der Bundeswehr
Universität München

DEPARTMENT OF COMPUTER SCIENCE

# Seminar Cyber Defense FT 2014

Prof. Dr. Gabi Dreo
Peter Hillmann
Frank Tietze
Sebastian Seeber

(Hrsg.)

Report 2014-07
Oktober 2014

Werner-Heisenberg-Weg 39 • 85577 Neubiberg • Germany

# Inhaltsverzeichnis

# Kapitel 1

# Elliptische Kurven

*Martin Wandtke*

*Durch die ständige Weiterentwicklung der Medien und insbesondere von Netzen und Technologien, die Netze nutzen, spielt Sicherheit eine immer größe Rolle. Die Elliptic Curve Cryptography (ECC) löst hierbei ältere Verfahren ab und sorgt aufgrund des Elliptic Curve Discrete Logarithmus Problem (ECDLP) für hohe Sicherheit. Diese Seminararbeit befasst sich mit den mathematischen Grundlagen von ECC und zeigt Vorteile wie das ECDLP und weitere von ECC in der kryptographischen Anwendung. Zuletzt werden die verschiedenen Einsatzbereich von ECC vorgestellt und einige Verfahren beispielhaft vorgestellt.*

# Inhaltsverzeichnis

## 1.1 Einleitung

> "Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication." [1]

Diese Definition von Kryptographie gibt an, dass Vertraulichkeit, Integrität von Daten, Authentizität von Datennutzern und Originalität von Daten durch Techniken der Kryptographie sichergestellt werden. Gerade heutzutage ist es aufgrund der Entwicklung von Medien, Technik und Netzen immer wichtiger, die Sicherheit von Informationen zu gewährleisten. So gilt als einfaches Beispiel für die Anwendung, dass jeder bei einer Kommunikation über E-Mails sicher sein will, von wem die Nachrichten kommen und ob die Nachrichten nur die richtigen Personen erreicht. Im Zuge der steigenden Sicherheitsanforderungen und der Schwierigkeit durch wachsende Rechenleistung sichere Verfahren zu entwickeln, sollen elliptische Kurven die Kryptographie-Verfahren verbessern. Bereits 1985 haben die beiden Mathematiker Koblitz und Miller unabhängig voneinander die mathematische Basis dafür gelegt. Mit dieser Basis konnten elliptische Kurven in asymmetrische Verfahren angewendet werden, so dass diese aufgrund des diskreten Logarithmus-Problem die Sicherheit von bekannten Verfahren erhöhen. Asymmetrische Verfahren oder auch Public-Key-Verfahren bestehen aus einem Schlüsselpaar, welches einen öffentlichen Schlüssel zur Verschlüsselung und einen privaten Schlüssel zur Entschlüsselung beinhaltet. Diese Verfahren werden unter dem Begriff *Elliptic Curve Cryptography (ECC)* zusammengefasst und von Institutionen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder auch dem *Institute of Electrical and Electronics Engineers (IEEE)* [2] standardisiert und aufgearbeitet.

In dieser Seminararbeit wird zunächst erklärt, welche Vorteile ECC bietet und weshalb es eingesetzt wird. Im Anschluss daran folgt die Erläuterung der Grundlagen für ECC im Kapitel 1.3, unter denen die mathematischen Grundlagen und die Basis aller ECC-Verfahren wie die Domain Parameter und das diskrete Logarithmus-Problem gehören. Im darauffolgenden Kapitel wird die Anwendung von elliptischen Kurven in verschiedenen Verfahren der Bereiche Nachrichtenverschlüsselung, Signaturalgorithmen und Schlüsselaustauschverfahren gezeigt und teilweise durch Beispiele veranschaulicht. Abschließend wird ein Fazit zum Einsatz von ECC gezogen und eine Zusammenfassung zur Seminararbeit gegeben.

Zusätzlich zu der oben aufgeführten Struktur wurden Konventionen getroffen, um die Verständlichkeit und Lesbarkeit dieser Seminararbeit zu verbessern. Um englische Begriffe zu kennzeichnen, werden diese *kursiv* geschrieben. Ferner werden Begriffe, die als Abkürzungen verwendet werden,

einmalig in der Einführung ausgeschrieben.

## 1.2 Warum “Elliptische Kurven Kryptographie”?

Bei der Anwendung von kryptographischen Verfahren wird immer die Frage gestellt, ob das jeweilige Verfahren alle nötigen Anforderungen erfüllt. In der Kryptographie haben sich dabei als Hauptkriterien die Sicherheit und Effizienz herauskristallisiert. Genau diese zwei Aspekte werden im Folgenden für die ECC diskutiert und zur besseren Evaluierung mit dem RSA-Verfahren (Rivest, Shamir und Adleman) verglichen.

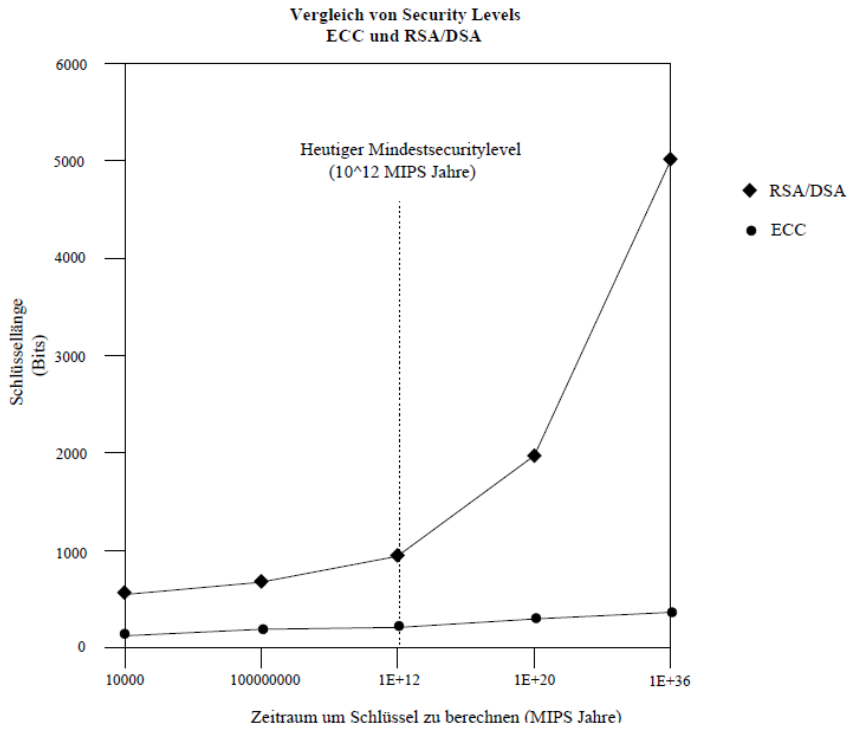


Abbildung 1.1: Vergleich der Security Levels [12]

**Sicherheit** Wenn es in der Kryptographie um Sicherheit geht, ist es wichtig, dass es möglichst schwierig ist, einen Schlüssel zu berechnen. Wie der Graph in der Abbildung 1.1 zeigt, steigt die Schlüssellänge bei dem RSA-Verfahren mit der Zeit enorm an. Dies bedeutet, dass sich die Schlüssel nach einer gewissen Zeit einfacher berechnen lassen. Der Grund dafür ist, dass für das Faktorisierungsproblem (siehe RSA-Verfahren) und ebenfalls das Diskrete Logarithmus-Problem subexponentielle Algorithmen zur Lösung existieren. Diese lassen sich beispielsweise mit heutigen Quantencomputern

sehr gut berechnen, während der beste bekannteste Algorithmus zur Berechnung des *Elliptic Curve Discrete Logarigthm Problem (ECDLP)* eine exponentielle Laufzeit besitzt. Damit und der Abbildung 1.1 ist eindeutig, dass ECC sicherer als RSA ist.

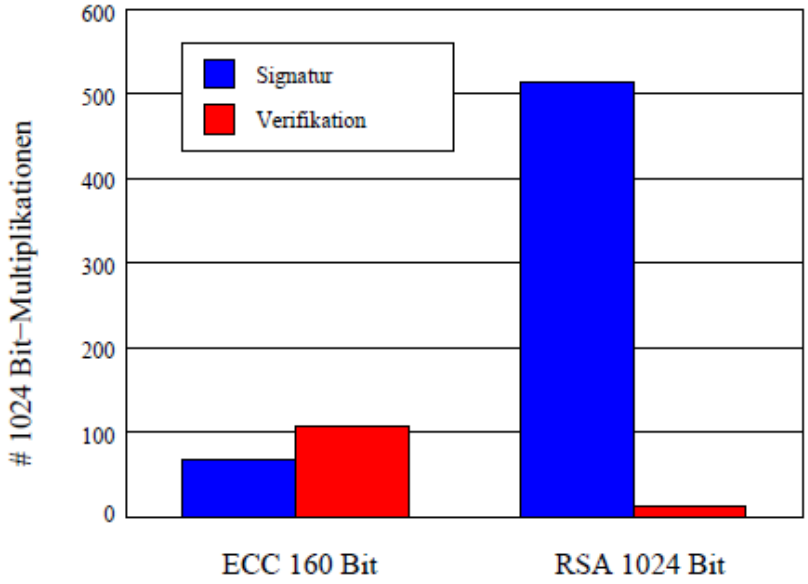


Abbildung 1.2: Vergleich Aufwand der Operationen Signieren und Verifizieren [3]

**Effizienz** Mit Effizienz ist gemeint, dass versucht wird mittels eines Verfahrens die Ressourcen möglichst sparsam zu verwenden. Im Falle der Kryptographie ist diesbezüglich das Ziel, eine hohe Sicherheit trotz kleiner Schlüssel zu gewährleisten. Die Abbildung 1.2 veranschaulicht dazu den Vergleich des Aufwands der nötigen Operationen beim Signieren und Verifizieren bei ECC und RSA. Beim Signieren fällt in der Abbildung auf, dass ECC wesentlich schneller ist, jedoch sich das Blatt beim Verifizieren wendet und RSA besser abschneidet. Als Anwendungsbeispiel dient hierzu die Smartcard, bei der Schlüssel immer auf der Karte gespeichert werden muss und weiterhin die Signierung auf dieser stattfindet. Da eine Verifikation jedoch nicht auf der Karte sonder später vollzogen wird, ist das ECC-Verfahren vorteilhafter. Da Signieren und Verifizieren zu einem Verfahren gehören, ist eine weitere Betrachtung die Summe des Aufwands der beiden Operationen. Bei dem Vergleich der Summe fällt jedoch schnell auf, dass ECC wesentlich besser abschneidet als RSA, wodurch die Einzelbetrachtung und Gesamtbetrachtung dies nun bestätigt hat. Ebenso ist aus der Abbildung 1.3 abzulesen, welche Berechnungszeiten bei den Verfahren ECC (für eine Schlüssellänge von 571) und RSA (für eine Schlüssellänge von 15380) der einzelnen Stufen Generierung, Signierung und Verifikation gebraucht werden. Trotz verschiedener Schlüssellängen ist die gleiche Sicherheit gewährleistet, weshalb diese Zeiten so verglichen werden können und

die bereits angesprochen Aspekte durch diese Abbildung nochmals bestärkt werden.

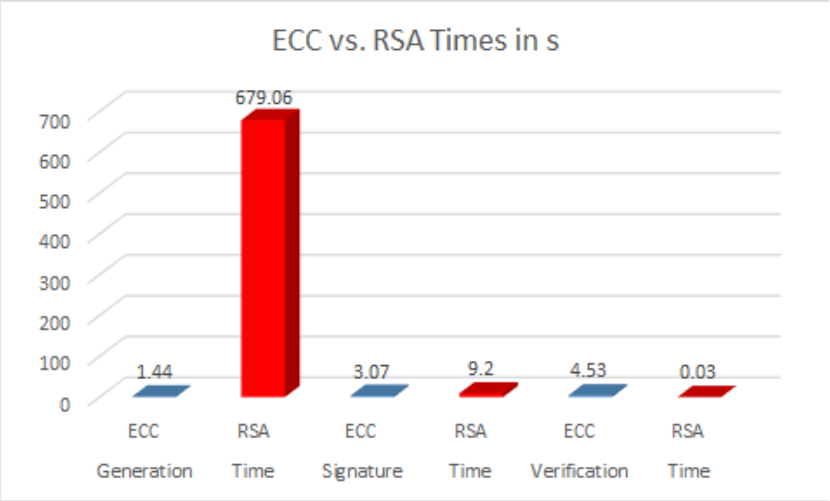


Abbildung 1.3: ECC und RSA Berechnungszeiten im Vergleich, vgl. [4]

Um aber zusätzlich auf die Schlüssellänge einzugehen, hilft der Blick zurück auf die Abbildung 1.1. In dieser wird deutlich, dass obwohl der Schlüssel des ECC-Verfahrens kleiner als der des RSA-Verfahrens ist, bringt dieser Schlüssel die gleiche oder eine bessere Sicherheit mit sich.

Wie sich in den zwei oben aufgezeigten Aspekten erwiesen hat, ist das ECC-Verfahren offensichtlich für kryptographische Anwendungen geeignet. Des Weiteren muss erwähnt werden, dass die Basis des ECC-Verfahrens nicht die elliptische Kurve ist sondern die Gruppe, die durch diese definiert wird. Insbesondere dies und die fehlenden Standards für das ECC-Verfahren führen dazu, dass sehr viele verschiedene Implementierungsmöglichkeiten existieren. Gleichzeitig wird durch die verschiedenen Implementierung zusätzlich die Sicherheit gesteigert, da somit nicht einfach ein Nachrichtenaustausch zwischen zwei verschiedenen Programmen durchgeführt werden kann und vorher ein Abgleich stattfinden muss.
Im folgenden Kapitel wird nun auf das ECC-Verfahren und dessen mathematischer Hintergrund genauer eingegangen. Da das ECC-Verfahren zu den Public-Key-Verfahren gehört, besitzt dieses dementsprechend die Funktionalitäten der Verschlüsselung, Signaturen und Schlüsselvereinbarungen, die nach der Erläuterung des Verfahrens mit Beispielen beschrieben werden.

## 1.3 Elliptische Kurven Kryptographie - ECC

Bevor ein Verfahren angewendet und an Beispielen erläutert werden kann, muss immer erstmal die Basis dafür geschaffen werden. Aufgrund dessen

werden anfangs in diesem Kapitel die mathematischen Grundlagen erläutert, so dass im Anschluss das kryptographische Verfahren im Abschnitt 1.3.2 beschrieben werden kann. Da die Kryptographie eingesetzt wird, um Sicherheit zu erhalten, wird nach dem Verfahren erklärt, dass die Sicherheit von ECC auf dem ECDLP beruht. Da nicht alle elliptische Kurven für den Einsatz in der Kryptographie sinnvoll sind, werden zum Abschluss des Kapitels im Abschnitt 1.3.4 gegeben.

### 1.3.1 Mathematische Grundlagen

Dieser Abschnitt beschreibt die mathematischen Grundlagen, die nötig sind, um das kryptographische Verfahren zu erläutern und zu verstehen. Zum einen werden die Voraussetzungen zur Definition von elliptischen Kurven erläutert und zum anderen wird darauf eingegangen, wie elliptische Kurve sich über verschiedenen Körpern verhalten. [5]
Eine bedeutende Operation mit elliptischen Kurven und vor allem in der Kryptographie ist *modulo*, bei welcher ein Integer $m > 1$, auch *modulus* genannt, existiert. Außerdem ist ein Integer a gegeben, welcher bei einer Division mit m den Rest r als Ergebnis bekommt und mathematisch folgendermaßen geschrieben wird:

$$r = a \bmod m \tag{1.1}$$

Mit der Formel wird deutlich, dass ebenso $0 \leq r \leq m - 1$ gilt. Diese Operation wird beispielsweise über den Körpern von Primzahlen genutzt, der im weiteren beschrieben wird, jedoch folgt zunächst die Definition von Gruppen und Körpern.

#### Gruppen und Körper

Zum genauen Verständnis für elliptische Kurven werden die beiden Begriffe *Gruppe* und *Körper* im Folgenden kurz eingeführt.

**Gruppe** Eine *Gruppe* ist eine nicht leere Menge G, ein algebraisches System, welche eine Verknüpfung $\diamond : G \times G \to G$ besitzt und die folgenden Eigenschaften erfüllt:

- abgeschlossen: $\forall x, y \in G, x \diamond y \in G$;
- assoziativ: $x \diamond (y \diamond z) = (x \diamond y) \diamond z$;

- Identität: $\exists e \in G, \forall x \in G : x \diamond e = e \diamond x = x$;
- Inverses Element: $\forall x \in G, \exists y \in G : x \diamond y = y \diamond x = e$.

Des Weiteren ist eine *Gruppe* eine *abelsche Gruppe*, falls diese kommutativ ist:

- kommutativ: $\forall x, y \in G, x \diamond y = y \diamond x$;

**Körper** Ein *Körper* ist eine nicht leere Menge F, welche zwei Verknüpfungen + und × besitzt und die folgenden Eigenschaften erfüllt:

- (F, +) ist eine *algebraische Gruppe*;
- (F\{0}, ×) ist eine *algebraische Gruppe*;
- distributiv: $\forall x, y, z \in F, (x + y) \times z = x \times z + y \times z$.

Die *Charakteristik* eines Körpers F (*char(F)*) ist die kleinste natürliche Zahl $n$, so dass die folgende Gleichung gilt:

$$\sum_{i=1}^{n} I = 0 \tag{1.2}$$

Dabei steht $I$ in der Gleichung 1.2 für die Identität der Multiplikation des Körpers F. Existiert keine solche natürliche Zahl $n$, dann ist $char(F) = 0$.

**Endliche Körper** Ein *endlicher Körper* ist ein Körper, der endlich viele Elemente beinhaltet. Dabei ist $q$ die Anzahl der Elemente eines Körpers F eine Primzahlpotenz, sprich $q = p^m$, wobei $p$ eine Primzahl und $m \geq 1$ eine ganze Zahl ist. Ein wichtiger Aspekte zu diesem Theorem ist, dass bis auf Isomorphie jeweils genau ein Körper mit $p^n$ Elementen existiert. Diese Körper werden $GF(p^n)$, *Galois Feld*, bezeichnet, wobei gilt $GF(p^n) = \mathbb{F}_{p^n}$.
Eine Besonderheit in der Kryptographie bilden die Körper $\mathbb{F}_p$ mit $p$ als Primzahl (Primkörper), welche den Körper der Restklassen ganzer Zahlen *modulo* $p$ bildet.

### Elliptische Kurven - EC

Im Folgenden wird nun definiert, welche Eigenschaften eine elliptische Kurve besitzt und wie diese aussieht. Im Anschluss an die Definition der elliptischen Kurve wird beschrieben, wie mit elliptischen Kurven über verschiedenen Körpern gerechnet wird.

**Weierstraß-Gleichung** Die *Weierstraß-Gleichung* lautet, wie folgt, wobei $x$, $y$ und $a_i \in$ K sind:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \tag{1.3}$$

Die Vereinigung der Lösungsmenge der Gleichung 1.3 und dem "unendlich fernen Punkt" $\mathcal{O}$ wird als *elliptische Kurve* E bezeichnet, wenn diese *nicht singulär* ist. Dies bedeutet, dass mindestens eine der beiden partiellen Ableitungen der Gleichung 1.3 für einen Punkt(x, y) $\in$ E ungleich 0 sind, sprich das folgende Kriterium erfüllt wird:

- $\frac{\partial F}{\partial x} \neq 0 \vee \frac{\partial F}{\partial y} \neq 0; \forall P(x, y) \in E$

Für das weitere Vorgehen bei der Vorstellung des Verhaltens einer elliptischen Kurve über den einzelnen Körpern muss verdeutlicht werden, dass die elliptische Kurve bei ECC zwar genutzt wird, um zu rechnen jedoch, die von der elliptischen Kurve erzeugte Gruppe das Kernstück der ECC-Verfahren ist. Aus diesem Grund wird bei jedem einzelnen Körper bewiesen, ob eine Gruppe erzeugte wurde, in dem geprüft wird, ob Abgeschlossenheit, Assoziativität, eine Identität und ein inverses Element vorhanden ist. Dazu werden die Operationen "Addition von zwei verschiedenen Punkten" und "Verdopplung eines Punktes" berechnet und dargestellt, wodurch die vier Kriterien einer Gruppe nachgewiesen werden.

### EC über reellen Zahlen

In diesem Abschnitt werden elliptische Kurven über den Körper der reellen Zahlen $\mathbb{R}$ betrachtet. Über $\mathbb{R}$ wird die elliptische Kurve E durch die Lösungsmenge der Gleichung 1.4 dargestellt:

$$y^2 = x^3 + ax + b : a, b \in \mathbb{R} \tag{1.4}$$

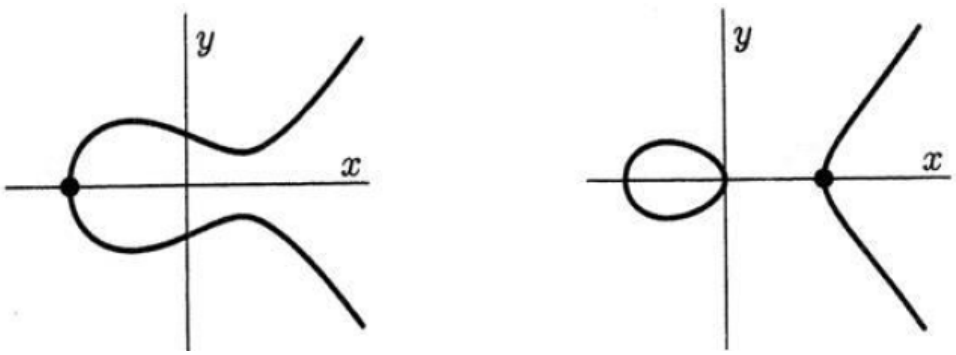


Abbildung 1.4: Elliptische Kurven in $\mathbb{R}$ [6]

Dabei ist das Aussehen der elliptischen Kurve E von $a$ und $b$ abhängig, wie die Abbildung 1.4 dies durch zwei unterschiedliche elliptische Kurven veranschaulicht. Jedoch muss weiterhin erfüllt sein, dass E nicht singulär ist. Dazu reicht es, dass für die Diskriminate von E die folgende Bedingung gilt:

$$4a^3 + 27b^2 \neq 0, a, b \in \mathbb{R} \tag{1.5}$$

Diese Bedingung sorgt dafür, dass die Graphen in der folgenden Abbildung keine elliptischen Kurven sind:

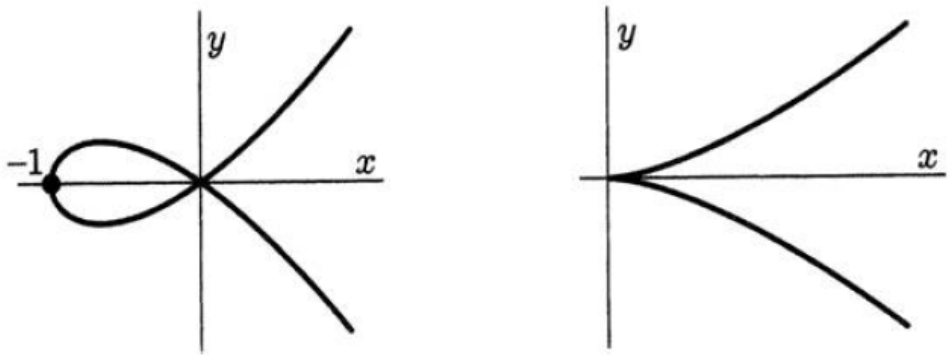


Abbildung 1.5: Singuläre elliptische Kurven in $\mathbb{R}$ [6]

Da für das kryptographische Verfahren die abelsche Gruppe, die durch die elliptische Kurve bestimmt wird, von Bedeutung ist, werden dazu ein geometrischer und arithmetischer Ansatz vorgestellt. Mit diesen Ansätzen wird gezeigt, dass die Addition auf dieser elliptischen Kurven existiert.

**Geometrischer Ansatz**
Für die nächsten Ausführungen ist zu beachten, dass die jeweiligen Summanden und Ergebnisse der Addition jeweils auf der elliptischen Kurven (dem Graph) zu finden sein müssen. Zur Beweisführung folgt immer ein eklärender Text und die jeweilige passende Abbildung, welches das Verfahren genau erklärt dazu.

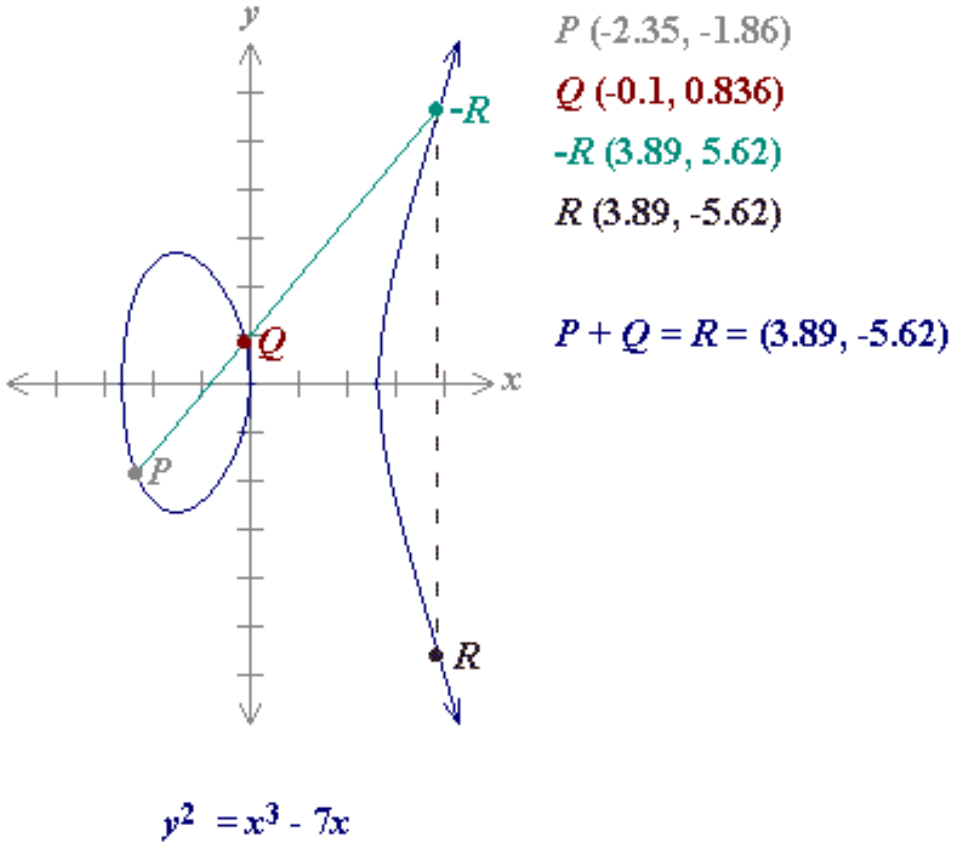


Abbildung 1.6: Addition der Punkte P und Q [7]

**Addition von zwei verschiedenen Punkten: P + Q** Seien P und Q zwei verschiedene Punkte auf der elliptischen Kurve und es gelte P $\neq$ -Q. Die Abbildung 1.6 zeigt dazu, dass eine Linie von P durch Q durchgezogen wird und die elliptische Kurven bei -R noch einmal schneiden wird. Wird -R an der X-Achse gespiegelt, so ist das Ziel der Punkt R, welcher das Ergebnis der Addition von P und Q auf elliptischen Kurven darstellt.

