einer verifizierenden Rolle, überprüft somit die Angaben der sich authentisierenden Person. Nachdem die Authentifikation

[1] `https://www.duden.de/suchen/dudenonline/authentisieren`
[2] `https://www.duden.de/suchen/dudenonline/authentifizieren`

abgeschlossen ist, *autorisiert* das System den Benutzer und erteilt ihm somit die festgelegten Zugriffsrechte auf Informationen und Ressourcen[Wol05].

Eine Person kann sich gegenüber einem System auf verschiedene Arten authentisieren[Mül11]:

- *Authentisierung durch Wissen:* Die wohl häufigst verbreitete Art der Authentisierung erfolgt durch das Vorbringen von Wissen. Bekannte Beispiele sind: Passworteingabe bei einem Login oder die PIN-Eingabe bei Verwendung der Bankomatkarte.

- *Authentisierung durch Besitz:* Bei einer Authentisierung durch Besitz muss der betreffende Benutzer einen physischen Gegenstand vorweisen beziehungsweise Verwenden können. Beispiele sind: Haustürschlüssel, Chipkarten, Token Generatoren oder Ausweise.

- *Authentisierung durch Merkmal:* Hierbei werden körpereigene Merkmale für den Authentisierungsvorgang herangezogen. Beispiele sind: Fingerabdruck, Retina-Scan, Geometriemerkmale oder Stimmmuster.

Diese verschiedenen Arten können beliebig untereinander kombiniert werden. Ein Beispiel für die Kombination von „Besitz“ und „Wissen“ ist die Verwendung einer Bankomatkarte mit PIN an einem Bankomat zur Bargeldbehebung. Je mehr Arten zur Authentisierung verwendet werden, desto aufwendiger wird es für einen potentiellen Angreifer diese Informationen für das System bereit zu stellen und erhöht somit die Sicherheit für die Benutzer[Pog07].

1.3 Informationssicherheit

Information kann auf vielen verschiedenen Möglichkeiten verteilt oder gespeichert werden. Egal ob gesprochen, elektronisch gespeichert und transportiert oder geschrieben auf Papier, sie sollte immer entsprechend geschützt sein[ISOd].

„Informationssicherheit ist der Schutz von Information vor einer Vielzahl an Gefahren, um die Betriebskontinuität, Minimierung des Geschäftsrisikos und der Maximierung der Kapitalrendite und Geschäftschancen sicherzustellen.“[ISOd, Seite viii]

Um dies zu erreichen, gibt es in der Informationssicherheit verschiedene Schutzziele, die für Informationen oder Systeme zu erreichen sind. Die drei wichtigsten Ziele sind *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*. Englischsprachige Literatur führt sie oft als das „CIA triangle“ an, da die entsprechende Übersetzung „confidentiality“, „integrity“ und „availability“ lautet. Im Detail bedeuten sie[Eck11]:

- *Vertraulichkeit (confidentiality):* Die Informationen beziehungsweise Daten dürfen nur von autorisierten Personen oder Programmen verwendet werden, unabhängig davon ob sie gespeichert sind oder gerade übertragen werden.
- *Integrität (integrity):* Ebenso dürfen nur autorisierte Subjekte die Daten oder Informationen verändern.
- *Verfügbarkeit (availability):* Autorisierte Subjekte müssen Zugriff auf die angeforderten Daten oder Informationen bekommen.

Diese Schutzziele wurden im Laufe der Zeit erweitert, um den Ansprüchen der sich laufend wandelnden IT-Industrie gerecht zu werden. Weiters sind wichtig[WM10]:

- *Authentizität (authenticity):* Die Echtheit des entsprechenden Subjekts oder Objekts muss festgestellt werden können.
- *Zurechenbarkeit (accountability):* Jeder Vorgang (z.B.: Log in, Datenübertragung) muss einer Person oder Prozess zugewiesen werden können.
- *Verbindlichkeit (non-repudiation):* Die Verbindlichkeit stellt sicher, dass bei einem getätigten Vorgang fälschungssicher nachgewiesen werden kann, welches Subjekt ihn ausgeführt hat[Gol11].

Bei „Data Loss Prevention“ oder „Data Extrusion“ liegt das Hauptaugenmerk auf dem Schutzziel *Vertraulichkeit*. Unberechtigte sollen nicht an interne Informationen einer Organisation gelangen, weder durch vorsätzliche Handlungen ihrerseits, noch durch Handlungen von autorisierten Personen.

1.4 Aktuelle Bedrohungslage

Die (digitale) Welt befindet sich stets im Wandel. Neue Technologien werden entwickelt, das Internet hält mehr Einzug auf mobile Geräte und in Geschäftsprozesse und immer mehr kriminelle Personen versuchen davon zu profitieren. Jeden Tag werden über 30.000 neue URLs gesichtet, die auf kompromittierte Webseiten verweisen. Dabei handelt es sich aber bei circa 80% um seriöse Internetauftritte, die mit Schadsoftware infiziert wurden[Sop12]. Die ständig vorangetriebene Automatisierung der Schadsoftwareentwicklung hat mittlerweile ein beträchtliches Ausmaß angenommen: es werden jeden einzelnen Tag über 200.000 *neue* Schadsoftware Samples im Internet entdeckt[Wis12].

Trotz jährlich detailliert durchgeführten Untersuchungen von Datendiebstählen (z.B.: [Tru12, Ver12]) lässt sich kein vollständiges Bild der aktuellen Bedrohungslage zeichnen. Diese Ergebnisse sind immer nur ein Spiegelbild der entdeckten und gemeldeten Vorkommnisse. In jedem dieser Berichte wird darauf hingewiesen, dass viele Vorfälle nicht gemeldet oder gar nicht entdeckt werden. Direkte Jahresvergleiche können durch große Einzelereignisse verfälscht werden. Eine genaue Angabe der gestohlenen Datensätze ist oft aus verschiedenen Gründen nicht möglich[Ver12, Seite 58]. Bei Kreditkarteninformationen können nur jene nachgewiesen werden, die auch wirklich missbräuchlich verwendet wurden, unabhängig von der gesamten Anzahl der gestohlenen Daten. Nichts desto trotz bieten diese Berichte interessante und wichtige Einblicke in einen Teilausschnitt des Umfangs der wirklichen Bedrohungslage. Durch die jährliche Analyse von neuen Fällen lassen sich Aussagen über Entwicklungen und Tendenzen ableiten.

Beide Berichte sehen „remote access“ als Einbruchstor Nummer Eins: zwischen 61% [Tru12] und 71% [Ver12]. Die Zugangsdaten sind entweder gestohlen oder bestehen aus einer schwachen Benutzername-Passwort Kombination. In 98% der untersuchten Datendiebstahlsfällen sieht [Ver12] externe Beteiligte und in 4% aller Fälle interne Beteiligte, wobei beide Gruppen gemeinsam auftreten können. Im Bericht wird bereits selbst eingeräumt, dass diese Zahlen die tatsächlich internen Beteiligten wahrscheinlich stark unterrepräsentieren. Zum einen haben vermehrte Aktivitäten von Hacker Gruppierungen 2011 die relativen Anteile verschoben, zum anderen werden Datendiebstähle durch Insider oft nicht entdeckt. Kreditkarteninformationen, Zugangsdaten oder Bankdaten werden bevorzugt von „Externen“ gestohlen und deren Missbrauch schneller entdeckt, als sensible oder geheime Daten über ein Unternehmen, die eher durch Insider gestohlen werden. Seit 2003 zeichnet [DLD] Informationen über Datenverluste auf und weist eine Insiderbeteiligung von 38% aus. 2007 bis 2010 verzeichnet [MGK10] einen starken Anstieg bei Insidervorfällen und [Koc11] nennt Insider als eine der schwierigsten Gefahren heutzutage.

In [Ver12] wurden die verschiedenen Phasen von Datendiebstählen auf ihre zeitliche Dauer analysiert. Folgende vier Phasen werden benannt:

1. *Erstattacke bis Kompromittierung:* Diese Dauer beschreibt die Zeit von der ersten Attacke eine Angreifers bis zur Kompromittierung des Systems. Meist stellt diese Phase den Einbruch ins System dar. Nur wenn der Angreifer noch keinen Zugriff zum System hatte, wird diese Phase berücksichtigt.

2. *Kompromittierung bis Datenextraktion:* In dieser Phase befindet sich der Angreifer bereits im Zielsystem. Die Daten werden gesucht und anschließend zum Angreifer extrahiert.

3. *Kompromittierung bis Entdeckung:* Diese Dauer beschreibt die Zeit, die das angegriffene Unternehmen benötigt, um den Einbruch in ihrem System zu erkennen.

4. *Entdeckung bis Eindämmung/Sanierung:* In dieser Phase reagiert das Opfer des Angriffs nach der Entdeckung des Vorfalls bis zur Eindämmung oder Wiederherstellung des Systems.

Phase Zwei (betrifft den Angreifer) läuft parallel zu Phase Drei und Vier (betrifft das angegriffene Unternehmen) ab. Abbildung 1.1 zeigt die Dauer der einzelnen Phasen bei den untersuchten Datendiebstählen in [Ver12]. Es ist ersichtlich, dass bei einem Großteil der Datendiebstähle nur wenige Stunden zwischen der Erstattacke und der Datenextraktion vergehen. Es muss für die Angreifer also relativ leicht gewesen sein in das System einzudringen und die Daten zu stehlen. Bei circa 40% der Fälle vergehen aber Tage bis Monate, bis die Daten extrahiert werden können.

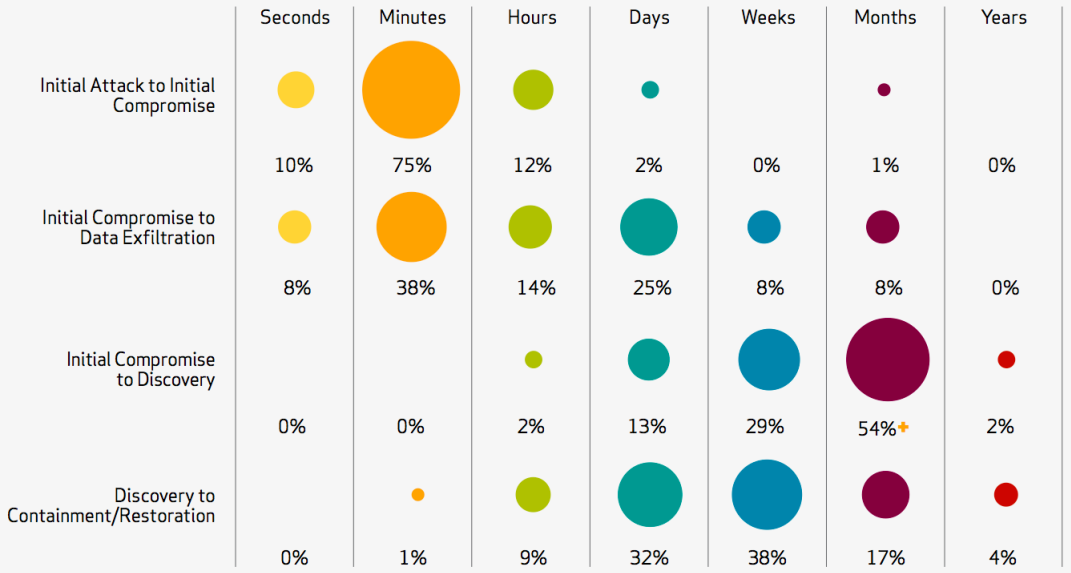


Abbildung 1.1: Zeitspannen bei Vorfällen [Ver12]

Ein Blick auf die dritte Phase *Kompromittierung bis Entdeckung* zeigt deutlich, dass die Unternehmen erst viel zu spät auf den Einbruch beziehungsweise Datendiebstahl aufmerksam werden. In nur 15% der Fälle wird der Einbruch innerhalb von Tagen erkannt, mehr als die Hälfte bemerkt es erst nach Monaten. Dieser Tatsache sollte entgegen gewirkt werden, indem die Unternehmen *Intrusion Detection Systeme* und *Data Loss Prevention Systeme* zum Einsatz bringen. Dieser Punkt bekommt durch [Ver12] noch

mehr Gewicht, da in 92% aller Fälle das Unternehmen nicht selbst auf den Diebstahl aufmerksam wird, sondern erst durch Dritte (Kunden, bei Ermittlungsverfahren, usw.) erfahren. Zu ähnlich bedenklich hohen Zahlen kommt auch [Tru12]: 84% der Vorfälle werden nicht durch das Unternehmen selbst entdeckt.

1.5 Bedrohung von innen - Insider

Wie zuvor bereits erwähnt wurde, zählen „Insider“ zu einer der herausforderndsten Bedrohungen und kommen bei bis zu einem Drittel aller Datendiebstähle vor. Sie haben Zugang zu verschiedenen internen Ressourcen, besitzen möglicherweise Zugriffs- oder Zutrittsberechtigungen für sensible Bereiche und verfügen über ein umfangreiches Wissen über die interne Struktur des Unternehmens. In vielen Fällen wissen sie auch über die eingesetzten Sicherheitsmaßnahmen Bescheid und können sie somit leichter umgehen.

1.5.1 Definition Insider

Das *Computer Emergency Response Team (CERT)* des Software Engineering Institutes der Carnegie Mellon Universität definiert einen Insider folgendermaßen[CMTS09]:

> *Ein derzeitiger oder vormaliger Mitarbeiter, Auftragnehmer oder Geschäftspartner, der*
>
> - *autorisierten Zugang zu Netzwerk, System oder Daten eines Unternehmens hat oder hatte und*
> - *diesen Zugang absichtlich überschreitet oder missbräuchlich verwendet und damit die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen des Unternehmens oder dessen Informationssysteme negativ beeinflusst.*

Als wichtigster Abgrenzungspunkt zum Angreifer von außen ist der *autorisierte* Zugang zu sehen. Durch ein (ehemaliges) Vertragsverhältnis gewinnt der Insider wertvolle Informationen über die vorhandenen Sicherheitsprozesse in einem Unternehmen und kann die eingesetzten Sicherheitsmaßnahmen leichter umgehen[CMTS09]. Oftmals wird das interne Netzwerk eines Unternehmens als vertrauenswürdiger Bereich angesehen, deshalb sind die Schutzmaßnahmen geringer ausgeprägt als bei der Schnittstelle nach außen. Eine größere Bandbreite an Handlungsmöglichkeiten eröffnen sich dem Insider auch dadurch, dass physischer Zugang zu Netzwerkkomponenten oder Arbeitsplätzen möglich ist[BG11].

Salem, Hershkop und Stolfo [SHS08] gehen noch weiter als das CERT: wenn ein Angriff von außen mit gestohlenen Zugangsdaten durchgeführt wird, also der unautorisierte Dritte nun einen autorisierten Zugriff hat, zählen sie diesen Angriff auch zu Insiderangriffen.

In dieser Masterarbeit wird der Begriff des *Insiders* nach der Definition des CERTs verwendet, da die Maßnahmen immer auf die Ursache, in diesem Fall eine Person innerhalb des Unternehmens mit kriminellen Absichten, abzielen müssen. Abschreckende Richtlinien oder Beweissicherungsverfahren zur Vermeidung von Insiderangriffen schützen nicht vor Passwortdiebstahl.

1.5.2 Klassifikation von bösartigen Insideraktivitäten

In den USA wurden von [CMTS09] 190 aufgeklärte Insidervorfälle einer Analyse und Klassifikation unterzogen. Ein Großteil dieser Fälle (ca. 88%) kann mit einer oder zwei der folgenden Kategorien klassifiziert werden:

1. *IT Sabotage:* Fälle in denen Insider ihre Zugriffsberechtigungen missbraucht haben, um einzelnen Personen, dem gesamten Unternehmen oder den täglichen Geschäftsbereichen zu schaden. Die Angriffe richten sich gegen Daten, Netzwerke

oder Systeme durch Personen, die hauptsächlich in höheren technischen Positionen angestellt waren. Die Hauptmotivation zur Durchführung war Rachegelüste wegen Verärgerung.

2. *Diebstahl oder Modifizierung für finanzielle Bereicherung:* Fälle in denen Insider ihre Zugriffsberechtigungen missbraucht haben, um durch Diebstahl oder Modifizierung von Daten oder Informationen persönliche finanzielle Bereicherung zu erlangen. Als Angreifer wurden Personen identifiziert, die hauptsächlich im nichttechnischen Positionen tätig waren und ihre Zugriffsberechtigungen genutzt haben um Kundeninformationen oder sensible Daten an Dritte weiter zu verkaufen.

3. *Diebstahl oder Modifizierung für Geschäftsvorteile:* Fälle in denen Insider ihre Zugriffsberechtigungen missbraucht haben, um mit gestohlenen Daten oder Informationen zukünftig Geschäftsvorteile erlangen zu können. Auch hier geht es in den meisten Fällen um eine finanzielle Bereicherung, allerdings werden diese Informationen nicht verkauft, um damit einmalig und kurzfristig zu Geld zu gelangen, sondern es soll ein längerfristiger Vorteil verschafft werden. Häufig werden diese Informationen genutzt, um eine neue Arbeitsstelle zu bekommen, diese in einer neuen Arbeitsstelle zu verwenden oder ein Konkurrenzunternehmen zu gründen.

Besonders auffällig ist, dass 95% aller Insider mit Motivation „Geschäftsvorteile“ vor oder nach dem Diebstahl gekündigt haben. Allgemein stellt [CER] fest, dass 70% aller Diebstähle innerhalb von 30 Tagen nach der Kündigung durch die Mitarbeiter erfolgen. Unternehmen sollten eigene Prozesse entwerfen, die die Mitarbeiter in ihrer letzten Phase im Unternehmen stärker überwachen, beziehungsweise die Aktivitäten rund um den Kündigungszeitpunkt genauer analysieren, um mögliche Manipulationen oder Diebstähle frühzeitig zu erkennen[HDS+11].

Muster anhand betrügerischer Absichten

Betrug durch Insider kann schwere finanzielle Schäden für Unternehmen bedeuten. Für den Finanzsektor zeigt eine Studie, dass Banken bis zu vier Prozent ihres Gesamtertrages durch Insiderbetrug verlieren[Hig09].

Wie Abbildung 1.2 zeigt, hat das CERT, basierend auf dem *Fraud Triangle* von Donald R. Cressey [Cre73], ein Modell entwickelt, um die psychologischen Abläufe bei einem Betrug darzustellen. Die drei Grundpfeiler[Nim09] sind:

- *Gelegenheit:* Es muss sich für den Betrug eine Gelegenheit bieten, das bedingt zwei Punkte: die technische Machbarkeit im System und die eigene Fähigkeit es durchzuführen. Diese Punkte stehen in starkem Zusammenhang mit den eingesetzten Sicherheitsmechanismen und ihren Schwächen.

- *Motivation:* Wird auch „Anreiz“ oder „Druck“ genannt. Die handelnde Person benötigt einen persönlichen Grund, um die Tat durchzuführen, z.B.: Gier, finanzieller Notstand, ...

- *Rechtfertigung:* Im Vorfeld der Tat legt sich der Täter einen Grund zurecht, der die anstehende Tat für sich selbst als berechtigt erscheinen lässt.

Das propagierte Modell enthält vier Rückkopplungsschleifen unterschiedlicher Typen: eine Ausgleichsschleife *(„B“ – balancing loop)* und drei Verstärkungsschleifen *(„R“ - reinforcing loops)*. Das Ziel der Ausgleichsschleife „B1“ ist es, entsprechende Handlungen zu setzen, um eine Variable einem bestimmten Wert zuzuführen. Meist wird damit versucht finanzielle Probleme auszugleichen. Im Gegensatz dazu streben die Verstärkungsschleifen „R1“, „R2“ und „R3“ nach einem stetig höheren oder niedrigeren Wert einer Variable. Getrieben durch die eigene Gier oder durch Druck von Außenstehenden wird der Prozess neu begonnen und das Risiko einer erneuten rechtswidrigen Tat erhöht sich[CER].

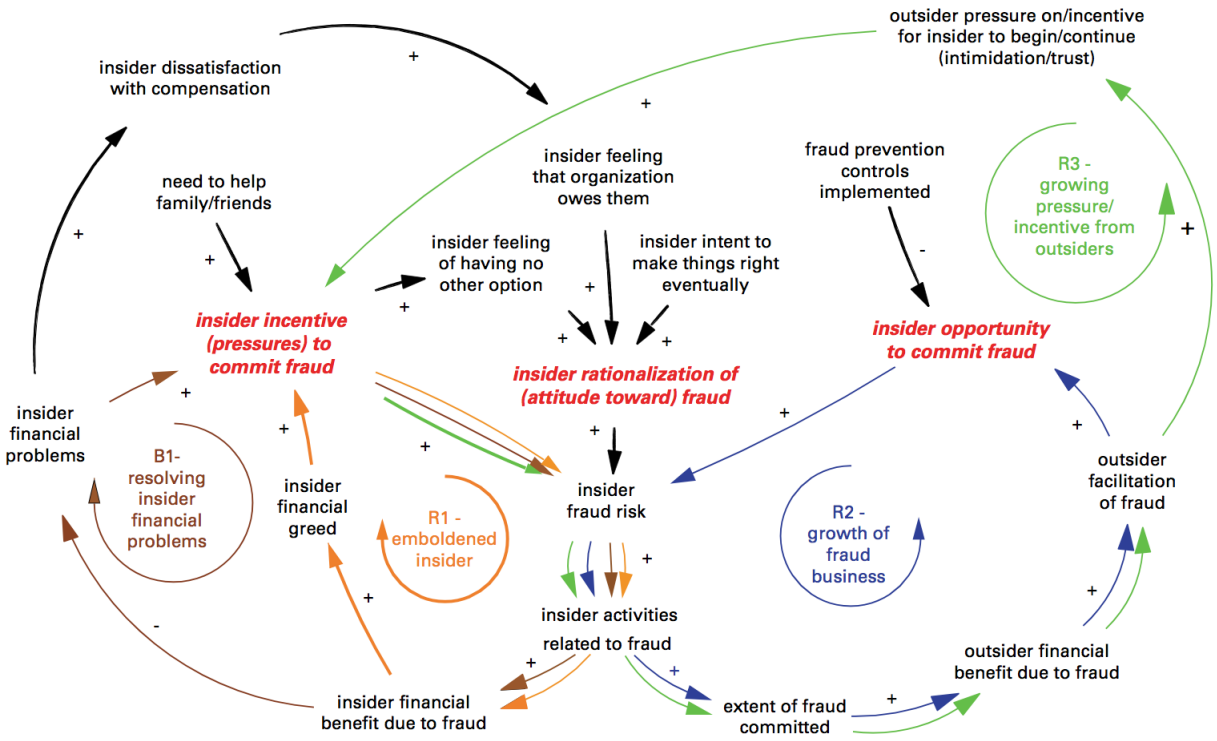


Abbildung 1.2: Muster von Insider-Betrügen [CER]

Wie [Jon08] ausführt, ist die Identifikation mit dem Unternehmen und die damit verbundene Loyalität ein wichtiger Faktor. Der soziale Wandel der letzten Jahrzehnte brachte mit sich, dass Personen oft nicht mehr ein Leben lang im selben Unternehmen tätig sind und auch von Anfang an damit kalkulieren den Arbeitgeber wieder zu wechseln. Konsequenzen daraus sind nicht nur weniger Loyalität und Identifikation mit dem Unternehmen, sondern auch ein Anstieg der Fluktuation der Mitarbeiter. Beides erhöht das Risiko von Betrug oder Informationsdiebstahl.

Aus Abbildung 1.2 ist erkennbar, dass „fraud prevention controls implemented“ den einzigen externen Faktor darstellt, der zu einer Verringerung des Betrugsrisikos durch Reduktion der *Gelegenheit* führt. Das kann sowohl durch organisatorische als auch technische Maßnahmen erzielt werden. Der Einsatz von DLP-Systemen kann abschreckend wirken und die tatsächliche Durchführung erschweren, zusätzlich sollten aber Richtlinien erlassen und auch überprüft werden. „Beweissicherung“ sollte, wie in [SIH10, Seite

467] beschrieben, eine Sicherheitsanforderung an das System sein. Die Benutzer müssen sich im Klaren sein, dass ihre Aktivitäten beim Auftreten von Sicherheitsvorfällen zurückverfolgt und zugeordnet werden können.

1.6 Kosten von Vorfällen

Die tatsächlichen Kosten von Datenlücken lassen sich nur schwer beziffern. Einerseits ist der Schaden davon abhängig, welche Art von Daten betroffen sind (Kreditkarteninformationen, sensible personenbezogene Daten, Baupläne, Strategiedokumente, usw.), auf der anderen Seiten kann nur geschätzt werden, wie viel Schaden durch Imageverlust oder neue Konkurrenzprodukte entsteht. Viele Unternehmen versuchen diese Vorfälle geheim zu halten, da sie um ihre Reputation am Markt fürchten.

1.6.1 Kosten im weltweiten Trend

Im Jahr 2007 wurden die Kosten pro betroffener Person bei einem Datenleck mit $150 bis $200 angegeben[Lay07]. Diese Aussage deckt sich mit den Zahlen mehrerer Studien [Pon10, Pon12a, Pon12b, Pon12c, Pon12d] durch das Ponemon Institute LLC[3] in den Vereinigten Staaten von Amerika, Deutschland, Frankreich, Australien und dem Vereinigten Königreich von Großbritannien und Nordirland. Wie Abbildung 1.3 zeigt, sind steigende pro Kopf Kosten Trend der letzten Jahre. Einzig in den USA sind diese Kosten erstmals im Vergleich zum Vorjahr gesunken. Als Grund dafür sieht [Pon12d], dass in 45 Bundesstaaten neue Gesetze eingeführt wurden, die die Unternehmen verpflichten die Kunden zu informieren wenn die Daten gestohlen werden. Dadurch würden die Unternehmen sich besser vorbereiten und die Gefahr ernst nehmen, damit sie keine Strafen zahlen müssen oder das Image des Unternehmens nicht gefährdet wird.

[3] `http://www.ponemon.org/`

Der Trend der Gesamtkosten eines Vorfalls ist nicht gleich jenem der pro Kopf Kosten. Ersichtlich ist aus Abbildung 1.4, dass die Gesamtkosten nicht im gleichen Maße ansteigen, sondern im Gegenteil, bis auf Ausnahme von Frankreich, sinken oder zumindest annähernd gleich bleiben. Das Ponemon Institute führt das darauf zurück, dass die Unternehmen besser auf Vorfälle reagieren, die Loyalität der Kunden besser aufrecht erhalten werden kann und dass insgesamt weniger Datensätze gestohlen wurden.

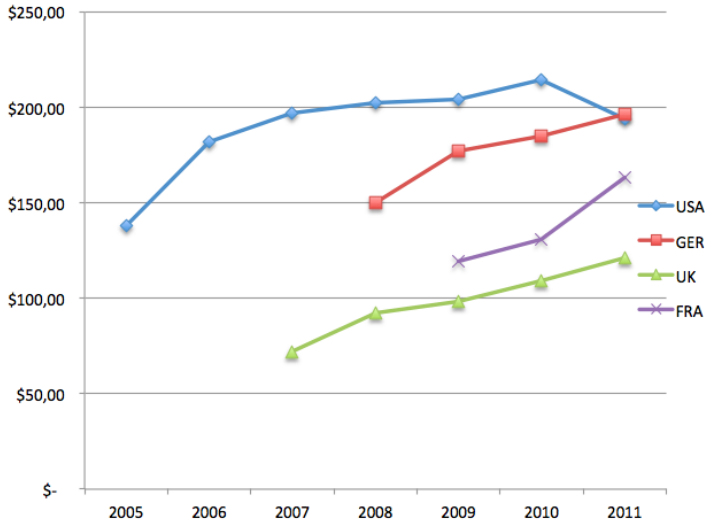


Abbildung 1.3: Trend der Kosten pro Kopf bei einem Datenverlust

Anmerkung zur Abbildung 1.3 und Abbildung 1.4: In den Einzelberichten der jeweiligen Länder [Pon12a, Pon12b, Pon12c, Pon12d] sind die Werte in der jeweiligen Landeswährung (Euro, Pfund Sterling und US-Dollar) angegeben. Um eine einheitliche Währung darstellen zu können, wurde als fixer Umrechnungsfaktor jener zum Zeitpunkt von [Pon10] verwendet. Das Diagramm soll hauptsächlich den gemeinsam Trend und nicht die exakten Kosten pro Kopf Werte darstellen.