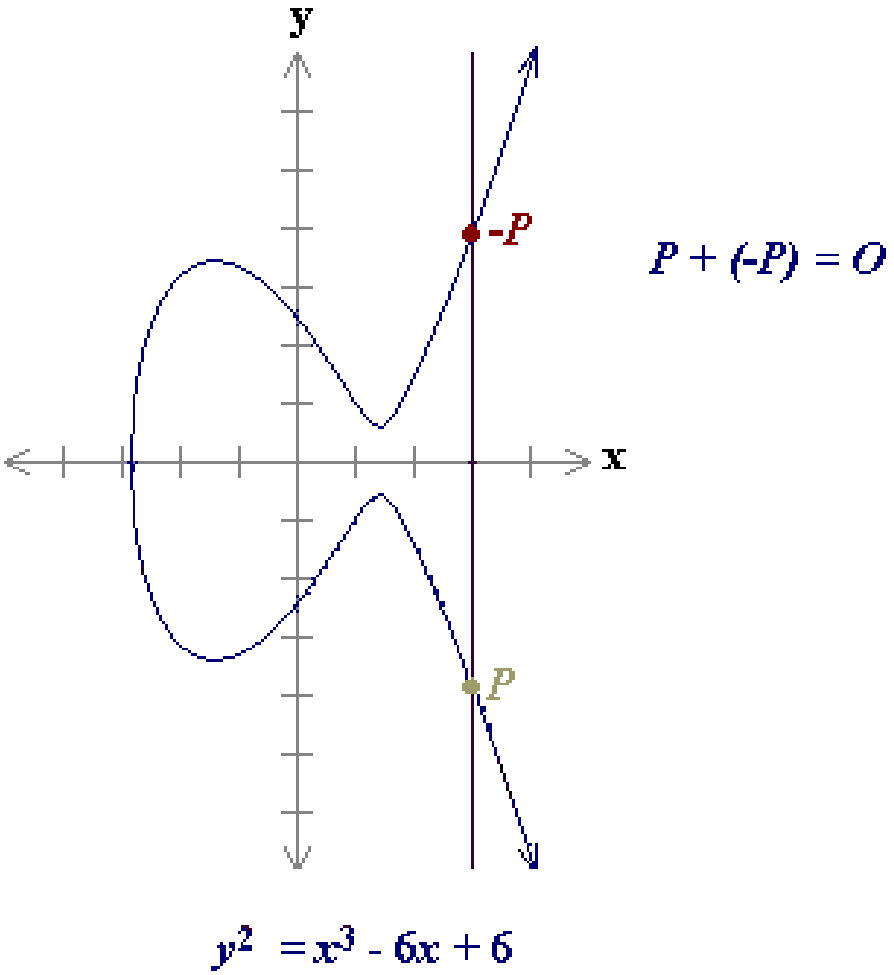


Abbildung 1.7: Addition der Punkte P und -P [7]

**Addition mit dem Inversen: P + (-P)** Das Inverse von P wird durch eine Spiegelung an der X-Achse auf der elliptischen Kurve gefunden. Ebenfalls wird, wie in der Abbildung 1.7, eine Linie durch beide Punkte gezogen. Offensichtlich wird dabei, dass diese Linie die elliptische Kurve kein drittes Mal schneiden kann. Da jedoch der Punkt $\mathcal{O}$ auf der elliptischen Kurve ist, wird somit ein Ergebnis dieser Addition gefunden. Mit der Umstellung der Gleichung zu P + $\mathcal{O}$ = P ist eindeutig, dass $\mathcal{O}$ die Identität der Addition präsentiert.

**Verdoppeln eines Punktes P** Bei der Verdopplung eines Punktes P wird eine Linie eine Tangente, wenn diese einen Punkte auf der elliptischen Kurve schneidet. Wenn yP $\neq$ 0 ist, so wird diese Tangente eine Sekante und schneidet die elliptische Kurve an dem zweiten Punkt -R. Auf einer elliptischen Kurve ist die Formel, wie folgt, definiert: P + P = 2P = R. In der Abbildung 1.8 ist zu erkennen, dass R hierbei der zu -R an der X-Achse

gespiegelte Punkt ist.

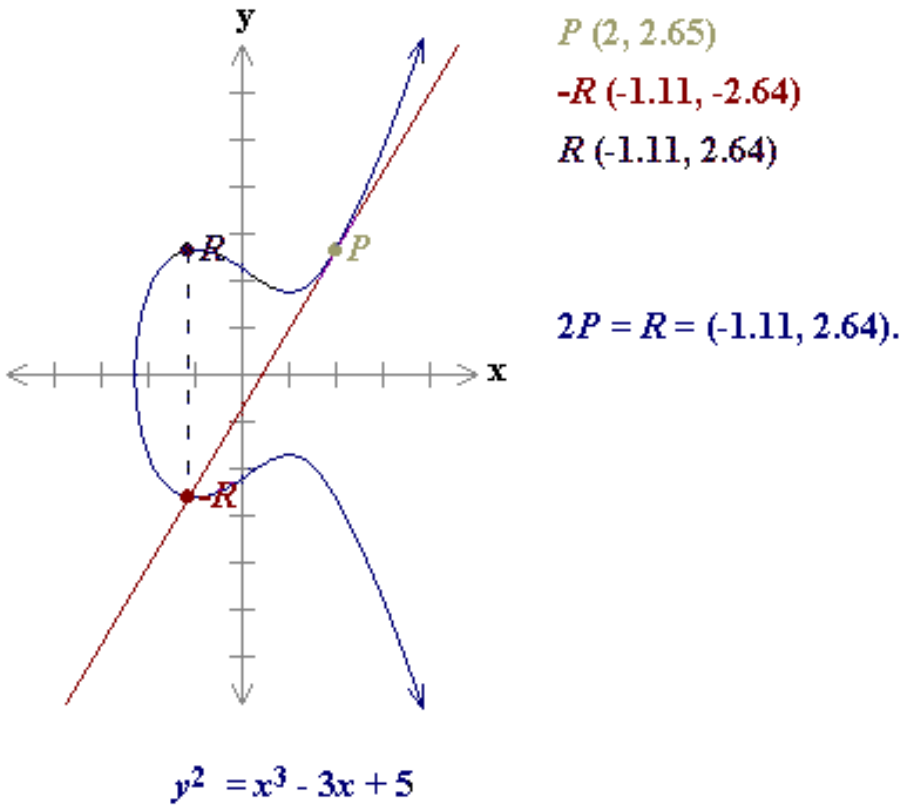


Abbildung 1.8: Verdopplung des Punktes P [7]

In dem Falle, dass yP = 0 ist, bleibt die Linie eine Tangente und schneidet die elliptische Kurve nur einmal. Jedoch ist dies definiert, da als Ergebnis dieser Gleichung den Punkt $\mathcal{O}$ geliefert wird, welches im Folgenden veranschaulicht wird.

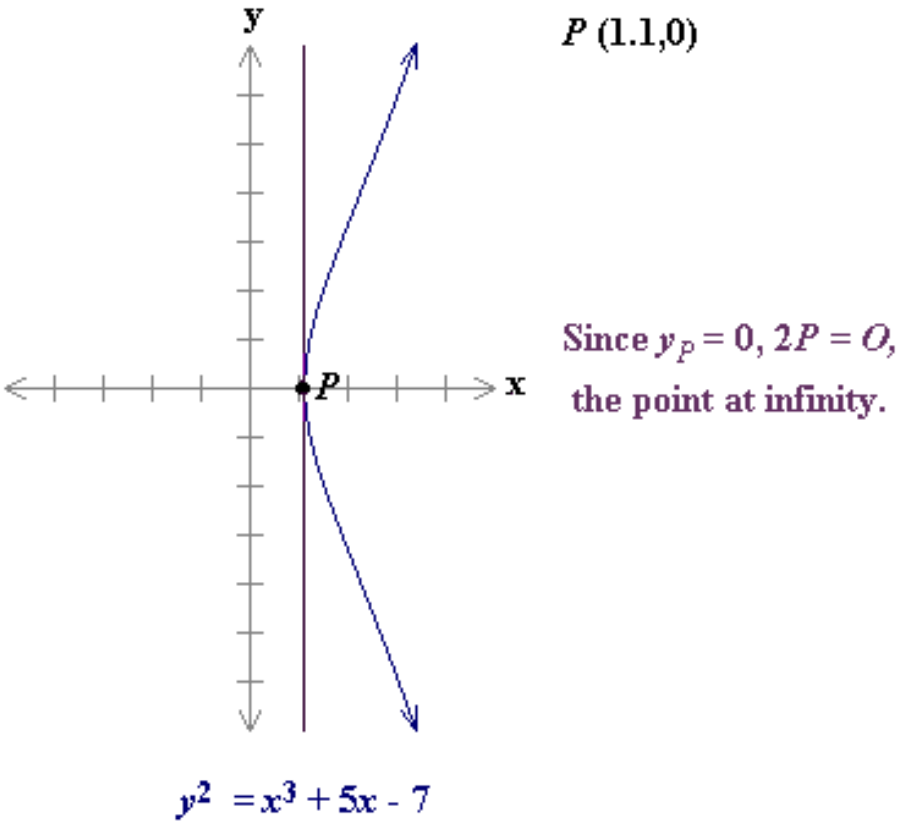


Abbildung 1.9: Vielfaches von einem Punkt P [7]

**Arithmetischer Ansatz**
Neben dem geometrischen Ansatz, bei dem durch einfaches Ablesen im Graphen der elliptischen Kurve die Ergebnisse der Addition identifiziert werden konnten, lassen sich die einzelnen Operationen ebenfalls durch arithmetische Operationen berechnen.

**Addition von zwei verschiedenen Punkten: P + Q** Hier gelten für die Punkte P = $(x_P, y_P)$ und Q = $(x_Q, y_Q)$ die gleichen Voraussetzungen wie beim geometrischen Ansatz, woraufhin der anknüpfende Ablauf zur Berechnung des Punktes R genommen werden kann. Als Hinweis für den Ablauf ist anzumerken, dass s die Steigung der Linie zwischen den Punkten P und Q ist.

- $P + Q = R$
- $s = (y_P - y_Q)/(x_P - x_Q)$
- $x_R = s^2 - x_P - x_Q$ und $y_R = -y_P + s(x_P - x_R)$

Mit dem letzten Schritt wurden die beiden Werte $x_R$ und $y_R$ des Punktes R berechnet.

**Verdopplung eines Punktes P** Ein wichtiger Aspekte bei der Verdopplung eines Punktes P ist, dass $y_P$ nicht 0 betragen darf. Die Berechnung des Ergebnisses geschieht dabei folgendermaßen:

- $2P = R$
- $s = (3x_P^2 + a)/(2y_P)$
- $x_R = s^2 - 2x_P$ und $y_R = -y_P + s(x_P - x_R)$

Weiterhin galt für diesen Ablauf, dass s die Steigung der Linie ist und a einer der Parameter der elliptischen Kurve ist.

Durch beide Ansätze wurde bewiesen, dass sich bei elliptischen Kurven über den reellen Zahlen eine abelsche Gruppe für kryptographische Zwecke definieren lässt. Jedoch sind Berechnung über den reellen Zahlen sehr langsam und aufgrund von Rundungen ungenau, weshalb in der Praxis die Körper über Primzahlen oder Binärzahlen hinzugezogen werden. Die elliptische Kurven über diese beiden Körper werden deshalb im Weiteren erklärt.

### EC über Primzahlen

Im Abschnitt 1.3.1 wurden bereits die Körper der Primzahlen oder $\mathbb{F}_p$ eingeführt und erwähnt, dass dieser die Zahlen von 0 bis p-1 beinhaltet und zugleich Berechnungen mit *modulo p* das Ergebnis in dem Zahlenbereich 0 bis p-1 mit umfasst. Dazu gilt die folgende Formel für die elliptische Kurve über $\mathbb{F}_p$:

$$y^2 \bmod p = x^3 + ax + b \bmod p \tag{1.6}$$

Die Parameter a und b in der Gleichung 1.6 sind wie x und y Elemente des zugehörigen Körpers $\mathbb{F}_p$. Für die elliptische Kurve über $\mathbb{F}_p$ gelten die gleichen Voraussetzungen, um eine Gruppe über diese zu bilden. Das heißt, dass $4a^3 + 27b^2 \bmod p \neq 0$ erfüllt sein muss und die Lösungsmenge der Gleichung 1.6 mit dem unendlichen Punkt $\mathcal{O}$ vereinigt die elliptische Kurve darstellt.
Als Beispiel für eine solche elliptische Kurve kann die nachfolgende Gleichung

über dem Körper $\mathbb{F}_{23}$ gewählt werden:

$$y^2 = x^3 + x \tag{1.7}$$

In dieser Gleichung sind die Parameter a = 1 und b = 0 und bilden damit eine elliptische Kurve, wie in der Abbildung 1.10 veranschaulicht wird. Ferner ist in der Abbildung 1.11 zu erkennen, dass eine Symmetrie zwischen den Punkten durch Spiegelung an der X-Achse vorliegt. Somit ist für jeden Punkt das Inverse auf der elliptischen Kurve zu finden, welches für die Definition der Gruppe notwendig ist.

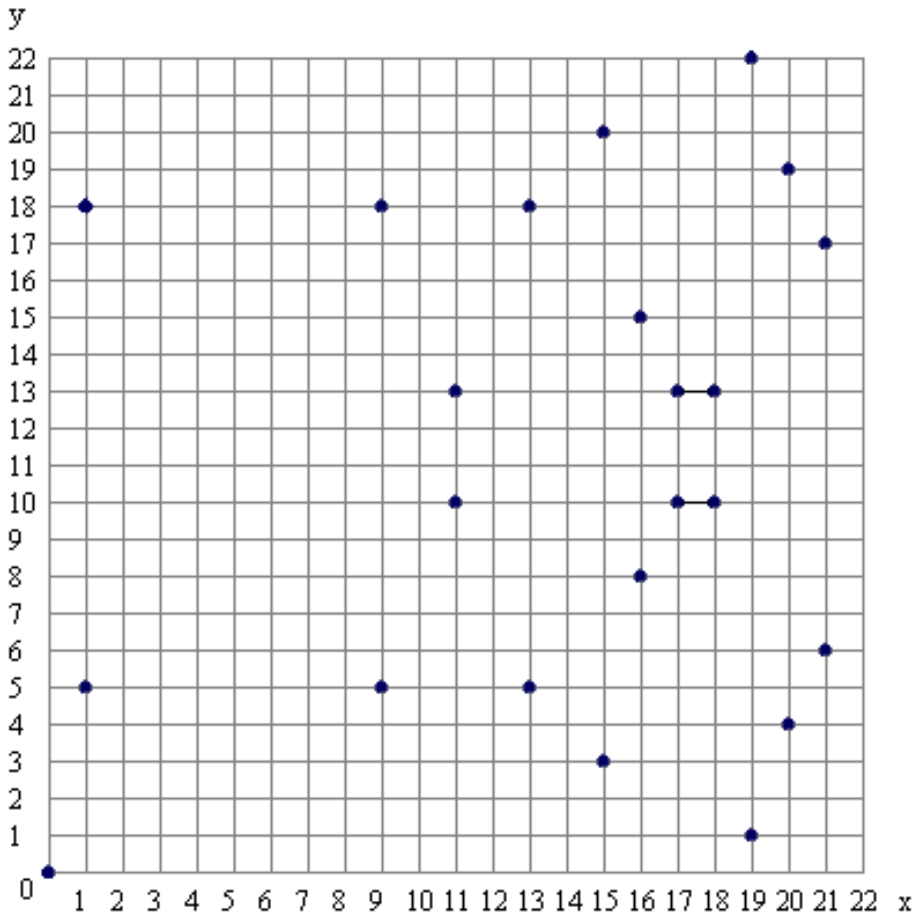


Abbildung 1.10: Beispiel einer elliptischen Kurve über $\mathbb{F}_{23}$ [7]

Für die Definition einer Gruppe wird im nächsten Abschnitt als Beweis der arithmetische Ansatz vorgestellt. Dieser ähnelt dem arithmetischen Ansatz für die elliptische Kurve über $\mathbb{R}$ bis auf den Aspekt, dass alles zusätzlich mit modulo p berechnet wird. Hierbei ist wichtig zu ergänzen, dass elliptische Kurve über $\mathbb{R}$ und $\mathbb{F}_p$ nicht so unterschiedlich sind. Der Hauptunterschied ist, dass elliptische Kurven über $\mathbb{F}_p$ endlich viele Punkte hat, weshalb in dem Graphen nur einzelne Punkte gekennzeichnet sind. Dies führt zwar zu Verwirrung, da keine wirkliche Kurve wie bei der elliptischen Kurve über

$\mathbb{R}$ zu erkennen ist, jedoch lässt sich mit dieser einfacher und genauer rechnen.

**Arithmetischer Ansatz**
Der Vollständigkeit halber wird in diesem Abschnitt nun auf den arithmetischen Ansatz eingegangen, mit dem die Gruppe auf der elliptischen Kurve über $\mathbb{F}_p$ definiert wird.

**Addition von zwei verschiedenen Punkten: P + Q** Wenn die Punkte P = $(x_P, y_P)$ und Q = $(x_Q, y_Q)$ von einander verschieden sind und Q $\neq$ -P ist, so gilt Folgendes:

- $P + Q = R$
- $s = (y_P - y_Q)/(x_P - x_Q) \bmod p$ (Steigung der Linie zwischen P und Q)
- $x_R = s^2 - x_P - x_Q \bmod p$ und $y_R = -y_P + s(x_P - x_R) \bmod p$

**Verdopplung eines Punktes P** Voraussetzung bei der Verdopplung des Punktes P ist, dass $y_p \neq 0$ ist, so dass die Berechnung folgendermaßen aussieht:
*Hinweis: a ist der Parameter der elliptischen Kurve über* $\mathbb{F}_p$

- $2P = P + P = R$
- $s = (3x_P^2 + a)/(2y_P) \bmod p$ (Steigung der Linie, die durch P geht)
- $x_R = s^2 - 2x_P \bmod p$ und $y_R = -y_P + s(x_P - x_R) \bmod p$

Mit dem arithmetischen Ansatz wurde bewiesen, dass eine Gruppe auf der elliptischen Kurve über $\mathbb{F}_p$ existiert. Somit kann diese für die Kryptographie genutzt werden.

**EC über Binärzahlen**

Dieser Abschnitt befasst sich mit den elliptischen Kurven über dem Körper der Binärzahlen oder $\mathbb{F}_{2^m}$. Die Elemente dieses Körpers können als m-bit Strings betrachtet werden, weshalb diese elliptischen Kurven praktisch für Hardwareimplementierungen sind. Im Gegensatz dazu sind elliptische Kurven über $\mathbb{F}_p$ aufgrund der Berechnung sinnvoll für Softwareimplementierungen.

Bei elliptischen Kurven über $\mathbb{F}_{2^m}$ wird vorausgesetzt, dass m $\geq 1$ ist, das gemäß der folgenden Formel a und b Elemente aus $\mathbb{F}_{2^m}$ sind und b ungleich 0 ist:

$$y^2 + xy = x^3 + ax^2 + b \tag{1.8}$$

Die Lösungsmenge der oberen Gleichung und der unendliche Punkt $\mathcal{O}$ bestimmen wie bei allen Körpern die elliptische Kurve. Weiterhin existieren bei dieser Art von elliptischen Kurven endlich viele Punkte, wie im Graph der Formel $y^2 + xy = x^3 + g^4x^2 + l$ in der Abbildung 1.11 beispielhaft zu erkennen ist.

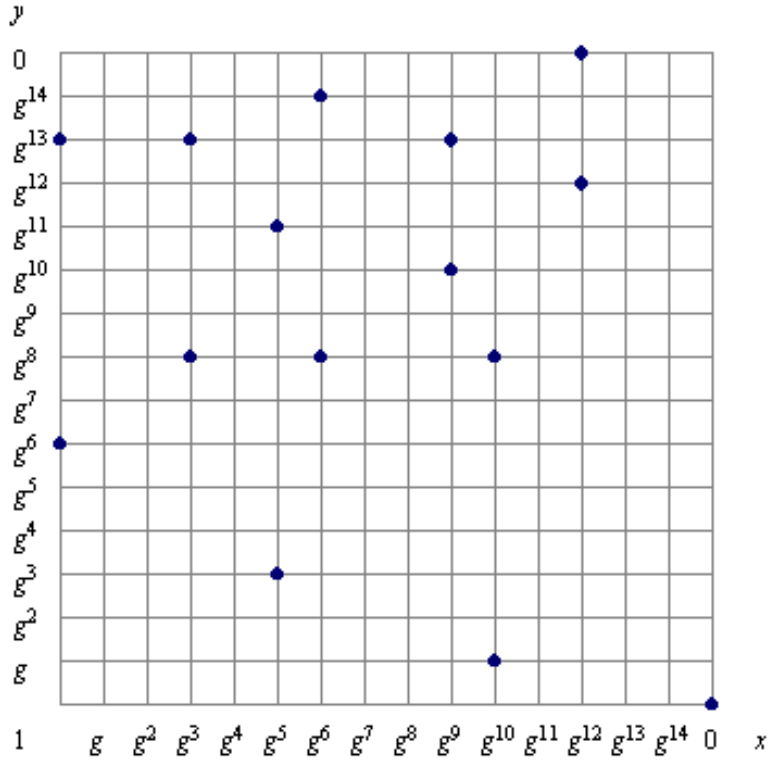


Abbildung 1.11: Beispiel einer elliptischen Kurve über $\mathbb{F}_{2^4}$ [7]

Um zu zeigen, dass durch die elliptische Kurve eine Gruppe definiert wird, wird im Weiteren der arithmetische Ansatz genutzt.

**Arithmetischer Ansatz**
Durch den binären Körper $\mathbb{F}_{2^m}$ lässt sich diese elliptische Kurve effizient am Computer berechnen, wodurch keine Rundungsfehler entstehen können. Die Gruppe einer solchen elliptischen Kurve hat eine endliche Anzahl an Punkten und die nötigen Voraussetzungen einer Gruppe werden im Folgenden bewiesen.

**Addition von zwei verschiedenen Punkten: P + Q** Bei zwei Punkten P = $(x_P, y_P)$ und Q = $(x_Q, y_Q)$, die von einer verschieden sind und Q ebenfalls nicht -P entspricht, sieht die Addition folgendermaßen aus:

- $P + Q = R$
- $s = (y_P - y_Q)/(x_P + x_Q)$ (Steigung der Linie zwischen P und Q)
- $x_R = s^2 + s + x_P + x_Q$ und $y_R = s(x_P + x_R) + x_R + y_P$

Des Weiteren gilt, dass P + (-P) = $\mathcal{O}$ ergibt und P + $\mathcal{O}$ = P die Neutralität von $\mathcal{O}$ in der Addition aufzeigt.

**Verdopplung eines Punktes P** Für die Verdopplung wird vorausgesetzt, dass $x_P$ nicht 0 ist. Falls dies jedoch der Fall ist, so ist das Ergebnis 2P = $\mathcal{O}$ und sonst gilt:
*Hinweis: a ist der Parameter der elliptischen Kurve über* $\mathbb{F}_{2^m}$

- $2P = P + P = R$
- $s = x_P + y_P/x_P$ (Steigung der Linie, die durch P geht)
- $x_R = s^2 + s + a$ und $y_R = x_P^2 + (s + 1) * x_R$

Nach den Ausführungen des arithmetischen Ansatzes für elliptische Kurven über $\mathbb{F}_{2^m}$ wurde deutlich, dass eine Gruppe exisitert, die für sich in der Kryptographie zu nutze gemacht werden kann.

### 1.3.2 Das kryptographische Verfahren

In diesem Abschnitt wird zunächst vorgestellt, wie die Basis der ECC-Verfahren, sprich *Domain Parameter*, definiert wird. Da ECC zu den Public-Key-Verfahren gehört, wird im Anschluss beschrieben, wie das Schlüsselpaar bestehend aus privaten und geheimen Schlüssel generiert wird.

#### Domain Parameter

Laut dem Standard IEEE P1363 ist fr die kryptographischen Verfahren, die auf elliptischen Kurven basieren, ein Satz an Parametern Grundvoraussetzungen. Diese Parameter werden im Folgenden vorgestellt und werden unter dem Begriff *Domain Parameter* zusammengefasst.

- $\mathbb{F}_p$ - Einer der drei oben vorgestellten Körper
- p - Größe des Körpers
- E - Elliptische Kurve
- a und b - Koeffizienten der elliptischen Kurve E mit a,b $\in \mathbb{F}_p$
- n - Primzahl und Teiler der Anzahl der Punkte auf E
- G - Ein Punkt der elliptischen Kurve E mit Ordnung n

Mithilfe dieser Parameter werden der Körper, dessen elliptische Kurve und ein Punkt der Kurve definiert, welche die benötige Gruppe der elliptischen Kurven umschreiben. Mit dieser Basis können die Verfahren aus Kapitel 1.4 durchgeführt werden.

**Schlüsselpaar**

ECC-Verfahren gehören zu den Public-Key-Verfahren, oder auch asymmetrisches Kryptosystem, weshalb bei diesen ein Schlüsselpaar erzeugt werden muss. Das Schlüsselpaar beinhaltet einen öffentlichen und einen privaten Schlüssel. Während der öffentliche Schlüssel zur Verschlüsselung und Authentifizierung genutzt wird, ist der private Schlüssel notwendig, um Daten zu entschlüsseln. Bei ECC-Verfahren wird, wie folgt, vorgegangen:

1. Bestimmung der Domain Parameter
2. privater Schlüssel s $\in$ Z aus dem Intervall [1, n-1]
3. öffentlicher Schlüssel W $\in$ E($\mathbb{F}_p$)
4. Berechnung für $W = s * G$ mit W $\neq \mathcal{O}$

Bei diesem Schlüsselpaar ist wichtig, dass sich s nicht aus W berechnen lässt. Dazu hilft die Tatsache, dass sich die Gleichung $W = s * G$ sich nicht nach s auflösen lässt, da die Division für zwei Punkte einer elliptischen Kurven nicht definiert ist. Ebenfalls darf s nicht zu klein sein, da es sonst durch Vielfachaddition geschätzt werden könnte. Somit besteht der Konflikt, dass s nicht zu klein und nicht zu groß sein darf. Zu groß darf s nicht sein, da sonst die Schlüsselgenerierung zu lange dauern würde. Mit diesen Hinweisen kann das jeweilige Schlüsselpaar für die Kryptoverfahren erzeugt werden.

### 1.3.3 Diskrete Logarithmus-Problem

Zum besseren Verständnis wird zunächst der Logarithmus allgemein eingeführt und anschließend wird das diskrete Logarithmus-Problem auf die elliptischen Kurven übertragen.

$$\alpha = \mu^x \tag{1.9}$$

Die Gleichung 1.9 bewegt sich in einer endlichen zyklischen Gruppe $G$ der Ordnung $r$. Dazu ist $\mu$ ein Erzeuger der Gruppe und $\alpha$ ein beliebiges Gruppenelement. In der Gleichung ist x der diskrete Logarithmus von $\alpha$ zur Basis $\mu$. Die Berechnung von x gilt dabei als schwierig und wird diskretes Logarithmus-Problem (DLP) genannt. Das folgende Beispiel soll dies zeigen:

- $G = F_{13}$, $\mu = 2 \in F_{13}$ und $\alpha = 5$
- $5 = 2^x$
- $x = 9$

Hierbei ist die 9 als Ergebnis schwer zu berechnen, während $2^9$ mod 13 als einfach zu berechnen gilt. (vgl. [8])
Um das DLP nun mit elliptischen Kurven, *Elliptic Curve Discrete Logarithmus Problem (ECDLP)*, zu assoziieren, wird die endliche Gruppe $G$ mit Ordnung n genommen, welche durch eine elliptische Kurve beschrieben wird. In der Gleichung $P = k * G$ ist G der Erzeuger der Gruppe und P ist ein weiteres Element der Gruppe. Im Vergleich zu x vom allgemeinen DLP ist in der Gleichung nun k der diskrete Logarithmus vom Punkt P zur Basis G. Diese Multiplikation sieht einfach aus, ist jedoch auf elliptischen Kurven sehr schwierig, da selbst eine Umstellung nach k nicht möglich ist, weil die Division auf elliptischen Kurven nicht definiert ist. Des Weiteren müsste das k gesucht werden, bei dem eine k-fache Addition von G den Punkt P als Lösung hat. Diese Suche ist jedoch sehr aufwändig, weshalb noch kein schneller Algorithmus bisher entwickelt wurde.
Für den diskreten Logarithmus existieren verschiedene Algorithmen, mit denen dieser berechnet werden kann. Als einer der bekanntesten Algorithmen ist hier der Pollard-Rho-Algorithmus zu nennen, da dieser das ECDLP in exponnentieller Laufzeit lösen kann. Jedoch wäre ein Algorithmus mit subexponnentieller Laufzeit wesentlich angenehmer und aufgrund der langen Laufzeiten sind die Schlüssellängen in der ECC viel kürzer als bei anderen Verfahren.

### 1.3.4 Hinweise

Wie aus den ECDLP hervorgeht, ist es bedeutend, dass dieses nicht schnell gelöst werden kann. Dementsprechend sollte eine elliptische Kurve möglichst

viele Punkte haben, um eine sehr große Gruppe zu erzeugen. Außerdem ist ein entscheidender Aspekt die Auswahl der Parameter einer elliptischen Kurve, da diese eine große Auswirkung auf die Lösbarkeit des ECDLP haben. [9] So sind elliptische Kurven für die Kryptographie ungeeignet, wenn diese anormale und supersinguläre Kurven sind. Anormale Kurven sind Kurven, die über $\mathcal{Z}_p$ genau aus einer Anzahl von p Elementen bestehen. Supersingulär bedeutet, dass das ECDLP auf das DLP in anderen endlichen Körpern vereinfacht werden kann und deshalb berechnet werden kann.

Dieses Kapitel hat das Fundament, wie die mathematischen Grundlagen, die Anwendung der elliptischen Kurven über verschiedenen Körpern und die Domain Parameter sowie den Sicherheitsaspekt durch das ECDLP, gelegt. Unter Beachtung dieses Fundaments kann nun im nächsten Kapitel auf einzelne Verfahren eingegangen werden.

## 1.4 Anwendung in der Praxis

Nachdem die Grundlagen im Kapitel 1.3 gelegt wurden, wird in diesem Kapitel gezeigt, wie die elliptischen Kurven in der Praxis eingesetzt werden. Dazu wurde deren Anwendung in die drei Bereiche, Nachrichtenverschlüsselung, Signaturalgorithmen und Schlüsselaustauschverfahren, gegliedert. [10] [11] [12] In jedem dieser Bereiche werden jeweils zwei Verfahren vorgestellt, um den Einsatz von elliptischen Kurven darstellen zu können. Die im Kapitel 1.3 vorgestellte Notation der Domain Parameter wird in den Beispielen ebenfalls benutzt, weshalb diese hier nochmals aufgelistet wurden:
*Hinweis: Dieses Domain Parameter werden zu Anfang beziehungsweise für jedes Verfahren jeweils bestimmt.*

- $\mathbb{F}_p$ - Einer der drei vorgestellten Körper
- p - Größe des Körpers
- E - Elliptische Kurve
- a und b - Koeffizienten der elliptischen Kurve E mit a,b $\in \mathbb{F}_p$
- n - Primzahl und Teiler der Anzahl der Punkte auf E
- G - Ein Punkt der elliptischen Kurve E mit Ordnung n
- s - privater Schlüssel s $\in \mathbb{F}_p$ aus dem Intervall [1, n-1]
- W - öffentlicher Schlüssel W $\in$ E($\mathbb{F}_p$), $W = s * G$ mit W $\neq \mathcal{O}$

### 1.4.1 The Elliptic Curve Public Key Cryptosystem

Bei *Elliptic Curve Public Key Cryptosystems* geht es um die Verschlüsselung von Nachrichten, welche in diesem Abschnitt anhand von EC ElGamal und ECRSA erläutert wird. Dabei gibt es einen festen Ablauf, der mit der Schlüsselgenerierung, sprich Erstellung von öffentlichen und privaten Schlüssel, beginnt. Im Anschluss verschlüsselt Teilnehmer A mit dem öffentlichen Schlüssel die Nachricht m und sendet diese an Teilnehmer B, so dass Teilnehmer B die verschlüsselte Nachricht m mit dem privaten Schlüssel entschlüsseln kann.

#### EC ElGamal

Das EC ElGamal Kryptosystem ist nach seinem Erfinder Taher Elgamal benannt und wird hier in der Anwendung mit elliptischen Kurven beschrieben.

- Schlüsselgenerierung:

  1. Teilnehmer B wählt einen Integer $s_B$ aus dem Intervall [1, n-1] als privaten Schlüssel aus
  2. Teilnehmer B berechnet $W_B = s_B * G$ und veröffentlicht diesen

- Verschlüsselung:

  1. Die Nachricht m ist der Punkt M auf der elliptischen Kurve E des Körpers $\mathbb{F}_q$
  2. Teilnehmer A bestimmt einen Integer r aus dem Intervall [1, n-1]
  3. Teilnehmer A berechnet $C_1 = rG$ und $C_2 = rW_B + M$

  C = $(C_1, C_2)$ ist der Geheimtext von m und wird an B gesendet.

- Entschlüsselung:

  1. $M = C_2 - s_B C_1$, weil $C_2 - s_B C_1 = rW_B + M - s_B rG = rs_B G + M - s_B rG$
  2. Nachricht m kann aus dem errechneten Punkt M der elliptischen Kurve E gewonnen werden.

**Beispiel [13]**

1. Domain Parameter:
   - $q = 11$
   - $a = -3$ und $b = 5$
   - $n = 15$
   - $G = (8, 3)$
   - $s = 2$
   - $W = sG = 2 * (8, 3) = (0, 7)$
2. Schlüsselgenerierung: W = (s, W) = (0, 7)
3. Verschlüsselung:
   - $M = (8, 8)$, Punkt auf E
   - $r = 13$
   - $C_1 = 13 * (8, 3) = (0, 4)$
   - $C_2 = 13 * (0, 7) + (8, 8) = (5, 7)$
   - Geheimtext: $C = (C_1, C_2) = ((0, 4), (5, 7))$
4. Entschlüsselung:
   - $z = -s * C_1 = -2 * (0, 4) = (1, 5)$
   - $M = z + C_2 = (1, 5) + (5, 7) = (8, 8)$✓

**ECRSA**

In diesem Unterabschnitt wird ECRSA vorgestellt, dessen Name durch die drei Mathematiker Rivest, Shamir und Adleman geprägt wird und hier jedoch auf elliptische Kurven übertragen wurde.

- Schlüsselgenerierung:

  1. Teilnehmer B wählt zwei verschiedene Primzahlen p und q mit der Bedingung: $p \equiv q \equiv 2 \bmod 3$
  2. $n = p * q$
  3. Teilnehmer B wählt die Integer $e_B$ und $s_B$ mit der Bedingung: $e_B * s_B \equiv 1 \bmod (kgV(p + 1, q + 1))$, kgV bedeutet "kleinste gemeinsame Vielfache"
  4. Teilnehmer B veröffentlicht $e_B$ und hält $s_B$ geheim

- Verschlüsselung:

  1. Teilnehmer A hat die Nachricht m als Integerpaar $(m_1, m_2)$ mod n
  2. Integerpaar auf elliptischer Kurve E als Punkt M
  3. E: $y^2 = x^3 + b \bmod n$ mit $b = m_2^2 - m_1^3 \bmod n$ (b muss nicht berechnet werden)
  4. $C = (c_1, c_2) = e_B M$

  C ist somit der verschlüsselte Text der Nachricht m und wird an B geschickt.

- Entschlüsselung:
  B berechnet $s_B C = M$ und M kann auf der elliptischen Kurve E gefunden werden.

### 1.4.2 The Elliptic Curve Based Signature Algorithms

Die Kryptographie wird weiterhin verwendet, um Nachrichten mit einer digitalen Signatur zu versehen, damit dieser Absender authentifiziert werden kann. *Elliptic Curve Based Signature Algorithm* handelt von solchen Verfahren, wie es in diesem Abschnitt beispielsweise an ECDSA und EC Schnorr gezeigt wird. Bei diesen Verfahren werden ebenfalls zuerst die Schlüssel generiert, welchen das jeweilige Schema zur Signierung folgt. Diese Signierung wird vom Gesprächsteilnehmer verifiziert, wodurch die Authentifizierung bei Erfolg abgeschlossen ist.

#### ECDSA

ECDSA ist eines der bekanntesten Signaturverfahren und wurde von dem *National Institute of Standards and Technology (NIST)* entworfen. Die Abkürzung ECDSA steht für *Elliptic Curve Digital Signature Algorithm* und deutet darauf hin, dass das DSA-Verfahren ebenfalls mit elliptischen Kurven funktioniert, wie es im Folgenden vorgestellt wird:

- Schlüsselgenerierung:

  1. Teilnehmer A bestimmt einen Integer $s_A$ aus dem Intervall [1, n-1] als öffentlichen Schlüssel
  2. Teilnehmer A berechnet $W_A = s_A * G$ als öffentlichen Schlüssel

- Signaturschema:

  1. Teilnehmer A wählt einen Integer k aus dem Intervall [1, n-1]
  2. Berechnet $k * G = (x_V, y_V) = V$ und $r = x_V \bmod n$, falls r = 0 zurück zu Schritt 1
  3. Berechne $k^{-1}$ mod n
  4. Berechne e = h(m) mit h als Hash-Funktion definiert durch SHA-1: 0, 1* $\longrightarrow \mathbb{F}_n$
  5. Berechne $d = k^{-1}(e + s_A r) \bmod n$, wenn $s = 0$ zurück zu Schritt 1

  Das Tupel (r, d) ist A's Signatur der Nachricht m.

- Verifikationsschema:

  1. Verifiziere, dass r und d Integer aus dem Intervall [1, n-1] sind
  2. Berechne e = h(m)
  3. Berechne $w = d^{-1} \bmod n$
  4. Berechne $u_1 = e * w \bmod n$ und $u_2 = r * w \bmod n$
  5. Berechne $u_1 * G + u_2 * W_A = (x_1, y_1)$
  6. Berechne $v = x_1 \bmod n$
  7. Akzeptiere die Signatur, nur wenn $v = r$

- Korrektheit:

  1. $u_1 G + u_2 W_A = u_1 G + u_2 s_A G = (u_1 + u_2 s_A) G$
  2. Wenn $u_1 + u_2 s_A = k \bmod n$, dann ist das Schema korrekt
  3. $e = kd - s_A r \bmod n$
  4. $u_1 + s_A u_2 = ew + s_A rw = ed^{-1} + s_A rw = k - s_A rw + s_A rw = k \bmod n$

**Beispiel**

1. Domain Parameter:
   - $q = 23$
   - $a = 3$ und $b = 22$
   - $n = 11$
   - $G = (6, 16)$
   - $s = 3$

- $W = sG = 3 * (6, 16) = (13, 2)$

2. Schlüsselgenerierung: W = (s, W) = (13, 2)
3. Signieren:
   - $k \in [1, 10], k = 6$
   - $e = 10$ (Hashwert von Nachricht m)
   - $V = 6 * (6, 16) = (21, 13) = (x_V, y_V)$
   - $r = 21 \bmod 11 = 10$
   - $d = 6^{-1} * (10 + 3 * 10) = 3$
   - Signatur: (r, d) = (10, 3)
4. Verifizieren:
   - $r$ und $s \in [1, 10]$
   - $e = 10$
   - $w = d^{-1} \bmod n$
   - $u_1 = 10 * 4 \bmod 11 = 7$
   - $u_2 = 10 * 4 \bmod 11 = 7$
   - $u_1 G + u_2 W = 6 * (6, 16) + 6 * (13, 2) = (x_1, y_1)$
   - $x_1 \bmod n = r$? 21 mod 11 = 10✓

**EC Schnorr**

Das EC Schnorr Verfahren besitzt die Besonderheit, dass hierbei eine Hashfunktion zum Einsatz kommt. Wie diese eingesetzt wird und das Verfahren unter elliptischen Kurven funktioniert, wird im Anschluss erläutert:

- Schlüsselgenerierung:
  1. Teilnehmer A bestimmt einen Integer $s_A$ aus dem Intervall [1, n-1] als öffentlichen Schlüssel
  2. Teilnehmer A berechnet $W_A = -s_A * G$ als öffentlichen Schlüssel
- Signaturschema:
  1. Teilnehmer A wählt ein Integer k aus dem Intervall [1, n-1]
  2. Berechne $R = k * G = (x_1, y_1)$ und bestimme $r = x_1 \bmod n$
  3. Berechne $e = h(r, m)$ mit h(r, m) als Hashfunktion: $F_q \times 0, 1^{|m|} \longrightarrow F_n$, falls e = 0, zurück zu Schritt 1

4. Berechne $w = k + s_A * e \bmod n$, falls w = 0, zurück zu Schritt 1

Das Tupel (e, w) ist A's Signatur der Nachricht m.

- Verifikationsschema:

1. Verifiziere, dass e und w Integer aus dem Intervall [1, n-1] sind
2. Berechne $V = w * G + e * W_A = (x_1, y_1)$ und bestimme $r' = x_1 \bmod n$ $(r = x_1)$
3. Berechne $e' = h(r', m)$
4. Akzeptiere, nur wenn e = e'

- Korrektheit:

1. $V = w*G+e*W_A = (k+s_A*e)*G+e*(-s_A)*G = k*G = R$

### 1.4.3 The Elliptic Curve Key Agreement Algorithm

*Elliptic Curve Key Agreement Algorithm* beinhaltet Verfahren, bei denen die Teilnehmer einen geheimen Schlüssel berechnen und austauschen, um Nachrichten zu verschlüsseln. In diesem Abschnitt werden dazu ECDH und ECMQV vorgestellt, welche nach dem Schema laufen, dass zunächst die Schlüsselgenerierung stattfindet. Nach dieser kann jeder Teilnehmer den geheimen Schlüssel zur weiteren Verschlüsselung berechnen und durch den Austausch prüfen, ob diese Berechnung richtig war.

#### ECDH

ECDH steht für *Elliptic Curve Diffie-Hellman*, bei dem jeder der beiden Parteien ein Schlüsselpaar einbringt. Dieses Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel, wobei der öffentliche Schlüssel ausgetauscht wird. Das Verfahren läuft folgendermaßen ab:

1. Domain Parameter bestimmen
2. Jeder Teilnehmer wählt s und berechnet W: $(s_A, W_A)$ und $(s_B, W_B)$
3. Die öffentlichen Schlüssel W werden ausgetauscht
4. Jeder Teilnehmer berechnet P mit
   $P = s_A W_B = s_A s_B G = s_B s_A G = s_B W_A$
5. Die x-Koordinate von P $(x_P)$ ist das gemeinsame Geheimnis:
   $z = x_P \bmod n$

**Beispiel**

1. Domain Parameter:
   - q = 23
   - a = 3 und b = 23
   - r = 11 und k = 3
   - G = (6, 16)
   - $s_A = 3, s_B = 9$
   - $W_A = s_A * G = 3 * (6, 16) = (13, 2)$
   - $W_B = s_B * G = 9 * (6, 16) = (20, 20)$
2. Generierung des geheimen Schlüssels:
   - $P = s_A * W_B = s_B * W_A = (21, 10)$
   - $z = 21 \bmod 11 = 10$

**ECMQV**

ECMQV ist ein Authentifizierungsprotokoll, welches auf dem Diffie-Hellman-Schema basiert und lautet mit vollem Namen *Elliptic Curve Menezes-Qu-Vanstone*. Im Vergleich zu anderen Authentifizierungen basierend auf Diffie-Hellmann bietet MQV Schutz vor aktiven Angreifern wie beispielsweise der Man-in-the-middle-Angriff. Der Ablauf des Verfahrens ist im Folgenden dargestellt:

1. Domain Parameter bestimmen
2. Jeder Teilnehmer wählt s und berechnet W: $(s_A, W_A)$ und $(s_B, W_B)$
3. A generiert das Schlüsselpaar (X, x) mit der Zufallszahl x und einem Punkt P auf der elliptischen Kurve für X = xP
4. B geht wie A vor und generiert (Y, y)
5. Teilnehmer A berechnet: $S_A = x + \overline{X} s_A$ und sendet X an B
6. Teilnehmer B berechnet: $S_B = y + \overline{Y} s_B$ und sendet Y an A
7. Nach dem Austausch berechnet A: $K = hS_A(Y + \overline{Y} * W_B)$
8. B berechnet: $K = hS_B(X + \overline{X} W_A)$
9. Das Ergebnis beider ist das gemeinsame Geheimnis

*Hinweis: In den Berechnungen steht h für einen Faktor, der zu den Domain Parametern gezählt werden kann. Dieser muss sehr klein sein und ist zur Erschwernis für Angreifer gedacht. Des Weiteren gilt, wenn R = (x, y) ist, so ist* $\overline{R} = (x \ mod \ 2^L) + 2^L$ *und* $L = [\frac{[log_2 n]+1}{2}]$.
Um Korrektheit nachzuweisen, gilt die folgende Formel zur Berechnung und Umstellung von K (hier wird von A nach B umgestellt):

- $K = h * S_A * (Y + \overline{Y} * W_B) = h * S_A * (y * P + \overline{Y} * s_B * P) = h * S_A * (y + \overline{Y} * s_B) * P = h * S_B * S_A * P = h * S_B * (x + \overline{X} * s_A) * P = h * S_B * (x * P + \overline{X} * s_A * P) = h * S_B * (X + \overline{X} * W_A) = K$
- Damit ist bewiesen, dass beide Teilnehmer das gleiche K berechnen.

Die in diesem Kapitel vorgestellten Verfahren werden in den verschiedensten Technologien angewendet, was schon die Einteilung in die verschiedenen Bereiche veranschaulicht. Zu der allgemeinen Nutzung von ECC und deren Verfahren wird ein Fazit im nächsten Kapitel gezogen.

## 1.5 Zusammenfassung

In den vorigen Kapiteln wurde gezeigt, dass ECC auf vielen mathematischen Grundlagen beruht, wie beispielsweise der Algebra und der Zahlentheorie. Dazu wurde die elliptische Kurven über verschiedenen Körpern abgebildet, um deren Vorteile und Berechenbarkeit darzulegen. Nach einer Erläuterung der allgemeinen Vorgehensweise von ECC und der Bestimmung der Domain Parameter wurde die Sicherheit von ECC anhand des ECDLP veranschaulicht. Mittels der Grundlagen konnten danach weiterhin einige Kryptographieverfahren vorgestellt werden, um die verschiedenen Anwendungsbereiche von ECC zu beschreiben.
Somit erweist sich, dass ECC für kryptographische Zwecke geeignet ist. Ein Beispiel für deren Anwendung ist die in Österreich eingeführte Bürgercard, welche eine Sozialversicherungskarte ist und als Chipkarte ebenfalls fungiert. Diese benutzt ECC bereits zur Verschlüsselung und ein weiteres berühmtes Beispiel ist der Informationsverbund Bonn-Berlin (IVBB). Weiterhin werden die alten Verfahren durch ECC-Verfahren eingesetzt, sprich RSA wird durch ECRSA ersetzt und weitere Anwendungen sollen für E-Mails und Online Banking entwickelt werden. Diese Beispiele zeigen, dass ECC derzeit schon voll in die Kryptographie integriert ist. So treibt vor allem in Deutschland das BSI die Weiterentwicklung und Standardisierung voran.
Wichtig bei der Nutzung von ECC ist, dass entweder fertige elliptische Kurven von vorhandenen Standards genutzt werden sollten oder eigene erstellte elliptische Kurven generiert werden können. Bei eigenen elliptischen Kurven ist es entscheidend, dass bestimmte Kriterien erfüllt werden, damit keine

schwachen elliptischen Kurven erstellt werden, welche für eine Anwendung ungeeignet sind, da diese die Verfahren ineffizient machen. Aus diesem Grund hat das BSI eine Liste veröffentlicht, die alle bedeutenden Kriterien aufweist, um selbst starke elliptische Kurven zu erzeugen.

# Literaturverzeichnis


[1] S. A. Vanstone A. J. Menezes, P. C. van Oorschot. *Handbook of Applied Cryptography.* CRC Press, August 2001.

[2] IEEE. *1363a-2004 - IEEE Standard Specifications for Public-Key Cryptography - Additional Techniques.* IEEE, 2004.

[3] Prof. Bernhard Esslinger und das CryptTool Entwickler-Team. *Das CryptTool-Skript - Kryptographie, Mathematik und mehr.*

[4] Nicholas Jansma and Brandon Arrendondo. *Performance Comparison of Elliptic Curve and RSA Digital Signatures.* 29. April 2004.

[5] Bundesamt für Sicherheit in der Informationstechnik. *BSI - Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, TR-02102.*

[6] Berit Grußien. *Einführung: Elliptische Kurven in der Kryptologie.*

[7] Certicom. *ECC Tutorial.*

[8] Birgit Henhapl. *Zur Effizienz von Elliptische Kurven Kryptographie.* TU Darmstadt, 2003.

[9] J. Buchmann. *Einführung in die Kryptographie.* Springer, 2009.

[10] A. Menezes D. Hankerson and S. Vanstone. *Guide to Elliptic Curve Cryptography.* Springer, 2004.

[11] Zhaohui Cheng. *Simple Tutorial on Elliptic Curve Cryptography.* Dezember 2004.

[12] Simon Blake-Wilson. *STANDARDS FOR EFFICIENT CRYPTOGRAPHY - SEC 1: Elliptic Curve Cryptography.* Certicom Research, 1999.

[13] Michaela Schuster. *Die Verwendung elliptischer Kurven in der Kryptographie.* TU Wien, 2004.

# Kapitel 2

# Virtuelle Währungen

*Moritz Kroß*

*Durch die fortschreitende Vernetzung und Technologisierung unserer Lebensbereiche ist es wichtig, auch unsere Währungen weiter zu entwickeln. Aus diesem Grund wurden in den letzten Jahren vermehrt virtuelle Währungen entwickelt, deren Wert einerseits an einfacher Nutzbarkeit und andererseits an Sicherheit und Stabilität gemessen werden. Diese Seminararbeit beschäftigt sich deshalb mit der Funktionsweise, Nutzungsmöglichkeiten, auftretenden Problemen und Auswirkungen auf die Finanzwelt. Als Vertreter der Kryptowährungen wird haupstächlich Bitcoin veranschaulicht, ausgewertet und beurteilt.*

# Inhaltsverzeichnis

## 2.1 Einleitung

### 2.1.1 Warum Virtuelle Währungen?

Durch den zunehmenden Kontakt mit dem Internet, wurde auch die Frage nach sicheren Zahlungsmethoden größer. Da es nicht ohne weiteres möglich ist, herkömmliches Geld in einer virtuellen Gemeinschaft zu benutzen und die Transfermöglichkeiten nicht immer vertrauenswürdig erscheinen, wurde in den letzten Jahren vermehrt an sicheren, stabilen und dezentralen Währungen gearbeitet.

Diese Seminararbeit behandelt zunächst die Definition und Klassifizierung der verschiedenen virtuellen Währungen. Anschließend werden Kryptowährungen, anhand des Beispiels Bitcoin, erläutert. Dabei wird auch auf Unterschiede innerhalb der Kryptowährungen eingegangen. Das darauffolgende Kapitel befasst sich mit einem Vergleich zu realen Währungen. Dazu werden erst die Funktionen von Geld aufgezeigt und diese dann den Kryptowährungen gegenübergestellt. Im Anschluss werden technische, wirtschaftliche und politische Probleme erläutert, die diese Art von Währungen mit sich bringen. Abschließend wird ein Fazit gezogen und eine Entwicklungsprognose behandelt.

### 2.1.2 Definition Virtueller Währungen

#### Definition: Europäische Zentralbank

Für die Europäische Zentralbank stellt eine virtuelle Währung eine Quelle für unreguliertes, digitales Geld dar, das nur durch ihre Entwickler herausgegeben und kontrolliert wird. Es wird nur akzeptiert und benutzt durch eine bestimmte virtuelle Gemeinschaft.

> *¨A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community."*[1]

#### Definition: US-Finanzministerium

Für das US-Finanzministerium ist eine virtuelle Währung ein Tauschmittel, das nur bedingt die Eigenschaften einer herkömmlichen Währung besitzt. Es wird darauf hingewiesen, dass diese Währungen keine gesetzlichen Grundlagen als Zahlungsmittel haben.

> *¨In contrast to real currency, "virtual"currency is a medium of exchange that operates like a currency in some environments, but*

*does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."*[2]

### 2.1.3 Klassifizierung

Die Europäische Zentralbank hat virtuelle Währungen in 4 verschiedene Typen aufgeteilt. Die Richtung des Zahlungsflusses bestimmt hauptsächlich die Klassifizierung der unterschiedlichen Währungen. Die Informationen zu diesem Kapitel stammen aus einem Dokument, das von der europäischen Zentralbank im Oktober 2012 veröffentlicht wurde.[1]


Abbildung 2.1: Klassifizierung Virtueller Währungen[1]

#### Typ 1 - ¨in-game-only¨-Währungen

Währungen vom Typ 1 haben keinen Bezug zu realem Geld. Deshalb werden sie auch als ¨in-game-only¨-Zahlungsmittel bezeichnet. Im Verlauf eines Spiels, wird dieses Geld verdient und kann nur für angebotene virtuelle Güter und Dienstleistungen benutzt werden. Ein Handel außerhalb der vorgesehenen Community wird ausgeschlossen. Ein typisches Beispiel hierfür ist Gold in "World of Warcraft".

#### Typ 2 [1]

Bei Währungen vom Typ 2 ist der Geldfluss eingeschränkt. Er ist nur in eine Richtung möglich. Allgemein wird durch reales Geld eine gewisse Menge an virtuellem Geld erworben. Ein Rücktausch ist jedoch nicht möglich. Die Tauschbedingungen werden vom Herausgeber der Währung festgelegt. Ein Beispiel für Währungen vom Typ 2 sind Facebook Credits (FB). Der Tauschwert lag bei 1 FB = 0,10 USD[2]. Diese wurden jedoch 2013 wieder durch landestypische Währungen ersetzt.