1.6.2 Kosten von gestohlenen Laptops

Geheime oder sensible Daten von Unternehmen werden heutzutage durch immer mobiler werdende Mitarbeiter der Gefahr des Diebstahls ausgesetzt. Aus diesem Grund hat

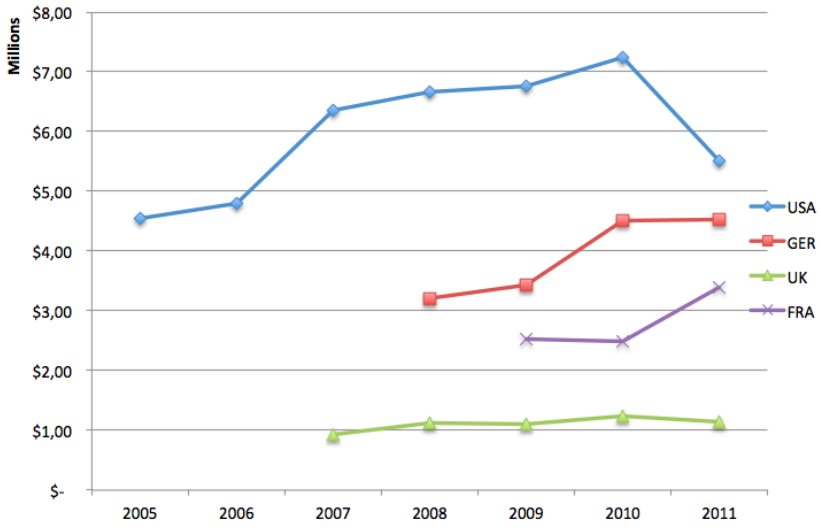


Abbildung 1.4: Trend der Gesamtkosten bei einem Datenverlust

das Ponemon Institute 2009 eine Studie [Pon09] erstellt, um Aussagen zu Kosten und Kostentrends bei verlorenen oder gestohlenen Laptops tätigen zu können.

Laut dieser Studie betragen die mittleren Kosten für einen abgängigen Laptop $49.246. 2002 wurde bereits ein Kostenpunkt von $89.000 in [Jon08] angegeben. Trotz den unterschiedliche Zahlen steht diese Aussage aber nicht im Widerspruch zu [Pon09], denn darin wird gezeigt, dass die Kosten sehr stark von folgenden Faktoren beeinflusst werden: Entdeckungszeitpunkt des Verlustes, organisatorische Position des Mitarbeiters, Vorhandensein von Backups, Einsatz von Verschlüsselung und Branche des Unternehmens. Je nach Ausprägung der Faktoren sind Zahlen wie in [Jon08] genannt ebenso möglich.

Drei wichtige Aussagen der Studie sind:

- *Verschlüsselung:* Werden die Daten auf dem Laptop verschlüsselt gespeichert, sinken die Kosten des Verlustes um ein Drittel. Im Durchschnitt bedeutet das crica $19.000 weniger Schaden pro Fall.
- *Backup:* Entgegen einer ersten ad hoc Annahme verhalten sich die Kosten bei Einsatz eines Sicherungssystemes umgekehrt proportional. Wird ein Backupsystem

eingesetzt, steigen die Kosten des Vorfalls von circa $39.000 auf $70.000. Dieser nicht intuitive Anstieg kann damit begründet werden, dass bei einer vorhanden Sicherung tatsächlich bestimmt werden, kann welche und wie viele vertrauliche Daten verloren gegangen sind. Es zeigt auch, dass bei ungenauer Kenntnis des Verlustes die Kosten von Unternehmen offensichtlich unterschätzt werden.

- *Entdeckungszeitpunkt:* Je früher ein Unternehmen den Verlust bemerkt, desto geringer ist der Schaden. Ist er bei Entdeckung am selben Tag relativ gering mit $9.000, steigt er innerhalb einer Woche um 1288% auf $116.000 an.

1.7 Klassifikation von Informationen

Um Informationen differenziert schützen zu können, ist eine Klassifikation dieser sinnvoll oder teilweise gesetzlich vorgeschrieben. Im Bereich der Dienststellen des Bundes der Republik Österreich wird eine Klassifizierung von Informationen durch §2 InfoSiG (Informationssicherheitsgesetz)[4] vorgegeben: „EINGESCHRÄNKT“, „VERTRAULICH“, „GEHEIM“ und „STRENG GEHEIM“. Für Organisationen im privatwirtschaftlichen Bereich ist diese Klassifikation nicht verbindlich. Das Österreichische Informationssicherheitshandbuch [SIH10] empfiehlt aber auch hier eine adäquate Klassifizierung der internen Informationen. Weiters sollten interne Regelungen getroffen werden wer wie auf welche Informationen Zugriff hat beziehungsweise wie mit klassifizierter Information umzugehen ist.

Werden personenbezogene Daten verarbeitet, gelten sowohl für den öffentlichen als auch privatwirtschaftlichen Bereich zusätzliche Bestimmungen. Entsprechend dem DSG 2000 (Datenschutzgesetz)[5] müssen diese Daten folgendermaßen klassifiziert werden:

[4] `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001740`

[5] `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597`

- *NUR INDIREKT PERSONENBEZOGEN:* Die Identität der jeweiligen Person ist mit rechtlich erlaubten Mitteln nicht feststellbar.
- *PERSONENBEZOGEN:* Durch die vorhandenen Daten wird die Identität der jeweiligen Person bestimmbar oder ist bereits bestimmt.
- *SENSIBEL:* Diese Daten werden im DSG 2000 als „besonders schutzwürdige Daten“ bezeichnet und sind „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben“.

1.8 Passwortsicherheit

Die teuersten und besten IT-Sicherheitsmaßnahmen sind de facto wirkungslos, wenn ein Angreifer ein leicht zu erratendes Administrator-Passwort knacken kann und sich somit „legalen“ Zugriff zum System verschafft. In den Berichten aus 2012 schreiben [Tru12] und [Ver12] noch immer davon, dass es große Mängel bei der richtigen Wahl von Passwörtern gibt. Bei über 2000 durchgeführten Penetration-Tests war das Netzwerkrisiko Nummer Eins ein schwaches oder überhaupt nicht gesetztes Passwort für Administrator-Accounts[Tru12].

Untersuchungen durch SpiderLabs von IT-Sicherheitsvorfällen haben ergeben, dass 90% der Angriffe erfolgreich waren, weil die Standardpasswörter der Hersteller oder andere leicht zu erratende Benutzername-Passwortkombinationen verwendet wurden, wie „temp:temp“ oder „admin:nimda“[Per10]. Andere häufig auftretende Kombinationen sind auch „administrator:password“, „guest:guest“ oder „admin:admin“. Das am häufigsten gefundene Passwort ist aber „Password1“, da es auch den Komplexitätsanforderungen von Microsoft Active Directory entspricht[Tru12].

Folgende Punkte[Eck11] sollten für eine sichere Passwortauswahl beachtet werden:

- Die Passwortlänge sollte mindestens acht Zeichen betragen, je länger es ist, desto aufwändiger wird es für Angreifer alle möglichen Kombinationen durch zu probieren
- Es sollte mindestens eine Ziffer sowie ein Sonderzeichen beinhalten
- Es soll nicht aus einem Wort bestehen, das in Wörterbüchern nachgeschlagen werden kann
- Die regelmäßige Änderung ist empfohlen
- Es soll für den Benutzer einfach zu merken sein

Der letzte Punkt ist von erheblicher Wichtigkeit. Kann sich der Benutzer das Passwort nicht gut merken, steigt die Wahrscheinlichkeit für Notizen und im schlimmsten Fall werden diese an dem Monitor angebracht[Bau09]. Eine einfache Möglichkeit, um lange, sichere und merkbare Passwörter zu erstellen, ist die Verwendung von Passwort-Sätzen[Pog07]. Dabei besteht das Passwort entweder selbst aus einem ganzen Satz, zum Beispiel: „DieSicherheitVonPasswörternIstWichtig“, oder es setzt sich aus den n-ten Buchstaben der Wörter eines Satzes zusammen, zum Beispiel: „Der Geburtstag meiner Tochter ist am dritten Juli, es war ein Montag“. Verwendet man den ersten Buchstaben der Wörter und dazu Zahlen und Sonderzeichen, erhält man ein sicheres Passwort: „`DGmTia3J,eweM`“. Bei einer Passwortänderung könnte man auf die zweiten Buchstaben wechseln: „`eeeosm3u,saio`“.

Kapitel 2

Intrusion Detection

Bereits seit 1980 beschäftigt man sich mit dem Analysieren und Vergleichen des Verhaltens eines Systems mit gesammelten Daten und Erfahrungen[And80]. In den späten 1980er Jahren veröffentlichte Dorothy E. Denning ein erstes Modell[Den87] für ein Echtzeit *Intrusion Detection System* genannt IDES (Intrusion Detection Expert System). Es basiert auf der Annahme, dass abnormales Systemverhalten, ausgelöst durch das Ausnützen von Schwachstellen, erkannt werden kann.

Bisher sind *Intrusion Detection* und *Data Loss Prevention* meist getrennt voneinander betrachtet und angewandt worden. Intrusion Detection kann aber als ein Teil von Data Loss Prevention gesehen werden und es ist sinnvoll, hier ein einheitliches und strukturiertes Vorgehen anzuwenden. Hauptsächlich wird versucht mit Hilfe von Intrusion Detection Systemen (IDS) Angriffe auf das Netzwerk der Organisationen von außen zu erkennen beziehungsweise mit Intrusion Prevention Systemen (IPS) zu verhindern. Im Idealfall erkennt und verhindert ein IDS/IPS auch Angriffe, die innerhalb des Netzwerkes durchgeführt werden (z.B.: durch Insider). Gelingt es dem Angreifer nicht Zugriff auf das Netzwerk beziehungsweise Daten zu bekommen, können diese auch nicht kopiert, verändert oder gelöscht werden. Je früher der Angriff abgewehrt werden kann, desto geringer ist das Risiko möglicher Schäden oder Verluste für das Unternehmen.

2.1 Klassifikation von Alarm-Events

Sowohl Intrusion Detection Systeme als auch Data Loss Prevention Systeme versuchen den vorhandenen Datenverkehr im Netzwerk zu interpretieren, um erlaubte Kommunikation zuzulassen und unerlaubte zu erkennen und gegebenenfalls Maßnahmen einzuleiten. Da die Systeme auf die Erkennung von unerlaubter Kommunikation ausgelegt sind, wird ein solcher Datenstrom als *positive* bezeichnet, die erlaubte Kommunikation als *negative*. Sie können diese Entscheidung fälschlicherweise (*false*) oder richtigerweise (*true*) treffen. Daraus resultieren vier mögliche Klassifikationen: *True Positive (TP)*, *True Negative (TN)*, *False Positive (FP)* und *False Negative (FN)*[GLT10]. Wie in Tabelle 2.1 zu sehen ist, kommt es zu Problemen, wenn ein System falsch entscheidet. Bei *FN* werden unerlaubte Datenflüssen als legitim klassifiziert und somit vom System nicht weiter beachtet. Im Falle eines IDS könnte so der Angreifer ungehindert in das Netzwerk einbrechen oder bei DLP-Systemen die schützenswerte Information erfolgreich aus dem Netzwerk transportierten. Bei *FP* werden legitimierte Datenflüsse als „unerlaubt“ interpretiert. Je nach Konfiguration des Systems wird diese Kommunikation geblockt und es kann ein Alarm ausgelöst werden. Wie [Lay07, Cal11, SER12] schreiben, ist eine hohe *False Positive* Rate sehr schlecht. Jeder Alarm muss durch Menschen überprüft und bestätigt werden. Bei einer Vielzahl an falschen Alarmmeldungen können gerechtfertigte Alarmmeldungen leicht übersehen werden oder die Sicherheitsverantwortlichen beginnen die Meldungen gänzlich zu ignorieren.

	Tatsächliche Kommunikation	Vorhergesagte Kommunikation
True Positive	Unerlaubt	Unerlaubt
False Positive	Erlaubt	Unerlaubt
True Negative	Erlaubt	Erlaubt
False Negative	Unerlaubt	Erlaubt

Tabelle 2.1: Alarm-Event-Klassifikation durch IDS [GLT10]

2.2 Klassifikation von Intrusion Detection Systemen

Eine grobe Klassifizierung von Intrusion Detection Systemen kann nach zwei verschiedenen Gesichtspunkten erfolgen[Koc11]: *Erkennungstechnik* und *Einsatzgebiet im Netzwerk.*

Bei der *Erkennungstechnik* unterscheidet man wiederum zwei Kategorien [Man04]:

- *Musterbasierte Systeme (signature/pattern based):* Diese Systeme verwenden zur Erkennung von Angriffsmustern oder Schadcode vorgefertigte Signaturen. Dadurch werden bekannte Angriffe verlässlicher und ressourceneffizienter als bei verhaltensbasierten Systemen erkannt. Es genügt ein einfacher Vergleich der auftretenden Signatur mit den gespeicherten Signaturen in einer Datenbank, um zu bestimmen ob ein Angriff stattfindet oder Schadcode transportiert wird. Nachteil dieser Systeme ist die fehlende Flexibilität. Verändert der Angreifer das Angriffsmuster oder den Schadcode, entspricht es nicht mehr den gespeicherten Signaturen und wird folglich nicht erkannt. Musterbasierte Systeme müssen durch ständige Aktualisierung der Signaturdatenbank auf den neuesten Stand gebracht werden, um neu auftretende Bedrohungen erkennen zu können.

- *Verhaltensbasierte Systeme (behaviour/anomaly based):* Diese Systeme verwenden zur Erkennung von Angriffsmustern eine Analyse des Systemverhaltens. Zu Beginn muss das „normale“ Verhalten des Systems bestimmt oder gelernt werden, um es später mit dem aktuellen Verhalten vergleichen zu können. Abweichende Events werden als Alarm gemeldet. Diese Technik ermöglicht es im Gegensatz zu musterbasierten Systemen auch neue und unbekannte Angriffe erkennen zu können. Dieser Gewinn wir durch komplexere Verfahren, wie z.B.: *machine learning* Techniken, mit höherer Ressourcenbelastung erzielt. Ein großes Problem stellt die *false positive* Rate dieser Systeme dar, da nicht jedes abweichende Systemverhalten automatisch einen Angriff darstellt. Ebenso ist die Trainingsphase des Systems sehr kritisch. Befindet sich bereits ein Angreifer oder Schadsoftware im Netzwerk,

lernt das Intrusion Detection System dieses Verhalten als „gut“ beziehungsweise „normal“ und wird in Zukunft keinen Alarm auslösen.

Moderne Systeme arbeiten nicht exklusiv mit nur einer Technik, sie können als *hybride Systeme* beide Techniken kombinieren, um Einbrüche ins Netzwerk möglichst gut zu erkennen. Durch Signaturerkennung sollen bekannte Angriffe schnell und treffsicher erkannt werden, die verhaltensbasierte Erkennung soll unbekannte Angriffe im Netzwerk finden. Ebenso können verschiedene verhaltens- oder musterbasierende Systeme kombiniert werden. Ziel ist es immer, die *false positive* Rate möglichst gering zu halten[GLT10].

Intrusion Detection Systeme können auch nach ihrem *Einsatzgebiet im Netzwerk* unterteilt werden:

- *Netzwerk-basierte Systeme:* Sehr häufig werden Netzwerk-basierte Intrusion Detection Systeme (NIDS) als eine zentrale Überwachungseinheit in einem Netzwerk eingesetzt. Somit stehen alle Informationen sofort zur Verfügung und es muss nicht, wie bei einem dezentralisierten Ansatz, mit verschiedenen verteilten Agenten im Netzwerk kommuniziert werden. Allerdings erfordert der Einsatz eines zentralen IDS eine hohes Maß an Rechenleistung für den nötigen Durchsatz bei hohem Traffic. Ist dieser Durchsatz nicht gewährleistet, kann es zu signifikanten Verzögerungen kommen. Der dezentrale Ansatz bietet den Vorteil die Rechenlast besser zu verteilen und bei entsprechender Verteilung auch Insider-Angriffe in Subnetzen zu erkennen[GLT10]. Eine essentielle Entscheidung beim Einsatz eines IDS ist die strategische Platzierung im Netzwerk. Dadurch wird festgelegt welche Teile des Netzwerkes beobachtet werden und welche nicht[Kap07]. Im Gegensatz zu Host-basierten Systemen können NIDS unbemerkt im Hintergrund arbeiten *(stealth mode)* und verteilte Attacken im Netzwerk erkennen[Lüs08].

- *Host-basierte Systeme:* So genannte Host-based Intrusion Detection Systeme (HIDS) werden direkt auf den Endgeräten (Server, Arbeitsplatz, ...) installiert und über-

wachen nur die jeweilige Maschine. Zur Analyse verwenden HIDS zwei verschiedene Informationsquellen: *audit logs* und *system calls*. Meist kommen verhaltensbasierte Systeme zum Einsatz, die Aufzeichnungen der Prozesse und Systemstatistiken, sowie Befehlsaufrufe im Betriebssystem, auf Unregelmäßigkeiten untersuchen. Diese gesammelten Informationen bergen aber auch ein Sicherheitsrisiko in sich, da potentielle Angreifer in den *audit logs* schnell zu relevanten Informationen über den Zielrechner kommen. Verschiedene Betriebssysteme (beziehungsweise Versionen), unterschiedliche Arbeitsplatzkonfigurationen und Softwarepakete erschweren den Einsatz und die Konfiguration von Host-based Intrusion Detection Systeme[GLT10]. Ein klarer Vorteil gegenüber den Netzwerk-basierten Systemen ist die Möglichkeit Attacken zu erkennen ,bevor sie verschlüsselt und übertragen werden. Wird Schadcode oder Informationen für eine Attacke verschlüsselt übertragen, hat ein NIDS keine Möglichkeit mehr den Inhalt zu analysieren und einen Alarm auszulösen[Lüs08].

Early Warning Systems – EWS

Ein *Early Warning System (EWS)* arbeitet im Gegensatz zu IDS nicht in lokalen Netzwerken, sondern verbindet Standorte oder Unternehmen über das Internet. Hauptaufgabe ist es, automatisierte ungerichtete Angriffe in Teilnetzwerken zu erkennen und die noch nicht betroffenen Netzwerke zu warnen und mit Informationen zu versorgen[Koc11]. Durch die Zusammenführung möglichst vieler Quellen lässt sich ein weltumspannendes Frühwarnsystem erstellen, um besser gegen global ausbreitende Virusinfektionen oder groß angelegten DoS-Attacken geschützt zu sein.

Choffnes und Bustamente [CB09] entwickelten das Plugin „NEWS“ (Network Early Warning System)[1] für den BitTorrent Client Vuze[2] (vormals: Azureus), um durch die

[1] `http://www.aqualab.cs.northwestern.edu/projects/123-news-reusing-p2p-for-early-detection-of-network-problems`

[2] `http://www.vuze.com`

verteilten Clients Echtzeitdaten über die Netzwerkperformance zu bekommen und damit Service Provider schneller Probleme erkennen lassen zu können. Nach diesem Prinzip könnten große Unternehmen Informationen verteilter Sensoren oder Netzwerkendpunktgeräte nutzen, um anderen Teilnetze vor der Durchdringung von Angriffen oder Schadsoftware zu schützen.

Beispiele für EWS sind das frei verfügbare *Internet Storm Center (ISC)*[3] des SANS Instituts oder das kommerzielle Angebot *Arbor Networks Active Threat Level Analysis System (ATLAS)*[4].

2.3 Mängel und Herausforderungen aktueller Systeme

Intrusion Detection Systeme haben ein komplexes Aufgabengebiet und ihr Erfolg wird von vielen Faktoren bestimmt. Je nach Typ des IDS sind dieselben Faktoren mehr oder weniger einflussreich beziehungsweise problematisch. Tabelle 2.2 zeigt eine Gegenüberstellung verschiedener Faktoren für unterschiedliche IDS Typen. Treten bei aktuellen Systemen Mängel in einem Bereich auf, sind sie mit $\times$ gekennzeichnet. Ein $\surd$ bedeutet, dass dieser Faktor unkritisch ist. Bei ($\surd$) kann der Einflussfaktor nur bedingt angewandt werden.

Die drei erste Faktoren *Konfiguration*, *Zero Day Attacken* und *Signatur Verzögerung* sind stark miteinander verbunden. Zu viele *false positive* Meldungen des IDS führen es ad absurdum. Die sicherheitsverantwortlichen Personen werden mit der Überprüfung der einzelnen Meldungen überfordert, was zur Folge hat, dass die Warnungen des Intrusion Detection Systems ignoriert werden und einem tatsächlichem Angriff nichts entgegengesetzt wird. Daher ist es unabdingbar das signaturbasierte System genau auf die Services und Hosts des Netzwerkes abzustimmen. Meist stellt dies für die Verantwortlichen eine aufwändige Aufgabe dar, die sic, bei größeren Netzwerken aufgrund

[3] `https://isc.sans.edu`

[4] `http://atlas.arbor.net/`

	Musterbasiert		Verhaltensbasiert	
	Host	Netzwerk	Host	Netzwerk
Konfiguration	×	×	√	√
Zero Day Attacken	×	×	√	√
Signatur Verzögerung	×	×	√	√
Bandbreite	×	×	√	(√)
Datenbankgröße	×	×	√	√
Anwendungsschicht	(√)	(√)	(√)	×
Verschlüsselte Kommunikation	√	×	√	(√)

Tabelle 2.2: Mängel und Herausforderungen in aktuellen IDS [Koc11]

der vielen Einzelkomponenten kaum bewerkstelligen lässt. Teil der Konfiguration und Wartung eines IDS ist die Bereitstellung neuer Signaturen, um Angriffe zu erkennen. Unregelmäßige oder nicht zeitnahe Veröffentlichungen von neuen Signaturen setzt das Netzwerk den neuen Gefahren aus. Sogenannte *Zero Day Attacken* bedeuten, dass Schwachstellen ausgenützt werden, die erst am selben Tag veröffentlicht worden sind. Für Signaturhersteller ist es unmöglich für diese Attacken rechtzeitig die entsprechenden Signaturen bereitzustellen[Koc11].

Wie in [Koc11] weiters ausgeführt wird, stellen die immer größer werdenden Übertragungsgeschwindigkeiten der Netzwerke die IDS vor neue Herausforderungen. Signaturbasierte Systeme müssen den Inhalt der Datenpakete mit ihren Signaturdatenbanken vergleichen, um einen Angriff erkennen zu können. Durch diese *Deep Packet Inspection (DPI)* kommt es zu hohem Rechenaufwand des IDS und somit zu einer Verschlechterung der Performanz des Netzwerkes durch Verzögerungen. Das weitverbreitete Open Sorce IDS *Snort* (siehe Abschnitt 2.4) verwendet laut Proutfoot et al. [PKAC07] 30-60% der Prozesszeit für das Vergleichen von Signaturen. Innerhalb von 8 Jahren bis 2011 ist die Signaturdatenbank von Snort um über 600% auf knapp 10.000 Einträge angewachsen. Die ständigen Erweiterungen durch immer neue Angriffe werden Optimierungen in den

Systemen erfordern. Um die Rechenzeiten zu verringern, wird sowohl auf Hardwareunterstützung durch *Field-Programmable Gate Arrays (FPGA)* [PKAC07], als auch auf Verbesserung der Algorithmen softwareseitig [AA11] gesetzt.

Die Verschlüsselung von Daten oder Kommunikationsvorgängen, bei denen der Schlüssel nicht bekannt ist, stellt ein Problem für Intrusion Detection dar. Hat das System keinen Zugriff auf den Inhalt der Pakete, können, vor allem für signaturbasierte Systeme, wichtige Informationen für eine Erkennung nicht mehr erschließbar sein. Verschiedenste Ansätze versuchen mit diesem Thema umzugehen, [Koc11] hat sie in drei Kategorien eingeteilt:

- *Protokollbasiert:* Es wird festgestellt, ob ein unerlaubtes Verschlüsselungsprotokoll zum Einsatz kommt oder erlaubte Protokolle falsch angewandt werden (z.B.: keine Verschlüsselung zwischen IP A und B erlaubt).

- *Invasiv:* Um an den Klartext der verschlüsselten Übertragung zu gelangen, müssen die betreffenden Protokolle und die Netzwerkstruktur geändert werden, damit das IDS Zugang zu den kryptografischen Schlüsseln bekommt.

- *Nicht invasiv:* Es wird versucht anhand statistischer Methoden Informationen aus und über die verschlüsselten Daten zu gewinnen.

Bei der Übertragung von verschlüsselten Paketen ist dennoch Klartextinformation über das Paket selbst enthalten. Durch flußbasierte Analyse können Anomalien im Datenverkehrstrom entdeckt werden, z.B.: IP-Adressmanipulation [Lüs08].

2.4 Snort

Snort ist ein weitverbreitetes Open Source Network Intrusion Prevention und Detection System unter der GNU General Public License (GPL). Bereits 1998 wurde es

veröffentlicht und wird seither stetig weiter entwickelt und betreut. Es arbeitet regelbasiert, kann Real-Time-Überwachungen durchführen und lässt sich durch eine modulare Plug-In-Architektur erweitern. Nach einem freiwilligen und kostenlosen Registrierungsprozess erhält man 30 Tage nach Erscheinen neuer Regeln die Updates der Regeldatenbank. Für Unternehmenskunden gibt es eine kostenpflichtiges Abonnement der Regeln, die durch das Sourcefire Vulnerability Research Team (VRT) sofort nach Erscheinen zur Verfügung gestellt werden[SNO].

Es kann als Sniffer wie *tcpdump*, als Packet Logger oder als voll funktionsfähiges IDS/IPS betrieben werden[CG07]. Durch die freie Verfügbarkeit und robuste Ausführung ist das Tool oft Grundlage oder Ausgangspunkt neuer Anwendungen oder Forschungsarbeiten wie [PKAC07, YW12, GGP+09].

Die Regeldatenbank ist der zentrale Teil der Applikation. Die Aktualität der Regeln ist Voraussetzung, dass neue auftretende Angriffe oder Gefahren erkannt werden können. SANS und CERT veröffentlichen teilweise auch Snort-Regeln, wenn neue Sicherheitshinweise ausgegeben werden[CG07]. Mit diesen Regeln lassen sich Vorgänge sehr genau spezifizieren, zum Beispiel[BBE+07]:

```
alert tcp $EXTERNAL_NET any -> $IIS_WEB_SERVERS $HTTP_PORTS (msg "/cmd.exe
going to the IIS Webserver"; flow:established,to_server; content:"/cmd.exe";
depth:30; )
```

In diesem Beispiel wird eine Alarmmeldung ausgegeben, wenn der String */cmd.exe* in den erste 30 Bytes einer Nachricht von einem beliebigen externen Netzwerk an die, in der Variable `$IIS_WEB_SERVERS` definierten, IIS Webserver, innerhalb einer aufgebauten TCP-Verbindung, geschickt wird.

Kapitel 3

Data Loss Prevention

Wie bereits in Kapitel 1 skizziert wurde, nimmt die wirtschaftliche Bedrohung durch Datendiebstahl zu. Immer mehr kleine und mittlere Unternehmen werden Opfer von Angriffen oder Diebstahlversuchen, da diese in der Regel weniger auf ihre Sicherheit bedacht sind. Der Einsatz von schlecht konfigurierten und schlecht verwalteten Sicherheitsmaßnahmen wiegt die Unternehmen in falscher Sicherheit, hindert aber Angreifer kaum am Einbruch. Der 2012 Data Breach Report [Ver12] von Verizon[1] zeigt, dass 68% aller Datendiebstähle eine Einbruchsschwierigkeit von nur „sehr gering“ oder „gering“ hatten. Somit war es mehr als zwei Drittel der Einbrecher möglich ohne spezielles Wissen oder nur mit Einsatz von vorgefertigten, automatisierten Mitteln einzudringen. Ist der Einbrecher erst einmal im internen Netzwerk, oder wird der Diebstahl direkt aus dem Netzwerk vollzogen, wird ihm meist nur mehr wenig entgegengesetzt, da das interne Netzwerk und dessen ausgehender Datenverkehr als „vertrauenswürdig“ angesehen wird. In 99% aller Fälle fand [Tru12] nicht ordnungsgemäß konfigurierte Ausgangsfilter der Firewalls vor.

Hier setzen aktuelle Entwicklungen und Forschungen zu Data Loss Prevention an: *nachdem* IDS/IPS überwunden wurde und sich jemand Zugriff verschafft hat. Dennoch ist

[1] `http://verizon.com/enterprise`

eine scharfe Definition nicht möglich beziehungsweise gar nicht sinnvoll. Data Loss Prevention umfasst nicht nur technische Komponenten, sondern es muss ebenfalls sehr stark beim Sicherheitsbewusstsein der Menschen angesetzt und innerhalb der Organisation entsprechende organisatorische oder prozesstechnische Maßnahmen getroffen werden. Erst das Zusammenwirken der personellen, organisatorischen und technischen Maßnahmen führt zu einem entsprechenden Schutz der Informationen. In Kapitel 4 werden einige Vorgehensweisen und internationale Standards zur Informationssicherheit beschrieben.

3.1 Verborgenheit

Für den Angreifer muss bei einem Datendiebstahl das oberste Ziel die Verborgenheit sein. Nicht nur aus reinem Selbstschutz, sondern je länger verborgen die Daten gestohlen werden können, desto mehr Schaden kann angerichtet beziehungsweise finanzielle Bereicherung erzielt werden. Nach Giani et al. [GBC06] setzt sich die Verborgenheit aus *Heimlichkeit* und *externen Faktoren* zusammen. Die Heimlichkeit ist proportional ($\sim$) zur Differenz der Kapazität des Mediums und der Übertragungsrate. Je größer der Abstand, desto „heimlicher“ ist die Übertragung.

$$Heimlichkeit \sim (Kapazität - Übertragungsrate)$$

Während Abbildung 3.1 die prinzipielle Idee der Heimlichkeit zeigt, müssen aber in jedem einzelnen Fall die externen Faktoren berücksichtigt werden. Befindet sich der Dieb mit einem Drucker alleine in einem Raum, ist der Ausdruck vieler Seiten weniger auffällig als mitten in einem Großraumbüro, selbiges gilt für Telefongespräche zur Weitergabe von Informationen[GBC06].