[1] Es gibt keine eindeutige Bezeichnung für diesen Typ
[2] US-Dollar

#### Typ 3 - Nicht-Kryptowährungen

Typ 3 beschreibt Währungen, bei denen der Geldfluss in beide Richtungen möglich ist. Dieses Konzept ermöglicht es virtuelles Geld mit echtem Geld zu erwerben, aber auch wieder zurück zu tauschen. Dabei gelten aktuelle Wechselkurse der Hartwährung. Ein Beispiel für Nicht-Kryptowährungen ist das deutsche Bonussystem PayBack. Durch ausgeben von realem Geld erhält man PayBack-Punkte. Gesammelte Punkte können in Echtgeld umgewandelt oder gegen Prämien eingetauscht werden.

#### Typ 3a - Kryptowährungen

Währungen des Typs 3a verhalten sich den Grundsätzen von Typ 3 entsprechend. Jedoch gibt es Börsen und Handelsplattformen, die Wechselkurse erzeugen. Weiterhin gibt es keine zentralen Erzeuger oder Kontrollorgane. Das populärste Beispiel für eine solche Währung ist Bitcoin.

## 2.2 Kryptowährungen

### 2.2.1 Warum Bitcoin?

#### Stellungnahme des Gründers

Der Gründer des Bitcoin-Netzwerks, Satoshi Nakamoto[3], stellt eindeutig die Vertrauenswürdigkeit der Zentralbanken in Frage. Seiner Meinung nach gab es in der Geschichte der zentralen Kontrollorgane von Geld ausreichend Beispiele an Vertrauensbrüchen. Er zieht weiterhin Parallelen zum Schutz von Passwörtern, die mittlerweile durch massive Verschlüsselung geschützt werden. Seine Absicht ist es Geld genauso gut abzusichern, wie es mit Passwörtern schon seit geraumer Zeit geschieht und Mittelsmänner, Organisationen oder Institute aus den Transaktionen der Nutzer auszuschließen.

> *"The root problem with conventional currency is all the trust thats required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust..."* [3]

[3]Das ist ein Pseudoynm. Die Person, Gruppe oder das Unternehmen ist unbekannt.

### 2.2.2 Wie funktioniert Bitcoin?

#### Allgemein

Angelehnt an das klassische Bankensystem hat jeder Benutzer von Bitcoin mindestens ein Konto. Von diesem Konto aus werden alle Überweisungen, im Folgenden Transaktionen genannt, getätigt. Jedes Konto besitzt ein eindeutiges Schlüsselpaar, bestehend aus öffentlichem und privatem Schlüssel. Mit diesem werden Transaktionen anderer Nutzer verifiziert und eigene Transaktionen signiert. Das führt dazu, dass eine digitale Münze (Bitcoin) als Kette von Signaturen definiert wird. Diese Münze wird durch Transaktionen an neue Besitzer weitergegeben und eventuell aufgeteilt.

#### Transaktionen

Eine Transaktion enthält 6 Teile:

1. Versionsnummer
2. Anzahl der Eingänge
3. Liste der Eingänge
4. Anzahl der Ausgänge
5. Liste der Ausgänge
6. Zeitstempel

Hierbei sind vor allem die Listen der Ein- und Ausgänge zu betrachten. Die Liste der Eingänge stellt den Geldbetrag dar, den ein Nutzer besitzt. Die Liste der Ausgänge beschreibt die ¨Ziele¨ einer Überweisung. Es können mehrere Empfänger angegeben werden und das ist auch notwendig, da innerhalb einer Transaktion immer der komplette Geldbetrag transferiert werden muss. Will man eine Transaktion tätigen die nur einen Teil seines gesamten Geldbetrages betrifft, so wird trotzdem das gesamte Kapital verschickt. Ein Teil an einen neuen Empfänger und der Rest an sich selbst. Den Teil des Geldbetrages, der an sich selbst transferiert wird, bezeichnet man als ”Wechselgeld”. Es kann vorkommen, dass sie Summe der Eingänge höher ist, als die Summe der Ausgänge. Die Ausgänge bestehen aus einer Liste von Bitcoin-Adressen, also Hashwerten von öffentlichen Schlüsseln. Eine vollständige Transaktion wird immer durch den privaten Schlüssel des Senders signiert. Der Sender schickt seine Transaktionen an alle ihm bekannten Bitcoin-Clients im Netzwerk. Diese verifizieren die Signatur und prüfen, ob die Transaktion gültig ist. Im folgenden werden sie weitergeleitet bis alle Clients im Netzwerk die Transaktion kennen. Nun wird begonnen sie

in der Block Chain zu verarbeiten.

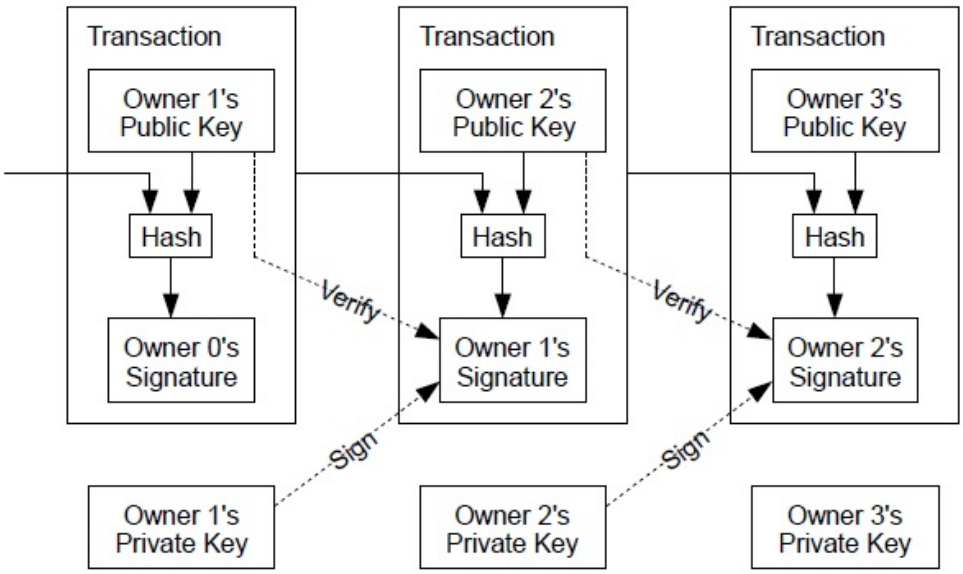


Abbildung 2.2: Signierung von Transaktionen[4]

Eine Transaktion kann nicht rückgängig gemacht werden. Es wird also sichergestellt, dass nur Personen, die den privaten Schlüssel eins Kontos kennen, eine Transaktion ausführen können. Da Eingänge und Ausgänge zusammenhängen, kann eine Person nur soviel Geld ausgeben, wie sie auch durch Eingänge besitzt.[5]

### Wallet

Die Geldbörse, also das Konto eines Nutzers, wird auch als ¨Wallet¨ bezeichnet. Diese speichert das Schlüsselpaar, mit öffentlichem und privatem Schlüssel. Insbesondere werden keine Bitcoins in der Geldbörse gespeichert. Der private Schlüssel wird benutzt um neue Transaktionen zu signieren und zu beweisen, dass der Besitz der Bitcoins, die an diese Adresse versendet wurden, gerechtfertigt ist. Die Adresse entspricht dem öffentlichem Schlüssel. Um einem Schlüsseldiebstahl zuvorzukommen, bieten die meisten digitalen Geldbörsen die Möglichkeit an, diese mit einem weiteren Passwort abzusichern. [8]

### Block Chain

Da das Bitcoin-Netzwerk keine zentrale Instanz zur Kontrolle vorsieht, ist der einzige Weg festzustellen, ob eine Transaktion gültig ist, alle vorherigen Transaktionen zu kennen. Dies geschieht durch die Block Chain. Beim

Tätigen einer Transaktion, wird diese im Netzwerk bekanntgegeben. Nach Überprüfung ihrer Korrektheit werden alle Transaktionen in einem Block zusammengefasst und mit einer Referenz auf den Vorgängerblock versehen. Ein Block enthält grundlegend Datum, Uhrzeit, eine Zufallszahl, Referenzen auf die enthaltenen Transaktionen und den Hash des vorhergehenden Blocks. Diese Datensammlung wird mit einer rechenintensiven kryptographischen Aufgabe verrechnet und die Lösung dieser Aufgabe bildet einen neuen Block innerhalb der Block Chain. Dieser wird nun wiederum im Netzwerk bekanntgegeben. Es besteht die Möglichkeit, dass annähernd gleichzeitig zwei Knoten im Netzwerk die kryptographische Aufgabe für verschiedene Transaktionen lösen, sodass zwei Überweisungen akzeptiert werden, die dasselbe Geld (die selben Eingänge) an unterschiedliche Ziele transferieren. Jedoch speichert jeder Knoten[4] nur die längste Block Chain. Durch die Latenzschwankungen im Internet, wird sich mit der Zeit immer nur eine Block Chain durchsetzen. Ein Block gilt wegen diesem Problem erst als verifziert, wenn mindestens 4 Folgeblöcke erzeugt wurden. Zudem wird immer der früher erzeugte Block als gültig angesehen.[8]

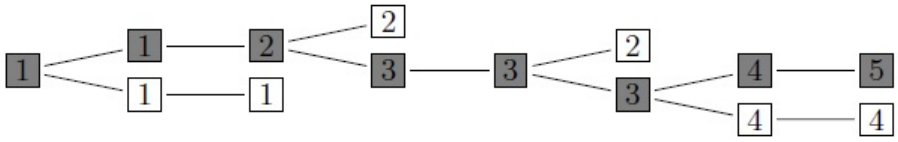


Abbildung 2.3: Verzweigung der Block Chain[5]

### Mining

Als Mining wird der Versuch bezeichnet die Lösung für die kryptographische Aufgabe zur Verifzierung eines Blocks zu finden. Allgemein besteht die Aufgabe darin, dem Block nach einem definierten Schema Bits hinzuzufügen und zu ¨hashen¨. Entsteht dabei eine gewisse Anzahl an Nullen, ist die Aufgabe gelöst. Da im Netzwerk etwa alle 10 Minuten eine Block erzeugt werden soll, ist die Anzahl der Nullen variabel und wird an die aktuell im Netzwerk vorhandene Rechenleistung angepasst. Eine Hashwertberechnung als Aufgabe zu benutzen hat den Vorteil, dass eine Lösung schwer zu finden, aber leicht zu überprüfen ist. Für den Knoten, der die Lösung findet, wird eine Belohnung in Form von Bitcoins ausgeschüttet. Mit der Zeit wird diese Belohnung immer geringer. Also auch der Anreiz Rechenleistung ins Netz zu investieren.[8]

[4]Benutzer, der als Schlüsselstelle zwischen sehr vielen Clients fungiert, die Block Chain lokal speichert und aktualisiert

### 2.2.3 Unterschiede innerhalb der Kryptowährungen

Über die Jahre haben sich einige verschiedene Kryptowährungen entwickelt. Dabei haben die Entwickler der jeweiligen Systeme auf verschiedene Bereiche Schwerpunkte gelegt. Während innerhalb von Bitcoin mittels SHA-256d gehasht wird, verlässt sich Ripple beispielsweise auf ECDSA und Litecoin gar auf scrypt. Ebenso gab es verschiedene Ansätze für die Überprüfung und Verifizierung von Transaktionen. Während sich Bitcoin als Branchenvorreiter nur auf eine Proof-of-Work Methode verlässt, kombiniert Peercoin diese und Proof-of-Stake. Ripple als Brückenwährung verzichtet gänzlich auf eine dieser Methoden. Weiterhin wird durch den Entwickler festgelegt, wieviele Coins einer Währung maximal durch das Netzwerk erzeugt werden können. So wurde ermittelt, dass es rund 84 Millionen Litecoins [5] geben wird, jedoch nur rund 21 Millionen Bitecoins [6]. Durch die zeitlich versetzte Entwicklung, die unterschiedlichen Erzeugungs- und Verifizierungssysteme und durch die unterschiedliche Maximalmenge an möglichen Coins haben sich auch deutlich verschiedene Kurse, gemessen an realen Währungen, etabliert. Im Anhang findet sich eine Tabelle (2.6.1), die die Unterschiede aufzeigt, und ebenso die Erklärungen zu den einzelnen Verfahren und Methoden. (2.6.2)

## 2.3 Vergleich

### 2.3.1 Zeitstrahl: Die Entstehung von Geld

**6. Jahrtausend v. Chr.:** Eine des ersten Formen von Währungen war das Naturalgeld. Als Naturalgeld werden Gegenstände bezeichnet, die als allgemeines Tauschmittel und als Wertmaßstab dienen. Sie wurden überall akzeptiert, angenommen und konnten wiederum gegen andere Güter eingetauscht werden. Beispiele für Naturalgeld sind Muscheln, Schmuck, aber auch Naturalien wie Salz oder Kakaobohnen.

**7. Jahrhundert v. Chr.:** Zu dieser Zeit wurden hauptsächlich Barren und linsenförmige Metallstücke als Zahlungsmittel verwendet.

**1. Jahrhundert v. Chr.:** Münzen setzen sich erstmals als Zahlungsmittel durch. Hierbei wurde unterschieden zwischen Kuper-, Messing-, Silber- und Goldmünzen.

[5] siehe http://altcoinmarkt.de/?p=18
[6] siehe https://de.bitcoin.it/wiki/FAQ

**8. Jahrhundert n. Chr.:** Der Denar, eine Münze, stellt die erste bekannte Einheitswährung in Europa dar. Diese konnte sich aber nicht durchsetzen und wurde sehr schnell wieder abgeschafft.

**10. Jahrhundert n. Chr.:** In China entwickelten sich Münzen aus Eisen. Diese waren sehr schwer und wurden so in einem Laden deponiert. Der Käufer erhielt dafür ein Stück Papier auf dem der Wert des Depots vermerkt war. In der Geschichte des Geldes war dies das erste Papiergeld.

**15. Jahrhundert n. Chr.:** In Europa entsteht ein ähnliches Papiergeld. Der aufgedruckte Wert stimmte aber nicht mit dem tatsächlichen Wert überein und so wurde das Geld von der Bevölkerung nicht gut angenommen.

**19. Jahrhundert n. Chr.:** Mit der Zeit setzte sich Gold als internationaler Währungsstandard und als Bemessungsgrundlage durch. Im späten 19. Jahrhundert wurden die ersten bargeldlosen Zahlungen getätigt.

**20. Jahrhundert n. Chr.:** Die Modernisierung im 20. Jahrhundert brachte einige Neuerungen im Zahlungssystem mit sich. So wurden Kreditkarten eingeführt und das Geld wurde erstmals durch Bankinstitute kontrolliert und es wurde versucht Währungen gezielt zu stabilisieren. Weiterhin wurde zu Ende des 20. Jahrhundert Online-Banking, sowie die Chip-Karte eingeführt.[12]

### 2.3.2 Funktionen von Geld

#### Tausch- und Zahlungsmittel

In erster Linie gilt Geld als Tauschmittel, das den Handel von Gütern ermöglichen soll. Da Geld auch dazu benutzt wird Kredite zu gewähren oder Schulden zu begleichen, wird es ebenfalls als Zahlungsmittel bezeichnet. Denn hierbei geht es nicht um den Austausch von Gütern, sondern um Finanztransaktionen.

#### Recheneinheit

Geld ist eine abstrakte Einheit. Sie erlaubt es Güter- und Vermögenswerte in einer allgemeinen Bezugsgröße auszudrücken und dadurch vergleichbar zu machen. So müssen nicht die Austauschverhältnisse aller Güter untereinander ermittelt werden, sondern nur das Verhältnis zu einer Währung.

**Wertaufbewahrungsmittel**

Zwischen dem Kauf und Verkauf von Waren kann ein zeitlicher Abstand entstehen. Aus diesem Grund dient Geld auch als Wertaufbewahrungsmittel. So lässt sich ein gewisser Wert ¨speichern¨ und zu einem späteren Zeitpunkt abrufen.[6]

### 2.3.3 Eigenschaften von Geld und virtuellen Währungen

Mit der Entwicklung der heutigen Zahlungssysteme haben sich zentrale Eigenschaften für Geld ergeben.

1. Zuverlässigkeit: Leicht zu handhaben und immer funktionsfähig
2. Fälschungssicherheit: Keine Fälschung ist möglich
3. Universalität: Einsetzbar in jeder Umgebung
4. Konvertierbarkeit: Der Geldfluss ist in beide Richtungen möglich
5. Unabhängigkeit: Unabhängig vom Herausgeber, kann die Währung getauscht oder mit ihr bezahlt werden
6. Anonymität: Es darf kein Bezug zwischen dem Kunden und seinen Transaktionen hergestellt werden
7. Übertragbarkeit: Die Währung muss jederzeit zu einem anderen Benutzer übertragbar sein
8. Teilbarkeit: Es muss möglich sein die Währung in kleineren Teilbeträgen auszugeben

Im Folgenden werden nun virtuelle Währungen, am Beispiel Bitcoin, auf diese Eigenschaften überprüft.

**Zuverlässigkeit** Die dezentrale Architektur des Bitcoin-Netzwerks stellt die Funktionsfähigkeit sicher.

**Fälschungssicherheit** Bis zum jetzigen Zeitpunkt sind keine Fälschungen oder Fälschungsmöglichkeiten bekannt.

**Universalität** Übertragungen durch diverse Geräte wie PC und Handy sind bekannt. Jedoch gibt es kein entsprechendes reales Pendant zu Bitcoins.

**Konvertierbarkeit** Eine Konvertierung in andere Währungen ist zwar jeder Zeit möglich, jedoch nur durch Handel mit dezentralen Börsen wie z.B. Mt. Gox.

**Unabhängigkeit** Da Bitcoins keine offiziellen Herausgeber hat, sondern übers Netzwerk erzeugt werden, gilt die Währung per Definition als unabhängig.

**Anonymität** Alle Transaktionen über das Netzwerk bekanntgegeben. Diese werden jedoch verschlüsselt und somit wird die Anonymität gewährleistet.

**Übertragbarkeit** Die Bitcoins können zu jeder Zeit einem anderen Nutzer übertragen werden.

**Teilbarkeit** Bitcoins können zur Ermittlung eines Warenwertes auf bis zu 8 Nachkommastellen geteilt werden.

**Fazit: Technisch gesehen verdeutlicht das Beispiel Bitcoin, dass virtuelle Währungen die zentralen Eigenschaften von herkömmlichen Zahlungssystemen erfüllen.**[6]

## 2.4 Probleme

### 2.4.1 Technisch

**Klassische Schwachstellen** Bitcoins nutzen kryptographische Algorithmen als Basis. Dementsprechend ist die Sicherheit des Netzwerks davon abhängig, das der verwendete Algorithmus nicht gebrochen wird. Innerhalb von Bitcoin betrifft das hauptsächlich die Verfahren SHA-256d und ECDSA. Sollten wesentliche Schwachstellen entdeckt werden, könnten die Hash- und Signaturverfahren jedoch von Seiten der Entwickler verändert und angepasst werden. Eine weitere Schwachstelle stellen die virtuellen Geldbörsen, die Konten, dar. Wie bei jeder Software, könnten die beteiligten Clients selbst kompromittiert werden. Da alle Transaktionen von den öffentlichen und privaten Schlüsseln abhängig sind, wird eine Geldbörse nahezu nutzlos, sollten diese bekannt bzw. geklaut werden. Mittlerweile werden auch die Geldbörsen verschlüsselt, was dieses Problem weitestgehend löst. Möglich sind auch Hintertüren in der Software selbst, um an Daten zu gelangen. Da sich mit der Zeit eine Vielzahl von verschiedenen Bitcoin-Plattformen entwickelt hat, wird auch dieses Problem auf das gesamte Netzwerk verteilt. So ist es zwar möglich, dass einzelne Client-Implementierungen fehlerhaft sind, das würde aber nicht alle Teilnehmer des Netzwerkes betreffen.

**Finney-Attacke** Ein Nutzer hat die Möglichkeit mehrere digitale Geldbörsen zu besitzen. Dies kann ausgenutzt werden, indem man Transaktionen an sich selbst durchführt. Wenn man es nun schafft die erzeugten Transaktionen für sich zu behalten und nicht dem Netzwerk mitzuteilen, kann man die schon benutzten Bitcoins noch einmal im Netzwerk gegen Waren oder Geld eintauschen. Danach übertragt man die ältere Transaktion an sich selbst in das Netzwerk. Da diese vor der zweiten getätigt wurde, wird sie vom Netzwerk als die richtige akzeptiert und einem Block hinzugefügt.[7]

**Cancer-Nodes** ¨Cancer-Nodes¨ sind krankhafte Netzknoten, die versuchen das Netz in irgendeiner Art zu stören. Dazu verbindet sich ein Angreifer mit sehr vielen Clients, die eine eigene IP-Adresse haben, zum Netzwerk. Hierbei ist denkbar, dass der Angreifer alle Clients z.B. durch ein Botnetz unter seiner Kontrolle hat. Durch die hohe Anzahl der Clients ist es sehr wahrscheinlich, dass sich ein ehrlicher Client zu dem krankhaften Knoten verbindet. Als Bindeglied zwischen dem funktionierenden und krankhaften Netzabschnitt, kann der Angreifer nun mehrere Aktionen durchführen. Er kann einerseits verhindern, dass Blöcke und Transaktionen den ehrlichen Client erreichen, die der Angreifer billigt. Andererseits kann er nun Ausgaben im krankhaften Netzabschnitt durchführen und ebenso im funktionierenden Netzabschnitt. Somit könnte er Transaktionen doppelt ausführen und die Integrität der Block-Chain verletzen.[5]

### 2.4.2 Wirtschaftlich

Ein zentrales Problem bei virtuellen Währungen besteht in der finanziellen Stabilität. Anders als bei realen Währungen gibt es kein zentrales Kontrollorgan, das durch eine Intervention eine Stabilität sicherstellen kann. Der Wert hängt von der Anzahl der Nutzer, der Transaktionen und der Händler ab. Schon jetzt ist deutlich, dass unter der Vielzahl der verschiedenen virtuellen Währungen, nur diejenigen stabil sind, die einen Bezug zu realen Werten haben. Jedoch kann nur ein Bruchteil der verschiedenen Coin-Währungen in reales Geld umgetauscht werden. Deshalb werden Kryptowährungen oft auch als Schneeballsystem betrachtet. Besitzer hoffen auf steigende Kurse, die aber nur zu Stande kommen, wenn neue Nutzer sich dem System anschließen und die Nachfrage erhöht wird. Wie in einem Schneeballsystem bricht der Kurs und der Wert ein, sobald keine neuen Nutzer ins System eintreten. Die Entwickler von Kryptowährungen sind der Meinung, dass sich der Wert über lange Sicht durch die technische Umsetzung und Verschlüsselung bemessen wird. Jedoch ist noch nicht abzuschätzen, wie sich der Wert über einen längeren Zeitraum entwickeln wird. Die Erfahrungen der letzten 3 Jahre zeigen, dass sich der Wert sehr sprunghaft verändern kann. 2011 war ein Bitcoin nur 0,785 USD wert. Innerhalb weniger Monate stieg der Kurs auf 30,99 USD und fiel genauso schnell wieder auf 3,24 USD. Im November 2013 explodierte der Kurs auf über 1200 USD pro Bitcoin und nur knapp 3 Monate später war

ein Bitcoin nur noch 340 USD wert. Diese Beispiele zeigen wie unbeständig die Kryptowährungen sind.

### 2.4.3 Politisch

Kryptowährungen werden von politischer Seite aus oftmals als Mittel zur Geldwäsche eingeschätzt. Durch die Anonymität innerhalb des Netzwerkes, können Konten nicht an Organisationen, Unternehmen oder Personen gebunden werden. Somit kann eine kriminelle Nutzung Einzelner nicht ausgeschlossen werden. In Zusammenhang damit, steht die Nichtabschaltbarkeit einzelner Bitcoinadressen. Das heisst, sollte eine kriminelle Nutzung nachgewiesen werden, gibt es keine Möglichkeit den Zugang zu den Geldreserven zu verwehren. Weiterhin wird darauf hingewiesen, dass Transaktionen nicht rückgängig gemacht werden könnten, was einen großen Nachteil für den Verbraucher darstellt. Außerdem wird von politischer Seite immer wieder auf das Problem der fehlenden zentralen Kontrolle hingewiesen.

## 2.5 Fazit

### 2.5.1 Funktionalität

Durch Kryptowährungen wurde eindeutig ein ganz neuer Ansatz an Online-Bezahlsystemen entwickelt. Die Funktionsweise gewährleistet einen Schutz der Privatsphäre, der bis dato noch nicht erreicht wurde. Aber schon nach wenigen Jahren zeigt sich, dass auch Systeme wie Bitcoin, Ripple und Litecoin keine vollständige Sicherheit bieten können. Ein weiteres Problem ist durch den schwierigen Einstieg gegeben. Für eine hohe Anzahl an Nutzern sind die virtuellen Währungen schwer nachzuvollziehen und so schreckt es eher ab, als das Sicherheit vermittelt wird. Weiterhin ist die Akzeptanz von Unternehmen eher gering, sodass die Währungen von kleinen virtuellen Gemeinschaften eher für Spekulationen auf die Wertentwicklung genutzt werden. Hierbei bleibt der eigentlich innovative Gedanke als Online-Bezahlmethode auf der Strecke. Hinzukommt das Problem der rechtlichen Grundlage. Die Dezentralisierung stellt für Finanzinstitute, sowie für Regierungen, eine nicht annehmbare Tatsache dar. So werden Kryptowährungen in einigen Ländern verboten, während sich andere Länder erst garnicht damit beschäftigen. Das führt dazu, dass der Rückhalt von politischer Seite ausbleibt und das Vertrauen für den Benutzer geschwächt wird. Ebenso sind die Kryptowährungen als Instrument für Zahlungsysteme noch ungeeignet, weil eine Preisstabilität nicht gegeben werden kann, wie im Kapitel 4.2 beschrieben. Allen Problemen zum Trotz hat dieser neue Ansatz sehr großes Potenzial. Erstmals erfolgt eine Art der Demokratisierung in der Geldpolitik. Die Nutzer des Systems tragen entscheidend zur Wertentwicklung bei. Anders als bei realen Währungen, die

durch Zentralbanken und letztendlich den Staat reguliert werden. Außerdem tragen die Kryptowährungen deutlich zu Globalisierung bei, da Zölle und Ländergrenzen keine Rolle spielen.