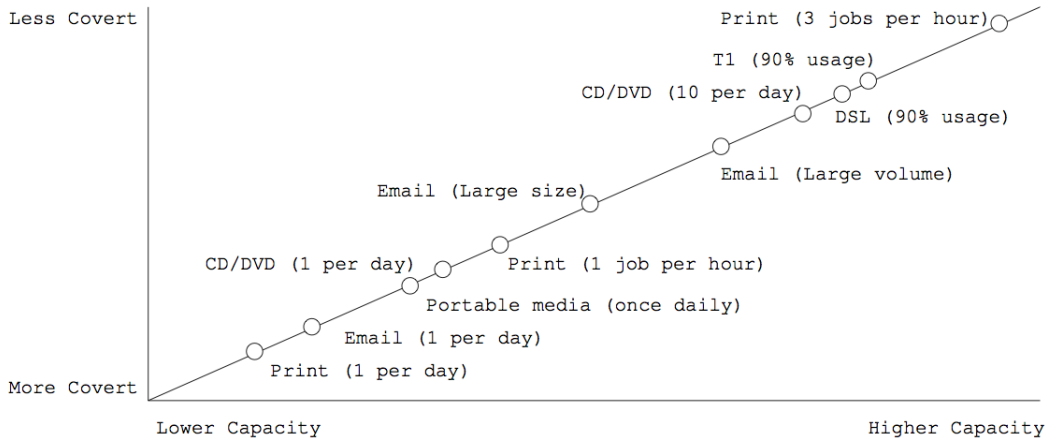


Abbildung 3.1: Heimlichkeit des Datendiebstahls bei verschiedenen Methoden [GBC06]

3.2 Data Loss Prevention Systeme

Mit Data Loss Prevention Systemen lassen sich sensible oder geheime Daten erfolgreicher schützen. Es kann nie absolute Sicherheit geben, aber DLP Systeme erschweren den Diebstahl von Daten, vorallem in großen Mengen. Zusätzlich setzt es, wie in Abschnitt 1.5.2 beschrieben, die Hemmschwelle für potentielle Insiderattacken höher. Vor allem unbeabsichtigte Veröffentlichung oder Weitergabe von Daten kann durch den Einsatz von DLP Systemen verhindert werden, gleichzeitig kann er auch zur wichtigen Bewusstseinsbildung der Mitarbeiterinnen und Mitarbeiter beitragen.

3.2.1 Kategorisierung

Verschiedenste Attribute können herangezogen werden, um Data Loss Prevention Systeme zu klassifizieren. Abbildung 3.2 zeigt eine Übersicht der gängigen Unterscheidungen beziehungsweise Merkmalen: *was* wird *wo* und *wie* geschützt.

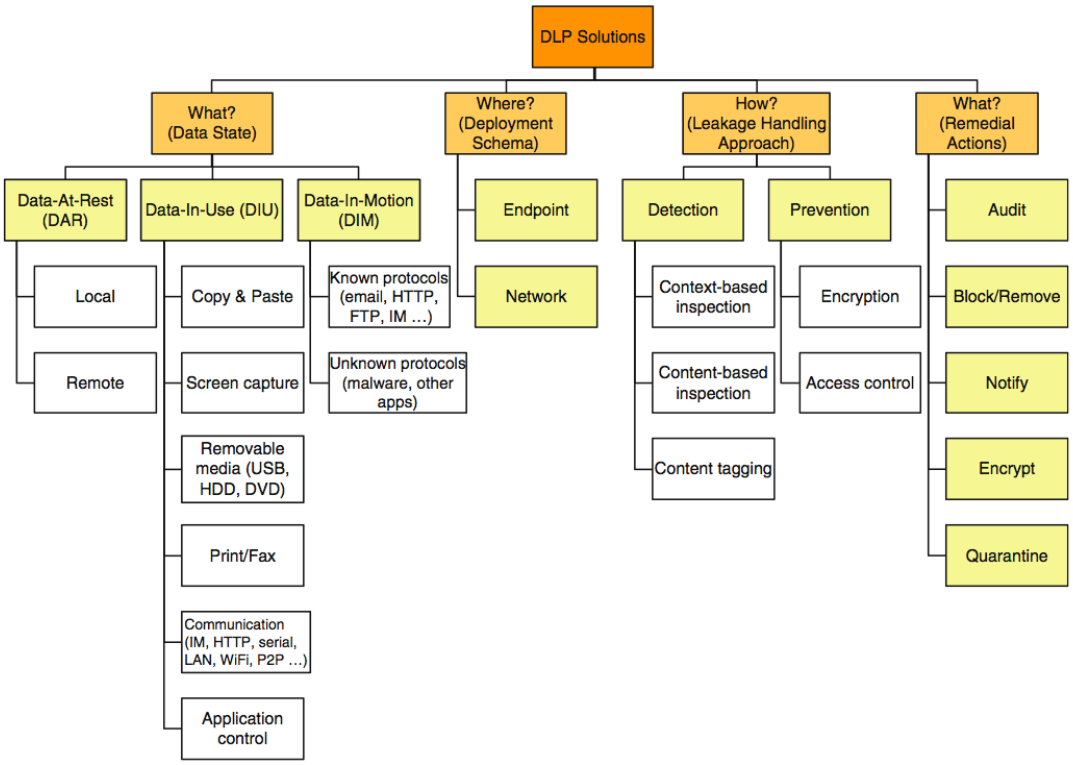


Abbildung 3.2: Übersicht von DLP Lösungen [SER12]

3.2.1.1 Was wird geschützt?

Um die Daten eines Unternehmens schützen zu können, muss das Data Loss Prevention System wissen in welchem „Verwendungszustand“ sich die Daten befinden[HMJ11]:

- *Data-in-rest:* Diese Daten befinden sich an dezidierten Speicherorten wie Fileserver, lokal am PC, Netzwerkspeichermedien, Datenbanken oder E-Mailserver.
- *Data-in-use:* Diese Daten befinden sich in Verwendung. Mitarbeiter schreiben E-Mails, kopieren oder brennen Daten auf Speichermedien oder drucken sie aus. Ebenso können Daten durch automatisierte Prozesse im Hintergrund verarbeitet werden.
- *Data-in-motion:* Diese Daten befinden sich gerade im Netzwerk unterwegs. Sie werden als E-Mail und Instant-Messaging Nachrichten gesendet oder ins Internet

transportiert (File-Upload, soziale Netzwerke, Webmail, usw.).

Für jeden dieser „Verwendungszustände“ gibt es eigenständige DLP Lösungen, die auf die separaten Bedürfnisse von vor allem kleinen und mittleren Unternehmen abzielen. Nicht jedes Unternehmen benötigt eine Enterprise Lösung die *data-in-rest*, *data-in-use* und *data-in-motion* überwacht citeLaw08.

3.2.1.2 Wo wird es geschützt?

Ähnlich wie bei Intrusion Detection Systemen werden, je nach dem in welchem „Verwendungszustand“ sich die Daten befinden, unterschiedliche Typen von Data Loss Prevention Software benötigt[LW11]:

- *Endpunkt DLP:* Für *data-in-use* und *data-in-rest* Daten. Die Software wird direkt am Netzwerkendgerät installiert und überwacht die Verwendung beziehungsweise den Zugriff auf die Daten. Eine zentrale Softwareeinheit nimmt Logs oder forensische Daten entgegen und verteilt Policies oder Updates.

- *Netzwerk DLP:* Für *data-in-motion* Daten. Der Datenstrom im Netzwerk wird durch die Software analysiert und bei einem Regelverstoß oder abnormalem Verhalten ein Alarm ausgelöst. Manche DLP Systeme greifen auch in den Datenstrom ein und blockieren den betreffenden Datenverkehr bei einem Alarm. Es ist auf eine niedrige false positive Rate zu achten!

3.2.1.3 Wie wird es geschützt?

Nach Shabtai et al.[SER12] gibt es zwei verschiedene Zugänge, um mit (potentiellen) Vorkommnissen umzugehen: *erkennende* und *präventive Ansätze*. Bei erkennenden Ansätzen unternimmt das System definierte Schritte beziehungsweise Maßnahmen, wenn eine Verletzung der Policies erkannt wird. Verwendet werden kann:

- *Kontextbasierende Analyse:* Das System inspiziert den Kontext des Traffics oder nutzt bereits vorhandene Sicherheitstechnologien, wie zum Beispiel: Spam Filter, Proxies, Firewalls, Intrusion Detection Systeme, usw. Zur Analyse werden keine Informationen aus den eigentlichen Daten herangezogen, sondern nur Kontextinformationen wie Dateiformat, Uhrzeit, Sender, Empfänger, Metainformationen, Programm oder Verschlüsselung.

- *Inhaltsbasierende Analyse:* Es gibt verschiedene Möglichkeiten ,um den Inhalt von Nachrichten bzw. Datenpaketen zu analysieren. Eine schnelle und einfache Form ist eine Mischung aus regulären Ausdrücken und Wörterbuchabgleichen. Bei unstrukturierten Daten kommen oft statistische Analysen mit *machine learning* Techniken zum Einsatz, wenn die Implementierung von deterministischen Analysemethoden zu aufwendig oder komplex ist. Ebenso können *fingerprints* von schützenswerten Daten erstellt werden, um nach diesen zu suchen. DLP Systeme sollten auch in der Lage zu sein sensible Daten in tieferen „Datenschichten“ zu finden, z.B.: eine in eine gezippte Microsoft Word Datei eingebettete Excel Tabelle.

- *Inhalt markieren:* Hierbei wird die Datei mit sensiblem Inhalt mit einem bestimmten *tag* versehen, sodass entsprechende Richtlinien im Umgang mit der Datei angewandt werden können. Es muss sichergestellt werden, dass dieser *tag* auch bei einer Verarbeitung durch eine andere Applikation (z.B.: verschlüsseln oder komprimieren) erhalten bleibt. Dieser *tag* kann automatisch je nach Speicherort oder Erstellungsprogramm generiert werden, durch inhaltsbasierende oder kontextbasierende Analyse, oder manuell durch den Benutzer.

Bei den *präventiven* Methoden[SER12] werden Zugriff oder Verwendungsmöglichkeit auf sensible Daten eingeschränkt und somit versucht einem Missbrauch vorzubeugen:

- *Zugriffskontrolle:* Durch die Umsetzung von Zugriffskontrollparadigmen[Ben06], wie *Discretionary Access Control (DAC), Mandatory Access Control (MAC)* oder

Role-Based Access Control (RBAC), kann der Zugriff auf bestimmte Ressourcen mit sensiblen Inhalten erlaubt oder unterbunden werden. Eine Erweiterung des RBAC Paradigmas stellt das *Dynamic Session RBAC* Konzept dar[MP09]. Wird einem Subjekt (Benutzer, Applikation, Prozess, usw.) der prinzipielle Zugriff auf eine Ressource gewährt, kann das eingesetzte DLP System gemäß den Richtlinien des Unternehmens die Verwendung der Informationen einschränken.

- *Gesperrte Funktionen:* Um einer missbräuchlichen Verwendung der sensiblen Daten vorzubeugen, können verschiedene Funktionen des Betriebssystems durch eine DLP Software gesperrt werden. Unterbindung von „kopieren und einfügen“, nur Leserechte bei portablen Speichermedien oder nur die Verwendung von „thin clients“ sind mögliche Beispiele.

- *Verschlüsselung:* Eine andere Art der Zugriffskontrolle kann auch durch Verschlüsselung erreicht werden. Wenn alle sensiblen Informationen standardmäßig verschlüsselt gespeichert werden, kann je nach Benutzer/Daten die Entschlüsselung individuell erlaubt oder untersagt werden.

- *Bewusstseinsbildung:* Die Mitarbeiter eines Unternehmens spielen eine wichtige Rolle. Es muss eine Bewusstseinsbildung angestrebt werden, indem mitgeteilt wird, welche Daten sensibel sind, und wie die entsprechende Handhabung sein soll. Dadurch kann die unbeabsichtigte Weitergabe oder Veröffentlichung von sensiblen Informationen reduziert werden.

3.2.2 DLP Markt

Relativ unbeschadet durch die Wirtschaftskrise 2008 sanken die Umsatzzahlen der Branche nur gering und stiegen in den darauffolgenden Jahren sehr stark an. 2008 betrug der Weltmarkt circa 100 Millionen US-Dollar[Law08]. Gartner[OM11] beziffert das Wachstum von 2010 auf 2011 um über 41% von 300 Millionen US-Dollar auf 425 Millionen

US-Dollar. Für 2012 wird ein weiterer Anstieg um 22% auf 520 Millionen US-Dollar erwartet.

Die Preise für Endpunkt-DLP-Systeme haben sich in den letzten Jahren auf unter ein Drittel reduziert und liegen jetzt zwischen $35 und $60 pro Lizenz. Sowohl bei den Endpunktsystemen als auch bei Gesamtunternehmenslösungen variiert der Preis mit den verschiedenen angebotenen Optionen beziehungsweise Konfigurationen. Gesamtunternehmenslösungen kosten im Mittel $300.000 bis $600.000 einmalig, mit jährlichen Supportkosten von 18% bis 23%[OM11].

Gartner bewertete Hersteller am Markt 2011 nach *ability to execute* (Produktfeatures, Preis, Kundenfreundlichkeit, usw.) und *completeness of vision* (Zukünftige Produktstrategie, Einfluss von Kundenbedürfnissen, Innovationen, usw.). Daraus ergibt sich eine Aufteilung in vier Quadranten, wie in Abbildung 3.3 dargestellt: *Leaders*, *Challengers*, *Visionaries* und *Niche Players*. Folgende sechs Anbieter führen den Markt an: CA Technologies[2], McAfee[3], RSA (EMC)[4], Symantec[5], Verdasys[6] und Websense[7].

3.2.3 Arbeitsablauf

Während des Betriebs eines Data Loss Prevention Systems werden folgende drei Aufgaben, wie in Abbildung 3.4 dargestellt, kontinuierlich ausgeführt[HMJ11]:

1. *Auffinden:* Das System muss durch aktive oder passive Überwachung die Daten in den drei Kategorien *data-in-rest*, *data-in-use* und *data-in-motion* auffinden.

2. *Identifizieren:* In diesen gesammelten Daten müssen nun die schützenswerten Daten identifiziert werden.

[2] `http://www.ca.com/at/data-loss-prevention.aspx`
[3] `http://www.mcafee.com/de/products/data-protection/`
[4] `http://austria.emc.com/security/rsa-data-loss-prevention.htm`
[5] `http://www.symantec.com/data-loss-prevention`
[6] `http://www.verdasys.com/solutions/dlp-3.0.html`
[7] `http://www.websense.com/content/data-security-solutions.aspx`

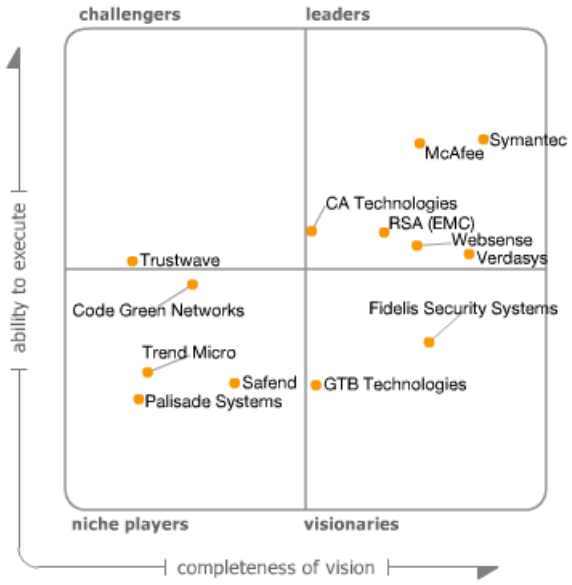


Abbildung 3.3: Gartners Magic Quadrant für Data Loss Prevention Anbieter[OM11].

3. *Durchsetzen:* Auf die nun identifizierten schützenswerten Daten müssen die definierten Regeln und Richtlinien des Unternehmens angewandt und durchgesetzt werden.

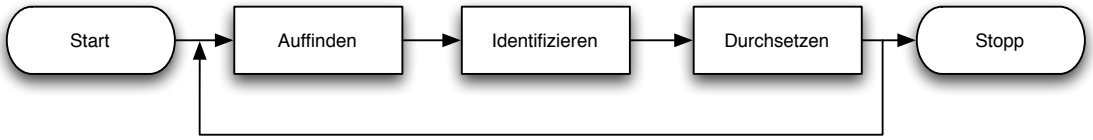


Abbildung 3.4: Arbeitsablauf eines DLP Systems [HMJ11].

3.2.4 Mängel und Herausforderungen aktueller Systeme

Eine der wichtigsten Aufgaben bei der Einführung von DLP ist das Festlegen der Richtlinien und die Zurverfügungstellung der sensiblen Dokumente beziehungsweise die Klassifikation dieser Dokumente. Speziell in großen Organisationen gibt es eine Vielzahl an strukturierten und unstrukturierten Daten aus heterogenen Prozessen oder Abteilun-

gen. Es können unter anderem Tabellendokumente, Textdokumente, Quellcode, Multimediadateien, CAD-Konstruktionsdaten, Bilder, Datenbanken oder eigene proprietäre Dokumenttypen sein. Stellt eine DLP-Software den Anspruch auf umfassenden Schutz, muss sie all diese verschiedenen Datenformate verarbeiten und interpretieren können. Dabei ist unbedingt auf eine geringe *false positive Rate* zu achten, um möglichst wenig unerwünschte Alarmmeldungen auszulösen[SER12]. Eine manuelle Klassifikation der Daten wird aufgrund der vorhandenen Menge schnell unmöglich. DLP Lösungen leisten gute Arbeit beim Erkennen, Aufzeichnen und Zusammensetzen von Informationsflüssen, sind aber stark eingeschränkt beim Erkennen von sensiblen Informationen. Die Einschränkungen betreffen sowohl die automatische Klassifizierung als auch die automatische Erkennung der Daten im Betrieb. Eingesetzte Techniken sind Schlüsselwörterlisten, reguläre Ausdrücke oder Identifizierung mittels Datei-Fingerabdruck. Werden die schützenswerten Informationen umgeschrieben oder umformatiert, können diese einfachen und limitierten Erkennungsmethoden relativ leicht umgangen werden. Aufgrund dieser großen Datenmengen geht der Trend klar zur selbstlernenden und selbstklassifizierenden Systemen mit Techniken des maschinellen Lernens. Hierbei ist eine große Schwierigkeit dem klassifizierenden Algorithmus eine geeignete Repräsentation der Daten zur Verfügung zu stellen, die *öffentlich* sein sollten (z.B.: nicht *geheim*)[HMJ11].

Die in [SER12] analysierten DLP-Produkte hatten keinerlei Alarmkorrelation implementiert. Das bedeutet, dass auftretende Warnungen oder Alarmmeldungen des selben DLP-Systems oder von anderen Sicherheitskomponenten (z.B.: Firewall, IDS, Anti-Virus, usw.) nicht in Zusammenhang gebracht werden. Folgendes Beispiel soll diese Problematik verdeutlichen: Ein Benutzer b versucht eine geschützte Datei f via E-Mail aus der Organisationen zu senden, wird aufgrund der DLP-Richtlinie jedoch blockiert. Wenn b nun eine Minute später erlaubterweise f ausdruckt, wird das in keinen Zusammenhang mit der Blockierung gesetzt. Dieser Umstand erschwert die Auswertung von Reports bei DLP-Systemen[SER12]. Durch diesen zeitliche kurzen Abstand zu einem fehlgeschlagenen Transferversuch liegt es nahe, dass b die ausgedruckte Datei f

nicht nur für den sachgemäßen internen Gebrauch nutzt. Können diese Aktionen des Benutzers beziehungsweise die Verwendungen einer Datei in Zusammenhang gebracht werden und damit eine Priorisierung der Alarmmeldungen, könnten die Untersuchung von Datenmissbrauchsvorfällen de facto in Echtzeit gestartet und b möglicherweise auf frischer Tat ertappt werden.

Der Umgang mit nicht interpretierbaren Daten ist ein weiteres Manko gängiger DLP Systeme. Der Inhalt der Daten ist für das System nicht verständlich und kann somit auch nicht klassifiziert werden. Es ist kein Schutz gegeben, außer sämtliche nicht interpretierbaren Daten werden geblockt. Allerdings gestaltet sich auch die Analyse von Multimedia-Daten wie Bilder oder Filme schwierig, denn es ist nicht oder nur kaum möglich den Inhalt zu überprüfen, und somit würden diese Multimedia-Daten ebenso geblockt werden[HMJ11]. Bei verschlüsselten Daten kann dies sinnvoll sein, wenn durch entsprechende Richtlinien und Maßnahmen gewährleistet ist, dass z.B.: sensible ausgehende Daten über E-Mail erst nach dem DLP-Scan am E-Mail-Gateway verschlüsselt werden.

Zu diesen nicht interpretierbaren Daten zählt aber auch der Datenverkehr über die verschlüsselten Protokolle HTTPS und SMTPS. Auf der einen Seite bieten sie für die übertragenen Daten Schutz vor Dritten, auf der anderen Seite könnte ein unsicherer Kommunikationspartner aufgrund der Verschlüsselung nicht überwacht werden. Einige Softwareanbieter sind deswegen übergegangen in ihre Produkte Funktionen einzubauen die nach dem „man-in-the-middle“ Prinzip (siehe [Cia11]) arbeiten und so ein Mitlesen der entschlüsselten Kommunikation ermöglichen. Dieses Vorgehen ist für die Informationssicherheit günstig, wirft aber Fragen und Probleme technischer als auch datenschutzrechtlicher Natur auf[Kin12].

Shabtai et al. [SER12] haben aktuelle akademische Forschungen analysiert und sie in sieben Kategorien unterteilt, die gleichzeitig die Herausforderungen für zukünftige DLP-Systeme darstellen:

- *Missbrauchserkennung in Information Retrieval (IR) Systemen:* Der Schwerpunkt der meisten Forschungen liegt auf der Verhaltenserkennung des berechtigten Benutzers bei normalem Verhalten, damit abweichende Muster erkannt werden können. Die Modellierung des Benutzerverhaltens ist die Kernfrage beim Versuch Anomalien zu entdecken.

- *Missbrauchserkennung in Datenbanken:* Ähnlich wie bei IR System wird hier versucht ungewöhnliches Verhalten von legitimierten Benutzer zu identifizieren. Zum Beispiel: Ein legitimierter Benutzer hat Lese- und Schreibzugriff auf eine bestimmte Tabelle und sucht beziehungsweise verändert Daten während der normalen Arbeitstätigkeit. Wenn dieser Benutzer nun mehrere Abfragen mit großen Ergebnismengen startet oder bestimmte untypische Attribute verknüpft, könnte dies auf eine böswillige Handlung deuten (z.B.: Daten sammeln).

- *Schutz vor Datenweitergabe über E-Mail:* Es werden zwei verschiedene Ansätze verfolgt: Inhaltsbasiert und Verhaltensbasiert. Eine Kombination aus Analyse der Daten im E-Mail und dem Verhaltensmuster (*wer* kommuniziert mit *wem* wie oft) könnte einen erhöhten Schutz gegen ungewollte Datenweitergabe bieten.

- *Netzwerk-/Webbasierter Schutz:* Eine ständig wachsende Menge an Datenverkehr in Netzwerken bereitet der Analysesoftware zunehmend Probleme. In diesen Forschungsarbeiten wird versucht, die brauchbaren von den unbrauchbaren Informationen im allgemeinen Netzwerkverkehr beziehungsweise speziell beim Datenverkehr ins Internet zu trennen und so die anfallenden Datenmenge für die Analyse zu reduzieren.

- *Verschlüsselung und Zugriffskontrolle:* Zur Absicherung von data-in-use, data-in-motion und data-in-rest sind der Einsatz von Verschlüsselung und Zugriffskontrolle die am meisten verwendeten Konzepte. In der momentanen Form schützen sie nur gegen unberechtigten Zugriff, aber ein legitimierter Benutzer kann trotzdem auf die Daten zugreifen und diese weitergeben. Hier werden neue Ansätze verfolgt

wie ein legitimierter Benutzer Zugriff auf sensible Daten erhalten kann, aber durch ein entsprechendes Umfeld sie nicht an unberechtigte Personen weitergeben kann.

- *Versteckte Informationen in Dateien:* Technisch nicht versierte Personen wissen oft nicht, dass in den Metadaten von Dokumenten oftmals Daten enthalten sind die nicht für eine Veröffentlichung bestimmt sind. Abseits dieser Metadaten erschwert die gute menschliche Leistung in Logik und Kombination den Schutz von sensiblen Daten. So erkennt ein Mensch sofort, dass z.B.: alle Patienten auf einer bestimmten Krankenstation ähnliche Krankheiten haben werden. Auch wenn mehrere einzelne Dokumente gemeinsam betrachtet werden, können sich unter Umständen Rückschlüsse ergeben, die eine Software bei der Einzelbetrachtung nicht erkennen kann.

- *Erkennung von bösartigen Insidern mit Honeypots und Honeytoken:* Honeypots sind isolierte Computersysteme (einzelne Programme, Computer oder ganze Netzwerke) die nicht dem Unternehmensbetrieb dienen, aber nach außen als solche dargestellt werden und für Angriffe interessant sind, in dem sie zum Beispiel weniger gut gesichert sind oder vortäuschen, wertvolle Informationen zu enthalten. Sobald eine Interaktion mit diesem System stattfindet, können alle Daten aufgezeichnet und verfolgt werden. Da die Interaktion mit einem Honeypot, oder die Verwendung eines Honeytoken (z.B.: bestimmte falsche Benutzername und Passwort Kombination), per Definition eine unnatürliche Verwendung der Infrastruktur darstellt, ist die false positive Rate sehr gering und es kann dementsprechend schnell und gezielt reagiert werden.

In [SER12] kommen die Autoren aber auch zu dem Schluss, dass sich die Forschung in Zukunft auf drei zusätzliche Felder konzentrieren sollte: *unabsichtlicher Datenverlust*, *absichtlicher Datendiebstahl durch Insider* und *Datenverlust bei mobilen Geräten*:
Bei dem Thema des *unabsichtlichen Datenverlustes durch Insider* wurden bisher die Aktivitäten und Kommunikationsvorgänge des Mitarbeiters auf die vorgegebenen Si-

cherheitsrichtlinien überprüft, um die Weitergabe von vertraulichen Informationen zu erkennen. In Zukunft sollten Sicherheitssysteme aber auch etwaige Informationen als kritisch erkennen, die selbst durchaus öffentlich sein können, aber durch Kombination mit anderen öffentlichen Informationen geschäftskritisch werden können. Zum Beispiel könnten für Konkurrenten etwaige, in einem sozialen Netzwerk veröffentlichte, Fotos der letzten Dienstreise hoher Firmenrepräsentanten interessant sein, wenn das Gerücht einer möglichen Firmenübernahme in den Medien kolportiert wird.
Bei dem *absichtlichen Datendiebstahl durch Insider* wird in Zukunft erschwerend wirken, dass die Mitarbeiter über eingesetzte DLP-Lösungen informiert sind und somit vorsichtiger agieren werden. Zusätzlich können Insider in Zukunft Teil von größer angelegten Angriffen werden und versuchen über lange Zeit langsam einen *advanced persistent threat (APT)*[Col12] aufzubauen, durch den Schwachstellen ausgenützt werden können und es schlussendlich zu einem Datendiebstahl kommt.
Zukünftig wird sich *Datenverlust bei mobilen Geräten* durch ihre immer stärker werdende Einbindung in Unternehmensprozesse zu einem noch wichtigerem Sicherheitsthema entwickeln. Ein möglicher Verlust, Diebstahl, bösartige Software sowie eine Vielzahl an Kommunikationskanälen (USB, UMTS, Infrarot, Bluetooth, SMS, usw.) bieten viele Möglichkeiten für Unbefugte, um Zugriff auf unternehmensinterne Daten zu bekommen. Aufgrund der beschränkten Energieversorgung und Rechenkapazität ist es nicht möglich komplexe Erkennungs- und Schutzsysteme zu verwenden. Hier bedarf es noch weiterer Forschung, wie man den Benutzer den Zugriff auf sensible Informationen gewährt und dabei das Datenverlustrisiko verkleinert.

Zusammenfassend lässt sich sagen, dass aktuelle DLP-Systeme keinen anspruchsvollen Schutzmechanismus gegen absichtlichen Datendiebstahl darstellen. Sie sind hauptsächlich dafür geeignet einer unabsichtlichen Datenveröffentlichung vorzubeugen. Aufgrund der Vielfalt und Komplexität der einzelnen möglichen Kanäle bedarf es intensiver weiterer Forschung, um automatisierte (Teil-)Lösungen mit einer *akzeptablen false positive Rate* zu entwerfen.