### 2.5.2 Entwicklungsprognose

Es gibt zwei mögliche Richtungen, in die sich virtuelle Währungen entwickeln können. Sollte eine gesetzliche Grundlage geschaffen werden und damit die gesellschaftliche Akzeptanz steigen, so werden Kryptowährungen deutlich zur Globalisierung und zur Revolutionierung der Geldpolitik beitragen. Hierfür müssen die Systeme aber durchsichtiger gemacht werden. Weiterhin muss sich der Kurs stabilisieren, um einen Austausch zu realen Währungen jederzeit zu gewährleisten und Sicherheit zu schaffen. Dies ist ein Grundsatz um einen täglichen Gebrauch zu ermöglichen. Die steigende Nutzung des Internets und die Zunahme von virtuellen Gemeinschaften arbeitet deutlich für eine Weiterentwicklung der Kryptowährungen. Sollte jedoch der Kurs in den nächsten Jahren verfallen oder ein Angriff eine der Währungen nutzlos machen, so wird sich das Vertrauen in virtuelle Währungen nicht etablieren und sie werden mit der Zeit wieder verworfen. Interessant ist auch der Vergleich mit Filesharing- und Streamingdiensten. So waren vor 10 Jahren Plattformen wie eMule oder LimeWire Vorreiter, was den illegalen Vertrieb von Filmen und Musik im Internet betrifft. Jedoch gibt es heutzutage ausreichend legale Ableger, die ihre Dienste gegen eine Bezahlung anbieten. Sollten Kryptowährungen sich in diese Richtung entwickeln, legal und anerkannt, so sind sie ein grandioses neues Instrument im Ausgleich zu realen Währungen. Alles in Allem bleibt die Entwicklung spannend und virtuelle Währungen sollten weiterhin als Option betrachtet werden, sein Geld zu investieren, zu vermehren und auszugeben.

## 2.6 Anhang

### 2.6.1 Anhang A - Tabelle zur Verdeutlichung der Unteschiede innerhalb von Kryptowährungen

Tabelle 2.1: Liste von Kryptowährungen

| **Name** | **Veröffentlicht** | **Gründer** | **Hashing** | **PoW** | **PoS** |
|---|---|---|---|---|---|
| Bitcoin | 2009 | Satoshi Nakamoto | SHA-256d | Ja | Nein |
| Namecoin | 2011 | unbekannt | SHA-256 | Ja | Nein |
| Litecoin | 2011 | Charles Lee | scrypt | Ja | Nein |
| Peercoin | 2012 | Sunny King | SHA-256 | Ja | Ja |
| Ripple | 2013 | Chris Larsen, Jed McCaleb | ECDSA | Nein | Nein |
| Dogecoin | 2013 | Jackson Palmer, Billy Markus | scrypt | Ja | Nein |
| Mastercoin | 2013 | J.R. Willet | SHA-256d | Nein | Nein |
| Auroracoin | 2014 | Baldur Friggjar Odinsson | scrypt | Ja | Nein |

### 2.6.2 Anhang B - Kryptographische Verfahren, Leistungsnachweisverfahren

#### SHA-256/SHA-256d

SHA-256 wird zu den kryptographischen Hashfunktionen gezählt. Es ist eine Weiterentwicklung von SHA-1, das wiederum von der NSA aus MD-4 entstanden ist. SHA-256 benutzt eine Hashwertlänge von 256 Bit. Das Urbild wird in Blöcken von 512 Bit verarbeitet. Auf dieses Urbild wird nach einer gewissen Vorschrift mehrfach eine Kompressionsfunktion angewendet.
Bei SHA-256d wird das kryptographische Verfahren zweifach ausgeführt um die Sicherheit zu erhöhen. [5]

#### ECDSA

DSA ist ein von NSA entwickeltes Verfahren zur Schlüsselerzeugung, das auf dem ElGamal- Verfahren beruht. Hierbei wird der diskrete Logarithmus benutzt. Bei ECDSA wird als Basis jedoch nicht der diskrete Logarithmus, sondern elliptische Kurven benutzt. Dies hat den Vorteil, das bei kleineren Schlüsseln und somit weniger Rechenleistung, dennoch die gleiche Sicherheit erreicht wird. [9]

#### scrypt

Scrypt ist eine Passwort-basierte Schlüsselableitungsfunktion. Hierbei wird das Passwort um eine Zufallszahl erweitert, um die Berechnung deutlich zu erschweren. [10]

#### Proof-of-Work

Proof-of-Work beschreibt in der Informatik eine Methode, die beispielsweise DoS-Attacken verhindern soll. Es wird in der Regel eine Lösung zu einer mäßig schweren Aufgabe gesucht. Das gefundene Ergebnis kann jedoch leicht überprüft werden. Innerhalb der Kryptowährungen wird dieses Verfahren beim Erzeugen und Verifzieren der Blöcke benutzt. [5]

#### Proof-of-Stake

Proof-of-Stake ist eine weitere Methode um Kryptowährungen abzusichern. Anders als bei Proof-of-Work, weisen die Benutzer des Netzwerks durch Überweisungen an sich selbst nach, dass sie einen gewissen Anteil, der im Netz bestehenden Coins, besitzen. [11]

# Literaturverzeichnis


[1] Europäische Zentralbank (Oktober 2012). *virtual currency schemes.* https://www.ecb.europa.eu/pub/pubbydate/2012/html/index.en.html

[2] US Department of Treasury (18. März 2013). *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.* https://web.archive.org/web/20130319213642/http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

[3] Satoshi Nakamoto (11. Februar 2009). *Bitcoin open source implementation of P2P currency.* http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

[4] Satoshi Nakamoto (24. Mai 2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf

[5] Lena Sophie Brüder (20. Februar 2012). *Bitcoin, Seminararbeit.* www.nds.rub.de/media/attachments/files/2012/03/bitcoin-lbrueder.pdf

[6] Syracom AG (30.01.2014). *Syracom Trendstudie, Virtuelle Währungen.* http://www.syracom.de/

[7] Harold Finney (13. Februar 2011). *Best practice for fast transaction acceptance - how high is the risk?.* https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384

[8] Gerion Entrup (6. September 2013). *Bitcoin, der Stärkere gewinnt.* http://www.thi.uni-hannover.de/fileadmin/forschung/arbeiten/entrup-ba.pdf

[9] Felix Merz (21. März 2014) *Digitale Signaturen mit elliptischen Kurven.* http://www.mathematik.uni-wuerzburg.de/ steuding/merz.pdf

[10] Colin Percival, Simon Josefsson (September 2012) *The scrypt Password-Bases Key Derivation Function* http://tools.ietf.org/pdf/draft-josefsson-scrypt-kdf-00.pdf

[11] Sunny King, Scott Nadal (19.August 2012) *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* http://wallet.peercoin.net/assets/paper/peercoin-paper.pdf

[12] Ulrich Van Suntum (09. November 2010) *Von der Muschel zum Papier* http://www.faz.net/aktuell/wirtschaft/wirtschaftswissen/die-geschichte-des-geldes-von-der-muschel-zum-papier-11066486.html

# Kapitel 3

# Security of Powerline Networks

*Stefan Horn*

*Powerline Netzwerke haben verglichen mit WLAN und LAN sehr geringe Verkaufs und Verbreitungszahlen, obwohl sich die Datenübertragungsraten von Powerline Netzen nicht hinter den der anderen Technologien verstecken müssen, zumindest auf dem Papier. Ob diese geringe Verbreitung technisch gerechtfertigt ist, oder ob sie einfach nur auf Misstrauen zurückzuführen ist, wird in dieser Seminararbeit untersucht. Powerline Netze werden mit LAN und WLAN verglichen, und es wird explizit die Sicherheit von Powerline Netzen untersucht, sowohl theoretisch als auch praktisch.*

# Inhaltsverzeichnis

## 3.1 Einleitung

### 3.1.1 Was ist ein Powerline Netzwerk?

Wer heutzutage ein lokales Netzwerk aufbauen will stellt sich oft die Frage: „LAN oder WLAN? “ Es gibt allerdings auch noch andere Alternativen. Diese Seminararbeit beschäftigt sich mit dem IEEE 1901-Standard und dessen Sicherheit. Er ist bekannt unter den Namen PowerLAN, dLAN (direct LAN) oder Powerline Communication (PLC).


Abbildung 3.1: Powerline Adapter TP-Link 200 von devolo

Zum Aufbau so eines Netzwerks werden mindestens 2 Powerline Adapter benötigt, welche an das bereits vorhandene Stromnetz angeschlossen werden. An die Adapter werden die Endgeräte mittels LAN oder WLAN angeschlossen. In ein solches Netz können prinzipiell beliebig viele Adapter eingebunden werden. Je mehr Adapter allerdings verwendet werden, desto schlechter wird die maximale Sendeleistung des einzelnen Adapters, da immer nur einer im Netz senden kann. Weitere Einflussfaktoren sind unter anderem die Länge der Leitung zwischen den Adaptern, die Qualität der Stromleitungen, ob andere Störquellen im Stromnetz liegen oder ob die Adapter an Steckdosen mit der selben Phase angeschlossen sind.

Um sich ein Urteil darüber bilden zu können, ob Powerline Netzwerke sicher sind, und ob sie eine Zukunft haben, muss man sich zunächst mit deren genauer Funktionsweise auseinandersetzen. Außerdem muss man sich mit deren Vor- und Nachteilen gegenüber von LAN und WLAN beschäftigen. Und man

muss wissen, welche Sicherheitsmaßnahmen die Hersteller von Powerline Adaptern ergriffen haben, um ihre Netzwerke vor fremden Zugriff zu schützen.

## 3.2 Hauptteil

### 3.2.1 Wie funktionieren Powerline Netzwerke?

Bei Powerline Adaptern handelt es sich technisch gesehen um Trägerfrequenzanlagen. Das Datensignal von dem Endgerät (PC, Drucker, Spielkonsole) wird vom sendenden Adapter im Hochfrequenzbereich (je nach Adapter zwischen 2 MHZ und 68 MHZ) auf die Stromleitung moduliert. Mit Hilfe von Frequenzmultiplexing wird auf Senderseite eine Vielzahl von Signalen gleichzeitig auf eine Trägerfrequenz moduliert. Das je nach Adapter zur Verfügung stehende Frequenzspektrum wird dabei in Kanäle aufgeteilt.

Bei Powerline Netzwerken werden die hauseigenen Stromleitungen verwendet, welche ursprünglich nicht zur Übertragung von hochfrequenten Signalen gedacht waren. Daraus resultieren viele Probleme auf die wir nun genauer eingehen. Die Stromleitungen haben einen relativ hohen Dämpfungseffekt, und der Hausstromanschluss ist ein Drehstromanschluss, was bedeutet, dass ein Stromanschluss aus drei Phasen besteht. In jedem Raum eines Hauses sind verschiedene Steckdosen an unterschiedlichen Phasen angeschlossen, um eine gleichmäßige Last auf allen drei Phasen zu haben.

Ältere Adapter können nur miteinander kommunizieren, wenn sie an Steckdosen mit der selben Phase angeschlossen sind. Aktuelle Adapter arbeiten auf so hohen Frequenzen, dass die Signale an parallel liegenden Leitungsstücken (z.B. vor dem Sicherungskästen) übersprechen, was bedeutet, dass sie auch auf den anderen Phasen empfangen werden können. Solch ein Übersprechen ist jedoch nicht verlustfrei, und senkt somit die maximale Datenrate und Reichweite. Dieses Übersprechen ist möglich, weil die Adapter die Stromleitung zu riesigen Antennen umfunktionieren. Allerdings hat das nicht nur positive Effekte, wie den eben beschriebenen, sondern sorgt für eine nicht unerhebliche Strahlenbelastung im Umkreis von ca. 100 Metern rund um die Stromleitungen. Diese Abstrahlungen sind so stark, das Amateurfunker in der Nachbarschaft nur noch schlecht bis gar nicht ihrem Hobby nachgehen können. [4]

Die Maximale Leitungslänge zwischen zwei Powerline Adaptern beträgt 400 Meter, allerdings nur unter idealen Bedingungen. Je länger die Leitung zwischen den Adaptern ist, desto geringer ist die maximale Datenübertragungsrate. Diese beträgt unter idealen Bedingungen je nach Standard bis zu 1200 Mbit/s. [2] Beide Werte werden in der Praxis nicht zu erreichen sein.

Dies liegt unter anderem an der Verschlüsselung und anderen Daten die ebenfalls über das Netz gesendet werden müssen. Dieser sogenannte Overhead

kann mit anderen Störeinflüssen dafür sorgen, dass von einer Bruttodatenrate von 500 MBit/s eine Nettotransferrate von 19 MBit/s für die eigentlichen Daten übrigbleiben. [1]

### 3.2.2 Vor und Nachteile gegenüber W-LAN und LAN

LAN hat von den 3 hier vorgestellten Technologien mit bis zu 100 Gbit/s und bis zu 40 km Reichweite (Glasfaserkabel) wohl die besten Leistungen, jedoch ist dies nicht weiter verwunderlich. LAN-Kabel sind dafür entwickelt worden, um Datensignale schnellst- und bestmöglich zu übertragen, wohingegen Stromkabel dafür zweckentfremdet werden. Außerdem sind die oben genannten Werte extreme, und kommen in üblichen Haushalten nicht vor. Dort ist eher mit einer Bandbreite von 1 Gbit/s und einer maximalen Reichweite von 100 Metern (Cat-5) zu rechnen.

LAN-Kabel haben eine deutlich höhere maximale Datenübertragungsrate, allerdings eine geringere Reichweite, im Labor. Die 100 Meter Reichweite gelten für ein einzelnes Kabel, welches zwischen zwei Geräten direkt verlegt ist. Wohingegen die 300 Meter von Powerline Netzwerken sich auf die Länge der Stromleitungen bezieht, die sich zwischen zwei Adaptern befindet.

Desweiteren lassen sich die 100 Meter von LAN-Kabeln mittels Repeater, Switches oder Router vervielfachen. Diese Geräte ermöglichen außerdem den Aufbau einer Netztopologie, welche dafür sorgt dass auch bei viel Datenverkehr zwischen vielen Endgeräten eine möglichst hohe Datenübertragungsrate gewährleistet werden kann. In Powerline Netzwerken ist es möglich virtuelle Netztopologien aufzubauen, welche allerdings nicht die Grenze von maximal 1500 Mbit/s auf dem gesamten Stromnetz aushebeln können. Somit bleibt der einzige Vorteil von Powerline-Netzwerken, dass man keine neuen Kabel verlegen muss, sondern die bereits vorhanden Stromleitungen nutzen kann.

Dies gilt allerdings auch für WLAN. Ein WLAN-Accesspoint im Raum, der Wohnung oder der Etage genügt, um im Umkreis von einigen Metern Drahtlos auf das Netzwerk zugreifen zu können. Die neuesten Router schaffen es dabei auf bis zu 900 Mbit/s wenn sie auf 2,4 GHz und 5 GHz senden, sowie pro Frequenz 3 Antennen zur Verfügung stehen. [5] Die Maximale Reichweite hängt von sehr vielen Faktoren ab, angefangen damit, welche und wie viele Antennen verwendet werden. Außerdem ob zwischen Sender und Empfänger nur freier Raum ist oder ob sich dort z.B. Wände befinden. Für WLAN gibt es genau wie für LAN Repeater, welche die maximale Reichweite erhöhen.

WLANs haben die gleichen Probleme wie Powerline-Netzwerke, es können keine richtigen Topologien aufgebaut werden, und somit sinkt die maximale Datenrate von jedem einzelnem Gerät mit jedem weiterem Gerät im Netz. Außerdem strahlen beide. WLAN mit 100 mWatt bei 2,4 GHz bzw. 5 GHz, Powerline-Netzwerke zwischen 2 MHZ und 68 MHZ mit viel höherer Leistung.

Zusammenfassend lässt sich sagen, jede Technologie hat ihre Vor- und Nachteile. Daher werden meistens Mischformen zwischen LAN und WLAN verwendet. Powerline-Netzwerke kommen nur selten vor, und fast ausschließlich in Privathaushalten.

### 3.2.3 Wie werden Powerline Netzwerke vor unerwünschtem Zugriff geschützt?

Die Hersteller der Powerline-Netzwerk Adapter haben viele verschiedene Sicherheitsmaßnahmen entwickelt und verbaut. Aber auch das Stromnetz an sich schützt schon im gewissem Rahmen. Während W-LAN frei empfangbar ist, muss man um auf ein Powerline-Netzwerk zugreifen zu können, Zugriff auf eine Steckdose haben. Dies behaupten jedenfalls die Hersteller, dazu später mehr. Die Signale der Adapter sollen nicht fähig sein den Stromzähler zu überwinden, somit kann der Datenverkehr im Netzwerk nur von Adaptern innerhalb der eigenen Wohnung oder Firma empfangen werden. Aber z.B. in Studentenwohnheimen oder in Firmen ist es zu empfehlen, dass nicht jeder, der Zugang zu einer Steckdose hat, auch den Datenverkehr mitlesen kann. Insbesondere da es sich bei Powerline-Netzwerken um eine einzige Broadcast Domain handelt, und somit im ganzen Netz der gesamte Datenverkehr empfangen werden kann.

Um sich vor solchem fremden Zugriff zu schützen verschlüsseln die Adapter den Datenverkehr. Die meisten Hersteller bieten AES (Advanced Encryption Standard) an, jedoch haben gerade einige ältere Adapter nur eine DES (Data Encryption Standard) Verschlüsselung. Um trotz der Verschlüsselung den Kunden „plug and play “ bieten zu können, bauen viele Powerline Adapter sobald sie an das Stromnetz angeschlossen sind eine unverschlüsselte Verbindung zu allen anderen Powerline Adaptern auf, die sich im Stromnetz befinden. Diese Verbindung zwischen beliebig vielen Powerline Adaptern können auf zwei verschiedene Arten verschlüsselt werden.

Die einfache Methode funktioniert über die „Verschlüsselungstaste“ oder auch ”Pair-Taste”. Diese muss innerhalb von ein bis drei Minuten (je nach Hersteller und Powerline Adapter) ein bis zwei Sekunden gedrückt werden. Die Powerline Adapter generieren nach dem drücken dieser Taste ein zufälliges Passwort, mit welchem sämtlicher künftiger Datenverkehr verschlüsselt wird. Auch bei einer Trennung von der Stromleitung merken sich die Powerline Adapter ihre Konfiguration. Dies ist sehr praktisch für die Erstellung eines Netzwerks, da die Powerline Adapter erst konfiguriert und anschließend im Haus oder der Firma verteilt werden können. Zudem wäre es sehr aufwendig nach jedem Stromausfall alles neu einstellen zu müssen. Auch das nachträgliche Hinzufügen von Powerline Adaptern zu einer verschlüsselten Gruppe gestaltet sich problemlos. Hierzu muss auf einem der Powerline Adapter im Netz die ”Verschlüsselungstaste”bzw. ”Pair-Taste”gedrückt werden und an-

schließend muss die gleiche Taste auf dem neuen Powerline Adapter gedrückt werden.

Die zweite Methode ist etwas aufwändiger, bietet dafür allerdings auch mehr Möglichkeiten. Zunächst einmal muss die Software „Powerline-Utility“ installiert werden. Danach werden alle Powerline Adapter mit dem Stromnetz verbunden. Nun kann man mit Hilfe der Software ein oder mehrere Netze aufbauen und deren Passwort manuell einstellen. Bei Bedarf können auch einzelne oder alle Adapter auf die Werkseinstellung zurückgesetzt werden, was jedoch die Verschlüsselung ausschaltet.

### 3.2.4 Mögliche Angriffsszenarien

Am technisch aufwendigsten wäre es wohl, wenn man versuchen würde die Abstrahlung von Powerline-Netzwerken zu empfangen und damit den Datenverkehr zu rekonstruieren. Diese Daten wären jedoch noch verschlüsselt. Das selbe Problem hat man, wenn man einen eigenen Adapter an einer Steckdose innerhalb der Wohnung oder Firma anbringt, was vor allem bei ersterem recht auffällig wäre. Glücklicherweise muss man gar nicht so nah heran. Die meisten Stromzähler verhindern, trotz Herstellerangaben, nicht, dass die Signale in der Nachbarwohnung oder gar der ganzen Straße empfangen werden können. „Abhilfe wäre durch Filter direkt an den Stromzählern möglich, die der Elektriker installiert. Doch die Kosten dafür dürfte kaum ein Vermieter schultern wollen.“ [1] Obwohl man ganz bequem aus dem Nachbarhaus den Datenverkehr mitlesen kann, ist er nach wie vor verschlüsselt, sollte er zumindest sein.

Ältere Powerline Adapter die dem Homeplug oder Homeplug Turbo Standard erfüllen müssen keine Verschlüsselung anbieten. Die meisten Geräte können trotzdem nach dem DES verschlüsseln. Die DES Verschlüsselung ist jedoch veraltet, und kann mit linearer und differentieller Kryptoanalyse gebrochen werden.[3]

Aktuellere Modelle die den Homeplug AV bzw. Homeplug AV2 Standard erfüllen müssen eine AES Verschlüsselung mit 128 Bit anbieten. Von der AES Verschlüsselung ist noch keine Schwachstelle bekannt.

Bei älteren Modellen ist es somit relativ einfach sich in das Netz einzuklinken, bei neueren wäre es technisch schon deutlich aufwändiger. Daher wendet man sich der größten Sicherheitslücke zu, dem User.

Wie bereits in dem vorherigem Kapitel beschrieben, bauen Powerline Adapter zunächst ein unverschlüsseltes Netz auf. Dieses Netz ist komplett ungeschützt, und jeden Powerline Adapter den man in Reichweite dieses Netzes an eine Steckdose anschließt, wird sich automatisch mit diesem verbinden. Weder eine Status-LED auf den Geräten noch eine Warnmeldung in der Software ”Powerline-Utility”weißt darauf hin, dass das Netz unverschlüsselt ist.

Es wäre nicht verwunderlich, wenn einige Nutzer den kleinen Hinweis in der Kurzanleitung übersehen würden, und ihr Netz nie verschlüsseln. Insbesondere technisch nicht besonders versierte Nutzer die sich auf ”plug and play”verlassen sind hiervon stark gefährdet.

Es wäre auch möglich, das einige Nutzer absichtlich die Verschlüsselung deaktivieren, da diese den enormen Overhead noch vergrößern soll, und somit die Nettodatenrate noch mehr reduziert. Insbesondere wenn die Verbindung relativ schlecht ist, kann die Verschlüsselung der Verbindung dafür sorgen, dass diese endgültig viel zu langsam wird. Darüber gibt es keinerlei Wissenschaftliche Studien, allerdings viele Meinungen und Erfahrungen. Genau diese werden Nutzer lesen, welche ein zu langsames verschlüsseltes Netz haben. Da Geschwindigkeit für die meisten Nutzer das wichtigste Kriterium ist, und sie ihre Informationen oft nicht als besonders schützenswert empfinden wäre es nicht weiter verwunderlich wenn sie die Verschlüsselung deaktivieren würden.

Aber auch Netze die mit 128 Bit AES verschlüsselt sind, können erfolgreich angegriffen werden. Als erstes stört man das Netz, beispielsweise mit ein paar Dimmern, oder einer alten Glühbirne die gerade so weit in das Gewinde geschraubt wird dass sie flackert. Das sollte dafür sorgen, dass das Netz zusammenbricht. Sämtliche Powerline Adapter sollten nun anzeigen, dass sie am Stromnetz angeschlossen sind, und dass sie mit einem Endgerät verbunden sind, jedoch keine anderen Powerline Adapter gefunden wurden. Nach einigen Minuten hört man auf das Netz zu stören. Nun gibt es drei Möglichkeiten die passieren können:

Im günstigstem Fall denkt sich der Nutzer das es ein Problem mit der Verschlüsselung gibt, und drückt auf allen Geräten die ”Verschlüsselungstaste”bzw. ”Pair-Taste”. Man muss nur auf seinem Powerline Adapter ebenfalls diese Taste drücken und schon ist man in seinem Netz.

Falls der Nutzer per Softwaretool das Netz neu konfiguriert kann er die Powerline Adapter manuell zum neuen Netz hinzufügen, und es ist davon auszugehen, das er unseren nicht mit einbinden wird. Daher stören wir nach einer Weile erneut. Mit etwas Glück wird der Nutzer, wenn sein Netz alle 15 Minuten zusammenbricht auf die Verschlüsselung verzichten.

Selbiges Vorgehen empfiehlt sich, wenn der Nutzer nach dem ersten Stören einfach nichts unternimmt, irgendwann wird er handeln, falls er sein Netz effizient nutzen möchte.

## 3.3 Fazit und Ausblick

### 3.3.1 Sind Powerline Netzwerke eine echte Alternative zu W-LAN und LAN?

Zusammenfassend lässt sich sagen, dass Powerline Netze wenn sie richtig konfiguriert sind sicher sind. Sie sind allerdings aufgrund ihrer Reichweite (insbesondere in Mehrfamilienhäusern) besonders gefährdet. Die Hersteller müssten mehr unternehmen, um sicherzustellen, dass ihre Powerline Adapter richtig eingestellt werden. Den Nutzern müsste eindeutig angezeigt werden ob ihre Netze verschlüsselt sind. Außerdem sollten die Hersteller deutlicher darauf hinweisen, das diese verschlüsselt werden sollten. Damit Powerline Netze eine größere Konkurrenz zu WLAN oder LAN werden wäre es nötig, dass die Hersteller den Overhead verkleinern, und somit mehr Nettodatenrate von der Bruttodatenrate übrig bleibt. Powerline Netze sind aktuell in etwa so schnell wie WLAN allerdings haben sie eine größere Reichweite, insbesondere wenn die baulichen Bedingungen für WLAN ungünstig sind. Gegenüber von LAN können sie in Sachen Anschaffungs-aufwand und kosten punkten.

Powerline Netze entwickeln sich wie alle anderen Technologien weiter, und haben mindestens als Nischenprodukt aber in zukunft vielleicht auch mit größeren Verkaufszahlen eine Zukunft.

# Literaturverzeichnis


[1] Ernst Ahlers. *c't 09/2012 Dicke Leitung*, Heise Zeitschriften Verlag

[2] devolo AG. *dLAN® 1200+ Powerline Adapter*, verfügbar auf `http://www.devolo.com/products/dLAN-Powerline/dLAN-1200+/data/Datenblatt-dLAN-1200+-de.pdf`, abgerufen am 24.09.2014

[3] Reiner Dojen, Tom Coffey. *On the Cryptographic Strength of Symmetric Ciphers Suitable for Power-Line Communications*, Department of Electronic and Computer Engineering, University of Limerick, Ireland

[4] Volker Lange-Janson. *Funkstörungen durch PowerLAN-Adapter*, verfügbar auf `http://elektronikbasteln.pl7.de/powerlan-stoerungen.html`, abgerufen am 24.09.2014

[5] CHIP Online. *Netgear N900: Datenturbo fürs WLAN mit 900 MBit/s - News - CHIP*, verfügbar auf `http://www.chip.de/news/Netgear-N900-Datenturbo-fuers-WLAN-mit-900-MBit_s_51664284.html`, abgerufen am 24.09.2014

# Kapitel 4

# Software defined Networks und neue Routingansätze

*Marcel Odenwald*

*Durch den stetigen Anstieg von Breitbandanbindungen und die steigende Zahl an Rechensystemen werden neue Wege gesucht den wachsenden Datenfluss zu verarbeiten. Denn überwiegend kommt es an Engpässen, wie an den Übergängen von Autonomen Systemen, zur Verzögerung der Datenverarbeitung. Um diesen Problemen fortan entgegen zu kommen sucht man neue Ansätze um die Datenverarbeitung zu beschleunigen. Eine Alternative bieten Software Defined Networks. Mit Hilfe dieser Neuerung soll es möglich werden neue Maßstäbe im Routing und Switching zu setzen.*

# Inhaltsverzeichnis

## 4.1 Einleitung

Diese Arbeit befasst sich mit Netzmodellen für neue Routing-Alternativen, welche durch die Implementierung von Software Defined Networks ermöglicht werden. Dazu werden im folgenden Beschreibungen von Routing und Software Defined Networks, sowie die Erläuterung zu einigen möglichen neuen Alternativen für Routing in Autonomen Systemen, gegeben.