3.3 Kategorisierung von Gefahrenkanälen

Datenexfiltration kann über eine Vielzahl unterschiedlicher Datenkanäle geschehen. In [GBC06] wurde eine Kategorisierung vorgestellt, die sich nach dem *verwendeten Medium* richtet: „Netzwerk“, „Physisch“ und „Kognitiv“. Jede dieser Kategorien benötigt andere Schutzmechanismen, um eine Exfiltration zu verhindern. Durch die zunehmende Verwendung und Leistungsfähigkeit von *mobilen Geräten* (Laptops, Smartphones und Tablets) ist es nötige diese Kategorisierung zu erweitern, denn sie erfordern eigene Schutzmechanismen. So wird der Punkt „Netzwerk“ aufgeteilt in „internes Netzwerk“ und „externes Netzwerk“.

3.3.1 Internes Netzwerk

Das „interne Netzwerk“ entspricht der Kategorie „Netzwerk“ aus [GBC06]. Es umfasst das gesamte Local Area Network (LAN) eines Unternehmens mit allen Endgeräten und IT-Sicherheitsvorkehrungen und schließt somit die Übertragung aus sämtlichen Applikationen, jeglicher Schadsoftware und mit allen Protokollen ein. Nachfolgend werden einige gängige beziehungsweise beachtenswerte Vorgehensmöglichkeiten zur Exfiltration beschrieben.

3.3.1.1 Covert Channels

Covert Channels (verborgene Kanäle) sind in Zusammenhang mit Computersystemen bereits aus den frühen 1970er Jahren bekannt[SK06]. Das US Verteidigungsministerium [DOD85] definierte *covert channels* folgendermaßen:

> *A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy.*

Grundlegend können diese verborgenen Kanäle in zwei unterschiedliche Kategorien eingeteilt werden[JK11]:

- *Storage channels:* Bei diesen Kanälen werden die zu übertragenden Informationen direkt oder indirekt an eine bestimmte Stelle geschrieben und von einem anderen Prozess direkt oder indirekt wieder ausgelesen, zum Beispiel: Verbergen der Information in gängigen Protokollen. Wie [SK06, Bor10] beschreiben, bieten die Protokolle IP, TCP, ICMP, HTTP und DNS dazu verschiedene Möglichkeiten, um beliebige Informationen verborgen übertragen zu können.
- *Time channels:* Die übertragene Informationen werden durch das (nicht) Auftreten zeitlicher Events kodiert, zum Beispiel: das Empfangen eines Pakets von einem bestimmten Sender A zu einer bestimmten Zeit t bedeutet eine logische „1“, das Fehlen eines Paketes zu $t+1$ bedeutet eine logische „0“.

Es gibt eine Vielzahl an Arten wie Information über verborgene Kanäle übertragen werden kann, zum Beispiel: Verbergen der Information als Klartext oder verschlüsselt in Protokollfeldern gängiger Kommunikationsprotokollen wie IP, SMTP oder HTTP, Verwendung von Paketen zum „Morsen“ oder eine Kombination verschiedener Kanäle, um mehr Zustände und Zeichen auszudrücken[SK06].

3.3.1.2 Remote Access

Remote Access Applikationen, darunter fallen auch VPN-Lösungen, stellen zugleich Einfallstor für Angreifer als auch den Weg der Daten nach außen dar. Während [Per10] den Anteil der Einbrüche über Remote Access Applikationen bei 45% der untersuchten Fälle sieht, beziffern [Tru12] ihn mit über 60% und [Ver12] über 85% in ihren jeweiligen Untersuchungen. Nach [Tru12] haben in knapp über 45% aller Fälle die Daten das Unternehmen über denselben Weg verlassen, wie zuvor der Einbruch getätigt wurde. In [Per10] wurden bei einem Viertel der Exfiltrationen Remote Access Applikationen verwendet. Die Hälfte aller gestohlenen Datensätze in den von [Ver12] untersuchten Fällen

wurden über den Weg eines Backdoors (das Remote Access/Control erlaubt) aus der Organisation gebracht. Capelli et al. [CMTS09] hat herausgefunden, dass die meisten Insider, die IT Sabotage durchführen (siehe Unterabschnitt 1.5.2), dies außerhalb der Arbeitszeiten über Remote Access tun.

Diese Zahlen zeigen deutlich, dass Remote Access Applikationen eine Gefahr für Unternehmen darstellen können. Die Hauptfehlerquelle ist die Passwortsicherheit, und wie gezeigt wird ist ihre Auswirkungen sehr weitreichend. [Per10] hat festgestellt, dass in den untersuchten Fällen 90% der Angriffe über Remote Access erfolgreich waren, weil eine schwache Benutzername und Passwort Kombination (dargestellt als „Benutzername:Passwort“) gewählt wurde, die leicht erraten werden oder durch Wörterbuchattacken gefunden werden konnten, z.B.: „temp:temp“ oder „admin:nimda“.

In Kombination mit Wartungsaufgaben von Drittfirmen erhöht sich das Risiko für die Unternehmen. Viele Firmen verwenden die Standardherstellerpasswörter oder dieselben (unsicheren) Passwörter für mehrere oder alle Kunden. Wird diese Schutzfunktion bei einem Angriff ausgehebelt, steigt das Risiko, dass die Angreifer dieselbe Kombination bei anderen Standorten oder Kunden der Firma verwenden. In einem untersuchten Fall waren mehr als 90 Kunden durch eine einzige Benutzername und Passwort Kombination betroffen[Tru12].

Darüber hinaus kann eine Remote Access Applikation nicht nur einen Ein- und Ausgang durch ihre Funktionalität darstellen, sondern die Schwachstelle im System selbst sein. Bei der von Trustwave durchgeführten Untersuchung wurde festgestellt, dass 22% der Organisationen eine unsichere Remote Access Applikation verwenden. Durch Schwachstellen in der Applikation kann es Angreifern ermöglicht werden Benutzernamen und Passwörter oder andere sensible Daten auszuspähen[Tru12].

3.3.1.3 Schadsoftware

Der Einsatz von Schadsoftware („Malware“ - *mal*icious soft*ware*) ist nach wie vor die Hauptgefahr für Datendiebstahl[Tru12, Ver12]. Sie wird nicht nur als Einfallstor von Angreifern verwendet, sondern kann automatisiert nach Daten suchen und diese Informationen nach außen transportieren. Am häufigsten wird Malware von Angreifern von außen in ein Unternehmen geschleust, wenn er bereits Zugriff auf das System erlangt hat. Vor allem bei „kleineren“ Unternehmen (weniger als 1000 Mitarbeiter) trifft dies in über 90% der Fälle zu. Bei großen Organisationen liegt der Wert noch immer bei drei Viertel aller Fälle, aber es treten auch vermehrt Infektionen durch Ausführen von E-Mail Attachements oder über Webseiten im Internet auf[Ver12].

In über zwei Drittel der untersuchten Fälle und bei 95% der gestohlenen Datensätze sah [Ver12] Schadsoftware involviert. Großteils wurden die Daten während ihrer Verwendung (*in transit* oder *data-in-motion*) abgefangen, bei circa einem Viertel der Fälle wurden gespeicherte Daten (*data-in-rest*) gestohlen. Dementsprechend waren die häufigsten gefundenen Funktionalitäten der Schadsoftware „Key Logger“ oder „Memory Parser“. In den meisten Fällen hatte die eingesetzte Malware mehrere Funktionalitäten und konnte umfangreich eingesetzt werden[Ver12].

Hat die Schadsoftware die Daten abgefangen oder gefunden, kann sie diese auf zwei verschiedene Arten bereitstellen[Tru12]:

- *Selbstständiges Senden:* Die Malware startet autonom einen Übertragungsvorgang nach außen. Das kann sowohl in Echtzeit beim Finden der Daten erfolgen, als auch nach einer definierten Zeit oder Menge. In über 80% der Fälle wurden die Daten mit Standardprotokollen wie HTTP(S), FTP oder SMTP exfiltriert, vor allem in kleineren Unternehmen. Diese sind anfälliger für großflächige, automatisierte Angriffe, bei denen die Schadsoftware selbstständig Ergebnisse zurück übermittelt[Tru12].

- *Auf Abholung warten:* Hierbei nimmt die Schadsoftware nicht selbstständig Kontakt auf beziehungsweise startet nicht automatisiert den Übertragungsvorgang. Der Angreifer hinterlässt mit der Schadsoftware ein Backdoor, um jederzeit wieder Zugriff auf das System erhalten zu können und kehrt nach einer gewissen Zeit zurück, um die gesammelten Daten zu stehlen. Dadurch werden weniger potentiell verräterische Muster erzeugt und die Software bleibt besser getarnt. Speziell in größeren Unternehmen bleibt somit mehr Zeit, um wertvolle Daten zu lokalisieren zu können[Tru12].

3.3.1.4 E-Mail

Wie auch die Schadsoftware ist die Verwendung von E-Mail ein mögliches Einfallstor für Angreifer oder ein leicht verwendbarer Kanal nach außen. Es ist ein täglich verwendetes Kommunikationswerkzeug, dessen Gefahren durchaus bekannt sind, dennoch sind Phishing- oder Malware-Attacken erfolgreich und bei Angreifern beliebt. Bei einer Umfrage des CERT[CSO] hatten 46% der befragten Teilnehmer angegeben, dass sie in den letzten 12 Monaten Ziel einer Phishing-Attacke geworden sind. In [Ver12] wird angegeben, dass in 8% aller untersuchten Fälle unter anderem Phishing verwendet und dabei 38% der Daten gestohlen wurden. Ebenso hat Verizon festgestellt, dass 18% aller Malwareinfektionen in großen Unternehmen durch das Ausführen von Attachements ausgelöst wurden. Die Anzahl der versandten E-Mails mit ausführbaren Attachements hat sich seit 2008 jedes Jahr verdoppelt. Hingegen ist seit 2011, zum ersten Ma,l die Anzahl von virusinfizierten E-Mails zurück gegangen. [Tru12] beobachtet den Trend, dass die Angreifer langsam weg von breit gefächerten Standardattacken gehen und stattdessen gezielte und spezialisierte Attacken einsetzen.

Wenn schützenswerte Daten per E-Mail versendet werden, erfolgt es entweder absichtlich oder unabsichtlich:

- *Absichtlich:* Versendet ein Mitarbeiter des Unternehmens geheime Daten absichtlich, wird er Insider genannt. [HDS+11] haben in ihren Untersuchungen festgestellt, dass circa 30% der Insider Informationen per E-Mail versandt haben. Dazu wurde der eigene unternehmensinterne Account verwendet und als Empfänger entweder die eigene private E-Mailadresse für spätere Verwendung angegeben oder direkt an einen Konkurrenten adressiert. Durch eingeschleuste Schadsoftware ist es für einen Angreifer ebenso möglich Daten per E-Mail zu versenden. Es wird eine eigene E-Mailapplikation installiert und verwendet, damit der Übertragungsvorgang nicht durch den unternehmensinternen E-Mail-Server erfolgen muss[Tru12].

- *Unabsichtlich:* Im Gegensatz zum absichtlichen Versenden von schützenswerten Daten, kann der unabsichtliche Versand nur einem Mitarbeiter des Unternehmens passieren. Dies kann aus zwei, sich nicht gegenseitig ausschließenden, Gründen erfolgen: entweder aus Unwissenheit über die Daten oder durch Fehler in der Empfängerliste. Wenn Mitarbeiter nicht hinreichend geschult und sensibilisiert sind, bemerken sie vielleicht nicht, dass Daten in das E-Mail geschrieben oder als Attachement angehängt worden sind, die nicht für diese Weitergabe bestimmt sind. Ebenso kann es zu manuellen Tippfehlern bei den Empfängern kommen oder die Autovervollständigung des verwendeten Softwareprodukts wählt nicht den intendierten Empfänger aus. Im April 2010 schickte ein Polizist aus Gwent in Großbritannien eine Liste mit 10.000 Vorstrafenregister an einen Journalisten, da die Autovervollständigung die falsche Person ausgewählt hatte[Cha11].

3.3.1.5 Mobile Geräte

Die Stärke und der Vorteil der mobilen Geräte als flexibler und ungebundener Arbeitsplatz ist auch gleichzeitig der Nachteil beziehungsweise das Problem für Sicherheitssysteme. Auf der einen Seite benötigen sie mittels LAN-Anschluss oder VPN-Verbindung Zugang zum internen Netzwerk und den vertraulichen Informationen sowie fixe Ar-

beitsplätze, auf der anderen Seite wird der gesicherte Bereich des internen Netzwerkes verlassen und die gespeicherten Informationen befinden sich in einem potentiell gefährlichen Umfeld. Das betrifft sowohl den physischen Zugriff, als auch die Verbindung in ungesicherte Fremdnetzwerke. Die portable Bauweise der Geräte erleichtert es den Angreifern sie zu stehlen. Eine Vielzahl an Schnittstellen zur Umwelt (z.B.: WLAN, Bluetooth, Infrarot, USB, Speicherkarten) erhöhen die Interaktionsmöglichkeiten des Gerätes, aber bieten zugleich eine Angriffsfläche von außen, die entsprechend geschützt werden muss.

Handelt es sich bei dem eingesetzten Gerät um kein Firmeneigentum sondern um ein Privatgerät des Anwenders (BYOD - Bring Your Own Device), kommen rechtliche Hürden für die Sicherstellung der Sicherheit hinzu. Durch das Fernmeldegeheimnis und das Grundrecht auf Datenschutz genießt die private Kommunikation Schutz vor Überwachung[SIH10]. Aus diesem Grund dürfte die eingesetzte Software nur die berufliche Kommunikation überwachen. Da dies nicht immer eindeutig trenn- oder bestimmbar ist, sollte von der Verwendung privater Geräte dringend abgesehen werden.

Laptops

Für Laptops gilt mindestens dieselbe Menge an Gefahren und Bedrohungen wie für den Standard-Arbeitsplatzrechner im internen Netzwerk, da sie auch wie ein solcher betrieben werden können. Wird dasselbe Betriebssystem verwendet, stehen somit aber auch dieselben Schutzmöglichkeiten zur Verfügung. Eine besondere Herausforderung für das Sicherheitskonzept ist die Transportierbarkeit des Geräts. Nicht nur der Diebstahl des Geräts muss bedacht werden, die Sicherheitspolicys des Unternehmens müssen auch das Verhalten bei Verlassen des geschützten Bereichs regeln. Die eingesetzte Software muss ihre Umgebung selbstständig erkennen und dementsprechend handeln[BGER08]. Eine zusätzliche Gefahr birgt das Arbeiten in öffentlichen Bereichen wie Bahnhöfen, Flughäfen oder Hotellobbys. Wie in Unterunterabschnitt 3.3.4.2 beschrieben können

Angreifer durch „shoulder surfing“ vertrauliche Informationen oder Passworteingaben ausspähen.

Smartphones und Tablets

Während sich Laptops und der Umgang damit im Geschäfts- und Sicherheitsbereich mittlerweile etabliert hat, stellen Smartphones und Tablets noch größere Sicherheitsunbekannten dar, die aber für Unternehmer immer wichtiger werden. In einer Umfrage von [Olt11] geben 86% der Befragten an, dass mobile Geräte „kritisch“ oder „wichtig“ für die Unternehmensprozesse und -produktivität sind. Durch die drastisch gesteigerte Performance und Flexibilität, kombiniert mit einer immer höher werdenden Bandbreite, steigt auch das Sicherheitsrisiko für Unternehmen. Steigende Verkaufszahlen der mobilen Geräte sowie deren verstärkter Einsatz in Unternehmen, bewirken immer größer werdendes Interesse bei potentiellen Angreifern. Während sich die entdeckten Schwachstellen in mobilen Betriebssystemen seit 2009 circa verdreifacht haben, ist die Anzahl der Ausnützungen dieser Schwachstellen um mehr als das Siebenfache gestiegen[Kao11]. Wie auch bei Laptops können gespeicherte Daten durch *Verlust*, *Diebstahl* oder *Schadsoftware* an Außenstehende gelangen.

Nicht nur durch das Ausnutzen von Schwachstellen im Betriebssystem kann Schadsoftware auf das mobile Gerät gelangen, sondern auch über die zahlreichen Quellen für Programme (Apps), die sogenannten *Appstores*. Beispiele dafür sind der Apple Appstore, Google Play (vormals Google Android Market) oder der Amazon Appstore für Android. Abhängig von den jeweiligen Geräteherstellen können diese Apps nur über einen oder über mehrere Appstores bezogen werden, die entweder unter Kontrolle des Herstellers stehen oder auch völlig unkontrolliert befüllt werden können. Diese Möglichkeit nützen immer mehr kriminelle Personen, um Schadsoftware auf mobilen Geräten zu verbreiten[DH11].

Die kleine Bauweise und Leistungsfähigkeit bergen noch weitere Gefahren für Unter-

nehmen. Aktuelle Endgeräte bieten die Funktionalität einer Digitalkamera, Videokamera und Audioaufzeichnung. So lassen sich unbemerkt Ausdrücke abfotografieren, Bildschirminhalte filmen oder interne Besprechungen durch das eingebaute Mikrofon aufzeichnen[SIH10]. Sind diese Informationen erst einmal auf dem Gerät gespeichert, ist es für den Benutzer einfach sie über viele verschiedene Kanäle (Mobilfunknetz, Firmennetzwerk, WLAN, Bluetooth, Infrarot, USB, ...) zu verteilen, während das Unternehmen nur sehr wenige davon überwachen kann.

3.3.1.6 Supply Chain

Potentielle Gefahr geht auch von der Beschaffungskette *(supply chain)* aus. Schadcode oder -funktionen können in neu gekauften Produkten bereits enthalten sein. Nach [MA10] können Hardware Supply Chain Attacken nach drei verschiedenen Implementierungsmethoden eingeteilt werden. Je nach der verwendeten Art kann ein Angreifer unbemerkt Schadsoftware einschleusen oder vorhandene Sicherheitsmaßnahmen umgehen oder funktionsuntüchtig machen.

- *Programmierbare Speicher:* Angreifer können veränderte Programme in Speicherbausteine wie EPROM, EEPROM, NVRAM oder Flashspeicher bringen. Zum Beispiel kann ein veränderter Bootloader das Cisco Router Betriebssystem „IOS“ (Internetworking Operating System) beim Laden in den RAM verändern, um Angreifern später Zugriff zum Netzwerk zu gewähren.

- *Firmware Angriffe:* Festplattenfunktionalitäten wie „Self-Monitoring, Analysis and Reporting Technology“ (S.M.A.R.T.) können korrumpiert und somit Schadcode eingeschleust werden. Durch S.M.A.R.T. können Sektoren auf der Festplatte als fehlerhaft markiert werden, wodurch das Betriebssystem keinen Zugriff mehr auf diese Sektoren erhält. Eine Veränderung könnte Sektoren mit Schadcode als fehlerhaft markieren und sie somit vor der Erkennung durch das Betriebssystem schützen.

- *Änderung der Schaltkreise:* Bereits bei der Herstellung können Schaltkreise verändert beziehungsweise (vom Kunden) ungewollte Zusatzfunktionalitäten geschaffen werden. Vor allem im militärischen Bereich ist eine Änderung der Schaltkreise (z.B.: in Waffensystemen) gefährlich. Diese Funktionalitäten können über WLAN, Funkwellen, Netzwerksignale oder vorgegebenen Bedingungen, wie GPS-Position, Datum/Uhrzeit, usw., aktiviert werden.

Auch wenn bei dem Begriff „Supply Chain“ meist an Hardwarebeschaffung gedacht wird, ist *Software Supply Chain Risk Management* wichtig für Unternehmen. Unabsichtliche oder absichtliche Fehler im Quellcode können ein Einbruchstor für Angreifer darstellen. Die Kunden sollten sich beim Anbieter unter anderem vertraglich absichern, dass dieser selbst Supply Chain Risk Management in der Softwareherstellung anwendet[EAC+10].

3.3.2 Externes Netzwerk

Dieser neu eingeführte Kategorie umfasst jegliche Netzwerk- oder Datenverbindungen, die abseits des unternehmenseigenen Netzwerkes existieren. Als Beispiele seien hier Smartphones, Tablets oder Laptops mit Mobilfunk-, Bluetooth- oder WLAN-Verbindung genannt, deren zweite Kommunikationsseite sich außerhalb des Unternehmensnetzwerkes befindet und somit der Datenverkehr nicht überwacht werden kann. Es ist für den Sender nicht nachvollziehbar welche anderen Systeme diese Daten mitlesen („sniffen“) können. Sobald sich IT-Geräte in ein WLAN verbinden, werden sie potentiell angreifbar durch Man-In-The-Middle-Attacken, bei denen sich ein dritter, unbefugter Kommunikationspartner in eine bestehende Kommunikation einklinkt und als Vermittler dient und somit Zugriff auf alle gesendeten Daten bekommt[Jun12]. Wie [SIH10, Seite 444] schreibt, können IT-Systeme, die ein Mobilfunknetz nutzen (z.B.: Smartphones oder Tablets), meist diese Verbindung auch freigeben, sodass sie als Mo-

dem oder Hotspot für andere IT-Systeme fungieren und eine unsichere Verbindung in ein externes Netzwerk herstellen können.

Befinden sich die Daten erst einmal auf einem Gerät mit Verbindung nach außen, kann der Exfiltration nur mehr sehr wenig entgegengesetzt werden. Handelt es sich um ein Endgerät, das in die Sicherheitsinfrastruktur eingebunden ist, müssen, wie in Unterabschnitt 3.3.1 beschrieben, die potentiellen Kommunikationskanäle geschlossen werden. Eine Einschränkung der Zugriffsrechte nach dem *principle of least privilege* [Bis03] verkleinert die Menge an einsehbaren Informationen, kann und soll je nach Benutzer aber nicht vollständig unterbunden werden.

3.3.3 Physische Datenträger

Immer neuere und hochmoderne Angriffstechniken bestimmen das Hauptaugenmerk bei Sicherheitsüberlegungen. Jedoch sollten auf keinen Fall die physischen Datenträger als Gefahrenkanal vergessen werden. Wie InfoWatch[Inf12] bei Untersuchungen herausgefunden hat, sind im Jahr 2010 bei Datendiebstählen circa in 28% der Vorfälle physische Datenträger verwendet worden, ein Jahr darauf circa 25%. Für den Zeitraum von 2007 bis 2010 weist KPMG International[MGK10] die Kategorie mit physischen Datenträger als jene aus, in der die zweitgrößte Anzahl an Datensätze gestohlen wurde, Nummer Eins war die Kategorie „Hacking“. Physische Datenträger können in zwei Kategorien eingeteilt werden: „digitale Speichermedien“ und als analoges Gegenstück das „Papier“.

3.3.3.1 Digitale Speichermedien

Im Alltag von Unternehmen ist die Verwendung von digitalen Speichermedien sehr weit verbreitet oder fixer Bestandteil von Geschäftsprozessen, da sich schnell und einfach Daten austauschen lassen und flexibel gearbeitet werden kann[Hof12]. Dazu zäh-

len unter anderem USB-Sticks, (mobile) Festplatten, Flash-Speicherkarten (z.B.: Secure Digital (SD)-, Compact Flash (CF)-, Multimedia Card (MMC)- oder xD-Picture-Card (xD)-Speicherkarten), Zip-Disketten, Magnetbänder oder optische Datenträger wie CDs, DVDs oder Blue-Ray-Discs. Durch ihre kompakte Bauweise können sie leicht in und aus Organisationen gebracht werden ohne Aufmerksamkeit zu erregen, wenn keine physischen Kontrollen von Kleidung und Taschen durchgeführt werden.

Im *Data Loss Barometer 2010*[MGK10] hat „KPMG International“[8] aus vielen unterschiedlichen Quellen Daten zu verlorenen oder gestohlenen Informationen erhoben. Vorfälle mit digitalen Speichermedien haben sich folgendermaßen aufgeteilt: 37% Festplatten, 19% Bänder, 11% CDs, 7% USB Speicher, 26% andere Medien. Es zeigt sich auch, dass seit 2007 der Anteil an gestohlenen oder verlorenen Festplatten kontinuierlich steigt. Durch die stetig wachsenden Kapazitäten und damit die wachsende Menge an Daten darauf, werden Festplatten zu immer beliebteren Diebstahlszielen.

Vor allem werden bei Informationsdiebstahl durch Insider häufig digitale mobile Speichermedien eingesetzt. Hanley et al. [HDS+11] haben bei ihren Untersuchungen herausgefunden, dass bei rund 30% der Diebstähle durch Insider transportable Speichermedien zum Entwenden der Daten benutzt wurden. Die *2007 E-Crime Watch Survey* [CSO] gibt an, dass in 36% der Insider bei Diebstahlsfällen die Daten auf mobile Speichermedien wie USB-Sticks, iPods, etc. kopiert haben.

Sensible Daten können nicht nur durch Entwenden oder bewusste Weitergabe an Unberechtigte gelangen. Gerade durch die kleine Bauweise von Speicherkarten oder USB-Sticks können diese sehr leicht verloren werden. Eine Studie im Auftrag der britischen Regierung hat ergeben, dass zwei Drittel der Befragten bereits einmal einen USB-Stick verloren hätten. In 60% der Fälle waren auch firmeninterne Informationen darauf gespeichert. Das bedeutet, dass vier von zehn Personen bereits einmal interne Informationen ihres Arbeitgebers verloren haben. Eine spätere Umfrage zeigt, dass 77% der befragten

[8] `https://www.kpmg.com`

Personen private Speichermedien auch in der Arbeit nutzen. Dadurch kommt es zu einer Durchmischung von privaten und sensiblen Firmendaten, die, bei privater Verwendung oder Weitergabe des Speichermediums, durch Unberechtigte eingesehen oder kopiert werden können[Hof12].

Die Nutzung von digitalen Speichermedien stellt nicht nur eine Gefahrenquelle für den Verlust oder Diebstahl von Daten dar, sondern birgt auch die Gefahr Angreifern den Einbruch am Computer oder im Netzwerk zu ermöglichen, die dann Daten auf demselben oder einem anderen Kanal stehlen können. Auf diesen mobilen Speichermedien können sich ganze Betriebssysteme befinden, die dem Insider vor Ort helfen können einen Datendiebstahl zu begehen. Es können sich aber auch versteckt Schadprogramme darauf befinden die aktiviert werden, sobald das Speichermedium mit einem Computer verbunden wird. Immerhin gaben 55% der Befragten einer Studie an, dass sie eventuell gefundene Daten einsehen würden[Kru09]. Dieses Ergebnis deckt sich mit einem Versuch der IT-Beratungsfirma NCC, bei dem anonyme aber ansprechende Einladungen zu einem Event und ein beiliegender USB-Stick an Führungskräfte aus Finanzabteilungen von 500 börsennotierten Unternehmen geschickt wurde. Knapp die Hälfte der Personen hatte den USB-Stick mit ihrem Firmenarbeitsplatz verbunden, was einem potentiellen Angreifer die Möglichkeit zum Einschleusen von Schadsoftware gegeben hätte[Hof12].

3.3.3.2 Ausdruck auf Papier

Die speicherbare Datenmenge auf einem Blatt Papier ist gegenüber digitalen Medien sehr stark begrenzt. Allerdings benötigen wichtige oder sensible Informationen nicht immer viel Speicherplatz. Interne Businesspläne, Strategiepapiere, Geschäftsberichte oder Kundendaten können trotz geringer Seitenanzahl einen großen Wert für das Unternehmen darstellen und müssen dementsprechend geschützt werden. Papier eignet sich für eine langsamen und unauffälligen Diebstahl. Die Informationen können über viele Tage

oder Wochen Stück für Stück ausgedruckt werden und in unauffälligen Mengen in jeder Tasche oder Mappe aus der Organisation gebracht werden.

Bei einer 2009 durchgeführten Umfrage durch „Lightspeed Research“[9] haben 40% der befragten Arbeitnehmer in Großbritannien angegeben, dass sie bereits einmal sensible Informationen am Drucker gesehen haben. Es gaben auch 47% an, dass sie unwissend, betreffend sicheren Druckprozessen oder Technologien zur Absicherung der Druckinfrastruktur, sind[Eva09].

Das Ausdrucken von sensiblen Informationen birgt folgende Risiken in sich[Por11]:

- *Abfangen oder mitlesen:* Wenn sensible Informationen über ein Netzwerk an einen Drucker gesendet werden, besteht die Gefahr, dass die Kommunikation durch Unbefugte mitgelesen oder ganz abgefangen wird. Aber auch das Druckergerät selbst kann angegriffen werden, und ein Angreifer sich somit Zugang zu den Informationen beschaffen. Speichert das Druckergerät die Druckaufträge auch auf einer Festplatte, könnte diese Ziel eines Diebstahls werden.

- *Diebstahl oder Schnüffelei:* Sind die Informationen ausgedruckt und liegen auf der Ablagefläche des Druckers, unterliegen sie nicht mehr den technischen Zugriffskontrollen oder Policies und können von jeder beliebigen Person eingesehen oder entwendet werden.

- *Zuverlässigkeit:* Auftretende Schwierigkeiten oder Probleme beim Drucker bedürfen manchmal besonderer interner oder externer Personen, um sie zu lösen. Diese Personen können eine Sicherheitslücke darstellen, wenn sie im Zuge der Problembehebung mit sensiblen Informationen aus dem Druckgerät in Kontakt kommen. Selbiges gilt, wenn das Gerät wegen eines Defekts oder Wartungsarbeiten aus der Organisation gebracht werden muss.

[9] `http://www.lightspeedresearch.com/`

Nicht nur während und kurz nach dem Druckvorgang besteht für ausgedruckte sensible Informationen eine Gefahr durch Diebstahl. Am Arbeitsplatz herumliegende Ausdrucke können durch andere Mitarbeiter oder durch das Reinigungspersonal entwendet oder ausgespäht werden, vor allem außerhalb der regulären Arbeitszeiten wenn sich weniger Personen im Unternehmen befinden. Diese Gefahr kann durch die konsequente Anwendung der *Clear Desk Policy* reduziert werden. Diese legt fest, dass alle Unterlagen zu Arbeitsende in versperrbaren Laden oder Kästen verstaut werden müssen, damit niemand Unbefugter Zugriff bekommt[CW05].

Wie in [Ber07] beschrieben wird, können Beschränkungen an verschiedenen Stellen ebenfalls dazu beitragen die Gefahren zu reduzieren:

- *Beschränkung der Dokumente:* Wenn gemäß den Richtlinien der Organisation die Dokumente mit sensiblen Inhalten entsprechend klassifiziert sind, kann, entweder pro Klassifizierung, pro Benutzer, pro Gruppenzugehörigkeit oder pro Mischform daraus, die Druckfunktion eingeschränkt werden. Durch diesen eingeschränkten Kreis an Personen mit Druckberechtigungen lassen sich die zuvor beschriebenen Risiken reduzieren.

- *Beschränkung der Drucker:* Nicht nur Dokumente können beschränkt werden, sondern auch die Druckergeräte selbst. Zum Beispiel kann ein exponierter Drucker in einem Gemeinschaftsbüro beschränkt werden, dass keine Dokumente einer bestimmten Sicherheitsklasse ausgedruckt werden können. Somit reduziert sich die Gefahr, dass unbefugte Personen Zugriff erhalten.

- *Beschränkung des Zugriffs:* Zusätzlich sollte der Zugriff auf Druckjobs am Drucker selbst beschränkt werden. Durch Chipkarten oder eine PIN Eingabe wird sichergestellt, dass nur die berechtigte Person den Druckauftrag starten kann. Eine wartende Person neben dem Drucker schreckt zusätzlich potentielle Diebe ab.

3.3.4 Kognition

In die Kategorie *Kognition* werden jene Gefahrenkanäle eingeteilt, die als eine Hauptleistung oder zumindest zu einem hohen Grad die Verwendung des menschlichen Verstandes benötigt. Es können dabei durchaus technische Hilfsmittel eingesetzt werden, aber um diese Kanäle abzusichern muss vor allem beim Menschen selbst und dem Informationsfluss zu ihm angesetzt werden.

3.3.4.1 Menschliche Aktionen

Nicht immer ist es nötig große Mengen an Informationen zu stehlen, die nur auf digitale Speichermedien aus dem Unternehmen transportiert werden können. Manchmal reicht es nur einige wenige Informationen an die Konkurrenz zu geben, um einem Unternehmen großen Schaden zuzufügen, zum Beispiel: noch nicht freigegebene Geschäftszahlen, Zutaten und Mischverhältnisse bei Produkten oder Zugangsdaten zu IT-Systemen und Gebäuden.

Als Vertreter in der Kategorie „Menschliche Aktionen“ seien Beispielhaft „merken“, „aufschreiben“ oder „weitererzählen“ genannt. Hier stößt der Einsatz von Technik an seine Grenzen. Es gibt (noch?) keine Software- oder Hardwarelösung, die das menschliche Gehirn am Speichern von Informationen hindern kann. Um hier einen Informationsdiebstahl verhindern zu können, müssen die Zugangsmöglichkeiten der Person zu diesen Informationen reglementiert und überwacht werden. Aber auch eine hohe Loyalität dem Unternehmen gegenüber und eine ausgeprägte Moralvorstellung der Personen verringern das Risiko des Diebstahls.

3.3.4.2 Social Engineering

Dem Faktor „Mensch“ sollte ein hoher Stellenwert in der (IT-)Sicherheitsplanung zugeschrieben werden. Selbst ein ausgeklügeltes und richtig konfiguriertes IT-Sicherheitssystem

schützt nicht, wenn ein unvorsichtiger Benutzer Zugangsdaten oder direkt sensible Information weitergibt. Mitnick et al. [MSD03] definiert *Social Engineering* folgendermaßen:

> *Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen.*

Abhängig von der Methodik und den Hilfsmitteln des Social Engineers kann die Attacke in eine oder mehrere Kategorien eingeteilt werden[Lip09]:

- *Human Based Social Engineering (HBSE):* Hierbei verzichtet der Social Engineer auf den Einsatz technischer Hilfsmittel und versucht im telefonischen oder persönlichen Kontakt die gewünschten Informationen zu erlangen. Bei unvorsichtigen Angriffszielen kann bereits eine einfache und direkte Frage nach der gewünschten Information (z.B.: Passwort) zielführend sein.

- *Computer Based Social Engineering (CBSE):* Der Angreifer verwendet technische Hilfsmittel, um an die gewünschten Informationen zu gelangen. Zum Beispiel können durch den Einsatz von veränderten Internetseiten (Phishing) oder Malware als E-Mail Attachement Zugangsdaten des betreffenden Benutzers gestohlen werden.

- *Reverse Social Engineering (RSE):* In dieser Kategorie bringt der Angreifer das Opfer dazu, von sich aus Kontakt mit dem Angreifer aufzunehmen. Zum Beispiel kann der Angreifer vorgeben Ansprechpartner bei bestimmten Störungen zu sein und eine solche selbst herbeiführen. Das ahnungslose Opfer wird Kontakt aufnehmen und bereitwillig bei der „Beseitigung“ der Störung helfen, durch Passwortweitergabe, ausführen von (Fremd-)Programmen, usw.

Wie [Lip09] ausführt, ist *Vertrauen* eine wichtige Komponente bei Social Engineering und erleichtert die Arbeit des Angreifers. Abbildung 3.5 zeigt den Zyklus eines Social Engineering Angriffs. Weitverbreitete soziale Medien wie facebook[10] oder Twitter[11] helfen dem Angreifer bei der vorangehenden Recherchearbeit rund um das Unternehmen und des konkreten Opfers. Je mehr Informationen zur Verfügung stehen, desto einfacher wird es gezielte Angriffe auf das Opfer zu starten und dessen Vertrauen zu erlangen. Für IT-Sicherheitssysteme steigt die Herausforderung stark an, da kaum generelle Muster in diesen individualisierten Angriffen zu erkennen sind[Koc11].

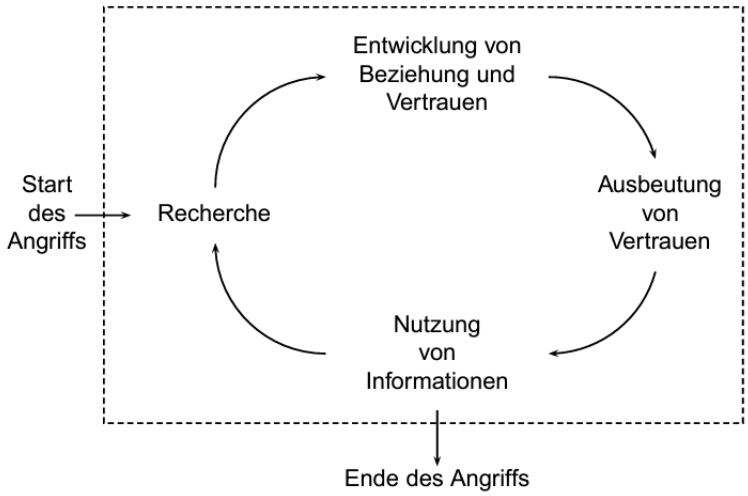


Abbildung 3.5: Zyklus eines Social Engineering Angriffs [Lip09].

Aber nicht nur der reine Informationsgewinn durch Personen kann für ein Unternehmen gefährlich werden. Sensible Informationen auf optischen Datenträgern oder Papier werden vor der Entsorgung nicht richtig zerstört, oder diese Aufgabe einem Fremdunternehmen überlassen. Bei der Rechercheaufgabe kann der Social Engineer zu wertvollen Informationen durch *dumpster diving* gelangen[HW10]. Ebenso arbeiten viele Mitarbeiter außerhalb des Büros an und mit firmeninternen Dokumenten, wodurch ein Angreifer mit *shoulder surfing* leicht Informationen ausspähen kann[Gou11]. Unter den Begriffen

[10] `http://www.facebook.com`
[11] `http://www.twitter.com`

piggybacking oder *tailgating* versteht man, dass der Angreifer physischen Zutritt zu einem geschützten Bereich bekommt, indem er elektronische und/oder mechanische Sicherheitsmechanismen, mithilfe einer autorisierten Person überwindet[Par89]. Dabei muss diese autorisierte Person nicht zwingend ein bösartiger Insider sein, sondern kann auch ein normaler Mitarbeiter sein, der aus Unachtsamkeit und Höflichkeitsgründen dem Social Engineer eine Türe aufhält, weil er denkt es handelt sich um einen anderen Mitarbeiter der Organisation.

Kapitel 4

Sicherheitsframeworks

Dieses Kapitel stellt einige bekannte und verbreitete Sicherheitsvorgehensweisen und Sicherheitsstandards vor. Es soll der Aufbau und prinzipielle Gedanke hinter den Werken vermittelt werden, um eine Übersicht über gängige Frameworks zu bekommen. Weiters dient es als Grundlage für die später getroffene Auswahl eines dieser vorgestellten Frameworks, um es auf Erweiterungsmöglichkeiten in Bezug auf Data Loss Prevention zu analysieren.

4.1 ISO/IEC 27000 Serie

Die *International Organization for Standardization (ISO)*[1] und *International Electrotechnical Commission (IEC)*[2] haben mit der ISO/IEC 27000 Serie eine weltweit verbreitete Standardspezifikation im Bereich *Information Security* geschaffen, die sich aus mehreren einzelnen, aber verknüpften, Standards zusammensetzt. Die Ursprünge gehen auf einen „Code of Practice“ als British Standard 7799 in den Mitte 1990er Jahren

[1] `http://www.iso.org`
[2] `http://www.iec.ch/`

zurück. Als Ergebnis einer grundlegenden Überarbeitung wurde 1999 der „Code of Practice“ als der erste Teil BS7799-1:1999 veröffentlicht, sowie eine Spezifikation im Teil 2 BS7799-2:1999 zur Überprüfung und Zertifizierung von Security Management Systemen in Organisationen. Nur ein Jahr darauf internationalisierten die ISO und IEC den British Standard 7799-2:1999 und veröffentlichten ihn als ISO/IEC 17799:2000. Als ISO/IEC 27001:2005 Standard wurde eine überarbeitete Version des BS7799-2 ausgegeben, gegen den *Information Security Management Systeme (ISMS)* bewertet werden können. Um den bisherigen „Code of Practice“ ISO/IEC 17799:2005 klarer an die Information Security Management Standards, die ISO/IEC 27000 Serie, zu binden, wurde er 2008 zu ISO/IEC 27002:2005 umnummeriert und somit eingebunden[Cal09].

In Abbildung 4.1 wird der Zusammenhang der Normen der *ISO/IEC 27000 Information technology - Security techniques* Reihe dargestellt. Kernelemente sind ISO 27001 und ISO 27006, die verpflichtende Anforderungen definieren und somit eine strukturierte, einheitliche und nachvollziehbare Zertifizierung möglich machen. Zur Unterstützung bei diesem Prozess wurden informative Standards geschaffen, die generelle methodische Richtlinien vorgeben oder aber auch konkrete Maßnahmen (z.B.: ISO 27002).

4.1.1 Wichtige Standards

Die wichtigsten Standards der ISO 27000 Reihe werden nachfolgend kurz beschrieben[ISOa]:

- *ISO 27000 - Information security management systems - Overview and vocabulary:*

  In diesem Dokument wird eine Einführung in ISMS und ein Überblick über die gesamte Serie gegeben. Die verwendete Terminologie wird erläutert sowie die Unterstützung und Beschreibung der wiederkehrenden Plan-Do-Check-Act (PDCA) Zyklen. Es kann kostenlos heruntergeladen[3] werden.

[3] `http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip`

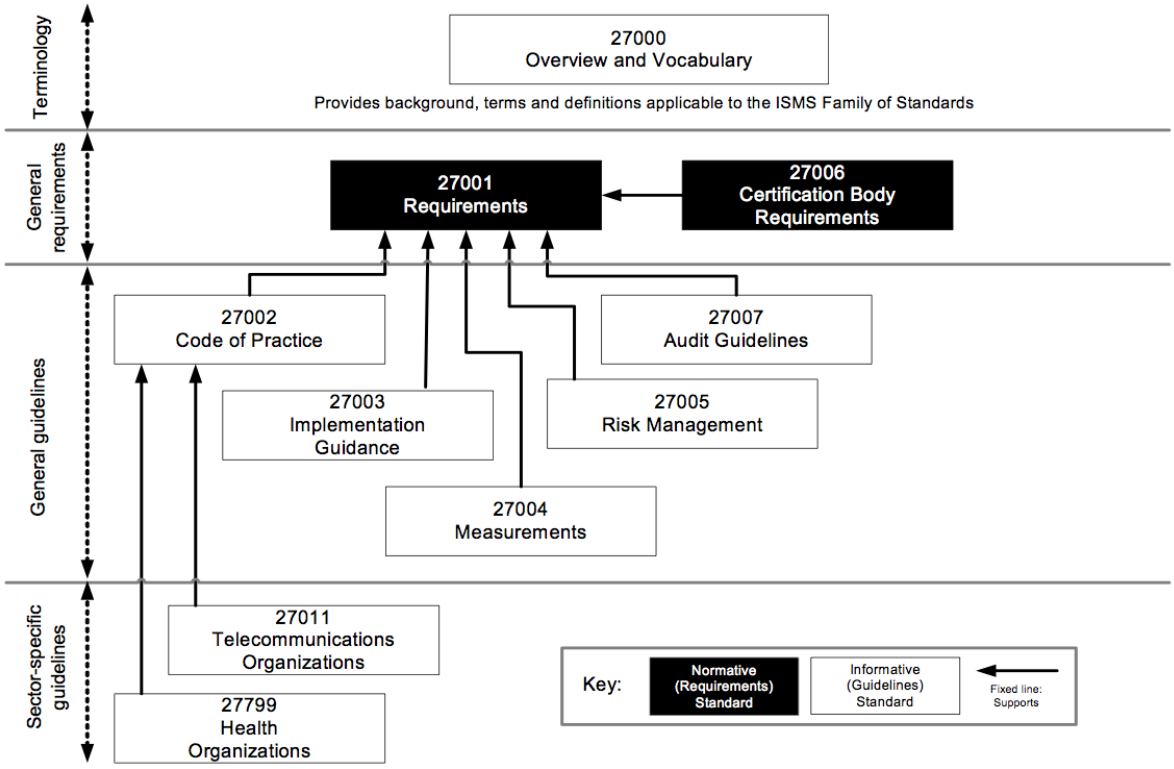


Abbildung 4.1: Zusammenhang der ISO/IEC 27000 Familie[ISOb]

- *ISO 27001 - Information security management systems - Requirements:*
  Es wird ein Modell vorgestellt, mit dem ein ISMS geplant, erstellt, betrieben, überwacht und verbessert werden kann. Es ist implementierungs- und produktunabhängig und für sehr kleine bis internationale Organisationen anwendbar. Dieses Dokument ist die Grundlagen gegen die sich Organisationen zertifizieren lassen können.

- *ISO 27002 - Code of practice for information security management:*
  Die Verwendung von ISO 27002 und ISO 27001 geht Hand in Hand. Es werden eine Vielzahl von konkreten Maßnahmen und Kontrollmechanismen vorgestellt, die Anhand einer vorangegangenen Risikoanalyse ausgewählt und im ISMS umgesetzt werden. Er hilft Sicherheitsstandards und -management in einer Organisation zu entwickeln.

- *ISO 27003 - Information security management system implementation guidance:*
  Dieser Standard ist ein Leitfaden und eine Hilfestellung zum Entwurf und der Umsetzung eines Information Security Management Systems nach dem ISO 27001 Standard. Der PDCA-Zyklus wird genauer betrachtet und die Umsetzung auf Projektebene gehoben.

- *ISO 27004 - Information security management - Measurement:*
  Um die Wirksamkeit eines bereits etablierten ISMS beziffern und kontinuierlich verbessern zu können, unterstützt ISO 27004 die Entwicklung geeigneter Maßnahmen, Regeln und die Auswahl von Metriken.

- *ISO 27005 - Information security risk management:*
  Es werden systematische und gründliche Methoden beschrieben, wie Informationssicherheitsrisikomanagement in allen Arten von Organisationen durchgeführt werden kann. Ein spezieller Fokus liegt natürlich auf ISMS nach dem ISO 27001 Standard.

- *ISO 27006 - Requirements for bodies providing audit and certification of information security management systems:*
  Für jene Prüfstellen, die eine Prüfung oder Zertifizierung nach ISO 27001 vornehmen, gibt der Standard ISO 27006 die Leitlinien zur Durchführung und Kriterien für die Gültigkeit des Zertifikats vor. Es ist vorgesehen, dass dieser Standard gemeinsam mit ISO 27001, ISO 17021 („Conformity assessment - Requirements for bodies providing audit and certification of management systems“) und ISO 19011 („Guidelines for auditing management systems“) verwendet wird.

- *ISO 27007 - Guidelines for information security management systems auditing:*
  Als Leitlinie zur Unterstützung bei der Durchführung von ISMS Audits wurde ISO 27007 veröffentlicht. Er definiert auch Anforderungen an Auditoren, die die Anforderungen von ISO 27001, anhand von ISO 27006, überprüfen.[ISOb]

Zum Stand Ende September 2012 gibt es weltweit 7940 Organisationen die nach ISO/IEC 27001 zertifiziert sind, davon befinden sich über 52% der Organisationen in Japan. Österreichweit gibt es 42 ausgestellte Zertifikate, unter anderem für das „Bundesministerium für Finanzen, Sektion V – IT, Kommunikation und Öffentlichkeitsarbeit“, die Fabasoft AG oder Austrian Lotteries[Reg].

Die beiden Standards ISO/IEC 27001 und ISO/IEC 27002 sind international von großer Bedeutung. Sie sind Grundlage für viele weitere Vorgehensweisen im Information Security Management und werden deshalb nachfolgend noch näher betrachtet.

4.1.2 ISO/IEC 27001

In diesem internationalen Standard wird ein Modell für ein *Information Security Management System (ISMS)* zur Verfügung gestellt, mit dem es eingeführt, implementiert, betrieben, überwacht, überprüft und verbessert werden kann. Unabhängig von der Organisation und Größe des Unternehmens kann es ein ISMS aufbauen und betreiben, abgestimmt und skaliert auf die Bedürfnisse wie Sicherheitsanforderungen, angewandte Prozesse oder Ziele. Der Standard ist darauf ausgelegt eine konsistente Implementierung und Betrieb mit verwandten Management-Standards wie ISO 9001 („Quality management systems - Requirements“) und ISO 14001 („Environmental management systems - Requirements with guidance for use“) zu unterstützen[ISOc].

Um die Prozesse in einem ISMS zu strukturieren, wird das „Plan-Do-Check-Act“ (PDCA) Modell adaptiert und, wie in Abbildung 4.2 dargestellt, angewandt. Die Informationssicherheitsanforderungen und -erwartungen der Interessenten fließen als Eingabewerte in das Modell, das durch die notwendigen Prozesse und Aktionen eine an die Anforderungen und Erwartungen angepasste Informationssicherheit liefert. Vier Hauptprozesse werden im PDCA Modell eingesetzt[ISOc]:

- *Plan (ISMS planen/festlegen):* Um die Informationssicherheit zu verbessern und Risikomanagement betreiben zu können, werden Prozesse, Richtlinien, Prozeduren und Ziele definiert. Anschließend wird die Risikomanagementstrategie gewählt und die Risiken dementsprechend identifiziert, analysiert und bewertet, um danach passende Maßnahmenziele *(control objectives)* und Maßnahmen *(controls)* zur Risikobehandlung wählen zu können.

- *Do (ISMS umsetzen/betreiben):* Anhand eines zu erstellenden Risikobehandlungsplans werden die Maßnahmen in der Organisation umgesetzt, um die Maßnahmenziele zu erfüllen. Ebenso muss definiert werden wie die Effektivität der Maßnahmen gemessen werden kann. Der Betrieb eines ISMS bedeutet auch, dass Schulungsprogramme für die Mitarbeiter erstellt werden, die Arbeitsprozesse kontrolliert und genügend Ressourcen zur Verfügung gestellt werden.

- *Check (ISMS überwachen/überprüfen):* Um zeitnah Fehler, Sicherheitslücken und Störfälle erkennen zu können, muss das ISMS kontinuierlich überwacht und regelmäßig Revisionen unterzogen werden. Dabei werden die Ergebnisse der Effektivitätsmessungen der Maßnahmen, Sicherheitsaudits, Störfallberichte, Vorschläge und Rückmeldungen der Stakeholder berücksichtigt, um die Gesamteffektivität des ISMS zu bewerten.

- *Act (ISMS instandhalten/verbessern):* In diesem Prozess werden neue Verbesserungsmöglichkeiten im ISMS-Prozess implementiert. Es sollen korrigierende und präventive Maßnahmen ergriffen und diese mit den Verbesserungen den jeweiligen Personen mitgeteilt werden. Danach wird wiederum ermittelt, ob die eingesetzten Maßnahmen die intendierten Ziele erreichen.

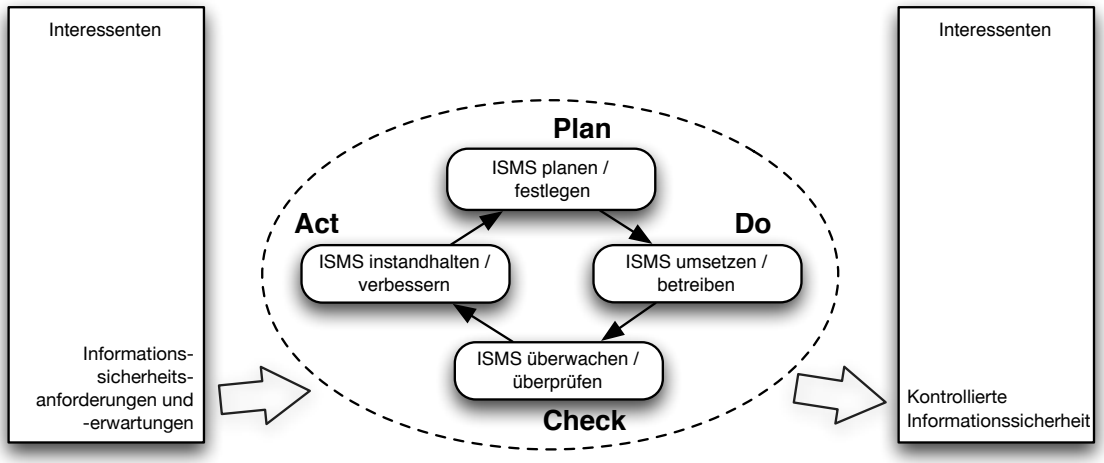


Abbildung 4.2: Das PDCA Modell auf ISMS-Prozesse angewandt[ISOc]

4.1.3 ISO/IEC 27002

Es werden für Organisationen generelle Verfahren und Richtlinien zum Initiieren, Implementieren, Instandhalten und Verbessern ihres Informationssicherheitsmanagements vorgestellt. Diese Ziele sind allgemein akzeptiert und können auf die meisten Organisationen angewandt werden. Sie dienen als gute Ausgangsbasis, um identifizierte Risiken adäquat zu behandeln, sollen aber auch anregen andere Verfahren aus unterschiedlichen Katalogen zu wählen oder eigene spezifische Richtlinien zu entwickeln, die zur individuellen Risikobehandlung förderlich sind[ISOd].

Der ISO 27002 Standard enthält 11 Abschnitte zu Sicherheitsmaßnahmen *(security control clauses)*, die insgesamt aus 39 Hauptsicherheitskategorien bestehen, sowie einen Abschnitt der in die Risikoeinschätzung und Risikobehandlung einführt[ISOd]. Nachfolgend werden die verschiedenen Abschnitte zur Sicherheit angeführt, um einen Überblick über die verschiedenen relevanten Themengebiete zu geben[BIT09]. In Klammer ist die jeweilige Anzahl an Sicherheitskategorien angegeben[ISOd]:

a) Sicherheitsleitlinie (1)

b) Organisation der Informationssicherheit (2)

c) Management der Organisationswerte (2)

d) Personalsicherheit (3)

e) Physische und umgebungsbezogene Sicherheit (2)

f) Betriebs- und Kommunikationsmanagement (10)

g) Zugangskontrolle (7)

h) Beschaffung, Entwicklung und Wartung von Informationssystemen (6)

i) Umgang mit Informationssicherheitsvorfällen (2)

j) Sicherstellung des Geschäftsbetriebs (1)

k) Einhaltung von Vorgaben (3)

Die Sicherheitskategorien in den unterschiedlichen Abschnitten beinhalten ein Maßnahmenziel und ein oder mehrere Maßnahmen zur Erfüllung dessen. Eine Maßnahme selbst wird immer durch drei Teile beschrieben: „Maßnahme“, „Implementierungsrichtlinie“ und „Weitere Informationen“. Im Teil „Maßnahme“ wird kurz und prägnant das jeweilige zu erreichende Ziel beschrieben. Die „Implementierungsrichtline“ schreibt nicht konkrete Handlungen vor, sondern erläutert das Ziel genauer, indem es verschiedene Teilaufgaben oder Teilziele aufzählt und beschreibt. Zusätzliche Informationen oder Verweise zu anderen Stellen im Standard beziehungsweise zur anderen Normen werden unter „Weitere Informationen“ dargestellt.

4.2 IT-Grundschutz des BSI

Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)*[4] ist die nationale Sicherheitsbehörde Deutschlands. Sie hat 1992 ihre Arbeit aufgenommen und widmet sich

[4] `https://www.bsi.bund.de`

seit dem gemäß §3 BSIG[5] unter anderem der „Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen“, „Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen“ oder „Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen“.

Mit dem „IT-Grundschutz“ hat das BSI einen kostenlosen und frei verfügbaren Leitfaden mit Werkzeugen und Methoden herausgegeben, um ein „angemessenes Sicherheitsniveau“ zu erreichen. Um dieses Sicherheitsniveau nach außen hin dokumentieren zu können, kann sich eine Organisation nach „ISO 27001“ auf der Basis von IT-Grundschutz zertifizieren lassen. Die *IT-Grundschutz-Standards (BSI-Standards)* und die *IT-Grundschutz-Kataloge* sind Grundlage für diesen Prozess[Grua]:

- *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS):*
  Dieser Standard ist vollständig kompatibel zum ISO 27001 Standard und beschreibt die Anforderungen, die an ein ISMS gestellt werden. Die eher generellen Aussagen aus ISO 27001 werden hier konkreter und praxisbezogener erläutert.

- *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise:*
  Die Anforderungen aus 100-1 werden in diesem Standard im ISMS erfüllt und umgesetzt. Es wird beschrieben wie ein ISMS in der Praxis geplant, aufgebaut und erhalten werden kann. Konkrete Hinweise, wie etwas umgesetzt werden könnte, werden durch die IT-Grundschutz-Kataloge gegeben, die Bestandteil der IT-Grundschutz-Vorgehensweise sind.

- *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz:*
  Ein Ziel der IT-Grundschutz-Vorgehensweise ist ein gutes und relativ leicht erreichbares Sicherheitsniveau durch Standard-Sicherheitsmaßnahmen. Für viele Systeme oder Organisationen ist diese Vorgehensweise ausreichend. Benötigt man aber

[5]Deutsches BGBl Nr. 54/2009

ein darüber hinausgehendes Sicherheitsniveau, muss eine detaillierte Risikoanalyse einer Maßnahmenauswahl vorausgehen. Dazu bietet der BSI-Standard 100-3 eine Vorgehensweise an, die mit dem vorhandenen IT-Grundschutz und dessen Analyse harmoniert.

- *BSI-Standard 100-4: Notfallmanagement:*
  Dieser Standard betrifft das *Business Continuity Management* und hilft bei der Umsetzung eines Notfallmanagements für Organisationen. Eine angemessene Reaktion auf Ereignisse und die richtige Einbindung in das ISMS ist wichtig, um den potentiellen Schaden möglichst gering halten zu können.

- *Baustein-Kataloge:* Durch eine Vielzahl an definierten Bausteinen ist es für eine Organisation leicht möglich ihre Struktur zu modellieren – sowohl Prozesse (z.B.: „B 1.6 Schutz vor Schadprogrammen“), als auch konkrete Komponenten (z.B.: „B 3.404 Mobiltelefon“ oder „B 2.4 Serverraum“). Für jeden dieser Bausteine gibt es eine allgemeine Beschreibung für dessen Einsatzzweck, sowie die Abbildung der Gefährdungslage mit Verweise auf die Gefährdungs-Kataloge und den daraus resultierenden Maßnahmenempfehlungen aus den Maßnahmen-Katalogen. Bausteine sind eingeteilt in die Kategorien analog zum IT-Grundschutz-Schichtmodell: „Übergreifende Aspekte“, „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“.