### 4.1.1 Routing

#### Allgemein

Routing beschreibt das Festlegen von Wegen die ein Paket bei der Nachrichtenübermittlung von einem absendendem System zu seinem Zielsystem zurücklegt. Ähnlich wie man es sich bei dem Verschicken eines Paketes vorstellen kann. Man gibt sein Paket in der Postfiliale auf, dieses wird zum Paketzentrum gebracht und dort wird entschieden in welches weitere Paketzentrum das Paket transportiert wird. Die Filiale als auch die Paketzentren sind quasi die Router der Deutschen Post, denn dort wird entschieden wohin das Paket als nächstes geschickt wird. In der elektronischen Wegfindung gibt es 3 Herangehensweisen. Zum einen das **statische Routen**, wobei manuell Routen vorgegeben werden. Des Weiteren die Möglichkeit des **alternativen Routings**, hier sind mehrere Routen festgelegt mit einer entsprechenden Gewichtung. Ist nun die Paketzustellung über die Route mit der höchsten Gewichtung nicht möglich wird absteigend der Priorität versucht ob eine andere Route aus den Vorgegebenen zur Zieladresse führt. Wenn keine Route verfügbar ist wird das Paket verworfen. Das dritte Prinzip nennt sich **adaptives Routing** hierbei wird automatisch eine Alternativroute um ein beschädigtes, überlastetes oder fehlendes Netzwerksegment gesucht, wenn die ursprüngliche Route nicht zielführend ist. Dies geschieht durch diverse Routingprotokolle. Im Internet gibt es prinzipiell zwei Arten von Routing das Intradomain-Routing,innerhalb autonomer Systeme, und das Interdomain-Routing, zwischen mehreren autonomen Systemen. Für die jeweiligen Arten gibt es verschiedene Routingprotokolle. Autonome Systeme sind große Netzwerke wie zum Beispiel die eines Providers mit vielen Subnetzen, in welchen sich der Dienstnutzer[1] finden lässt. Für das Routing innerhalb Autonomer Systeme werden Interior-Gateway-Protokolle wie „OSPF“ genutzt. Das OSPF-Protokoll nutzt Routing-Algorithmen für das Link-State-Routing. Beim Link-State-Routing wird mitgeteilt wer die Nachbarn des jeweiligen Netzelementes sind und so lässt sich nach kurzer Zeit eine Map des Netzwerkes erstellen und die entsprechenden Netzelemente können selbst den schnellsten Weg berechnen. Diese Technik basiert auf Dijkstras „shortest path“ Algorithmus.

[1] Endkunde, welcher die Dienste eines Providers in Anspruch nimmt.

### Inter Domain Routing

Für das Routing zwischen Autonomen Netzen, Interdomain-Routing, wird vorwiegend das Border Gateway Protocol (BGP) genutzt. Dieses Protokoll arbeitet auf Basis eines abgewandelten Distanzvektor-Algorithmus, dem Pfadvektor-Algorithmus und wird allgemein als Exterior Gateway Protocol (EGP) bezeichnet. Bei der Verwendung des Pfadvektor-Algorithmus teilt der Router[2] mit wie für ihn der Rest des Netzwerkes aussieht, dadurch lassen sich auch hier im Netzelement selbst die schnellsten Pfade errechnen. Das BGP aktualisiert die Einträge in der Routing Information Base (RIB), hier sind alle verfügbaren Routen eingetragen. Der Router errechnet für sich aus der gegebenen RIB und unter Berücksichtigung der vorgeschriebenen Routingkriterien und der betriebswirtschaftlichen Vorgaben seine Forwarding Information Base (FIB). Die FIB ist eine optimierte Version der RIB, in welcher der Router nachschaut wenn er entscheiden soll wohin Pakete weitergeleitet werden sollen. Damit Netzelemente diese Entscheidung treffen können, müssen sie den IP-Header des Paketes auslesen, in diesem ist die Zieladresse vermerkt. Die Zieladresse setzt sich zusammen aus der IP-Adresse und der Netzadresse. Die Netzadresse wird berechnet, indem die IP-Adresse und die Netzmaske logisch „AND“ verknüpft werden. Mit den Informationen aus dem Paket-Header und der FIB leitet der Router die Pakete an den nächsten Router weiter, entweder den Router eines anderen Autonomen Systems oder an einen Router im eigenen System. Hierbei kommt auch das Zusammenspiel von Interior-Gateway-Protokollen und Exterior-Gateway-Protokollen zur Geltung, denn die Exterior-Gateway-Protokolle bauen auf durch Interior-Gateway-Protokolle verwaltete Infrastrukturen auf.

## 4.1.2 MPLS

### Was ist Multiprotocol Label Switching und wie funktioniert es?

Multiprotocol Label Switching ,kurz MPLS, ist eine Technik um priorisiertes routen in IP-Netzen zu ermöglichen. MPLS arbeitet zwischen Layer 2 (Sicherungsschicht) und Layer 3(Vermittlungsschicht) des OSI-Schichtenmodells. Der Unterschied zum normalen Routing in IP Netzen besteht darin, dass nicht für jedes Datenpaket in jedem Router den es passiert die Route neu ermittelt wird. Stattdessen wird für jede Route ein Label vergeben. Der erste Router den das Datenpaket passiert analysiert die Zieladresse und ermittelt daraufhin welche Route am besten geeignet ist. Dies geschieht nur beim Eingang in das Netzwerk, danach nicht mehr. Dem Datenpaket wird das Label der Route zugewiesen. Für dieses Datenpaket und weitere Datenpakete der selben Übermittlung steht nun die Route fest, welche sich als Tunnel durch das Netz bemerkbar macht, Ende zu Ende Verbindung. Diese Art des Transports bietet Vorteile in der Sicherheit der Verbindung. Im Label sind Routing-

[2]Gerät zur Pfadfindung und Weiterleitung von Daten

und Service-Informationen enthalten, welche von MPLS-Routern aus dem Header ausgelesen werden. Der MPLS-Header besteht aus dem Label für das Forwarding, dem Class-of-Service-Feld (CoS) für die Traffic Class (TC) zur Unterscheidung von Dienst-Klassen, dem Bottom-of-Stack-Feld (S) und dem Time-to-Live-Feld (TTL). Diese Informationen vergleicht der MPLS-Router mit den Eintragungen in der Label Forwarding Information Base (LFIB),eine Lookup Tabelle wie die FIB, und entscheidet, abhängig von den enthaltenden Informationen, durch welches Interface die Pakete weitergeleitet werden. Bevor das Datenpaket den MPLS-Router verlässt wird dem Datenpaket ein neues Label zugewiesen. Durch die Verwendung von Labeln kann man somit MPLS-Router anweisen die Datenpakete immer über die gleiche Route zu übertragen. Für den Fall das einem Datenpaket kein MPLS-Header zugewiesen wurde, wird der für das Datenpaket zuständige Router ermittelt und von diesem ein Label für die Zieladresse des Paketes angefordert. Dem Datenpaket wird das Label im MPLS-Header eingetragen und an den nächsten Router weitergeleitet. Labelanfragen und Labelupdates werden im Normalfall mit Hilfe des Label Distribution Protocol (LDP) verbreitet, jedoch ist es auch möglich das, bereits für den Austausch von Routinginformationen genutzte, BGP-Protokoll zu nutzen, welches auch im Falle des normalen Routings für den Informationsfluss zuständig ist.

**Welche Vorteile bietet MPLS?**

Der größte Vorteil von MPLS und der Nutzung von MPLS-Routern ist, dass nur noch das Label im MPLS-Header betrachtet wird. Dadurch ist es nicht mehr nötig ein bestimmtes Protokoll in der Schicht 3 zu verwenden. Dieses ist somit austauschbar, da es für das Routing mit MPLS keine besondere Aufgabe mehr erfüllt. MPLS-Router haben die Fähigkeit, aufgrund der Labelbetrachtung, automatisch IPv6 zu routen. Weiterhin wird Quality-of-Service (QoS) besser durch MPLS unterstützt, denn Pakete mit höherer Priorität bekommen ein anderes Label, deren Route schneller zum Ziel führt. Somit ist es möglich für QoS Parameter, wie zum Beispiel Transit Delay und Packet Loss, zu definieren. Weiterhin besteht die Möglichkeit den Label Stack zu nutzen. Das bedeutet, dass einem Datenpaket gleichzeitig mehrere Label angehängt werden. Geht nun solch ein Datenpaket mit mehreren Labeln bei einem MPLS-Router ein wird das jeweils erste Label verworfen und das nächste Label für die Routingentscheidungen genutzt. Durch dieses Verfahren wird von Anfang an genau eine Route durch das Netzwerk festgelegt. Im Normalfall ist dies nicht ratsam, da Routen sich kurzfristig ändern oder ausfallen können. Handelt es sich hierbei jedoch zum Beispiel um ein Paket einer VPN-Verbindung ist es besser wenn das Paket nicht beim Empfänger ankommt, als es über eine unsichere Backup-Route weiter zu leiten. Sofern man dieser zuvor festgelegten Route genug Vertrauen entgegenbringen kann bezüglich Sicherheit und Stabilität könnte man somit auf eine Verschlüsselung der Daten verzichten. Jedoch ist dies nicht besonders ratsam, da eine vollständige Sicherung der Route nicht möglich ist und auf verschiedenen We-

gen kompromittiert werden könnte. Beispielsweise durch physischen Zugang zu den Datenleitungen.

**Wo ist der Einsatz von solchen MPLS-Routern sinnvoll?**

Routing-Performance ist normalerweise bei extrem hohen Bandbreiten mit z. B. Multi-Gigabit-Glasfaserstrecken der Carrier ein Problem. Durch die Anwendung von MPLS werden hier Geschwindigkeitsengpässe möglichst vermieden. Mit zunehmender Verbreitung von Breitband-Internet-Zugängen und zurückgehenden Zahlen der Zugangsoptionen ISDN oder über analoge Telefonleitungen wird MPLS-Routing zu einer Ernst zunehmenden Alternative gegenüber IP-Routing.

## 4.2 Software defined Networks

Software defined Networks stehen seit wenigen Jahren im Mittelpunkt der Betrachtung von vielen Netzadministratoren. Bei diesem neuen Ansatz von Netzwerken und Netzen wird die Hardwarekomponente von der Softwarekomponente abstrahiert, siehe dazu den Vergleich Abbildung 4.1 und 4.2.

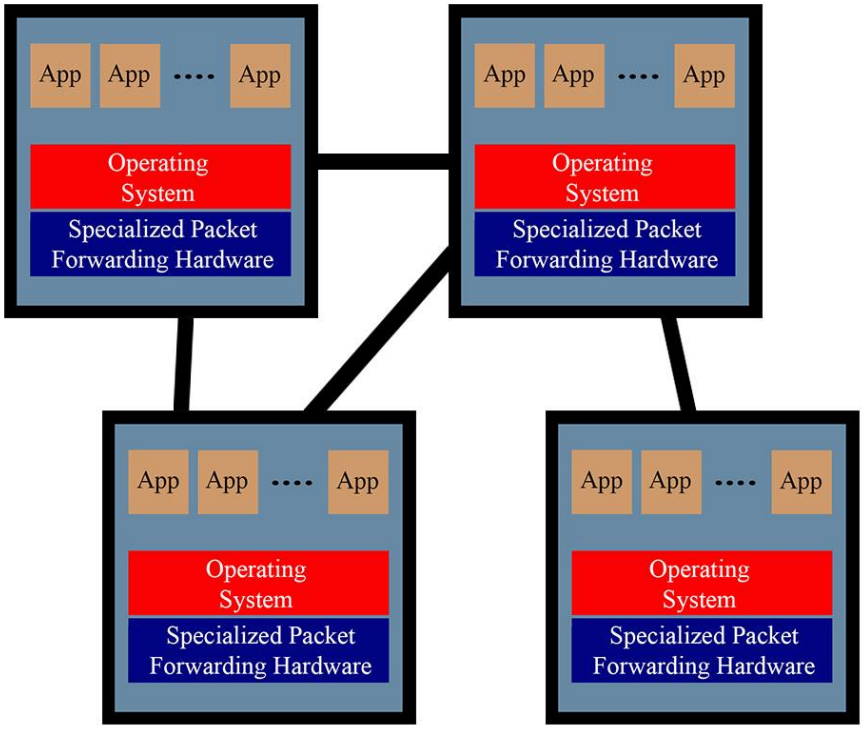


Abbildung 4.1: Aufbau eines traditionellen IP-Netzes

Das bedeutet die Control-Plane wird von den einzelnen Netzwerkelementen, wie Routern oder Switches, zu einem zentralen Controller ausgelagert, einem

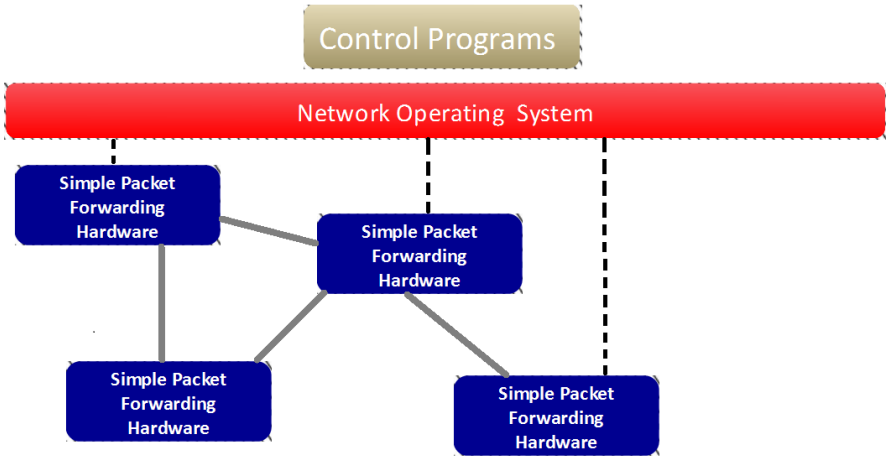


Abbildung 4.2: Aufbau von Software defined Networks

sogenannten Network Operation System. Einer der Gründe warum in diese Richtung geforscht und entwickelt wurde, ist die Skalierbarkeit der Netzwerke. Da herkömmliche Netztechnik auf die Netzanforderung der einzelnen Netze zugeschnitten und dimensioniert ist, ist die Erweiterung des Netzes eine technisch umständliche Arbeit, da Programmcode bei der Implementierung neuer oder veränderter Protokolle in jedem Netzelement aktualisiert werden muss. Das und die zunehmende Virtualisierung von Diensten und von Infrastruktur ließen den Wunsch nach einer Möglichkeit für vereinfachte Konfiguration aufleben. Diese Möglichkeit ist nun durch die Abstraktion der Control-Plane gegeben. Der Controller übernimmt die Aufgaben der Control-Plane, er kartographiert das Netzwerk und empfängt alle Routing-Informationen und speichert diese in seiner Routing Information Base und errechnet daraus die Forwarding Information Base für das gesamte Netzwerk. Dadurch das die Aufgaben der Control-Plane auf einen externen Controller ausgelagert werden, brauchen die Netzwerkelemente fortan keine hochspezialisierte Hardware sondern lediglich eine sehr einfach gestrickte Forwarding Hardware. Die Abstraktion bietet zusätzlich die Fähigkeit des Network-Global-View, dass bedeutet das der Controller die Möglichkeit hat alle für ihn relevanten Daten, wie Statistiken und Monitoringergebnisse, des Netzwerkes zu sammeln und dieser hat somit einen Überblick über den Status des gesamten Netzes. Aufgrund der Fähigkeit alle Daten des Netzes zu sammeln kann der Controller auch zur Überwachung des Netzes eingesetzt werden und die Sicherheit des Selbigen verbessern. Ebenfalls kann er schneller auf ausgefallene oder ausgelastete Netzsegmente reagieren und die Netzlast optimal umleiten und Ausweichrouten festlegen, als traditionelle Netze.

Das Routing in Software defined networks kann nach verschiedenen Kriterien betrieben werden [3].

### 4.2.1 Einsatzmodelle

#### Symmetrisch oder asymmetrisch

In einem **asymmetrischen** Modell versucht man die Konfiguration weitestgehend zu zentralisieren, während die Switches möglichst breit verteilt sind. Man verspricht sich durch das Prinzip der Zentralisierung eine Vermeidung von zu vielen Redundanzen und möglicher Inkonsistenzen. Während dessen sorgt dir Verteilung des Datenverkehrs dafür, dass Engpässe an zentralen Stellen vermieden werden. Doch auch wenn diese Technik Vorteile bietet gibt es dennoch auch mögliche Nachteile zu bedenken. Allem voran wie störungsanfällig ein solches Modell ist und ob solche Systeme ausreichend groß werden können. Beim entgegengesetzten, **symmetrischen** Prinzip kennt jedes Netzelement zusätzlich alle für sich relevanten Control-Plane-Konfigurationen. Auf diese Weise wird sichergestellt, dass auch bei beliebigen Teilausfällen die verbleibenden Teilstrukturen in ihren Grenzen normal weiter arbeiten können. Praxisrelevant sind hauptsächlich Ansätze bei denen die Zahl der Control Planes minimal ist, jedes Element zur Not autonom arbeiten kann ohne einen Single Point of Failure.

#### Floodless oder Flood-based

Als **Flood-based** wird ein Modell bezeichnet, dass einen beachtlichen Anteil der globalen Informationsverteilung erreicht, basierend auf Broadcast- und Multicast-Mechanismen die jede Veränderung kommunizieren. Dies unterstützt SDN-Modelle in ihrer Eigenschaft der Symmetrie. Um Informationen und Identitäten von Netzteilnehmern zu verbreiten wird transparentes Bridging eingesetzt. Der Nachteile eines solchen Modells liegt im Anstieg der Netzlast für jeden Knoten der im Netz implementiert ist. Diese Tatsache begrenzt die Skalierbarkeit des Netzes. Die korrekte Funktion aller Komponenten im **Floodless-Modell** wird hingegen über lokale Caches von SDN-Lookup-Tables sichergestellt. Diese werden in regelmäßigen Abständen synchronisiert.

#### Host-based oder netzwerk-zentriert

Das **host-based** Modell nimmt an, dass das es bei einem Einsatz von vielen virtuellen Maschinen günstig ist, die SDN-Verarbeitung auf dem Hypervisor-System zu erledigen. Denn aufgrund der relativ geringen entstehenden Auslastung gibt es hier immer freie Kapazitäten. Der **netzwerk-zentrierte** Ansatz hingegen nutzt wie üblich die dedizierten Router und lagert die Routing-Funktionen nicht auf virtuelle Hosts aus. Einige Grenzen verschwimmen jedoch, so können CPU-lastige SDN-Aufgaben wie beispielsweise die Verschlüsselung des Datenverkehrs auf virtuellen Hosts erfolgen, während das abarbeiten von anderen Aufgaben auf dedizierten SDN-Servern erfolgt. Es entstehen

gewisse Abhängigkeiten so das ein Host-basierter Ansatz eine asymmetrisches Struktur benötigt.

#### Proaktiv oder reaktiv

Bei einem **Proaktivem** Ansatz werden die Flow-Tabellen in Routern und Switches von vorne herein mit Einträgen gefüllt, so dass bei einem Verlust der Verbindung von Controller zu Switch oder Router dieser eigenständig weiterarbeiten kann und es wird keine zusätzliche Zeit für das Setup eines neuen Flows benötigt. Jedoch benötigt dieses Konzept integrierte Regeln für Switch und Router zur Nutzung.

Das Pendant ist die Arbeit mit einem **Reaktivem** Modell, bei diesem werden die Einträge in der Flow-Tabelle erst beim ersten auftreten des Flows vorgenommen. Somit benötigt ein Flow eine kleine zusätzliche Setup Zeit und falls es zu einem Verbindungsabbruch zwischen Controller und Switch oder Router kommt, hat das Netzelement nur sehr eingeschränkte Möglichkeiten des Handelns. Jedoch ist der reaktive Ansatz derjenige von beiden Modellen welcher das Prinzip der Flow-Tabellen effizienter nutzt.

### 4.2.2 Anwendungsfälle

#### Infrastructure as a Service

Software definierte Netzwerke können in verschiedenen Szenarien zum Einsatz kommen, zum einen als Infrastructure as a Service. Das bedeutet das SDN im Zusammenspiel mit virtuellen Systemen und virtuellem Speicher eine flexible Ressourcenallokation erlaubt. So profitieren vor allem Scale-Out-Szenarien von der Automatisierung, da bei Bedarf weitere Systeme zugeschaltet werden können.

#### Host-Performance

Ein weiteres Szenario zielt darauf ab das weniger Hosts, diese dafür jedoch besser, genutzt werden. Hier kann die Nutzung von Software definierten Netzen für eine Re-Allokation von virtuellen Systemen auf den Virtualisierungshosts sorgen, was den zuvor genannten Effekt hervorruft.

#### Load-Balancing

Weiterhin erlauben SDN die automatische Verteilung von Lasten auf viele Verbindungen, beispielsweise zwischen den Anwendungsservern und dem

Netzwerk-Backbone. Normalerweise werden dafür manuell VLANs und Routen konfiguriert. Das ist jedoch sehr aufwändig und lässt keine dynamische Anpassung an wechselnde Lasten zu.

#### Managed Network Services

SDN ist auch in der Lage Managed Network Services (MNS) in großen Netzen zu übernehmen. Dabei geht es um die Einhaltung der Service Level Agreements. Das bedeutet, dass auch bei Änderungen am Netzwerk jedem Teilnehmer seine laut Vertrag garantierten Bandbreiten, Latenzzeiten, Verfügbarkeiten und Sicherheitsfeatures zur Verfügung stehen.

### 4.2.3 Schwachstellen SDN

Der Controller wird in Software definierten Netzwerken das primäre Angriffsziel darstellen, da durch die Übernahme oder die Modifizierung des Controllers das gesamte Verhalten des Netzes verändert oder der Datenverkehr abgefangen werden kann. Die Fähigkeit den Controller programmieren zu können, ist ein zweischneidiges Schwert. Auf der einen Seite kann er die Sicherheit erhöhen, indem er Angriffe schneller entdecken kann und es Administratoren ermöglicht zum Beispiel auf DDOS Angriffe zu reagieren. Durch manuelle Eingriffe in die Forwarding-Tabellen können so Pakete umgeleitet oder verworfen werden die sonst das Ziel des Angriffs lahmlegen würden. Auch können bei Bedarf Sicherheitsrichtlinien schneller geändert werden. Auf der anderen Seite jedoch könnten kompromittierte Applikationen über den Controller das Netzwerk beeinflussen. Die momentan noch fehlende „Intelligenz“ bei Controllern lässt keine Priorisierung von Applikationen, welche für Sicherheit verantwortlich sind zu. So kann es passieren das sich Anwendungen widersprechen. Zum Beispiel wird eine interne Maschine von einer Sicherheitsanwendung unter Quarantäne gestellt, während dessen sieht eine Applikation für Load-Balancing, dass diese unausgelastet ist und leitet den Datenfluss zu ihr um. Jedoch sind schon Anwendungen in der Entwicklung, welche diese Priorisierung ermöglichen sollen.

> ”Passt jemand nicht auf den Controller auf, wird dieser zu einem sehr profitablen Ziel für einen Angreifer. Er könnte diesen relativ einfach kompromittieren, die Code-Basis modifizieren und die Kontrolle des Traffics übernehmen. In diesem Fall kann der böswillige Hacker Daten extrahieren oder an einer Stelle speichern, an der sich diese weiter analysieren lassen.”

So Dave Shackleford, führendes Mitglied bei IANS und Security-Consultant bei Voodoo Security.[4]

Wenn jedoch der SDN-Overlay nicht auf die Eigenschaften der Netzwerkinfrastruktur eingeht, werden Ineffizienz und geringer Durchsatz die Folge sein. Deshalb sind insbesondere Carrier an SDN-Lösungen interessiert, welche Rücksicht auf Datenmenge, Topologie und Hardware des Netzwerks nehmen und äquivalent reagieren.

Die Verbindung zwischen dem Controller und den Netzwerkelementen erfolgt in den meisten Fällen über das „Open-Flow“ Protokoll. Neben dem OpenFlow Protokoll unternimmt vor allem Cisco Versuche hauseigene Protokolle und Standards, wie OpFlex, zu etablieren[5].

### 4.2.4 OpenFlow

OpenFlow ist ein Standard für ein Protokoll das Zugriff auf die Hardware-Komponente, welche die Verarbeitung des Netzverkehrs, von Switches und Routern ermöglicht. Der Zugriff kann physisch oder auch virtuell (Hypervisor basiert) stattfinden. OpenFlow bietet somit eine Möglichkeit Routing Services direkt zu modifizieren. Das kann von kleinen Debugging-Modifizierungen bis hin zur Modifizierung von ganzen Bibliotheken für Routing Entscheidungen reichen.

Entwickelt und verwaltet wird der Standard von der Open Networking Foundation, eine Organisation mit dem Ziel SDN zu verbreiten.

#### Schwachstellen OpenFlow in Software defined Networks

Da Switches und Router fortan eine sehr viel geringere Attraktivität für Angriffe bieten und auch die Kommunikation zwischen Controller und Switch selbst kein sehr lohnendes Ziel darstellt, ist die Wahrscheinlichkeit für einen Angriff in diesem Bereich eher unwahrscheinlich. Auch wenn man nur das Netzwerk lahmlegen möchte gibt es einfachere Möglichkeiten um für Störungen zu sorgen. Man könnte einerseits die Control-Plane beschäftigen oder auch die Schnittstelle zwischen Control-Plane und Data-Plane auslasten. Nichts desto trotz ist unter anderem darauf zu achten das die Schnittstelle korrekt implementiert wird.

## 4.3 Outsourcing Modell für Inter Domain Routing

Inter Domain Routing basiert momentan auf einem vollkommen dezentralisierten Design in welchem mehrere Autonome Systeme mit Hilfe des Border

Gateway Protokolls (BGP) interagieren. Ein Autonomes System ist eine Ansammlung von mehreren IP-Netzen, welche als Einheit von einer gemeinsamen Verwaltung beispielsweise einem Internet Service Provider (ISP), einer internationalen Firma oder einer Universität verwaltet werden. Durch die Verbindung der Autonomen Systeme untereinander entsteht das Internet. BGP ist sozusagen der „Kleber“ der das Internet zusammen und funktionsbereit hält. Doch Inter Domain Routing sieht sich aufgrund dieser verteilten Infrastruktur vielen Problemen gegenüber. Dazu gehören die Komplexität, die Sicherheit, die Skalierbarkeit und die Durchsetzung von Richtlinien. Auch die Verwendung von BGP birgt einige Probleme, unter anderem langsame Konvergenzzeiten bei der Pfadfindung oder auch Route Flap damping[3]. Weiterhin besteht die Gefahr, dass Richtlinien Konflikte zu globaler Instabilität oder Divergenz führen können.