- *Gefährdungs-Kataloge:* Jede Gefährdung besitzt eine genauere Beschreibung, wie sie sich auf die Sicherheit auswirken kann und wird mit einem praktischen Beispiel verdeutlicht. Gefährdungen sind eingeteilt in die Kategorien: „Höhere Gewalt“, „Organisatorische Mängel“, „Menschliche Fehlhandlung“, „Technisches Versagen“ und „Vorsätzliche Handlungen“.

- *Maßnahmen-Kataloge:* Neben einer ausführlichen Beschreibung was erzielt werden soll wird angegeben, welche Person oder Gremium verantwortlich ist für die Initiierung und Umsetzung der Maßnahme. Zusätzlich gibt es ergänzende Kon-

trollfragen oder Prüffragen, die bei einer korrekten Umsetzung helfen. Maßnahmen sind eingeteilt in die Kategorien: „Infrastruktur“, „Organisation“, „Personal“, „Hardware und Software“, „Kommunikation“ und „Notfallvorsorge“.

Um Organisationen zu motivieren sich nach ISO 27001 auf der Basis von IT-Grundschutz zertifizieren zu lassen, wurden zwei Vorstufen eingeführt, die Anreize für eine schrittweise Umsetzung geben. Mit dem zwei Jahre gültigen Auditor-Testat „IT-Grundschutz-Einstiegsstufe“ wird bescheinigt, dass die unabdingbaren Standard-Sicherheitsmaßnahmen (ca. 55%) realisiert worden sind. Das Auditor-Testat „IT-Grundschutz-Aufbaustufe“ ist ebenfalls zwei Jahre lang gültig und stellt sicher, dass die wichtigsten Standard-Sicherheitsmaßnahmen (ca. 72%) realisiert wurden. Beide Testate können nicht verlängert werden. Das ISO 27001 Zertifikat auf Basis von IT-Grundschutz erfordert ca. 82% der bereitgestellten Maßnahmen und ist drei Jahre lang gültig, wobei danach wiederholt zertifiziert werden kann[Grub].

4.3 Österreichisches Informationssicherheitshandbuch

Das „Österreichische Informationssicherheitshandbuch“ richtet sich sowohl an die öffentliche Verwaltung als auch an die Privatwirtschaft und bietet Unterstützung bei der Einführung, Umsetzung und Aufrechterhaltung eines Informationssicherheits-Managementsystems. Es ist stark angelehnt an ISO/IEC 27001, unter Einbeziehung des IT-Grundschutz und Arbeiten von MELANI (Melde- und Analysestelle Informationssicherung)[6] und CASES (Cyberworld Awareness Security Enhancement Services)[7]. Es ist kostenlos über die Webseite des Bundeskanzleramt Österreich (BKA)[8] verfügbar[9]. 2001 wurde das „IT-Sicherheitshandbuch für die öffentliche Verwaltung“ in „Österreichisches IT-Sicherheitshandbuch“ geändert[SBH02]. Im Auftrag des BKA hat das Zentrum für

[6] `https://www.melani.admin.ch/`
[7] `https://www.cases.lu/`
[8] `https://www.bka.gv.at/`
[9] `https://www.sicherheitshandbuch.gv.at`

sichere Informationstechnologie - Austria (A-SIT)[10] die Fassung des Informationssicherheitshandbuchs aus dem Jahr 2007 grundlegend überarbeitet und es im Jahr 2010 in der Version 3 neu veröffentlicht. Damit wurde der Aufbau aus den zwei Teilen „Informationssicherheitsmanagement“ und „Informationssicherheitsmaßnahmen“ geändert und mehr an die ISO/IEC 27001 Norm angepasst. Es besteht nun in der Version 3 aus 15 Kapiteln, wobei Kapitel 2 und 3 Anleihe an ISO/IEC 27001 nehmen und die Anforderungen für das Informationssicherheits-Managementsystem beschreiben und die Kapitel 4 bis 15 auf die konkreten Maßnahmen wie in ISO/IEC 27002 eingehen, um das ISMS umzusetzen[SIH10].

Der Informationssicherheitsmanagementprozess, wie in Abbildung 4.3 dargestellt, ist der zentrale Ablauf, um die Informationssicherheit in der Organisation zu etablieren, aufrechterhalten oder zu verbessern. Fünf Hauptaktivitäten bilden das Rahmenwerk für den Prozess[SIH10]:

1. *Entwicklung einer organisationsweiten Informationssicherheitspolitik:* Dieses Dokument ist der Leitfaden und die Grundlage für eine langfristige Informationssicherheitspolitik, die die Werte, Ziele und Organisation der Institution berücksichtigt. Es ist allgemein gehalten und nennt keine konkreten Maßnahmen oder Umsetzungen, diese werden separat ausgearbeitet.

2. *Risikoanalyse:* Drei verschiedene Risikoanalysestrategien werden vorgestellt, um die vorhandenen und zukünftigen Risiken finden, bewerten und behandeln zu können. Bei der *detaillierten Risikoanalyse* wird für jedes System ein genauer Risikoanalyseprozess durchgeführt, der zu einer individuellen und optimalen Lösung führt, aber dadurch langwierig und kostenintensiv ist. Im Gegensatz dazu wird beim *Grundschutzansatz* von einer pauschalen Gefährdungslage für alle Systeme ausgegangen, zu einer raschen Umsetzung eines guten Sicherheitsniveaus führt. Allerdings kann dieses Sicherheitsniveau für bestimmte Systeme nicht ausreichend

[10] `https://www.a-sit.at`

sein. Deshalb verbindet der *kombinierte Ansatz* die Vorteile der beiden anderen Analysemethoden. Hier werden durch eine vorausgehende Sicherheitsanalyse jene Systeme bestimmt, die einen erhöhten Sicherheitsbedarf haben und diese einer detaillierten Risikoanalyse zugeführt. Für die restlichen Systeme wird ein Sicherheitsniveau nach dem Grundschutzansatz umgesetzt.

3. *Erstellung eines Sicherheitskonzeptes:* Nachdem die Risiken für die Systeme ermittelt wurden, werden nun die erforderlichen Maßnahmen ausgewählt, um die Risiken auf ein akzeptables Niveau zu bringen. Zur Umsetzung der Maßnahmen werden kurz-, mittel- und langfristige Aktionen ausgeführt und in einem Informationssicherheitsplan dargestellt. Für einzelne wichtige Anwendungen oder IT-Systeme müssen spezifische Sicherheitsrichtlinien erstellt werden, die die konkreten Aktionen oder Vorgehensweisen darlegen.

4. *Umsetzung des Informationssicherheitsplans:* Die gewählten Maßnahmen können technischer, organisatorischer oder personeller Natur sein und müssen in einem entsprechenden Rahmen innerhalb der Organisation umgesetzt werden. Ein sehr wichtiger Bestandteil sind die eigenen Mitarbeiter, diese gehören diesbezüglich geschult beziehungsweise ausgebildet. Sind alle Maßnahmen umgesetzt, müssen sie abgenommen und ein System zur Feststellung ihrer Effektivität erstellt werden.

5. *Informationssicherheit im laufenden Betrieb:* Informationssicherheit kann mittel- oder langfristig nicht durch eine einmalige Aktion erreicht werden. Es bedarf einer kontinuierlichen Überwachung und Prüfung der Sicherheitsziele sowie ihrer Maßnahmen und Aktionen. Sicherheitseinrichtungen müssen gewartet werden, Netzwerke und Systeme einem Monitoring unterzogen werden, sowie auf auftretende Ereignisse richtig und möglichst schnell reagiert werden.

Es ist keine Zertifizierung nach dem Österreichischen Informationssicherheitshandbuch möglich, allerdings werden bei Einhaltung bereits viele wichtige Schritte zu einer ISO/IEC 27001 Zertifizierung gesetzt. Darüber hinaus ist das Informationssicherheitshandbuch

auf gesetzliche Bedürfnisse und Normen in Österreich ausgelegt und beinhaltet hilfreiche Verweise oder Auszüge, sowie eine Sammlung von Mustern für Verträge, Verpflichtungserklärungen und Dokumentationen.

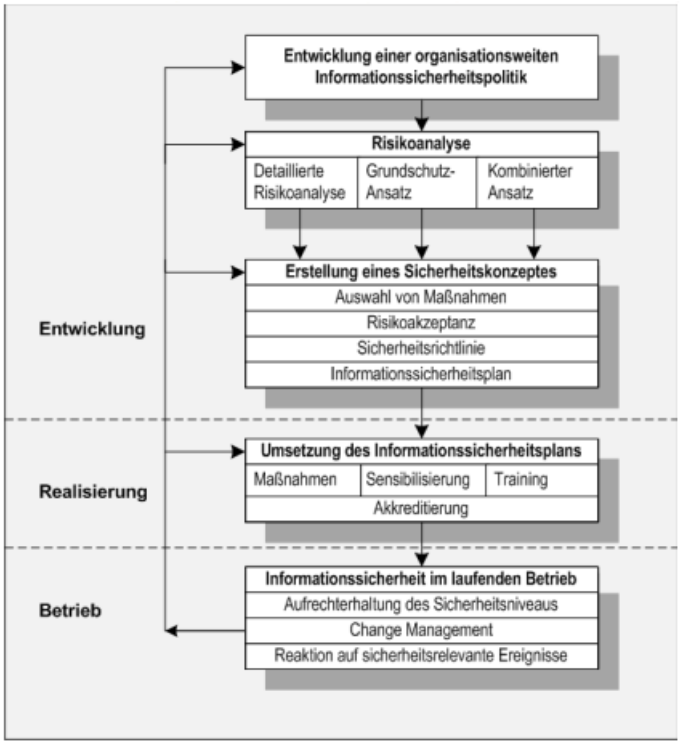


Abbildung 4.3: Der Informationssicherheitsmanagementprozess des Österreichischen Informationssicherheitshandbuchs[SIH10]

4.4 Common Criteria

Die *Common Criteria (CC)* sind international harmonisierte Kriterien zur Evaluierung von IT-Produkten auf ihre Sicherheit. Sie entwickelten sich aus den U.S. *Trusted Computer System Evaluation Criteria (TCSEC)*, den *Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)* und dem europäischen Pendant, den *Information Technology Security Evaluation Criteria (ITSEC)*, im Jahr 1996. Durch kontinuierliche Weiterentwicklung wurde 1999 die Version 2.1 veröffentlicht und als ISO/IEC 15408

Standard veröffentlicht[MB04]. Aktuell liegen die Common Criteria in der Version 3.1 Release 4 vor[CC].

Es werden drei verschiedene Hauptzielgruppen adressiert[CCP12a]:

- *Konsumenten:* Anhand der CC sollen die Konsumenten erkennen können, ob das evaluierte Produkt ihren Sicherheitsbedürfnissen entspricht. Durch die standardisierte Evaluierung ist ein Vergleich verschiedener Produkte (*Target of Evaluation (TOE)*) möglich. Der Einsatz von *Protection Profiles (PP)* erlaubt es, die implementierungsunabhängigen Sicherheitsanforderungen in einer eindeutigen Weise zu beschreiben.

- *Entwickler:* Auf Basis eines oder mehrerer PP werden implementierungsabhängige Sicherheitsanforderungen (*Security Targets (ST)*) erstellt, um den Sicherheitsanforderungen der Konsumenten zu genügen, die in den Protection Profiles genannt werden. Die Entwickler werden zusätzlich unterstützt in der Vorbereitung, damit die geforderten Nachweise im Evaluierungsprozess präsentiert werden können.

- *Evaluatoren:* Es werden durch die CC generelle Kriterien skizziert, die von Evaluatoren verwendet werden, um die Konformität des TOE mit den Sicherheitsanforderungen sicherzustellen.

Die Common Criteria v3.1 bestehen aus drei zusammenhängenden Dokumenten[Cad11]:

1. *Teil 1 - Introduction and general model:*
   Beinhaltet die Einführung zu CC, generelle Konzepte und Prinzipien zur Evaluierung von IT-Sicherheit sowie ein allgemeines Vorgehensmodell. Es zeigt Konstrukte auf, um die Sicherheitsanforderungen zu definieren und zu wählen, Spezifikationen auf hoher Ebene zu schreiben und die IT-Sicherheitsziele auszudrücken.

2. *Teil 2 - Security functional requirements:*
   Führt eine Menge von Standardausdrucksweisen ein, um die funktionalen Anfor-

Stufe	*Bedeutung*
EAL1	funktionell getestet
EAL2	strukturell getestet
EAL3	methodisch getestet und geprüft
EAL4	methodisch entworfen, getestet und überprüft
EAL5	semiformal entworfen und getestet
EAL6	semiformal verifizierter Entwurf und getestet
EAL7	formal verfizierter Entwurf und getestet

Tabelle 4.1: Zusammenfassung der EAL1 - EAL7 [CCP12b]

derungen des TOE beschreiben zu können. Dazu werden Komponenten, Klassen und Familien verwendet.

3. *Teil 3 - Security assurance requirements:*
   Führt eine Menge von Standardausdrucksweisen ein um die Anforderungen an die Vertrauenswürdigkeit des TOE beschreiben zu können. Zusätzlich werden Evaluationskriterien für Protection Profiles und Security Targets präsentiert sowie die Vertrauenswürdigkeitsstufen.

Es sind sieben hierarchisch aufgebaute Vertrauenswürdigkeitsstufen für ein TOE vorhergesehen: die *Evaluation Assurance Level (EAL) 1 - 7*. Je höher der EAL ist, desto genauer und formaler wurde geprüft. Der Kunde kann somit ein höheres Vertrauen in das Produkt setzen und sicher sein, dass es den Sicherheitsanforderungen entspricht[CCP12b]. Damit für eine internationale Verwendung des Produkts keine Mehrfachzertifizierung möglich ist, haben im Mai 2010 insgesamt 27 Staaten eine Vereinbarung unterschrieben, gegenseitig Zertifizierungen bis inklusive EAL4 anzuerkennen[Bun13]

Kapitel 5

Erweiterungsmöglichkeiten des Österreichischen Informationssicherheitshandbuchs in Bezug auf Data Loss Prevention

Im Rahmen dieser Masterarbeit sollte eine Informationssicherheitsnorm oder Informationssicherheitsvorgehensweise ausgewählt und überprüft werden, in wieweit Konzepte oder Maßnahmen von Data Loss Prevention enthalten und die identifizierten Gefahrenkanäle berücksichtigt worden sind. Im Gegensatz zu dessen Vorlage, der ISO/IEC 27001 Norm, ist das Österreichische Informationssicherheitshandbuch kostenlos über das Bundeskanzleramt Österreich beziehbar und bietet eine gute Grundlage in kompakterer Form als der deutsche IT-Grundschutz. Es berücksichtigt in der beschriebenen Vorgehensweisen österreichische Regelungen wie Gesetzestexte, nationale Normen (z.B.: Vernichtung von Akten und Daten, Brandschutz, Sicherheitstüren und einbruchhemmende Türen), IKT-Board Beschlüsse oder Verordnungen. Aufgrund des vorherrschenden Interesse für die Sicherheitslage in der heimischen IT-Landschaft und des

passenden Gesamtpakets des Österreichischen Informationssicherheitshandbuchs wurde diese österreichische Vorgehensweise ausgewählt und überprüft.

An dieser Stelle sei festgehalten, dass im Informationssicherheitshandbuch die Konzepte und Maßnahmen von Intrusion Detection Systeme explizit zu finden, im Gegensatz dazu aber Extrusion Detection Systeme, Data Loss Prevention, Data Leakage Detection oder synonyme Begriffe, beziehungsweise die gesamten Konzepte dahinter, *nicht* erwähnt werden. Dieser Umstand bedeutet aber nicht, dass die Umsetzung des Österreichischen Informationssicherheitshandbuchs keine Maßnahme zum Schutz der sensiblen Informationen in Unternehmen darstellt. Da es auf ISO/IEC 27001 und IT-Grundschutz basiert, enthält es wohldurchdachte, umfangreiche, aber auch manchmal sehr allgemein gehaltene Prozesse und Maßnahmen, die den Datenfluss nach außen reglementieren oder beschränken.

Nachfolgend werden einige Stärken des Informationssicherheitshandbuchs in Bezug auf DLP erläutert und Maßnahmen und Prozesse exemplarisch beschrieben, um wichtige Sicherheitsmaßnahmen für verschiedene Gefahrenkanäle darstellen zu können. Anschließend werden neue Erweiterungsmöglichkeiten vorgestellt, damit das Österreichische Informationssicherheitshandbuch im Bereich der Data Loss Prevention mehr Sicherheit bietet.

5.1 Stärken

Bei Data Loss Prevention steht die *Vertraulichkeit* von Daten als Schutzziel im Mittelpunkt. Da die internationalen Normen und Vorgehensweisen auf verschiedene Schutzziele der Informationssicherheit eingehen, stellen einige Prozesse und Maßnahmen des Informationssicherheitshandbuchs adäquaten Schutz der Vertraulichkeit von Daten zur Verfügung.

5.1.1 ISMS Prozess

> *„Informationssicherheit entsteht nicht von selbst aus Technik oder Know-How, sondern zunächst aus dem Bewusstsein des Managements und der Mitarbeiter/innen einer Organisation, dass Informationen schützenswerte und gefährdete Werte für alle Beteiligten darstellen.“* [SIH10, Seite 24]

> *„Die Mitarbeiter/innen stellen eine der wichtigsten Ressourcen einer Organisation dar. IT-Sicherheit kann auch bei den besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter/innen ein ausgeprägtes Sicherheitsbewusstsein haben und bereit und fähig sind, die Vorgaben in der täglichen Praxis umzusetzen. Andererseits stellen Mitarbeiter/innen auch potentielle Angriffs- oder Fehlerquellen dar.“*[SIH10, Seite 190]

Ein Grund, weshalb das Österreichisches Informationssicherheitshandbuch wirksam und erfolgreich erscheint, ist dadurch begründet, dass es das Thema der Informationssicherheit nicht als eine einmalige Aufgabe einer IT-Abteilung betrachtet, sondern als einen sich wiederholenden Ablauf unter Einbindung der gesamten Organisation inklusive aller Mitarbeiter. Dabei kommt der Managementebene eine besondere Bedeutung zu. Es muss die Gesamtverantwortung übernehmen und einen Prozess zum Management von Informationssicherheit etablieren.

Ausgehend von der Managementebene müssen die Mitarbeiter der Organisation sensibilisiert und geschult werden. Sie sollen die Bedeutung und Wichtigkeit von Informationssicherheit für das Unternehmen erkennen, verstehen wie die Risiken analysiert wurden, welche entsprechenden Sicherheitsmaßnahmen warum ausgewählt wurden und welche Konsequenzen es bei Verstößen gegen die Sicherheitsvorgaben gibt. Sie sind ein wichtiger Teil im gesamten Informationssicherheitsprozess. Erreicht werden kann dieser durch Sensibilisierungsmaßnahmen wie regelmäßige Informationsveranstaltungen oder Druckwerke. Zusätzlich sollte es spezielle Schulungen für Personen geben, die in ihrer Tätigkeit besonders mit Informationssicherheit konfrontiert werden.

Um Informationen schützen zu können, müssen sie entsprechend ausgezeichnet und der Umgang mit ihnen festgelegt werden. Deshalb verlangt das Informationssicherheitshandbuch eine Definition von Vertraulichkeitsklassen und den dazugehörigen Regeln für den Umgang, wie zum Beispiel: die Art der Kennzeichnung, Übermittlung, Lagerung, Speicherung, Weitergabe oder Deklassifizierung. Dabei verweist es auf die Vorschläge und Bestimmungen des InfoSiG und DSG wie in Abschnitt 1.7 auf Seite 17 beschrieben.

5.1.2 Remote Access

Remote Access ist im Informationssicherheitshandbuch als „jede Art von Fernzugriff auf Geschäftsinformationen [...] über ein unsicheres resp. öffentliches Netz gemeint“[SIH10, Seite 321]. Erreicht wird dieser Fernzugriff meist mittels VPN-Verbindungen. Dem großen Bedrohungspotential von Remote Access Verbindungen wird Rechnung getragen, in dem sich drei Kapitel ausführlich mit Konzeption, Implementierung und sicheren Betrieb von VPN-Systemen auseinandersetzen (10.6.10 bis 10.6.12). Aus dem Ergebnis einer Anforderungsanalyse werden ein organisatorisches Konzept, ein technisches Konzept und ein Sicherheitskonzept erstellt. Dabei müssen wichtige Punkte wie Schutzbedarf, Verschlüsselung, Benutzerkreis, Richtlinien oder Berechtigungskonzept ausgearbeitet werden. Anschließend muss eine geeignete VPN-Systemarchitektur ausgewählt werden, die danach sicher installiert und konfiguriert wird.

Wie in Abschnitt 1.4 beschrieben wurde, geht von Fernwartungen über Remote Access ein erhebliches Risiko aus. Mit einem eigenen Kapitel „12.7.3 Fernwartung“ geht das Informationssicherheitshandbuch auf diese Thematik ein und empfiehlt verschiedene Maßnahmen, zum Beispiel: „Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne“.

5.1.3 Laptops

Für den sicheren Umgang mit Laptops beziehungsweise für deren sichere Einbindungsweise in die IT-Landschaft stellt das Österreichische Informationssicherheitshandbuch ausreichend Informationen zur Verfügung.

Während im Kapitel „9.5.4 Nutzung und Aufbewahrung mobiler IT-Geräte“ allgemeiner darauf hingewiesen wird wie mobile IT-Geräte außer Haus physisch geschützt werden sollen, wird in „11.7 Mobile Computing und Telearbeit“ konkreter auf verschiedenste Gefahren und Maßnahmen (für Laptops in „11.7.1.1 Laptop, Notebook“) eingegangen. So werden bei den typischen Gefährdungen unter anderem folgende Punkte angeführt: „Verlust, Diebstahl“, „Gefährdung durch Reinigungs- oder Fremdpersonal“, „Unzureichender Umgang mit Passwörtern“ oder „Unberechtigte Datenweitergabe“. Als Maßnahmenempfehlungen werden angegeben, dass eine „Richtlinie für die Nutzung von Laptops“ erstellt wird, um zu regeln welche Einsatzszenarien geplant sind, wie die Anbindung ans Organisationsnetzwerk gestaltet wird oder wie die Verbindung zum Internet erlaubt wird. Beschaffung, Installation und Konfiguration der Hardware und Software muss kontrolliert und sicher ablaufen, damit eine Basis für den sicheren Betrieb geschaffen werden kann. Virenschutzprogramme müssen die Virenfreiheit feststellen, bevor ein Laptop direkt am Organisationsnetzwerk oder über VPN angeschlossen werden darf/kann.

5.1.4 Mobile Speichermedien

Um stets eine Übersicht der eingesetzten Speichermedien zu haben, wird eine Bestandsliste empfohlen. Darüber hinaus müssen „Archiv- und Backup-Datenträger“, „Datenträger für den Austausch mit externen Kommunikationspartnern“, „Externe Festplatten, USB-Sticks, Smartphones für den mobilen Einsatz“ dezidiert als Vermögenswerte in der Strukturanalyse erfasst werden, siehe Kapitel „7.1 Vermögenswerte“ im Informationssicherheitshandbuch.

Der gesamte Lebenszyklus von mobilen Speichermedien (im Informationssicherheitshandbuch auch oft „Datenträger“ genannt) wird im Kapitel „10.7 Betriebsmittel und Datenträger“ dargestellt und es wird beschrieben, wie die einzelnen Phasen möglichst sicher zu gestalten sind. Bereits vor dem Einsatz der Datenträger ist ein Prüfverfahren vorgesehen. Es wird öfters darauf hingewiesen, dass Datenträger prinzipiell nur verschlüsselt versandt werden dürfen und immer auf eine irreversible Löschung geachtet werden muss, damit die Daten nicht wieder hergestellt werden können. Bevor ein Datenträger schlussendlich ausgeschieden wird, ist ebenfalls auf die korrekte und irreversible Löschung zu achten. Darüber hinaus befinden sich zusätzliche Informationen im Kapitel „7.1.3.6 Absicherung von Wechselmedien“ im Informationssicherheitshandbuch.

5.2 Erweiterungsmöglichkeiten

Wie bereits zuvor beschrieben bietet die Vorgehensweise nach dem Österreichischen Informationssicherheitshandbuch grundsätzlich einen guten Schutz. Allerdings unterliegen heutzutage sowohl die Bedrohungsszenarien als auch der technologische Fortschritt einem immer schneller werdenden Wandel. Diesem Umstand versucht das Informationssicherheitshandbuch Rechnung zu tragen, indem meist allgemeine und technologiebeziehungsweise produktunabhängige Formulierungen verwendet werden, doch das ist nicht immer ausreichend. So wie das erstellte Sicherheitskonzept kontinuierlich evaluiert und an neue Gegebenheiten angepasst werden muss, bedarf es auch einer regelmäßigen Anpassung des Österreichischen Informationssicherheitshandbuchs an veränderte oder neue Situationen.

5.2.1 Data Loss Prevention als Faktum

Die Begriffe wie „Data Loss Prevention“, „Extrusion Detection Systeme“ oder sinnverwandte Bezeichnungen finden sich im Informationssicherheitshandbuch nicht wieder.

Einzelne Komponenten wie Prozesse oder Maßnahmen sind vorhanden und werden nachfolgend nicht erschöpfend beschrieben. Es gibt ein eigenes Kapitel „10.10.6 Intrusion Detection Systeme“, analog dazu könnte man ein neues Kapitel „10.10.7 Extrusion Detection Systeme“ hinzufügen. Das Kapitel „10.10.7 Zeitsynchronisation“ müsste dazu neu nummeriert werden: „10.10.8 Zeitsynchronisation“. Das neue Kapitel könnte wie folgt hinzugefügt werden.

10.10.7 Extrusion Detection Systeme

ISO Bezug: 27002 10.6.1, 10.10.2, 15.1.4, 15.1.5
Aufgabe von Extrusion Detection Systemen ist die Überwachung bzw. Analyse des Datenverkehrs bzw. der Aktivitäten auf IT-Systemen, mit dem Ziel, unerlaubte Informationsflüsse aus der Organisation und unerlaubte Informationsverwendungen zu erkennen, weiterzumelden und gegebenenfalls Gegenmaßnahmen einzuleiten.

Dies umfasst folgende Teilaufgaben:

- *Auffinden von Daten:*
  Aktive oder passive Sammlung der wesentlichen Ereignisdaten aus gespeicherten Daten, Netzpaketen oder Daten die in Verwendung sind
- *Erkennen von schützenswerten Daten:*
  Untersuchung der gespeicherten Aktivitäten auf Verstöße gegen die Informationssicherheitspolitik oder systemspezifischer Sicherheitsrichtlinien durch den Kontext („Context Based Systems“) oder Inhalt („Content Based Systems“) der Daten
- *Speicherung der erkannten Daten*
- *Durchsetzen von Richtlinien:*
  Generierung von Warnmeldungen und Durchsetzen von Gegenmaßnahmen entsprechend der Richtlinien

Im Unterschied zu Intrusion Detection Systemen, die Eindringversuche im Netzwerk oder IT-Systeme erkennen, unterstützen Extrusion Detection Systeme die Erkennung

unberechtigter Informationsflüsse und Informationsverwendungen, sowohl externer als auch interner Benutzer, innerhalb eines lokalen oder logischen Netzes oder auf IT-Systemen.

Extrusion Detection Systeme können andere Sicherheitsmaßnahmen wie Authentisierung, Zugriffsschutzsysteme, Firewalls und Intrusion Detection Systeme nicht ersetzen, sie können jedoch zu einer weiteren Erhöhung des Schutzes der Vertraulichkeit von Informationen, insbesondere in sensiblen Bereichen, beitragen.

Im Informationssicherheitshandbuch ist es üblich, dass die beschriebenen Maßnahmen auf die jeweiligen Kapitel in der ISO/IEC 27002 Norm verweisen. Eigentlich müsste die neue Beschreibung von Extrusion Detection Systeme auch auf die ISO/IEC 27002 Kapitel „10.7.3 Information handling procedures“, „10.8.1 Information exchange policies and procedures“ und „10.8.4 Electronic messaging“ verweisen, da Extrusion Detection Systeme das Ziel der ISO Maßnahmen unterstützten. Allerdings lassen diese Kapitel einen gewissen Interpretationsspielraum zu, deshalb sollte bei den angeführten Implementierungsrichtlinien dezidierter darauf eingegangen werden, dass nur erlaubte Datenflüsse möglich sind und die internen Richtlinien zur Anwendung kommen. Damit könnten auch Extrusion Detection Systeme oder DLP-Konzepte Einzug in die ISO/IEC 27002 Norm finden und ihre Sicherheit in Bezug auf Vertraulichkeit der Daten erhöhen. Dieser Umstand sollte in diesem Zusammenhang nur kurz aufgezeigt werden, eine nähere Betrachtung beziehungsweise Einbringung von Verbesserungsvorschlägen ist nicht Gegenstand dieser Arbeit.

5.2.2 E-Mail

Für die Verwendung von E-Mail als Medium für Kommunikation beziehungsweise Datenaustausch findet man im Österreichischen Informationssicherheitshandbuch viele Informationen. Sehr zum Vorteil von Data Loss Prevention wird im Kapitel „10.8.2

Festlegung einer Sicherheitspolitik für E-Mail-Nutzung“ festgelegt, dass die E-Mail-Sicherheitspolitik beschreiben muss „bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Informationen per E-Mail versandt werden dürfen“[SIH10, Seite 364]. Die Betrachtung dieses und der zugehörigen Kapitel lässt den Schluss zu, dass diese Bestimmung auf einer Richtlinien-Ebene bleibt und nicht durch technische Maßnahmen unterstützt wird. Hier fehlen klare Verweise darauf, dass es mittlerweile Lösungen gibt, die ausgehende Daten entsprechend ihrer Klassifikation oder durch trainierte Algorithmen erkennen können und entsprechend der Richtlinien Maßnahmen einleiten.
Weiters wird darauf hingewiesen, dass festgelegt werden muss ob, und wenn ja wann, Attachements oder ganze E-Mails verschlüsselt übertragen werden dürfen. Es wird erwähnt, dass eine Prüfung auf Viren (die auch bei ausgehenden E-Mails vorgeschrieben wird) behindert oder ganz verhindert wird, aber es fehlt der Hinweis, dass durch die Verschlüsselung auch DLP-Systeme die Daten nicht mehr erkennen und schützen können. Dazu müsste das DLP-System nach dem „Man-in-the-Middle“ Konzept eingesetzt werden, um Zugang zu den Daten zu erhalten. Besser wäre es die Verschlüsselung erst am E-Mail-Server, und somit für die Endbenutzer transparent, durchzuführen. Dabei ist auf eine sichere Übertragung bis zum E-Mail-Server zu achten.

Im Kapitel „10.8.3 Regelung für den Einsatz von E-Mail und anderen Kommunikationsdiensten“ des Österreichischen Informationssicherheitshandbuchs wird die Verwendung von Virenscannern vorgeschrieben: „[. . .] Vor dem Absenden bzw. vor der Dateiübermittlung sind die ausgehenden Dateien explizit auf Viren zu überprüfen“[SIH10, Seite 366]. In diesem Kapitel bedarf es einer Vorschreibung für die Verwendung von Extrusion Detection Systeme. Eine Möglichkeit ist:

- *Verwendung von Extrusion Detection Systemen für ausgehende E-Mails und Anhänge: Vor dem Absenden bzw. vor der Dateiübermittlung sind die Inhalte der ausgehenden E-Mail sowie deren optionale Anhänge explizit durch ein Extrusion Detection System auf die Einhaltung der Richtlinien entsprechend ihrer Sicherheitsklasse zu überprüfen.*

Für die konkrete Umsetzung ist zu beachten, dass es Lösungen für das Netzwerk oder den Endpunkt gibt, siehe Abschnitt 3.2. Wird die Maßnahme auf den Endgeräten umgesetzt, kann das Konzept *„User Driven Security“*, beschrieben in [Cha11] und [TIT11], angewandt werden. Dabei kommt es zu einer starken Einbindung der Mitarbeiter in den Sicherheitsprozess. Es kann selbst bestimmt werden, welche Sicherheitsklasse das E-Mail besitzt (wenn es durch die Informationssicherheitspolitik erlaubt wird), und das Extrusion Detection System kann Warnungen oder Vorschläge anzeigen, wenn unerlaubte Empfänger oder eine höhere Sicherheitsklasse erkannt wird. Dadurch erfolgt eine wichtige Sensibilisierung für den Benutzer. Gemachte Fehler können selbst ausgebessert werden oder es kann, unter Angabe entsprechender Gründe, die Warnung verworfen werden, um den Geschäftsprozess fortzusetzen. Diese Aktion muss natürlich protokolliert werden und kann somit die verantwortlichen Personen auf unbefugten Informationsfluss hinweisen, aber kann auf der anderen Seite auch als Lernfaktor für das eingesetzte System dienen oder ein Anstoß für die Überarbeitung der Richtlinien auf Praktikabilität sein.

Auch im Kapitel „10.8.5 Einrichtung eines Postmasters“ fehlt die Aufgabe, dass eine Überprüfung der E-Mails auf die richtige Verwendung gemäß ihrer Sicherheitsklasse erfolgen muss.

Die Problematik, die sich mit einer (generellen) Verwendung des Internets ergibt, betrifft auch den Punkt „10.8.8 Verwendung von WebMail externer Anbietern“. Es muss sichergestellt werden können, dass keine Daten mit entsprechend schutzwürdiger Klassifikation in das Internet hochgeladen werden können, unabhängig davon ob der Kommunikationspartner ein Webmaildienst oder eine andere Webseite ist. Grundsätzlich wird die Verwendung von verschlüsselten Verbindungen (z.B.: SSL/TLS) empfohlen oder wie in „10.8.8“ sogar *vorgeschrieben*. Dadurch wird es für Extrusion Detection Systeme schwer bis unmöglich die Daten zu überprüfen. Eine Lösung dafür ist wieder der Einsatz von Endpunkt-Lösungen, die eine Dateiübertragung rechtzeitig unterbinden können. Dieser Punkt sollte explizit in „10.8.8 Verwendung von WebMail externer

Anbietern“ angeführt werden, zusätzlich muss es in „10.9.2 Erstellung einer Internet-Sicherheitspolitik“ oder „10.9.3 Festlegung einer WWW-Sicherheitsstrategie“ Berücksichtigung finden.

5.2.3 Mobile IT-Systeme und externes Netzwerk

Im Kapitel „11.7.1 Mobile IT-Geräte“ sollte verstärkt darauf hingewiesen werden, dass die Verwendung von externen Netzwerken erhebliche Sicherheitsrisiken mit sich bringen kann. Öffentliche WLAN-Hotspots finden immer mehr Verbreitung und werden zunehmend öfters, gerade durch die steigende Verwendungszahl von Smartphones und Tablets, verwendet. Jede unverschlüsselte Informationsübertragung kann dabei von allen im WLAN befindlichen IT-Geräten mitgelesen werden („Sniffing“), welche Geräte das sind bleibt den Benutzern jedoch verborgen. Das betrifft nicht nur die wissentliche und absichtliche Dateiübertragungen (z.B.: Dokumentversand via E-Mail), sondern auch laufende Hintergrundprozesse, die sich bei verschiedenen Diensten anmelden und dabei Benutzername und Passwort, oder andere sensible Daten, übertragen können. Je nach Gerät und Einstellungen können sich mobile IT-Geräte automatisch mit zugänglichen externen Netzwerken verbinden, sodass die Benutzer noch weniger Kontrolle über aktive Kommunikationsverbindungen haben. Diese Einstellung sollte auf jeden Fall deaktiviert werden, sowohl bei Smartphones und Tablets als auch bei Laptops. Jede offene oder aktive Verbindung zu einem externen Netzwerk eröffnet potentiellen Angreifern die Möglichkeit Schwachstellen im Betriebssystem oder anderer Software auszunutzen und sich somit unberechtigten Zugriff auf das System zu verschaffen.

5.2.3.1 Smartphones und Tablets

„Laptops, PDAs oder Mobiltelefone“ werden im Kapitel „7.1.3.3 Geeignete Aufbewahrung tragbarer IT-Systeme“ bereits in der Aufzählung der tragbaren IT-Systeme angeführt, daher sollten die „Tablets“ ebenso erwähnt werden, um eventuellen Missver-

ständnissen oder Unklarheiten vorzubeugen. Ebenso sollten bei „9.5.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems“ „Tablets“ erwähnt werden, denn nicht nur Laptops müssen gegen unbefugte Beobachtung oder Diebstahl gesichert werden. Auch in „11.7 Mobile Computing und Telarbeit [sic]“ und „11.7.1 Mobile IT-Geräte“ sollten „Tablets“ angeführt werden.

Im Kapitel „7.1.3.5 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Videokameras“ wird immer „(vernetze) Rechner“ verwendet. Hier sollte die Bezeichnung auf neutraleres „IT-Systeme“ geändert werden, da auch Smartphones und Tablets Kameras und Mikrofone integriert haben können. Damit wird dieses Kapitel auch in Zukunft auf neue informationstechnische Arbeitsgeräte direkt anwendbar sein.

So wie in anderen Kapiteln zählen Smartphones und Tablets mittlerweile auch zu mobilen IT-Geräten in „9.5.4 Nutzung und Aufbewahrung mobiler IT-Geräte“, aber da eine explizite Auflistung „[. . .] Notebooks, Palmtops, Handhelds und Personal Assistants“ angeführt wird, sollten sie der Vollständigkeit halber erwähnt werden. Es wird auch festgehalten, dass „Disketten und Streamerbänder“ nur verschlüsselte Daten enthalten sollten. Diese Aussage sollte auf eine generellere Bezeichnungen wie „mobile Speichermedien“ zurückgreifen, um nicht technologie- und zeitabhängig zu sein und somit auch aktuelle Speichermedien wie USB-Sticks, Speicherkarten, usw. Berücksichtigung finden. Aufgrund des technologischen Fortschritts ist es bei einer Überarbeitung des Österreichischen Informationssicherheitshandbuchs nötig verschiedene Begrifflichkeiten, wie zum Beispiel „Disketten“ oder „Palmtops“ auf ihre Aktualität zu überprüfen und gegebenenfalls auf zeitgemäße Äquivalente zu ändern oder gänzlich aus dem Informationssicherheitshandbuch zu entfernen.

Eine Aktualisierung ist auch in „10.4.5 Empfohlene Virenschutzmaßnahmen auf Client-Ebene und Einzelplatzrechnern“ angebracht, da hier nur von Maßnahmen auf „(Einzelplatz-)Rechnern“ geschrieben wird. Mittlerweile gibt es aber auch bereits Programme, sogenannte „Apps“, die auf Smartphones und Tablets den Virenschutz erhöhen können.

In drei Unterpunkten zu „11.7.1 Mobile IT-Geräte“ werden typische Gefährdungen und Maßnahmenempfehlungen für „Laptop, Notebook“, „PDA (Personal Digital Assistant)“ und „Mobiltelefon, Smart Phone“ angegeben. Die immer stärkere Durchdringung von Tablets im Arbeitsalltag rechtfertigt das Einfügen eines neuen Kapitels „11.7.1.4 Tablets“ (das aktuelle Kapitel „11.7.1.4 Wechselmedien und externe Datenspeicher (USB-Sticks, -Platten, CDs, DVDs)“ müsste auf „11.7.1.5“ neu nummeriert werden). Da Tablets meist über einen annähernd gleichen Funktionsumfang wie Laptops verfügen und zusätzlich auch wie Mobiltelefone das Mobilfunknetz nutzen können, können die typischen Gefährdungen und Maßnahmen aus den Kapiteln der anderen IT-Geräte abgeleitet beziehungsweise übernommen werden. Ein eigenes Kapitel einzuführen ist trotz der selben oder ähnlichen Probleme und Maßnahmen empfehlenswert, da es den handelnden Personen zur Übersicht und als Check-Liste dient, um ihre mobilen IT-Geräte umfassend schützen zu können.

Nicht vertrauenswürdige Quellen beim Apps-Download stellen ein großes Sicherheitsrisiko dar. Es wird in „11.7.1.3 Mobiltelefon, Smart Phone“ explizit vor „Unerlaubte Installation von Software (z.B. Apps)“ gewarnt und vorgeschlagen auf Dienstgeräte das „Herunterladen von Software oder Daten aus dem Internet (Apps, Klingeltöne, Displaysymbole oder Ähnliches) [...]“ zu verbieten oder zu unterbinden. Durch den stärker werdenden Trend „Bring Your Own Device“ werden die Möglichkeiten der Organisation eingeschränkt. Das Österreichische Informationssicherheitshandbuch sollte die Erstellung eines Leitfadens vorhersehen, in dem Empfehlungen (z.B. nur moderierte Appstores mit ein Überprüfung der Apps, Rechtevergabe der Apps, usw.) zum Umgang mit Software auf mobilen Geräten gegeben werden. Dieses Thema sollte auch in Schulungen und Sensibilisierungsprogrammen vorkommen. Dabei bedarf es das Kapitel „8.3.3 Schulung und Sensibilisierung zur IT-Sicherheit“ um einen Punkt „Der Umgang mit mobilen IT-Geräten“ zu erweitern.

5.2.3.2 Laptops

Wie in Unterabschnitt 5.1.3 erwähnt, sind die Beschreibungen zur Absicherung von Laptops gut und unterstützen Data Loss Prevention, aber sind nach dem Stand der Technik nicht aktuell. Mit Verweis auf das fiktiv eingeführte neue Kapitel des Österreichischen Informationssicherheitshandbuchs „10.10.7 Extrusion Detection Systeme“ sollte der Einsatz dieser Softwarelösungen, genauso wie Anti-Viren-Software, Firewalls und Intrusion Detection Systeme, empfohlen oder vorgeschrieben werden. Unter den Maßnahmenempfehlungen im Kapitel „11.7.1.1 Laptop, Notebook“ kann der notwendige Punkt eingeführt werden. Ebenso sollte in diesem Kapitel bei den „typischen Gefährdungen“, in Bezugnahme auf die Gefahrenkanalkategorie „Externes Netzwerk“, der Punkt „Unsichere Datenverbindungen“ aufgenommen werden.

5.2.4 Covert Channels

In „10.6.13 Entwicklung eines Firewallkonzepts“ wird bei den Grenzen der Firewall darauf hingewiesen, dass, sobald eine erlaubte Verbindung über die Firewall aufgebaut ist, beliebige Protokolle darüber getunnelt werden können. Netzwerk-DLP-Lösungen mit maschinellen Lerntechniken könnten in Zukunft selbstständig diese versteckte Kommunikation erkennen. Als Präventivmaßnahme kann eine Endpunkt-DLP-Lösung eingesetzt werden, damit die sensiblen Daten nicht durch unerlaubte Prozesse verarbeitet werden können. Im Österreichischen Sicherheitshandbuch sollte auf diese Möglichkeiten verwiesen werden.

5.2.5 Social Media

Einer der jüngeren Entwicklung im Internet, den Sozialen Medien und Sozialen Netzwerken, wird im Österreichischen Informationssicherheitshandbuch nicht Rechnung getragen. Laut eigenen Angeben hat „facebook“ rund 1 Milliarde Nutzer[Zuc12] und davon

rund 2,8 Millionen in Österreich[Dig12], „Google+“[1] 400 Millionen (davon 100 Millionen monatlich aktiv)[Gun12] und „Twitter“ 200 Millionen monatlich aktive Nutzer[Twi12]. Der bekannte Blogging-Dienst „WordPress“[2] verzeichnet über 59 Millionen Blog-Seiten insgesamt und mehr als 3,7 Milliarden Seitenaufrufe pro Monat[Wor12], der Dienst „Tumblr“[3] weist über 85 Millionen Blog-Seiten insgesamt und knapp 18 Milliarden Seitenaufrufe pro Monat aus[Tum12]. Diese Zahlen zeigen deutlich, dass reges Interesse am digitalen Informationsaustausch herrscht und Soziale Medien fixe Bestandteile der heutigen Informationskultur sind. Wie [Sop13] beschreibt, haben Angreifer ihre Tätigkeitsfelder ausgeweitet und sind im Jahr 2012 verstärkt in Richtung Social Media gegangen. Kompromittierte Benutzerkonten, gestohlene Passwörter, Social Engineering Attacken oder SPAM-Verbreitung sollen nur exemplarisch ein paar der Aktivitäten der Angreifer skizzieren.

Aus rein technischer Sicht müssen sich Organisationen wenig neue Gedanken darüber machen. Wird die Nutzung sozialer Medien untersagt, muss es in einer entsprechenden Richtlinie festgehalten und die Dienste durch Blacklists gesperrt werden. Erlaubt die Organisation die Nutzung, werden die Inhalte wie jeder andere Datenverkehr ins Internet über Standardprotokolle hochgeladen und müssen genauso durch DLP-Lösungen überprüft werden. Da viele Dienste eine verschlüsselte Verbindung über SSL/TLS erlauben oder sogar standardmäßig aktiviert haben, ist wieder der Einsatz von Endpunkt-Lösungen anzudenken.

Wenn eine Organisation sich aber dazu entschließt, Social Media selbst zu nutzen beziehungsweise ihre Mitarbeiter nutzen zu lassen, muss das *Wie* festgelegt werden. Aus diesem Grund sollte das Österreichische Informationssicherheitshandbuch das Thema Soziale Medien eigens behandeln und den Organisationen einen strukturierten Leitfaden anbieten, um auch hier einen adäquaten Schutz von Informationen erreichen zu

[1] `https://plus.google.com`
[2] `https://www.wordpress.com`
[3] `https://www.tumblr.com`

können. Soziale Medien erlauben einen großen Freiheitsgrad bei der Informationsverbreitung, darum bedarf es einer Sensibilisierung und Schulung der Mitarbeiter für den richtigen Umgang mit diesem neuen Medium.

Dabei sollten folgende wichtige Punkte berücksichtigt werden:

- *Professionalität – „Das Internet vergisst nichts“:* Eine scheinbare Anonymität im Internet sollte die Professionalität des eigenen Verhaltens auf keinen Fall beeinflussen. Datendiebstahl bei Betreibern von Sozialen Medien oder gecachte Webseiten von Suchmaschinen oder dem „Internet Archiv“[4] können auch viele Jahre später online getätigte Aussagen wieder zu Tage bringen.

- *Umgang mit Fotos:* Auch im Internet beziehungsweise in den neuen Sozialen Medien ist darauf zu achten, dass keine Persönlichkeits- oder Urheberrechte durch die Verbreitung von Fotos verletzt werden. Plattformbetreiber von Sozialen Medien können sich weitreichende Rechte für die Verwendung scheinbar privater Fotos einräumen, wenn die Benutzer diese Plattformen verwenden. Ebenso muss bedacht werden, dass auch reine Schnappschüsse am Arbeitsplatz bereits interne und vertrauliche Informationen abbilden können. Wie auch im Punkt zuvor gilt hier, dass diese Fotos/Daten über Jahre hinweg dezentral gespeichert werden und somit ein echtes nachträgliches „Löschen“ nicht mehr möglich ist.

- *Gesundes Misstrauen:* Social Media Angebote werden von Social Engineers genutzt um an zusätzliche Informationen über ein Unternehmen und ihre Mitarbeiter (und deren Umfeld) zu sammeln. Gegenüber unbekannten Personen sollte deshalb immer eine Grundskepsis vorhanden sein und die weitergegebenen Informationen wohl überlegt sein.

- *Geheimnisse wahren:* Auch in Sozialen Medien gelten weiterhin etwaige Verschwiegenheitspflichten. Betriebs- oder Geschäftsgeheimnisse dürfen weder angedeutet, umschrieben oder direkt weitergegeben werden.

[4] `http://archive.org`

- *Privatsphäreeinstellungen überprüfen:* Jedes Soziale Medium hat seine eigenen Privatsphäreeinstellungen, mit denen der Benutzer die Sichtbarkeit der geteilten Inhalte festlegen kann. Die Benutzer haben sich mit den möglichen Einstellungen vertraut zu machen und diese auch in regelmäßigen Abständen zu kontrollieren, da auch hier immer wieder Änderungen oder Neuerungen vorkommen können.

Das Österreichische Informationssicherheitshandbuch sollte folgende Punkte für Unternehmen vorschreiben, die einen eigenen Social Media Auftritt verwenden wollen:

- *Social Media Strategie:* Jede Organisation muss verpflichtend eine Social Media Strategie erstellen, in der grundlegend festgelegt wird, welche Ziele die Organisation verfolgt, welche Plattformen verwendet werden, wie die Zielgruppe definiert ist und wer für die Redaktion verantwortlich ist.

- *Zentrale Genehmigungsstelle:* Es bedarf einer zentralen Genehmigungsstelle innerhalb der Organisation, bei der vorab eine Genehmigung für einen Social Media Auftritt eingeholt werden muss. Die Antragsteller müssen festlegen, welche Person (und Stellvertreter) für das Unternehmen oder einen Teilbereich schreiben darf und welche Inhalte mit welchem Ziel veröffentlicht werden sollen.

- *Koordination der Inhalte:* Damit eine einheitliche Kommunikation nach außen stattfindet und keine unerwünschten Informationen veröffentlich werden, sollten die veröffentlichten Inhalte zuvor mit den zuständigen Kommunikationsabteilungen (z.B.: Presseabteilung, Konzernkommunikation, Public Relations Abteilung, ...) koordiniert werden.

- *Schulungen:* Sowohl für die Redakteure der jeweiligen Social Media Auftritten als auch für die anderen Mitarbeiter in der Organisation müssen Sensibilisierungs- und Schulungsmaßnahmen durchgeführt werden, damit eine effektive, effiziente und sichere Verwendung erzielt werden kann.

- *Verbindlichkeitsgrad:* Jede Organisation muss für sich selbst definieren, bis zu welchem Verbindlichkeitsgrad die Sozialen Medien verwendet werden dürfen. Zum Beispiel: Gelten Veröffentlichungen als offizielle und rechtlich verbindende Statements? Werden Rückmeldungen der Kunden/anderer Nutzer als offizielle Eingänge gesehen (z.B.: bei Supportanfragen, Beschwerden, usw.)?

- *Leitfaden:* Für die Redakteure und Mitarbeiter soll ein Leitfaden erstellt werden, der alle relevanten Informationen zur Social Media Strategie, der korrekten Einsatzweise und den organisatorischen Richtlinien und Maßnahmen beinhaltet. Dieser sollte in ausgedruckter Form zur Verfügung für jeden Arbeitsplatz zur Verfügung gestellt werden.

Kapitel 6

Zusammenfassung und Resümee

Informationssicherheit in Unternehmen gewinnt an immer größerer Bedeutung. Immer mehr Geschäftswerte oder -geheimnisse werden nur mehr in digitaler Form gespeichert und Geschäftsprozesse rein elektronisch abgewickelt. Gleichzeitig steigt die Bedrohung durch Angriffe und Diebstahl der Daten, sowohl quantitativ als auch in der technologischen Komplexität. Aber auch die Sensibilität der Gesellschaft für das Thema Informationssicherheit steigt, da immer öfter negative Beispiele in den Medien aufscheinen.

Zusammenfassung

Obwohl es viele einzelne Quellen über aktuelle Sicherheitsvorfälle oder zur allgemeinen Bedrohungslage gibt, kann kein vollständiges Bild gezeichnet werden. Viele Unternehmen versuchen, diese Vorfälle geheim zu halten, um keinen Imageverlust zu riskieren. Die vorliegenden Berichte sind Teilausschnitte aus der Realität, aber sie weisen teilweise große Übereinstimmungen auf, wodurch man auf allgemeine Trends schließen kann. Nicht adäquates Passwortmanagement oder Schadsoftware sind die Haupteinbruchstore für Angreifer. Insider stellen aufgrund ihres Wissens und Fertigkeiten ein großes Problem für Sicherheitssoftware und -strategien dar.

Intrusion Detection Systeme oder auch Intrusion Prevention Systeme sind mittlerweile bekannt und verbreitet. Sie versuchen Angreifer zu erkennen beziehungsweise ihre Aktionen zu verhindern, noch bevor diese Schaden anrichten können. Sie können hinsichtlich ihres Einsatzgebietes in *Netzwerk-basierte Systeme* und *Host-basierte Systeme* unterteilt werden und arbeiten entweder mit Mustererkennung oder versuchen das Verhalten zu analysieren. Immer schneller werdende Übertragungsraten und die steigende Anzahl an verschiedenen Attacken stellen große Probleme für aktuelle Systeme dar. Vor allem musterbasierte Systeme haben im Vergleich zu gut trainierten verhaltensbasierten Systemen einige Nachteile. Das wichtigste Kriterium für IDS oder IPS ist die *false positive Rate*.

Für Data Loss Prevention Systeme wird im dritten Kapitel gezeigt, dass sie Daten in drei verschiedenen Verwendungszuständen erkennen können müssen: *Data-in-rest*, *Data-in-use* und *Data-in-motion*. Wie IDS/IPS können DLP-Systeme auch am Host als *Endpunkt DLP-System* eingesetzt werden oder im Netzwerk als *Netzwerk DLP-System*. Um die Daten zu analysieren, wird entweder der *Kontext* oder der *Inhalt* betrachtet. Auch hier haben die Systeme mit steigenden Übertragungsgeschwindigkeiten und -mengen sowie mit der *false positive Rate* zu kämpfen.

Es gibt sehr viele Gefahrenkanäle, über die sensible Information aus einer Organisation transportiert werden kann. Eine Einteilung kann in vier Kategorien durchgeführt werden: *internes Netzwerk*, *externes Netzwerk*, *physische Datenträger* und *Kognition*. Die wichtigsten Gefahrenkanäle in jeder Kategorie werden näher beschrieben, z.B.: „E-Mail“, „Schadsoftware“, „Digitale Speichermedien“ oder „Social Engineering“.

Um einen wirklich umfassenden Schutz für Informationen zu erreichen, bedarf es mehr als nur rein technischer Maßnahmen. Es haben sich sowohl national als auch international verschiedene Sicherheitsframeworks und Standards etabliert, die einen umfassenderen Schutz durch technische, personelle und organisatorische Maßnahmen sicherstellen.

Die wichtigsten Vertreter wie zum Beispiel *ISO/IEC 27001* oder das *Österreichische Informationssicherheitshandbuch* werden in Kapitel 4 dargestellt und näher erläutert.

Im fünften Kapitel der Masterarbeit wird auf die Erweiterungsmöglichkeiten des Österreichischen Informationssicherheitshandbuchs in Bezug auf Data Loss Prevention näher eingegangen. Es werden exemplarisch einige Stärken des Informationssicherheitshandbuchs beschrieben, bevor dann konkret auf Erweiterungsmöglichkeiten eingegangen wird. Data Loss Prevention ist per se als Konzept ist nicht niedergeschrieben, deshalb wird ein eigenes Kapitel über Extrusion Detection Systeme vorgeschlagen, damit vor allem auf der Ebene des „internen Netzwerks“ und „externen Netzwerks“ bewusst über unbeabsichtigte Datenflüsse aus der Organisation nachgedacht wird. Weitere Erweiterungsmöglichkeiten bei E-Mail oder mobilen Speichermedien werden vorgeschlagen. Abschließend wird angeregt, das Thema „Social Media“ im Informationssicherheitshandbuch explizit zu berücksichtigen und gleichzeitig werden Vorschläge für Inhalte unterbreitet.

Resümee

„Data Loss Prevention“ als Begriff hat weder eine definierte Bedeutung noch einen speziellen wissenschaftlichen Hintergrund. Es ist als Marketing- und Modewort der Industrie zu sehen, welches die Thematik rund um die Verhinderung von unerwünschten Informationsflüssen aus einer Organisation zusammenfasst. Deshalb ist bei einer eingehenden Auseinandersetzung mit diesem Thema zu beachten, welche Bedeutung eine bestimmte Quelle „Data Loss Prevention“ oder ähnlichen Begriffen zuweist.

Versteht man Data Loss Prevention wie in dieser Masterarbeit als vielschichtiges Informationssicherheitskonzept, dann wird dessen Bedeutung sehr breit und lässt sich nicht mehr exakt eingrenzen. Wer tatsächlich umfassende Informationssicherheit in einer Organisation erreichen will, muss sowohl technische, personelle als auch organisatorische Maßnahmen treffen. Der Einsatz von Softwarelösungen alleine ist nicht ausreichend, da aufgrund der Komplexität von Daten beziehungsweise der Vielzahl an Gefahrenkanälen

(noch) kein ausreichender Schutz gegeben ist. Der Einsatz dieser DLP-Softwarelösungen kann zurzeit hauptsächlich zur Verhinderung einer unbeabsichtigten Informationsweitergabe eingesetzt werden. Bei einer vorsätzlichen Weitergabe wird der Angreifer oder Insider immer eine Umgehung der Software bewerkstelligen können, auch wenn diese die Weitergabe erschwert.

Um diese umfassende Informationssicherheit zu erreichen, empfiehlt sich der Einsatz von nationalen oder internationalen Sicherheitsframeworks. Wird eine Zertifizierung angestrebt, ist das Zertifikat nach „ISO 27001 auf der Basis von IT-Grundschutz“ zu empfehlen. Andernfalls stellt das Österreichische Informationssicherheitshandbuch einen guten Kompromiss in Kompaktheit und Abstraktionsniveau dar und ist somit zur Umsetzung empfehlenswert. Die meisten relevanten Themen werden dort ausreichend behandelt, auch wenn einige Teile merkbar älter und von der Wortwahl nicht mehr zeitgemäß sind. Allerdings darf man sich darin keine näheren Informationen zu Extrusion Detection Systemen oder Social Media erwarten, hier hinkt das Informationssicherheitshandbuch nach.

Ausblick

Diese Masterarbeit versteht sich als Grundlagenbetrachtung zum Thema Data Loss Prevention. Aufgrund der Breite dieses Themas gibt es eine Vielzahl an weiteren Forschungsrichtungen. Vor allem bei den DLP-Software-Systemen bedarf es einer intensiven Weiterentwicklung hinsichtlich der Flexibilität und Intelligenz bei der Datenerkennung, sowie der Ausweitung auf mehr Gefahrenkanäle.

Auf diese Arbeit aufbauend ist als weiteres Forschungsgebiet „Data Loss Prevention & Cloud Computing“ interessant. Wie müssen DLP-Systeme oder Prozesse verändert werden, wenn auch Datenflüsse mit sensiblen Informationen in diesem Maße nach außen erlaubt sind? Das Österreichische Informationssicherheitshandbuch thematisiert Informationssicherheit in Verknüpfung mit der „Cloud“ nicht. Sind die vorhandenen

Maßnahmen für „Outsourcing“ ausreichend, oder müssen neuen Wege beschritten werden?