Doch aufgrund der Tatsache das BGP so weit verbreitet ist und quasi den de facto Standard für Inter Domain Routing bildet, lässt sich BGP nicht so einfach ersetzen. Doch ein neues Routingmodell basierend auf Outsourcing[17] und der Verwendung von SDN Prinzipien, welches zugleich noch Abwärtskompatibel ist, könnte eine neue Alternative gegenüber klassischen Routingverfahren darstellen. Bei diesem Modell wird die Control-Plane der Hardwarekomponenten von Autonomen Systemen an einen externen Dienstleister ausgelagert. Solch eine logisch zentralisierte Multi-AS-Control-Plane, welche auf SDN Prinzipien basiert, ist der wichtigste Aspekt für effizientere Routing Entscheidungen oder um Richtlinienkonflikte oder Fehler zu entdecken und zu beheben. Hierbei gilt es jedoch drei große Bereiche zu beachten.

### 4.3.1 Zentralisierung der Control-Plane

Durch die Zentralisierung der Control-Plane kann die Verwaltung des Routings drastisch vereinfachen werden. Weiterhin könnte durch die Zentralisierung eine schnellere Konvergenzzeit für die Findung von Routen erreicht werden, da Interior Gateway Protokolle (IGP) und Exterior Gateway Protokolle (EGP) in einem Controller zusammen laufen. Somit wird die Implementierung von Richtlinien für das Routing erleichtert, genauso wie die Modifizierung von IGP-Protokollen. Um weiterhin die Ausfallsicherheit und eine bessere Netzlastverteilung (load-balancing) zu gewährleisten, werden in einem Netzwerk mehrere Controller installiert. Auch ist das Klonen der Control-Plane leichter und ermöglicht so ein einfacheres und sichereres modifizieren der Konfiguration.

[3]Route Flaps werden von Routen verursacht, welche über längere Zeiträume hinweg annonciert und zurückgezogen werden.

### 4.3.2 Outsourcing

Der zweite Punkt ist das Outsourcing an sich, denn Routing umfasst wesentlich mehr als das pure Wissen wie BGP oder andere Protokolle arbeiten. Es umfasst das Wissen wie Pakete gesendet und weitergeleitet werden, die Sicherung des Netzes, die Problematik der Skalierbarkeit, den Fluss des Netzverkehrs, die Fehlerbehebung und die ständige Optimierung des Netzes. Da jedoch viele Netze eher von Administratoren, welche aufgrund ihrer Tätigkeit das praxisrelevante Wissen besitzen jedoch nicht die Theorie, betreut werden ist das Wissen für diesen notwendigen Optimierungen nicht immer vorhanden. Weiterhin muss jeder ISP seinen eigenen Routercode entwickeln, updaten und debugen. Die Entwicklung dieses Codes ist sehr kostspielig und die manuelle Aktualisierung der Router nimmt sehr viel Zeit in Anspruch. Manuelle Konfiguration birgt immer eine große Fehlergefahr und durch die falsche Konfiguration funktioniert das Routing nur noch fehlerhaft. Dies kann teuer werden oder gar ganze Teile des Netzes lahmlegen. Wenn man diese Kompetenzen und Verantwortung zu einem externen Dienstleister auslagert, welcher umfassendes Wissen und spezialisierte Arbeitskräfte zur Verfügung hat sinkt die Wahrscheinlichkeit der fehlerhaften Konfiguration. Angst das die bisherigen Richtlinien nicht eingehalten werden können besteht hierbei nicht, denn der ISP kann zusammen mit dem externen Dienstleister einen Plan für die Richtlinien und deren Umsetzung erstellen. Trotz der gleichen Richtlinien kann dennoch die beste Routingperformance erreicht werden. Vor allem bei vorher nicht intelligenten Netzwerken sieht man sofort enorme Vorteile in Bezug auf Performance und Lastverteilung. Durch das Outsourcen zu externen Dienstleistern kann eine verbesserte Stabilität, Erreichbarkeit, Sicherheit und Performance erzielt werden. Der Dienstleister aktualisiert selbstständig die Routing Information Base (RIB), Routingtabelle, und die Forwarding Information Base (FIB), Tabelle in welcher der Router nach dem nächsten Netzelement (HOP) sucht. Von dem zentralen Controller aus kann dieses Update wesentlich schneller durch BGP mit dem gesamten Netz geteilt werden. Die BGP Nachrichten von anderen Netzen werden direkt von den „Grenzroutern“ zum Controller geleitet und umgekehrt auf die gleiche Weise verteilt. Der ISP stellt hierbei die Infrastruktur, Topologie, Bandbreite und Messdaten, sowie Jitter Delay und Netzwerkzeuge zur Verfügung. Dies wird ebenso wie die Richtlinienpolitik des ISP vom Outsourcing Dienstleister geheimgehalten, auch gegenüber anderen ISP's, welche auch ein Dienstleistungsvertrag mit dem Dienstleister abgeschlossen haben. Durch die Dienstgütevereinbarung bzw. Service-Level-Agreement (SLA) werden Leistungseigenschaften der Beziehung zwischen ISP und Dienstleister geregelt. Im Gegensatz zu normalen Verträgen bietet ein SLA die Wahlmöglichkeit verschiedener Gütestufen für Dienstleistungsparameter. Das ist für den Auftraggeber wichtig um aus betriebswirtschaftlichen Gründen Entscheidungen der Dienstgüte treffen zu können. Außerdem ist im SLA auch die Sichtbarkeit des Netzverkehrs nach außen hin und die Vertrauenswürdigkeit des Dienstleisters geregelt.

### 4.3.3 Formung von Clustern Autonomer Systeme

Wenn nur ein einziger ISP die Control-Plane seines Autonomen Systems an einen Dienstleister auslagert bleiben die Anfangs erwähnten Probleme beim Inter Domain Routing bestehen. Wirkungsvolle Vorteile kommen erst zum Tragen wenn mehrere Autonome Systeme unter einer gemeinsamen Federführung verwaltet werden. Dabei ist es nicht von Belang ob die einzelnen ISP's sich untereinander in einem Vertragsverhältnis befinden. Je mehr Autonome Systeme von einem Anbieter verwaltet werden, je größer das Cluster, umso enormer wirken sich die Vorteile des Routingmodells aus. Durch diese Clusterbildung ist es dem Dienstleister möglich das Inter Domain Routing zu optimieren, da er die unterschiedlichen Richtlinienpolitiken, Topologien und Monitoring Informationen seiner Kunden kennt. Er erkennt frühzeitig schon bei der Konfiguration mögliche Richtlinienkonflikte und kann diese umgehen. Weiterhin können Routingpfade optimiert werden, auch wenn die ISP's auf verschiedene Routingoptimierungskriterien zurückgreifen wollen. Dies schafft Vorteile in Bezug auf die Stabilität der Routen und die Abmilderung der Pfadinflation betrifft auch ISP's oder andere Autonome Systeme welche selber nicht im Cluster vertreten sind. Denn für diese wirkt es sich durch kürzere und stabilere Ende zu Ende Pfade auch positiv auf die Reduzierung der Netzlast aus. Zusätzlich hat der Dienstleister die Möglichkeit die Einhaltung der SLAs innerhalb des Clusters zu überprüfen, wenn es um das respektieren der Richtlinien des Nachbarn geht. Außerdem besteht für den Dienstleister die Möglichkeit neue Routingprotokolle innerhalb seines Clusters zu verwenden, um somit die Entwicklung und Verbesserung zu beschleunigen. Während dessen wird nach außen hin die Interoperabilität gewährleistet in dem weiterhin die selben Protokolle wie zuvor genutzt werden. Durch die Einführung neuer Technik und die Zusammenfassung der Autonomen Systeme in einer zentralen Kontrolllogik ergeben sich niedrigere Konvergenzzeiten und der Aufwand zum durchsuchen des Netzes auf der Suche nach dem schnellsten Pfad wird reduziert. Ein weiterer Vorteil wird aus der hierarchischen Topologie gewonnen. Welche die Skalierbarkeit des gesamten Systems vereinfacht. Ein weiterer positiver Aspekt ist die Gelegenheit der Einführung von Sicherheitsschemata und Fehlerbehebungsschemata. Durch das Sammeln der Daten seiner Klienten und den gleichzeitigen Abgleich mit anderen vertrauenswürdigen Quellen, die restlichen Systeme im Cluster und [1, 2] zur Verifikation und zur Validierung ergeben ein neues Konzept von gemeinsamer und damit verbesserter Sicherheit.

Der beispielhafte Aufbau eines Clusters ist in Abbildung 4.3 zu sehen.

### 4.3.4 Wirtschaftliche Aspekte

Neben den positiven technischen Gesichtspunkten machen sich auch viel versprechende wirtschaftliche Aspekte bemerkbar. Um Kosten zu sparen mussten Netze aus Sicht der Operatoren immer ausgelastet sein und erst dann

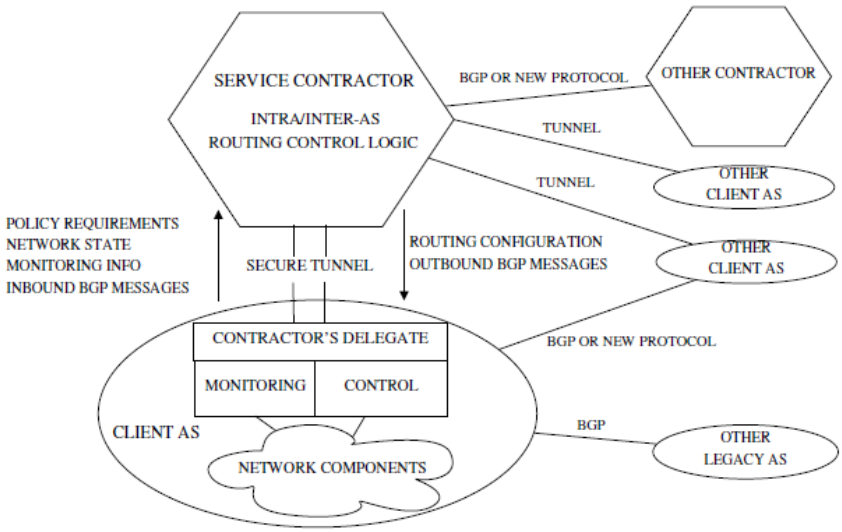


Abbildung 4.3: Clusteraufbau

konnten neue Serviceleistungen angeboten werden. Wenn man nun die Managed Services zu einer außenstehenden Partei auslagert können die Betriebskosten reduziert werden. Der ISP kann nun niedrigere Serviceleistungen auslagern und spart somit Arbeitskräfte für die höheren Serviceleistungen ein. Er kann neue Serviceleistungen in sein Portfolio aufnehmen und somit seine wirtschaftliche Attraktivität steigern. Diese Form des Routingmodells bevorzugt jedoch zu meist kleinere und mittelgroße Autonome Systeme, wobei die größeren Unternehmen mit einer entsprechenden Expertise in Sachen Routing den Dienstleister stellen können.

## 4.4 Hybridmodell für Intra Domain Routing mit Auswirkung auf Inter Domain Routing

Eine saubere Trennung der Funktionalität von der Infrastruktur eines Netzes oder eines Systems steht an erster Stelle. Aufgrund dieser Priorität gab es bereits Arbeiten [6] über eine zentralisierte Routing Control Platform (RCP) in traditionellen IP Netzen und diese waren auf Internal BGP (iBGP) Lösungen ausgelegt. iBGP wird genutzt, um Routing Informationen im eigenen Autonomen System zu propagieren. Die RCP baut auf 3 architektonischen Prinzipien auf. Das erste Prinzip ist die Pfaderrechnung basierend auf einem konstanten Überblick über den Zustand des Netzes. Eine weitere Direktive ist die Kontrolle der Interaktion zwischen den Protokollen und Schichten. Der dritte und letzte Grundsatz verlangt aussagekräftige Spezifikationen über die gewählten Routingrichtlinien. Die vielen Vorteile beim flexiblen Routing,

der Sicherheit und dem Verbindungsmanagement führten schon zu mehreren erfolgreichen geteilten Netzwerkarchitekturen wie zum Beispiel SS7[8] oder PCE[7]. In der heutigen Gegenwart verwendet AT&T, ein amerikanischer Dienstleister für Telekommunikation, eine RCP namens Intelligent Route Service Control Point[9]. Ein Modell das mit Hilfe von SDN die Data-Plane und die Control-Plane separiert, welches auf traditionelles IP Routing und Forwarding[10] trifft, bekommt bei Weitem nicht die gleiche Aufmerksamkeit wie eine Implementierung auf reinen SDN Prinzipien basierend. Doch ein hybrides Netzmodell bietet die einzigartige Gelegenheit etablierte Funktionsweisen rund um IP Routing und BGP aus einem anderen Blickwinkel zu betrachten. Ein Netzmodell dient zur Abbildung der Architektur, Topologie und Implementierung von Netzen. Ein alternativer Aufbau eines Netzes mit einer zentralen RCP unter Einbeziehung der Prinzipien von Software definierten Netzwerken und OpenFlow ermöglicht einen abstrakten BGP Routingservice im gesamten Autonomen System. Heutzutage gibt es drei Arten des Einsatzes von BGP in autonomen Systemen:

- Voll vermascht
- als Verbund
- als Route Reflector

Letzteres ist die am meisten genutzte Form, um Routen zwischen Routern des gleichen Autonomen Systems auszutauschen. Zur Vermeidung von Routingfehlern, wie beispielsweise Schwingungen im Netz, Schleifen oder Pfadineffizienz, ist es wichtig eine zuverlässige Topologie, gut ausgewählte Platzierungen für die Route Reflektoren und Link Metrik Anweisungen zu besitzen. Normalerweise werden solche Route Reflektoren an den Grenzen des Autonomen Systems in der Data-Plane implementiert oder in Schwerpunkte im Netz integriert. Diese Form der Architektur hat allerdings auch Nachteile, der größte liegt in seiner Effizienz der Pfadfindung da es auf IGP Protokollen basiert und die Informationen an viele Route Reflektoren verteilt werden müssen. Je größer das Netzwerk ist und je mehr Route Reflektoren(RR) sich im Netz befinden umso langsamer können die benötigten Informationen verteilt werden.

Doch auch bei Routing Control Plattformen, welche mit iBGP, arbeiten gibt es ein ähnliches Problem wie bei der Verwendung von Route Reflektoren. Die Anzahl der adressierbaren Router für eine effiziente Nutzung sind beschränkt. Selbst wenn die RCP mit eBGP arbeitet, so arbeiten dennoch die Router in der Provider Edge (PE), Übergang zu anderen Autonomen Systemen, mit iBGP Präfix Regeln. Dieses Modell eines hybriden Netzwerkes zielt unter anderem darauf ab die Route Reflektoren aus der Data-Plane herauszunehmen und durch eBGP fähige Applikationen zu ersetzen. Dies soll unter anderem durch eine Edge zu Edge Kapselung ermöglicht werden. Unter Berücksichtigung von MPLS oder IP Kapselung können so auch andere

Protokollabwandlungen aus der BGP Familie genutzt werden, welche auch das Internetrouting von IPv6 ermöglichen. Weiterhin wird die Verwendung der eBGP fähigen Applikationen durch die SDN Prinzipien und die Verwendung von OpenFlow wirksam, denn dadurch erhält man vollen Zugriff zur Modifizierung der Forward Information Base. Die Forward Information Base, Lookup Tabelle für Forwarding Einträge, wird in diesem Fall durch die OpenFlow-Tabelle ersetzt. Mit der Separierung der Control-Plane aus den Routern in eine Route Flow Control Platform (RFCP), Prinzip wie RCP nur mit SDN und OpenFlow kompatibel, wird ein BGP freier Übergangsraum geschaffen. Denn die gesamten Entscheidungen werden nur noch in einer höheren Instanz getroffen und nicht mehr in den Routern oder den jeweiligen RCP's und mit OpenFlow an die Netzelemente verteilt. Dies löst das Problem, dass entweder ein vollvermaschtes iBGP Netz oder Route Reflektoren benötigt werden um Routen intern zu veröffentliche.

### 4.4.1 Design

Um eine reibungslose Migration zu gewährleisten, ist der Ausgangspunkt das traditionelle Netzmodell, von PEs verbunden über iBGP durch RR. Es entsteht eine neue Steuerungsebene in der Form eines BGP-Controllers, der Route Flow Control Platform (RFCP), welche als Gateway zwischen OpenFlow-Controllern und bestehenden RRs agiert. Das Ausmaß dieser Einsatzmöglichkeit kann variieren und vom Netzbetreiber vollständig kontrolliert werden.

#### RFCP Komponenten

Die RFCP ist eine Entwicklung hin zu einem verbesserten geschichteten und verteilten System, das flexibel genug ist um Platz für verschiedene Anwendungsfälle der Virtualisierung (m:n-Abbildung von virtuellen Schnittstellen der Routing-Engine zu physikalischen OpenFlow kompatiblen Ports) zu bieten. Auch erleichtert Sie die Entwicklung von fortgeschrittenen routingorientierten Anwendungen. Im Vorgriff auf die Notwendigkeit für die Aktualisierung (oder sogar Ersetzung) von Teilen der Infrastruktur, während RFCP die Multisteuerung unterstützt, ist die Umsetzung in die folgenden drei Komponenten getrennt (siehe 4.4).:

#### RF-Client

Sammelt Routing und Forwarding Informationen durch die Routing-Engine (z.B. Quagga) des Linux Systems, wo es als User-Space-Daemon läuft. Optional kann es, um zusätzliche Routing-Informationen zu extrahieren (z.B. alle BGP Pfade in der RIB-IN) in die Routig-Engine mit eingeflochten werden.

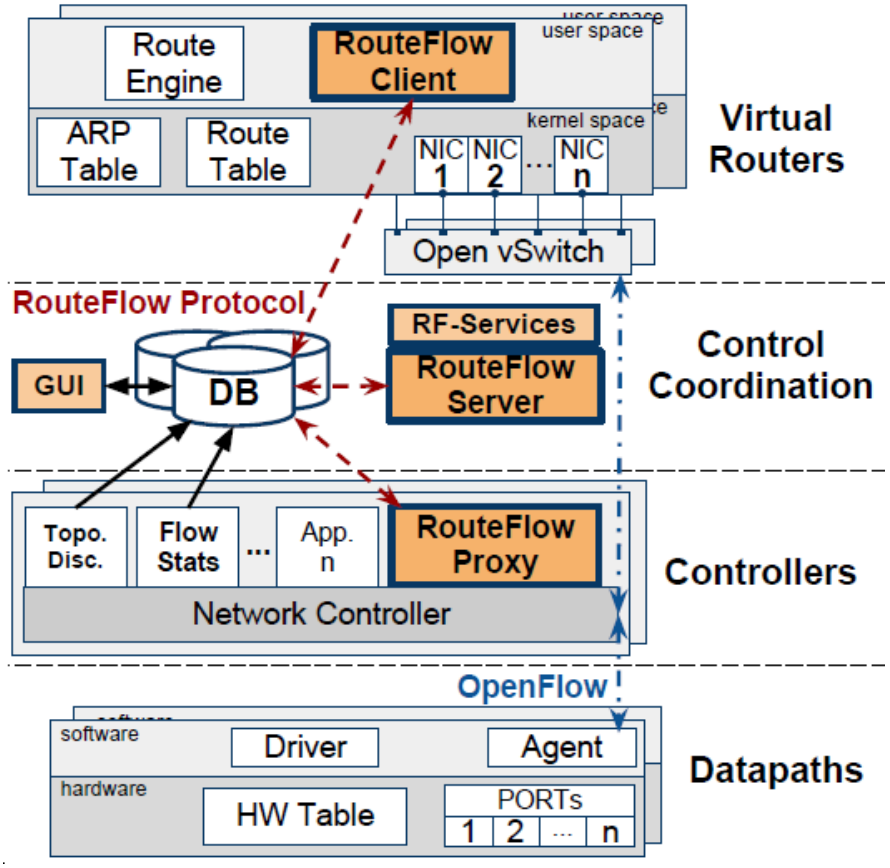


Abbildung 4.4: Architektur der Routing Flow Control Platform

### RF-Server

Bezeichnen Standalone-Anwendung, welche für die Kernlogik des Systems (zum Beispiel die Ereignisverarbeitung, etc.) verantwortlich sind. RFCP Dienstleistungen werden als auf den Operator zugeschnittene Module umgesetzt, welche auf Datensätze in der Informationsdatenbank zurückgreifen um High-Level-Routing-Logiken zu liefern (beispielsweise Lastverteilung, bevorzugte Austrittsstellen, etc.).

### RF-Proxy

Simple "ProxyÄnwendung, die auf einem OpenFlow Controller (zB NOX, POX) implementiert ist und die RFCP mit Daten bezüglich Topologie und Netzzustand von Monitoringanwendungen beliefert. Im Einklang mit den besten Design-Praktiken von Cloud-Anwendungen setzt man auf einen skalierbaren, fehlertolerante Datenspeicher, welcher die RFCP Kernkomponenten (z.B. Ressourcenzuordnungen), die Netzwerkübersicht (logisch, physikalisch und protokollspezifisch) und weitere Informationen (wie zum Beispiel Netzwerkverkehr Histogramme / Prognosen, Datenflussüberwachung, Verwaltungsrichtlinien) zentralisiert und dazu beiträgt Routing Anwendungen zu

entwickeln. Der Datenspeicher umfasst die so genannte Network Information Base (NIB) und die Knowledge Information Base (KIB). In diesen Datenspeichern werden Datensätze zu Netzressourcen und deren Status, logische, physikalische und Protokoll spezifische Informationen sowie Monitoring Ergebnisse gespeichert. Darüber hinaus wird eine dezentrale NoSQL-Datenbank als PubSub (Publish-Subscribe, bedeutet die Anwendung verschickt die Daten nicht an einen bestimmten Empfänger sondern unterteilt die Nachrichten in Klassen) als Message-Queuing inter-process communication (IPC) eingesetzt , die lose die Module über eine erweiterbare auf JavaScript Object Notation basierte Umsetzung des RouteFlow Protokolls verbindet. Die Datenspeicher basierte IPC erleichtert das Fehlermanagement, das Debugging und das Monitoring ohne das Leistungseinbußen eintreten. Insgesamt versucht das RFCP Design Prinzipien zu folgen, welche eine weitere architektonische Entwicklung zu lassen: Indirektionsschichten, System Modularität und Erweiterbarkeit der Schnittstelle.

### Protokolle und Abstraktionen

Das RouteFlow Protokoll hält die verschiedenen Module mit einer einfachen Befehl / Antwort-Syntax, northbounded[4], mit den RF-Clients und einer Teilmenge von OpenFlow-Nachrichten, southbounded[5], an die RF-Proxy-Anwendung zusammen. Als ein Ansatz der OpenFlow Mehrsprachigkeit abstrahiert die RouteFlow Protokollschicht die meisten Unterschiede von der Controller Implementierung mit OpenFlow-Versionen 1.x und den etwas höhergestellten RouteFlow APIs. Abgesehen davon, dass OpenFlow die API zur Data-Plane ist, wird es auch für die Übermittlung von Nachrichten an oder von der Control-Plane an die Schnittstellen der VMs, auf denen die Routing-Engine implementiert ist, und die Schnittstellen der RF-Clients genutzt. Bei der Programmierung der virtuellen Switches kann man eine Betriebsart auswählen bei der entweder Routing-Protokoll Nachrichten an die physischen Geräte "nach unten"gesendet oder in der virtuellen Netzebene „oben“ gehalten werden. Die virtuelle Netzebene kann hierbei eine Reproduktion der erkannten physischen Konnektivität oder eine vereinfachte Version der Hardware Ressourcen sein. In der erst genannten Betriebsart folgen die Nachrichten dem physischen Weg, so dass kein weiterer Fehlererkennungsmechanismus auf Kosten der Laufzeit erforderlich ist. In der Letzteren, bei der die Nachricht in der virtuellen Domäne gehalten wird, profitiert man von niedrigen Latenzzeiten und einer besseren Skalierbarkeit. Diese Option bietet eine homogene Unterstützung für virtuelle Netzwerke, aber erfordert zusätzliche Programmierbarkeit und eine Fehlererkennungserweiterung um logische Zuordnungen, passend zu Veränderungen der physikalischen Links, in der virtuellen Maschine zu aktualisieren.

[4]Vom SDN-Controller in der Schichtansicht übergeordnete Anwendungen.
[5]Vom SDN-Controller in der Schichtansicht untergeordnete Data-Plane

Alles in allem werden folgende Voraussetzungen unter Berücksichtigung von IP Forwarding und Adressen betrachtet: Die Fähigkeit gewünschte Routenkriterien in einer Abstraktionsebene zu definieren , in der es nicht erforderlich ist eine individuelle Konfiguration von mehreren Routing-Prozessen vorzunehmen. Eine einheitliche Datenbank, die Wissen und Netz-Informationen bereitstellt für die Versorgung von Route Control Services und skalierbare virtuelle Elemente in der Control-Plane, die starke Automatisierung und Flexibilität der Speicherbelegung für vorgesehene Kontrollszenarien zulassen.

### 4.4.2 Anwendungsfälle

Es ist nicht erforderlich Änderungen an Routern oder Protokollen vorzunehmen. Vorherige Anwendungsfälle (zum Beispiel geplante Wartungsarbeiten) können weiterhin wie gewohnt unterstützt werden. Aus Gründen der Aktualität wird man besonderes Augenmerk auf neue OpenFlow fähige Szenarien legen die vorher nicht oder schwerer umsetzbar waren aufgrund einer Umgebung mit vielen Provider, welche unterschiedliche Protokolle nutzen.

#### Ausgereifte Pfadauswahl

Da die RFCP alle verfügbaren Pfade kennt ist sie in der Lage ein verbessertes Load-Balancing und eine bessere Preis/Leistungspfadauswahl für Anwendungen oder Kunden welche OpenFlow nutzen anzubieten. Außerdem ermöglicht OpenFlow die direkte Vorbereitung für optisches Switching im Kern des Netzes als auch von Provider Edge zu Provider Edge, der Übergang von einem Autonomen System zu einem anderen Autonomen System. Neuere Forschungen[18] haben gezeigt, dass die netzwerkweite Transparenz und Kontrolle eine gemeinsame Netztechnik und Fehlerbehebung durch effizientes Load-Balancing ermöglichen.

#### Optimale „beste Route“ Reflexion

Route Reflexionen ergeben nicht qualitativ gleichwertige Routenauswahlergebnis wie ein voll vermaschtes iBGP Netz. Dies hindert das System daran hot-potatoe Routing zu betreiben und so den dem RR am nächsten gelegenen Ausgangspunkt zu finden. Mit voller Einsicht in alle Routen und die OpenFlow-Steuerung kann die 'optimale' Routenwahl und der FIB 'Download' aus der Perspektive jedes einzelnen Datenpfades erfolgen. Mit der Flexibilität für jeden Eingangspunkt im Netz und auch für Kunden die über Layer 3 VPNs kommunizieren, die besten Routen zu berechnen .