Kapitel 7

Vortrag am 2^{nd} Young Researcher's Day

Die Österreichische Computer Gesellschaft (OCG)[1] ist ein gemeinnütziger Verein der 1975 von dem österreichischen Computerpionier Univ.-Prof. Dr. Heinz Zemanek gegründet wurde. Ziel dieses Vereins ist „die Förderung der Informationstechnologie und Informatik unter Berücksichtigung ihrer Wechselwirkungen auf Mensch und Gesellschaft"[OCG12]. Die OCG betreibt ca. 25 Arbeitskreise, die sich schwerpunktmäßig mit Detailgebieten der Informationstechnologie und Informatik auseinandersetzen, z.B.: „Cloud Computing & Big Data", „IT-Governance" oder „Rechtsinformatik".

Der Arbeitskreis „IT-Sicherheit" hat am 29.11.2012 den „2^{nd} Young Researcher's Day" veranstaltet, bei dem jede österreichische Institution mit Security-Schwerpunkt einen Studenten entsenden kann, der über seine Master- oder PhD-Arbeit vorträgt. Es soll ein österreichweiter Informationsaustausch über die aktuellen Security-Forschungsschwerpunkte und eine Vernetzung unter den Studenten stattfinden. Diese Masterarbeit wurde für die JKU im Rahmen des „2^{nd} Young Researcher's Day" vorgetragen. Nachfolgend sind die PowerPoint-Folien des Vortrags angehängt.

[1] `https://www.ocg.at`

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Challenges of Data Loss Prevention

2nd Young Researcher's Day

Simon Bauer

Johannes Kepler University Linz

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Agenda

- Introduction and Motivation
- Categories of Data Extrusion Channels
- Application Areas of DLP Software
- Shortcomings and Challenges of DLP Software
- Personnel and Organisational Framework

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Introduction and Motivation (1)

- What is "Data Loss Prevention (DLP)"?
  - Also called: Data Leakage Prevention, Data Extrusion Prevention, Data Extrusion Detection, Enterprise Information Protection
  - No new topic. Early steganography or cryptography had same goals: *confidentiality*
- Big breaches:
  - Sony (2011): > 70 million user accounts, Heartland Payment Systems (2009): 130 million credit card numbers, TJX Company (2007): 43 million customer records
  - Coca Cola (2009): acquisition $2.4 billion failed, because of hacking?

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Introduction and Motivation (2)

- Threat status
  - Automated attacks, fast and "easy" intrusion
  - Large amount of social engineering attacks: e-mails with malware
  - Detection of data breaches by outsiders: > 80%
- Data states
  - Data-in-rest
  - Data-in-use
  - Data-in-motion
- DLP software
  - Endpoint-/Network-based
  - Context-/Content-based

Categories of Data Extrusion Channels (1)

- Internal network
  - Remote access
  - E-mail
  - Covert channels
  - Malware
  - Mobile devices
  - Supply chain
- External network
  - Mobile service, Wi-Fi, Bluetooth, Infrared

Categories of Data Extrusion Channels (2)

- Physical mediums
  - Digital memory mediums:
    - (USB) hard drives, tapes, CDs, memory sticks, music players, …
  - Hard copies
- Cognition
  - Social engineering, human actions

Application Areas of DLP Software (1)

- Data-in-rest
  - Primarily access control
- Data-in-motion
  - Control of information flow and content inspection
- Data-in-use
  - Software enforces restrictions: printing, screenshots, copy & paste, application-dependent restrictions

Application Areas of DLP Software (2)

- Use cases
  - Misuse of privileges
  - Public sharing of data
  - Hidden data in files

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Shortcomings and Challenges of DLP Software (1)

- Shortcomings
  - Large number of heterogeneous data exfiltration channels
  - Poor recognition of sensitive information
  - No intra-organisational defence
  - No alert-correlation capability
  - Unknown data types
  - High false positive rate
  - DLP software itself

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Shortcomings and Challenges of DLP Software (2)

- Challenges and Academic research
  - Misuse detection in information retrieval systems
  - Misuse detection in databases
  - E-mail data leakage protection
  - Network-/Web-based protection
  - Encryption and access control
  - Data hidden in files
  - Detection of malicious insiders using honeypots and honeytokens
  - Unintentional data leakage
  - Intentional data leakage
  - Data leakage on mobile devices

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

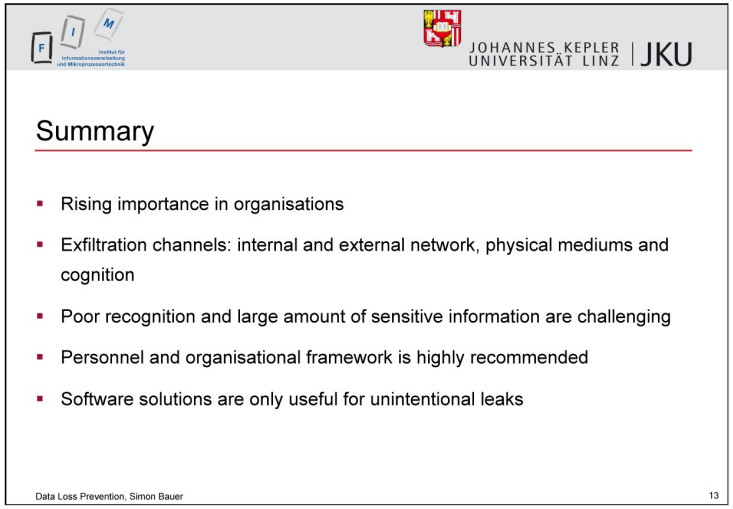
Personnel and Organisational Framework (1)

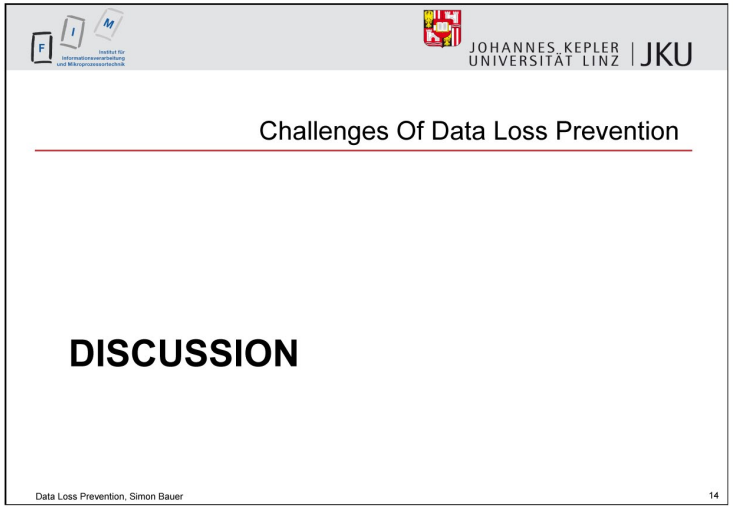
- Implementation of management process
  - Management awareness of overall DLP organisation
  - Classification of data
  - Policies and guidelines
- Nomination of Chief Information Security Officer
  - Responsible for risk management, compliance, technology controls, etc.

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

Personnel and Organisational Framework (2)

- Raise awareness of employees
  - Sensitisation regarding crucial information and its use
  - Awareness of threats
  - Periodical trainings
- Allow user-driven security
  - Involve and empower users


JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU
Summary
Rising importance in organisations
Exfiltration channels: internal and external network, physical mediums and cognition
Poor recognition and large amount of sensitive information are challenging
Personnel and organisational framework is highly recommended
Software solutions are only useful for unintentional leaks
Data Loss Prevention, Simon Bauer
13


JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU
Challenges Of Data Loss Prevention
DISCUSSION
Data Loss Prevention, Simon Bauer
14

Literaturverzeichnis

[AA11] M. Aldwairi and D. Alansari. Exscind: Fast pattern matching for intrusion detection using exclusion and inclusion filters. In *Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on*, pages 24 –30, oct. 2011.

[And80] James P. Anderson. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.

[Bau09] Raphael Baumberger. IT-Sicherheit und IT-Organisation in der Praxis, 2009. Johannes Kepler Universität.

[BBE+07] J. Beale, A.R. Baker, J. Esler, T. Kohlenberg, and S. Northcutt. *Snort: IDS and IPS Toolkit*. Jay Beale's Open Source Security Series. Syngress, 2007.

[Ben06] M. Benantar. *Access Control Systems: Security, Identity Management and Trust Models*, page 26. Springer Science+Business Media, 2006.

[Ber07] Ray Bernard. Information lifecycle security risk assessment: A tool for closing security gaps. *Computers & Security*, 26(1):26 – 30, 2007.

[BG11] Elisa Bertino and Gabriel Ghinita. Towards mechanisms for detection and prevention of data exfiltration by insiders: keynote talk paper. In *Proceedings of the 6th ACM Symposium on Information, Computer and Commu-*

nications Security, ASIACCS '11, pages 10–19, New York, NY, USA, 2011. ACM.

[BGER08] Matt Beaumont-Gay, Kevin Eustice, and Peter Reiher. Information protection via environmental data tethers. In *Proceedings of the 2007 Workshop on New Security Paradigms*, NSPW '07, pages 67–73, New York, NY, USA, 2008. ACM.

[Bis03] M. Bishop. *Computer Security: Art and Science*, page 343. Addison-Wesley, 2003.

[BIT09] BITKOM und DIN. Kompass der IT-Sicherheitsstandards, August 2009. 4. Auflage, `http://www.din.de/sixcms_upload/media/2896/Kompass%20der%20IT-Sicherheitsstandards.pdf` (Abruf: 16.11.2012).

[Bor10] Kenton Born. Browser-based covert data exfiltration. *In Proceedings of the 9th Annual Security Conference, Las Vegas, NV*, April 2010.

[Bun13] Bundesamt für Sicherheit in der Informationstechnik. Anerkennung von CC– Zertifikaten im Rahmen des CCRA, 2013. `https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/InternatAnerkennung/CCRA_Anerkennung.html` (Abgerufen: 18.01.2013).

[Cad11] Tom Caddy. Common criteria. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 227–229. Springer US, 2011. 10.1007/978-1-4419-5906-5_186.

[Cal09] A. Calder. *Information Security Based on ISO 27001/ISO 27002: A Management Guide*. Best Practice. Van Haren Publishing, 2009.

[Cal11] Tracy Caldwell. Data loss prevention – not yet a cure. *Computer Fraud & Security*, pages 5–9, September 2011.

[CB09] David R. Choffnes and Fabián E. Bustamente. Using the crowd to monitor the cloud: Network event detection from edge systems. Northwestern University, November 2009. `http://www.aqualab.cs.northwestern.edu/index.php/component/attachments/download/161` (Abruf: 08.08.2012).

[CC] Common Criteria, `http://www.commoncriteriaportal.org/` (Abruf: 26.09.2012).

[CCP12a] Common criteria part 1 v3.1 release 4, September 2012. `http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf` (Abruf: 26.09.2012).

[CCP12b] Common criteria part 3 v3.1 release 4, September 2012. `http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf` (Abruf: 26.09.2012).

[CER] CERT. Research report 2010. Software Engineering Institute, Carnegie Mellon University.

[CG07] K. Cox and C. Gerg. *Managing Security with Snort & IDS Tools*. O'Reilly Series. O'Reilly Media, 2007.

[Cha11] Stephane Charbonneau. The role of user-driven security in data loss prevention. *Computer Fraud & Security*, 2011(11):5 – 8, 2011.

[Cia11] M. Ciampa. *Security+ Guide to Network Security Fundamentals*, pages 99–100. Course Technology Ptr, 2011.

[CMTS09] Dawn Capelli, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall. Cert common sense guide to prevention and detection of insider threats 3rd edition – version 3.1. Software Engineering Institute, Carnegie Mellon University, January 2009.

[Col12] E. Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Elsevier Science, 2012.

[Cre73] Donald R. Cressey. *Other People's Money: A Study in the Social Psychology of Embezzlement*. Patterson Smith, 1973.

[CSO] CSO. ecrime watch survey 2007. CSO magazine, U.S. Secret Service, CERT® Program, Microsoft Corp.

[CW05] A. Calder and Steve Watkins. *IT Governance: A Manager's Guide to Data Security and BS 7799/ IS0 17799*. Kogan Page Series. Kogan Page, 2005.

[Den87] D.E. Denning. An intrusion-detection model. *Software Engineering, IEEE Transactions on*, SE-13(2):222 – 232, feb. 1987.

[DH11] Marnix Dekker and Giles Hogben. Appstore security - 5 lines of defence against malware. ENISA - European Network of Information Security Agency, September 2011. `http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware/at_download/fullReport` (Abruf 20.12.2012).

[Dig12] Digital Affairs. Facebook Userzahlen, Oktober 2012. `http://digitalaffairs.at/facebook-userzahlen-oesterreich/` (Abruf 03.01.2013).

[DLD] Data loss statistics. Open Security Foundation. `http://datalossdb.org/statistics?timeframe=all_time` (Abruf 20.06.2012).

[DOD85] Department of Defense Trusted Computer System Evaluation Criteria. US Department of Defense, Dezember 1985. `http://csrc.nist.gov/publications/history/dod85.pdf` (Abruf: 25.07.2012).

[EAC+10] Robert J. Ellison, Christopher Alberts, Rita Creel, Audrey Dorofee, and Carol Woody. Software Supply Chain Risk Management: From Products to Systems of Systems, Dezember 2010. Software Engineering Institute, Carnegie

Mellon University, `http://www.sei.cmu.edu/reports/10tn026.pdf` (Abruf 10.01.2013).

[Eck11] C. Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg Wissenschaftsverlag, 2011.

[Eva09] Steve Evans. Printing confidential docs poses security risk: survey, June 2009. `http://www.cbronline.com/news/printing_confidential_docs_poses_security_risk_survey_170609` (Abruf: 13.11.2012).

[GBC06] Annarita Giani, Vincent H. Berk, and George V. Cybenko. Data exfiltration and covert channels. In *in Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V*, 2006.

[GGP+09] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez. Design of a snort-based hybrid intrusion detection system. In Sigeru Omatu, Miguel Rocha, José Bravo, Florentino Fernández, Emilio Corchado, Andrés Bustillo, and Juan Corchado, editors, *Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living*, volume 5518 of *Lecture Notes in Computer Science*, pages 515–522. Springer Berlin / Heidelberg, 2009. 10.1007/978-3-642-02481-8_75.

[GLT10] Ali A. Ghorbani, Wei Lu, and Mahbod Tavallaee. *Network Intrusion Detection and Prevention. Concepts and Techniques*. Springer US, 2010.

[Gol11] D. Gollmann. *Computer Security*. Wiley, 2011.

[Gou11] Wendy Goucher. Look behind you: the dangers of shoulder surfing. *Computer Fraud & Security*, 2011(11):17 – 20, 2011.

[Grua] IT-Grundschutz. `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html` (Abruf 08.10.2012), Bundesamt für Sicherheit in der Informationstechnik, Bonn, Deutschland.

[Grub] PDF zu „Webkurs IT-Grundschutz“. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/gskurs_pdf.pdf?__blob=publicationFile` (Abruf 04.10.2012), Bundesamt für Sicherheit in der Informationstechnik, Bonn, Deutschland.

[Gun12] Vic Gundotra. 400,000,000 people have upgraded to google+, September 2012. `https://plus.google.com/u/1/+VicGundotra/posts/2YWhK1K3FA5` (Abruf 21.12.2012).

[HDS+11] Michael Hanley, Tyler Dean, Will Schroeder, Matt Houy, Randall F. Trzeciak, and Juan Montelibano. An analysis of technical observations in insider theft of intellectual property cases. Technical report, Software Engineering Institute, 2011. `http://repository.cmu.edu/sei/666`.

[Hig09] Kelly Jackson Higgins. Bankers gone bad: Financial crisis making the threat worse, Oktober 2009. `http://www.darkreading.com/security/news/220301087` (Abruf: 09.06.2012).

[HMJ11] Michael Hart, Pratyusa Manadhata, and Rob Johnson. Text classification for data loss prevention. In Simone Fischer-Hübner and Nicholas Hopper, editors, *Privacy Enhancing Technologies*, volume 6794 of *Lecture Notes in Computer Science*, pages 18–37. Springer Berlin / Heidelberg, 2011.

[Hof12] J. Hoffmann. *Risikomanagement für mittelständische Unternehmen: Risikopotenziale erkennen und erfolgreich bewältigen- mit zahlreichen Praxissituationen.* Books on Demand, 2012.

[HW10] C. Hadnagy and P. Wilson. *Social Engineering: The Art of Human Hacking.* Wiley, 2010.

[Inf12] Global Data Leakages & Insider Threats Report: 2011. InfoWatch Analytical Labs, 2012. `http://infowatch.com/sites/default/files/report/InfoWatch_global_data_leakage_report_2011.pdf` (Abruf 19.11.2012).

[ISOa] The ISO 27000 Directory. `http://www.27000.org` (Abruf 01.10.2012).

[ISOb] ISO 27000:2009. *Information technology - Security techniques - Information security management systems - Overview and vocabulary.* International Organisation of Standardization, Schweiz.

[ISOc] ISO 27001:2005. *Information technology — Security techniques — Information security management systems — Requirements.* International Organisation of Standardization, Schweiz.

[ISOd] ISO 27002:2005. *Information technology — Security techniques — Code of practice for information security management.* International Organisation of Standardization, Schweiz.

[JK11] J. Jaskolka and R. Khedri. Exploring covert channels. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1 –10, jan. 2011.

[Jon08] Andrew Jones. Industrial espionage in a hi-tech world. *Computer Fraud & Security*, 2008(1):7 – 13, 2008.

[Jun12] Juniper Networks. Malicious Mobile Threats Report 2010/2011, 2012. `http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf` (Abruf: 10.01.2013).

[Kao11] I-Lung Kao. Securing mobile devices in the business environment. IBM Security Services, Oktober 2011.

[Kap07] Martin Kappes. *Netzwerk- und Datensicherheit. Eine praktische Einführung*, chapter 11. Netzwerküberwachung. Springer Verlag, 2007.

[Kin12] John Kindervag. Rethinking DLP. Forrester Research Inc., Jänner 2012. `http://www.titus.com/resources/marketo/WEB_CLS_WP_Forrester_Rethink_DLP.pdf` (Abruf: 30.10.12).

[Koc11] R. Koch. Towards next-generation intrusion detection. In *3rd International Conference on Cyber Conflict (ICCC)*, pages 1 –18, june 2011.

[Kru09] W. Kruth. *IT-Grundlagenwissen: Kompaktwissen Informationstechnik für Datenschutz- und Security-Management*. Datakontext, 2009.

[Law08] G. Lawton. New technology prevents data leakage. *Computer*, 41(9):14 –17, sept. 2008.

[Lay07] Robin Layland. Data leak prevention: Coming soon data leak prevention: Coming soon to a business near you. *Business Communications Review*, pages 44–49, May 2007.

[Lip09] M. Lipski. *Social Engineering - Der Mensch Als Sicherheitsrisiko in Der IT*. Diplomica Verlag, 2009.

[Lüs08] Cécile Lüssi. Signature-based extrusion detection. Master's thesis, Eidgenössische Technische Hochschule Zürich, 2008.

[LW11] Hyun-Jung Lee and Dongho Won. Protection profile for data leakage protection system. In *Future Generation Information Technology*, volume 7105 of *Lecture Notes in Computer Science*, pages 316–326. Springer Berlin / Heidelberg, 2011.

[MA10] F.E. McFadden and R.D. Arnold. Supply chain risk mitigation for it electronics. In *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, pages 49 –55, nov. 2010.

[Man04] Salvador Mandujano. *A Multiagent Approach A Multiagent Approach to Outbound Intrusion Detection*. PhD thesis, Instituto Tecnologico y de Estudios Superiores de Monterrey, 2004.

[MB04] M.S. Merkow and J. Breithaupt. *Computer Security Assurance Using the Common Criteria*. Delmar Learning, 2004.

[MGK10] Malcom Marshall, Leah Gregorio, and Hitesh Kargathra. KPMG Data Loss Barometer 2010. Publication number: RRD-228500, November 2010. `http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG-Data-Loss-Barometer-November-2010.pdf` (Abruf: 17.08.2012).

[MP09] J.R. Mühlbacher and C. Praher. DS RBAC-Dynamic Sessions in Role Based Access Control. *Journal of Universal Computer Science*, 15(3):538–554, 2009. Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM), Johannes Kepler Universität.

[MSD03] K.D. Mitnick, W. Simon, and J. Dubau. *Die Kunst der Täuschung: Risikofaktor Mensch*. mitp-Verlag, 2003.

[Mül11] K.R. Müller. *IT-Sicherheit mit System: Integratives IT-Sivherheits-, Kontinuitäts- und Risikomanagement - Sicherheitspyramide - Standards und Practices - SOA und Softwareentwicklung*. Vieweg+Teubner Verlag, 2011.

[Nim09] Sebastian Nimwegen. *Vermeidung und Aufdeckung von Fraud*, pages 18–20. BoD – Books on Demand, 2009. `http://goo.gl/qhTKH`.

[OCG12] OCG. *Imagefolder OCG*. Österreichische Computer Gesellschaft, 2012. `http://www.ocg.at/sites/ocg.at/files/medien/pdfs/imagefolder_ocg_2012-web.pdf` (Abruf: 10.01.2013).

[Olt11] Jon Oltsik. White paper: Dlp for tablets: An intelligent security decision. Enterprise Strategy Group, Inc., November 2011.

[OM11] Eric Ouellet and Rob McMillan. Magic quadrant for content-aware data loss prevention, August 2011. http://www.gartner.com/technology/reprints.do?id=1-16XQWWD&ct=110810 (Abruf 20.02.2012).

[Par89] Donn B. Parker. *Criminal Justice Resouce Manual (Second Edition)*. U.S. Department of Justice, August 1989.

[Per10] Nicholas J. Percoco. Data exfiltration: How data gets out, March 2010. http://www.csoonline.com/article/570813/data-exfiltration-how-data-gets-out (Abruf 20.02.2012).

[PKAC07] R. Proudfoot, K. Kent, E. Aubanel, and Nan Chen. High performance software-hardware network intrusion detection system. In *Field-Programmable Technology, 2007. ICFPT 2007. International Conference on*, pages 309 –312, dec. 2007.

[Pog07] W. Poguntke. *Basiswissen IT-Sicherheit: Das Wichtigste für den Schutz von Systemen und Daten*. IT lernen. W3L GmbH, 2007.

[Pon09] Larry Ponemon. The cost of a lost laptop, April 2009. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Cost%20of%20a%20Lost%20Laptop%20White%20Paper%20Final%203.pdf (Abruf 20.02.2012).

[Pon10] Larry Ponemon. Five countries: The cost of data breach, April 2010. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf (Abruf 20.02.2012).

[Pon12a] Larry Ponemon. 2011 cost of data breach study: France, März 2012. http://www.symantec.com/content/de/de/about/downloads/press/2011_CODB_FRANKREICH.pdf (Abruf 11.06.2012).

[Pon12b] Larry Ponemon. 2011 cost of data breach study: Germany, März 2012. http://www.symantec.com/content/de/de/about/

downloads/press/2011_CODB_FINAL_Deutschland.pdf?om_ext_cid=biz_socmed_de_pv_090312_scom_socialmedia_CostDataBreach (Abruf 11.06.2012).

[Pon12c] Larry Ponemon. 2011 cost of data breach study: Uk, März 2012. http://www.symantec.com/content/de/de/about/downloads/press/2011_CODB_UK.pdf (Abruf 11.06.2012).

[Pon12d] Larry Ponemon. 2011 cost of data breach study: Usa, März 2012. http://www.symantec.com/content/de/de/about/downloads/press/2011-cost-of-data-breach-USA.pdf (Abruf 11.06.2012).

[Por11] Sue Marquette Poremba. Remote printing, even at home, is far from secure, Jänner 2011. http://www.technewsdaily.com/1957-remote-printing-even-at-home-is-far-from-secure.html (Abruf: 13.11.2012).

[Reg] International Register of ISMS Certificates. http://www.iso27001certificates.com/ (Abruf 30.09.2012).

[SBH02] Ingrid Schaumüller-Bichl and Manfred Holzbach. Das Österreichische IT-Sicherheitshandbuch. In E. Erasim and Wien Fachtagung SIS 2002, editors, *Sicherheit in Informationssystemen: Proceedings der Fachtagung SIS 2002*, pages 241–255. Universität Wien, Institut für Informatik und Wirtschaftsinformatik, Abteilung Wissenstechnologie, vdf, Hochsch.-Verlag an der ETH, Oktober 2002.

[SER12] Asaf Shabtai, Yuval Elovici, and Lior Rokach. *A Survey of Data Leakage Detection and Prevention Solutions*. Springer US, Boston, MA, 2012.

[SHS08] Malek Ben Salem, Shlomo Hershkop, and Salvatore J. Stolfo. A survey of insider attack detection research. In *Insider Attack and Cyber Security*, volume 39 of *Advances in Information Security*, pages 69–90. Springer US, 2008.

[SIH10] *Österreichisches Informationssicherheitshandbuch.* Bundeskanzleramt Österreich (BKA), 27. Mai 2010. Version 3.1.002, https://www.sicherheitshandbuch.gv.at/dojo/downloads/sicherheitshandbuch.pdf (Abruf 11.09.2012).

[SK06] Marc Smeets and Matthijs Koot. Research report: Covert channels. University of Amsterdam, 2006. https://alumni.os3.nl/~mrkoot/courses/RP1/researchreport_2006-02-15_final2.pdf (Abruf: 25.07.2012).

[SNO] SNORT - Network Intrusion Prevention and Detection System. http://www.snort.org/ (Abruf: 23.10.2012).

[Sop12] Security Threat Report 2012. Sophos Ltd., 2012. http://www.sophos.com/de-de/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf (Abruf 26.11.2012).

[Sop13] Security Threat Report 2013. Sophos Ltd., 2013. http://www.sophos.com/de-de/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf (Abruf 11.01.2013).

[SSP08] J. Swoboda, S. Spitz, and M. Pramateftakis. *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen- eine Einführung.* Vieweg+Teubner Verlag, 2008.

[TIT11] TITUS. *User Driven Security - 5 Critical Reasons Why It's Needed for DLP.* Titus Inc., 2011. http://www.titus.com/resources/marketo/WEB_DLP_WP_User_Driven_Security_5_Reasons_why_its_needed_w_DLP.pdf (Abruf: 18.12.2012).

[Tru12] Global Security Report. Trustwave, 2012. https://www.trustwave.com/global-security-report (Abruf 13.02.2012).

[Tum12] Tumblr.com. Über tumblr, Dezember 2012. http://www.tumblr.com/about (Abruf 21.12.2012).

[Twi12] Twitter.com. more than 200m monthly, Dezember 2012. `https://twitter.com/twitter/status/281051652235087872` (Abruf 21.12.2012).

[Ver12] Data Breach Investigations Report. Verizon RISK Team, 2012. `http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf` (Abruf 18.06.2012).

[Wis12] Chester Wisniewski. Exposing the Money Behind the Malware. Sophos Ltd., Juni 2012. `http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophosmoneybehindmalwarewpna.pdf` (Abruf: 11.01.2013).

[WL10] Duane Wilson and Michael K. Lavine. A discretionary access control method for preventing data exfiltration (de) via removable devices. In Sanjay Goel, editor, *Digital Forensics and Cyber Crime*, volume 31 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 151–160. Springer Berlin Heidelberg, 2010.

[WM10] M.E. Whitman and H.J. Mattord. *Management of Information Security*. Course Technology, 2010.

[Wol05] M. Wolschon. *Konzeption und Implementation eines Authentifizierungssystems auf Basis von biometrischen Merkmalen und Transpondertechnologie*. GRIN Verlag, 2005.

[Wor12] WordPress.com. Wordpress sites in the world, Dezember 2012. `http://en.wordpress.com/stats/` (Abruf 21.12.2012).

[YW12] Li Yang and Daiyun Weng. Snort-based campus network security intrusion detection system. In Rongbo Zhu and Yan Ma, editors, *Information Engineering and Applications*, volume 154 of *Lecture Notes in Electrical Engineering*, pages 824–831. Springer London, 2012. 10.1007/978-1-4471-2386-6_106.

[Zuc12] Mark Zuckerberg. One billion people using facebook, Oktober 2012. `https://www.facebook.com/zuck/posts/10100518568346671` (Abruf 21.12.2012).

Lebenslauf

Persönliche Daten

Name	Simon Bauer
Akademischer Grad	Bakk. techn.
Geburtsdatum/-ort	20. Jänner 1985 in Leoben
Wohnort	Polgarweg 29, 4040 Linz
e-Mail-Adresse	simon@bauer-baeck.at

Ausbildung

2010 – 2013	Masterstudium Informatik (Netzwerke und Sicherheit) an der Johannes Kepler Universität Linz
2010 – 2011	Auslandssemester an der University of Reading, United Kingdom
2005 – 2010	Bakkalaureatsstudium Informatik an der JKU Linz
1999 – 2004	HTL Leonding für Elektronik mit Schwerpunkt Telekommunikationstechnik

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Masterarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe. Die vorliegende Masterarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Ort und Datum Simon Bauer, Bakk.