### Pfadschutz mit Präfix unabhängiger Konvergenz

Der komplette Überblick über die Zustände der Routen in der RFCP ermöglicht es neuen IP-Route Schutzsystemen wie Berechnungen für primäre und sekundäre Pfade, von jeder Provider Edge ausgehend, für jedes Präfixobjekt unter Berücksichtigung gemeinsamer Rückschlüsse auf Risikogruppen. Openflow v1.1 Gruppen und Multi-Tabellen gestatten eine schnelle Erholung von Fehlern, für hierarchische Implementierungen der FIB Organisation, in der Provider-Edge. Netzweit können schleifenfreie alternative Next-Hops vorberechnet und in den Gruppentabellen verwaltet werden, dies nimmt die Last eines Updates für jeden Flow-Präfix heraus. Dies ermöglicht eine schnelle vor Ort Reparatur durch zum Beispiel eine Bidirectional Forwarding Detection (BFD) ausgelöste Zustandsänderung, vorausgesetzt eine Operation and Maintenance (OAM)-Extension ist vorhanden.

Das allgemeine Design-Prinzip wendet sich ab von der dynamischen Routenberechnung durch die Entkopplung der Wiederherstellung von Routen nach Ausfall der Pfadberechnung.

### Sicherheit der Datenebene

Die Verwendung von Openflow und SDN kann dazu beitragen die Sicherheit zu verbessern, indem beispielsweise ein OpenFlow Switch installiert wird, um die Netzströme zu überwachen und abnorme Muster zu erkennen. Mit SDN können Firewall- und IPS/IDS-Funktionalitäten entlang des Pfades verteilt werden, die beispielsweise auf Kundenbasis implementiert werden,anstatt den gesamten Datenverkehr zu zwingen diese Vorkehrungen zu passieren oder den Datenverkehr in eine extra Box weiterzuleiten. Einmal erkannt, kann eine selektive DDoS blackholing Strategie zum Einsatz kommen bei der Einträge in der Flow-Tabelle mit höherer Priorität versehen werden, welche einen Paketdrop an den unter Angriff stehenden Eingangsports veranlassen. Die durch OpenFlow fein abstimmbaren Regeln (inport, src, dst, tp - Port) erlauben den Verkehr, ohne Außerbetriebnahme der Ziel IP, zu dropen (wie es bei den heute üblichen Filtern und BGP-basierten Mechanismen der Fall ist).

### Sicheres Inter-Domain-Routing

Zentralisiertes BGP ermöglicht es einem einzigen Autonomen System leichter die Herkunft von BGP Validierungen und Vorteile der Routenwahl von am Adressregister teilnehmenden vertrauenswürdigen Autonomen Systemen zu kontrollieren, wie PKI, DNSSEC oder neue Sicherheitstechniken jenseits der heutigen Konzepte. Zum Beispiel die Plattform Morpheus[19], welche Algorithmen(beispielsweise auf früherer Anomalieerkennung basierende) vor schlägt um eine 'ziemlich gute' BGP Sicherheit zu erreichen ohne die massive Adaption von S*BGP. Ein RFCP-ähnlicher Ansatz eliminiert doppelte

Verarbeitung und zusätzlich die zuvor benötigten Software und Hardware-Upgrades von AS Grenzrouter. Der Einsatz von viel CPU-Leistung und Kryptounterstützung auf dem Controller erleichtert das zentralisierte Key-Management und reduziert den Aufwand für Zertifikate auf einmal pro Nachbar und nicht einmal pro Peering Einrichtung.

#### Vereinfachung von Kunden Multi-Homing und IPv6-Migration

Unternehmensnetzwerken mangelt es an kundenfreundlichen, effektiven Multi-Homing-Lösungen, insbesondere in Abwesenheit von IP-Adressen oder Dual-Stack-IPv4 / v6. RFCP könnten als vorgeschaltete Verbund Mechanismen verwendet werden, die Pakete,welche von ISP-1 Netzwerken stammen, nur über das Netz von ISP-1 senden (und 2 über 2), auf Grundlage von Flow-matching bezüglich der Quell-IP-Subnetze. Im Prinzip liefert es ein Virtual Routing Forwarding via WAN-Verbindung mit Quelladress-basierter Virtual Routing Forwarding Auswahl für ausgehenden Datenverkehr.

Die Openflow-API erlaubt es Flows Performance und/oder Kosten basiert zu aktualisieren. Gleichzeitig wird die Migration zu IPv6 in den Provider Edges beschleunigt und kostengünstig mit OpenFlow ausgerollt werden können, das möglicherweise die Entstehung neuer Dienstleistungen, welche die Stärken von IPv6 nutzen und die Schwächen der Control-Plane mindern, vorantreibt.

### 4.4.3 Vorteile

#### Vereinfachte Edge Architektur

Es sind geringere Anforderungen für jedes Gerät in der Edge nötig und dennoch sind sie in der Lage mit neuen, zukünftigen Services oder Erweiterungen umzugehen. Die Notwendigkeit der Speicherung und effektiven Verarbeitung des gleichen Datensatzes von Daten der Control-Plane entfällt und die selben Aufgaben werden zentral für eine große Zahl von Edge Geräten ausgeführt.

#### Geringere Kosten und höhere Geschwindigkeit in der Edge

Aufbauend auf der Nutzung von Commodity Switches und Remote Open-Source-Routing-Software werden Anforderungen für Hardware Upgrades entkoppelt, welche vom Anbieter durchgeführt werden müssen, weil bestimmte Betriebssysteme nicht mehr supported werden. Der Anstieg der Beschleunigung in der Edge ist eng mit den neuesten Silizium Switching Technologien verbunden , für ein optimiertes Flowswitching.

**Innovationskraft führt zu Differenzierung und neuen Einnahmen**

Die Fähigkeit in der Weiterentwicklung des Netzwerkes, entweder durch interne Entwickler / Operatoren Teams oder durch vom Verkäufer unabhängige Produkte von Drittanbietern ermöglicht, gestattet es das Dienstleistungsportfolio des Betreibers zu differenzieren. Es besteht dabei nicht die Notwendigkeit des Austausches von Innovationen oder die Nachfrage um Unterstützung bei anderen Anbietern. Die Unterteilung in einzigartige auf Kundenwünsche zugeschnittene Netzdienste ermöglichen einen größeren Umsatz für Dienstleister.

**BGP Sicherheit, Stabilität, Kontrolle und Richtlinien Management**

Wie bereits vorher erwähnt werden neue Ideen zum Thema Sicherheit rund um BGP Praxis fähig und Kosten effektiv, wenn sie in Systemen mit starker CPU ausgeführt werden. Die Stabilität der Control-Plane (Reduktion des bekannten BGP Welleneffektes) kann durch die Eliminierung der Intra-Domain-BGP Pfad Schwingungen erhöht werden. BGP-Überwachung und Reporting-Schnittstellen können leicht implementiert werden, daher gibt es keine Notwendigkeit, alle BGP "Rohdaten"von allen Grenzrouter zu sammeln. APIs aus dem Datenspeicher der RFCP ermöglichen einen Überblick über das gesamte BGP in einem Autonomen System. Zentralisierung des BGP Richtlinien-Managements ist ein wichtiger Schritt in Richtung OPEX-Reduktion und um Konfigurationsfehler zu vermeiden.

## 4.5 Modell für Intercloud Routing

### 4.5.1 Einführung

Endnutzer oder Kunden brauchen mehr Möglichkeiten um die Einrichtung von Inter Provider Links zu erleichtern und zu automatisieren. Ihnen muss die Fähigkeit gegeben werden die Steuerung, Konfiguration und Instanziierung der Verbindung zu spezialisieren um alle Vorteile von Rechen-,Speicher- und Netzwerkvirtualisierung nutzen zu können. Die Cloud Community hat sofort auf Neuerungen durch SDN reagiert nur liegt dieser Fokus eher auf der IntraCloud. Somit können Cloud User zwar ihre Anwendungen steuern und managen, jedoch haben sie keinen Zugriff auf die Konnektivität oder das Networking für ihre verteilten Cloud Services. Doch diese Flexibilität brauchen die Endnutzer um ihre Ressourcen einfacher und effizienter zu managen.

Die SDN Lösung in diesem Modell[16] basiert auf einem Controller, der als Cloud Networking Gateway Manager bezeichnet wird. Er soll das Arbeiten mit verteilten Cloud Ressourcen verbessern und bietet autorisierten Kunden die Möglichkeit das Netzwerk zu konfigurieren und zu kontrollieren. Der

CNG Manager verbindet Cloud übergreifend virtuelle Maschinen von verschiedenartigen Ressourcen und Services unterschiedlicher Anbieter durch die Nutzung eines generischen Gateways. Dieser Controller ist Bestandteil eines Frameworks für Cloud Broker.

### 4.5.2 Der Cloud Broker

Der Cloud Broker agiert als Vermittler zwischen Cloud Providern und Endnutzern um Services und andere Angebote von verschiedenen Clouds zu nutzen. Das Konzept funktioniert wie folgt:

1. Endnutzer sendet Anfrage an Cloud Broker 2. Broker teilt komplexe Anfrage in weniger komplexe Anfragen auf 3. Broker schickt in Absprache mit den Cloud Providern ein Angebot an Endnutzer

Der Broker bietet eine Plattform ähnlich eines Marktplatzes an, in dem Cloud Provider ihre Services mit verschiedenen Kapazitäts- und Preismodellen anbieten können. Da mehrere Provider ähnliche oder gar gleiche Services anbieten, kommt es zu einem Wettbewerb in welchem auch versucht wird den Preise für Endnutzer möglichst gering zu halten. Die Cloud selbst bleibt dabei relativ unangetastet, so kann jeder Provider intern seine Verwaltung und Topologie belassen, lediglich eine Installation des CNG Managers und des CNG ist notwendig. Diese stellen in Zusammenarbeit mit einem Framework des Cloud Brokers eine Verbindung untereinander her.

#### Cloud Broker Framework

Das Cloud Broker Framework besteht aus drei großen Komponenten.

#### Request Splitting

Der Request Splitter teilt die komplexen Anfragen in weniger komplexe Anfragen auf. Er geht dabei nach verschiedenen Optimierungskriterien vor: Preis, Einnahmen, Quality of Service und Beachtung von sicherheitsrelevanten Aspekten. Das Ziel ist es dem Kunden bei gleichbleibender Auftragserfüllung ein günstigeres Angebot machen zu können. Dazu sucht der Broker bei den Providern nach deren Angeboten und vergleicht diese in der Leistung und dem Preis. Gewählt wird das beste passende Angebot, welches dennoch günstig ist.

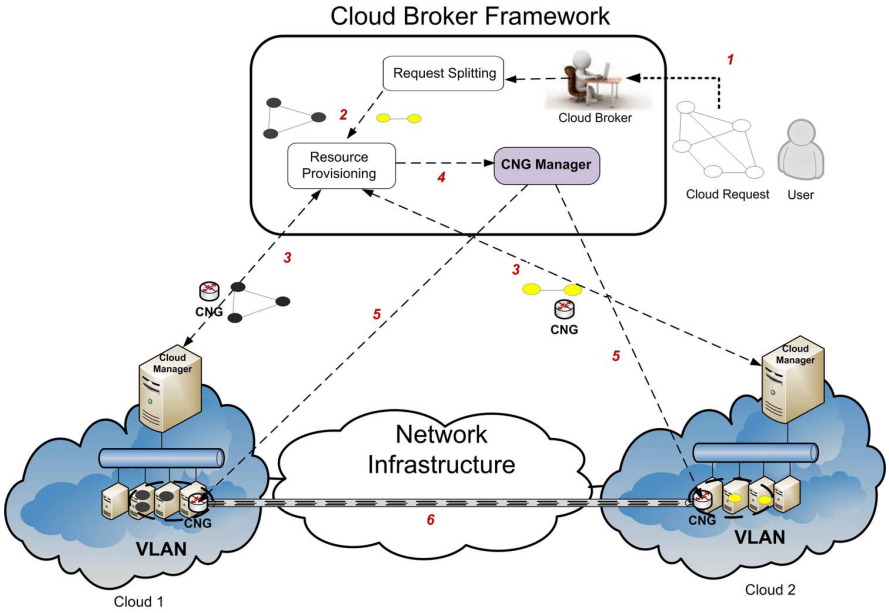


Abbildung 4.5: Beispielhaftes Cloud Framework[10]

### Resource Provisioning

Sobald der Request Splitter den Graphen (Anfrage) in Subgraphen runter gebrochen hat, werden diese Ergebnisse an das Resource Provisining Element gesendet – Schritt 2 in Abbildung 4.5. Das Resultat des Splittings beinhaltet ein Tupel aus Subgraph und zugeordnetem Provider und einen virtuellen Link für den Verbindungsaufbau zwischen 2 oder mehr Providern. Das Resource Provisioning Element bearbeitet die Komposition der Subgraphen in Rechenzentren durch die Interaktion mit den Cloud Managern in den jeweiligen Rechenzentren. Es sorgt für die Implementierung der CNG als virtuelle Maschine in der Infrastruktur des Providers wie in Schritt 3 der Abbildung 4.5 zu sehen ist. Sobald dies geschehen ist wird eine Liste mit Identifikationsmerkmalen, bestehend aus Name und/oder Adresse der eingerichteten VM, erstellt um InterSubgraph Links und die entsprechende Netzwerktopologie anzulegen. Informationen werden nach Abarbeitung der eben beschriebenen Schritte an den Cloud Networking Gateway Manager geschickt, Schritt 4.

### Cloud Networking Gateway Manager

Die Aufgabe des CNG Managers besteht in der Konfiguration der CNG durch Aktivierung der gewünschten Funktionen des Netzes in den CNG der verschiedenen Rechenzentren (Schritt 5). Durch Eintragungen der Routing Regeln in die CNG werden Tunnel zwischen den CNG aufgebaut.

Um mit den verschieden Topologien und Protokollen der Provider arbeiten zu können, wird der Cloud Networking Gateway Manager mit „Treibern“

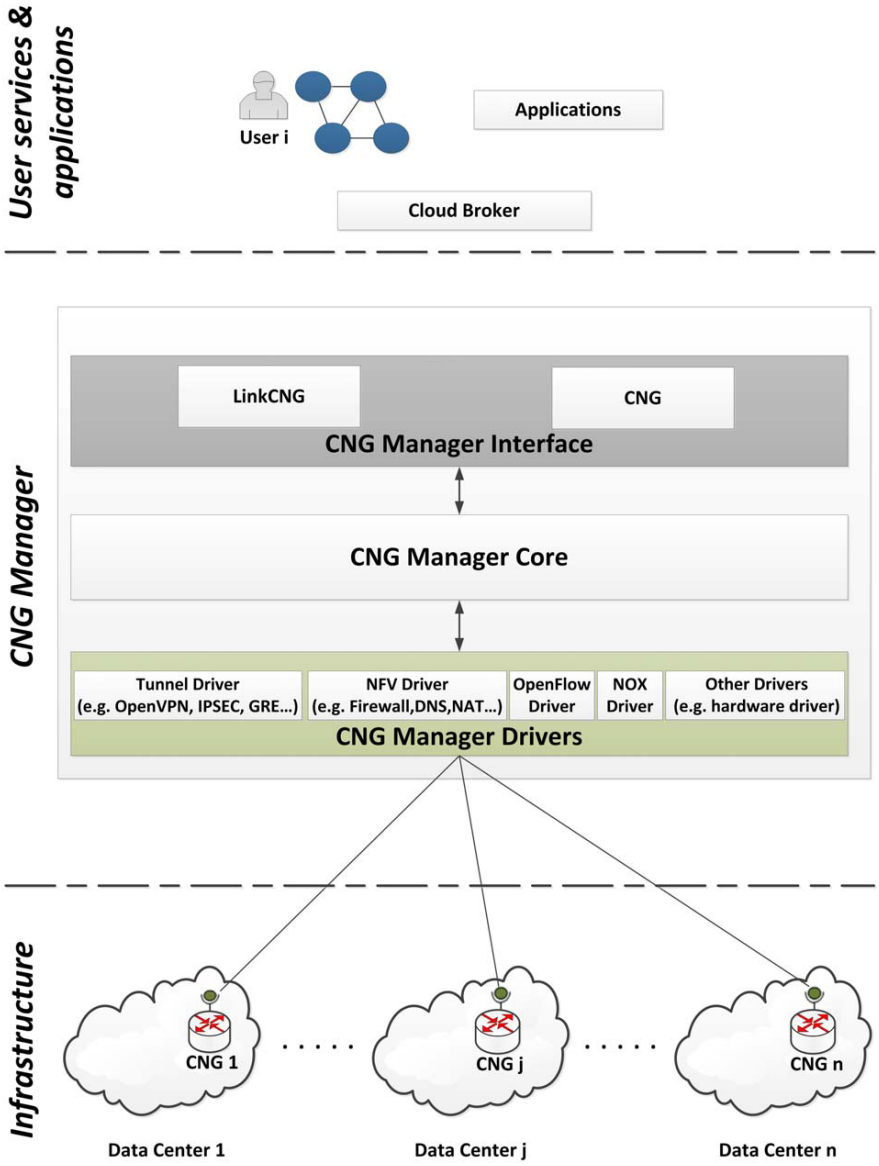


Abbildung 4.6: Aufbau des Cloud Networking Gateway Managers

ausgestattet, welche für die Interoperabilität verantwortlich sind. So gibt es, wie in Abbildung 4.6 zu sehen, hauptsächlich 2 Arten von Treibern:

- Treiber für die Einrichtung von Tunneln zwischen zwei CNG (z.B. OpenVPN, IPSEC)
- Treiber für die Netzwerkfunktionsvirtualisierung (z.B. Firewall, DNS, NAT)

Gleichzeitig versteckt der CNG Manager die Heterogenität der ihm unterlegten Infrastruktur und unterstützt den Broker in besonderem Maße bei der Aufgabe seine vielfältigen Funktionen ordnungsgemäß ausführen zu können.

### 4.5.3 Performance Evaluation

Eine erste Performance Evaluation[10] bezieht sich auf den Delay der vom CNG Manager bei dem Verbindungsaufbau erzeugt wird. Bei einer sequenziellen Konfiguration der CNG kommt es zu einem Anstieg des Delays je mehr Knoten betroffen sind. Bei einer parallelen Konfiguration jedoch ist der Delay immer ähnlich der geringsten Zeit einer sequenziellen Konfiguration, 6 Sekunden.

Weitere Tests[10] untersuchten den Delay der beim aufteilen der Anfragen in weniger komplexe Requests im Request Splitter entsteht. Wenn der Originalgraph (Requestgraph) nicht über 20 Knoten und mehr als 6 Provider einbezieht, ist der zu erwartende Delay nicht größer als 4 Sekunden.

Eine dritte Analyse[10] mit Augenmerk auf die Kostenentwicklung bei der Aufteilung auf mehrere Provider führte zu dem Ergebnis, dass je mehr Provider eingebunden sind die Kosten umso geringer ausfallen.

### 4.5.4 Sicherheit

Durch das, vor die Provider geschaltete, Framework des Brokers, welches auch über Sicherheitsmechanismen wie Firewalls und Monitoringanwendungen verfügt, wird die Sicherheit des Verbundes ebenfalls leicht erhöht. Ein weiterer Vorteil sind die durch den Broker eingerichteten getunnelten Verbindungen von Provider zu Provider. Denn ein Tunnel ermöglicht eine Ende-zu-Ende Verschlüsselung auch für Dienste, die sonst keine Verschlüsselung bieten. Dies ermöglicht den Providern untereinander einen komplett verschlüsselten Datenaustausch.

## 4.6 Zusammenfassung

Aufgrund der aufwendigen Konfiguration von Hard- und Software wird der Ausbau und der technische Fortschritt von Netzen stark eingeschränkt. Zudem bietet die manuelle Konfiguration von Netzelementen[6] ein großes Potenzial für Fehler. Solche Fehler können die Sicherheit, Stabilität und Konnektivität des Netzes oder auch von mehreren Netzen beeinflussen, es könnte aufgrund eines einzelnen Konfigurationsfehlers zu einem globalen Teilausfall von mehreren Autonomen Systemen führen.

Durch die Umsetzung der SDN-Prinzipien kann diesen Problemen begegnet werden. Mit Hilfe des Controllers kann eine automatisierte Konfiguration,

[6] Router, Switches etc.

welche menschliche Fehler verhindern kann, durchgeführt werden. Wenn jedoch der Controller fehlerhaft implementiert ist, wird auch die automatisierte Konfiguration zu Fehlern führen. Weiterhin kann das verbesserte Load-Balancing, wie bereits im Abschnitt Software defined Networks erwähnt, zu einer Steigerung der Performance führen, in dem die Netzlast besser verteilt und somit Datenstau oder die Auslastung einzelner Netzelemente verringert wird. Auch wenn der SDN-Controller ein zweifelsfrei lohnendes Ziel darstellt, so wird dennoch die Sicherheit des gesamten Netzes verbessert. Denn durch die Verwendung von SDN ist es möglich das gesamte Netzwerk zu überwachen[7] und mit der Vielzahl an Datensätzen Anomalien mit erhöhter Wahrscheinlichkeit und schneller zu entdecken. Dadurch können beispielsweise DDOS-Angriffe früher erkannt und zum Schutz des Ziels in ein Blackhole[8] geleitet werden. Weiterhin können Sicherheitsrichtlinien schneller aktualisiert und an laufende Bedrohungen angepasst werden. Wichtig für die Sicherheit eines auf SDN-Prinzipien basierten Netzes ist der Schutz des Controllers als primärer Angriffspunkt. Ist der Controller nicht ausreichend gesichert und wird kompromittiert, sind viele Sicherheitsmaßnahmen leicht zu umgehen oder gar zu deaktivieren.

Im ersten vorgestellten Modell (4.3) beruht das Prinzip des Designs in der Formung eines oder mehrerer Cluster von Autonomen Systemen mit einer gemeinsamen Control-Plane. Die Autonomen Systeme stellen der Control-Plane alle Monitoring-Daten zur Verfügung und tragen so dazu bei, die Sicherheit des ganzen Clusters zu erhöhen. Denn je mehr Daten dem Controller zur Auswertung vorliegen, umso genauer werden seine Berechnungen und die Chance, einen Angriff zu entdecken, steigt. Auch ist es möglich die Lücken in den Sicherheitsrichtlinien weitestgehend zu schließen, da der Betreiber der Control-Plane Konflikte im Zusammenspiel der Richtlinien seiner im unterlegten Autonomen Systeme entdecken kann. Je höher die Anzahl an beteiligten AS innerhalb eines Clusters, umso sicherer ist das Autonome System selbst und das Cluster. Nachteil ist hier jedoch, wenn ein erfolgreicher Angriff auf den Controller erfolgt, sind alle Netze des Clusters betroffen, nicht nur einzelne.

Das Hybridmodell (4.4) umfasst das traditionelle IP-Routing mit einer zentralen Control-Plane, Route Flow Control-Plane, genannt. Durch die Zentralisierung der Control-Plane und die dadurch entstehende Fähigkeit das Border Gateway Protocol ebenfalls zentral zu verwalten, wird dem einzelnen Autonomen System eine vereinfachte Validierung von an Adressregistern, wie PKI und DNSSEC, teilnehmenden vertrauenswürdigen Autonomen Systemen ermöglicht. Auch könnten neue momentan nicht realisierbare Sicherheitsmaßnahmen entwickelt und eingesetzt werden. Zudem ist es möglich Sicherheitsmechanismen nur an bestimmten Punkten der Pfade zu implementieren und somit für einzelne Kunden deren Wünsche an Sicherheit an

[7] Monitoring des Netzwerkes
[8] Ankommende Datenpakete werden verworfen

zu passen ohne das gesamte Netz zu beeinflussen, weil nicht sämtlicher Datenverkehr durch die Sicherheitsmechanismen überprüft wird.

Modell 3, Intercloud Routing (4.5), beschäftigt sich mit der Zusammenfassung von mehreren Cloud Providern unter der Führung eines Cloud Brokers. Die Provider behalten dabei ihre Autonomie, werden jedoch durch den Cloud Broker nach außen hin angeboten, welcher sich auch um die Einrichtung der Verbindungen der Provider untereinander kümmert. Durch diese zusätzliche Instanz, welche ebenfalls Sicherheitsmechanismen im Einsatz hat, wie auch die Provider selber, wird die Sicherheit geringfügig verbessert. Auch durch das Tunneln der Verbindung von Providern wird die Sicherheit erhöht. Denn Tunnel sind eine Ende-zu-Ende Verbindung, welche eine Verschlüsselung von Daten für sonst unverschlüsselte Dienste ermöglichen. Somit können auch Provider untereinander ihre Daten verschlüsselt austauschen.

Aus meiner Sicht bietet die Verwendung von SDN-Prinzipien und Techniken eine deutliche Verbesserung der Sicherheit und Performance für Intra- und Inter Domain Routing. Denn wie in den Modellen deutlich wird, ist die Konfiguration weniger aufwendig und somit kann das Netz schneller an aktuelle Bedrohungen angepasst werden. Jedoch ist es wie bereits erwähnt von immenser Bedeutung, den Controller richtig abzusichern. Vor allem bei dem Modell für das Inter Domain Routing durch Outsourcing ist eine deutlich gesteigerte Sicherheit ersichtlich. Dies beruht hauptsächlich auf der größeren Anzahl an auswertbaren Datensätzen zur frühzeitigen Erkennung von Angriffen, jedoch auch durch die Möglichkeit der feineren Abstimmung der Sicherheitsrichtlinien.

# Literaturverzeichnis


[1] http://www.routeviews.org/.

[2] http://www.nanog.org/.

[3] http://www.rehobolab.com/sdn.html

[4] http://www.searchnetworking.de/news/2240223892/Security-Schwachstellen-bei-Software-defined-Networking-SDN

[5] http://www.lanline.de/fachartikel/cisco-bollwerk-gegen-openflow.html

[6] Matthew Caesar, Donald Caldwell, Nick Feamster, Jennifer Rexford, Aman Shaikh, Jacobus van der Merwe. Design and Implementation of a Routing Control Platform. USENIX Association Berkeley, CA, USA 2005.

[7] A. Farrel, J.-P. Vasseur, J. Ash. A Path Computation Element (PCE)-Based Architecture. The Internet Society, VA, USA 2006.

[8] Guy Redmill. An Introduction to SS7. Brooktrout Technology, MA, USA 2001.

[9] J. Van der Merwe, A. Cepleanu, K. D'Souza, B. Freeman, A. Greenberg,D. Knight, R. McMillan, D. Moloney, J. Mulligan, H. Nguyen, M. Nguyen,A. Ramarajan, S. Saad, M. Satterlee, T. Spencer, D. Toll, S. Zelingher. Dynamic Connectivity Management with an Intelligent Route Service Control Point. ACM New York, NY, USA 2006.

[10] Christian E. Rothenberg, Marcelo R. Nascimento, Marcos R. Salvador, Carlos N. A. Corrêa, Sidney C. de Lucena, Robert Raszuk. Revisiting Routing Control Platforms with the Eyes and Muscles of Software-Defined Networking. ACM New York, NY, USA 2012.

[11] Thomas Zinner, Michael Jarschel, Tobias Hossfeld, Phuoc Tran-Gia ,Wolfgang Kellerer. A Compass Through SDN Networks. University of Würzburg, BY, GER 2013.

[12] A. Vidal, F. Verdi, E.L. Fernandes, C.E. Rothenberg, M.R. Salvador. Building upon RouteFlow: a SDN development experience. SBRC - Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, Brasil, 2013.

[13] Hyojoon Kim, Theophilus Benson, Aditya Akella. The Evolution of Network Configuration: A Tale of Two Campuses. ACM New York, NY, USA 2011.

[14] Ali Reza Sharafat, Saurav Das, Guru Parulkar, Nick McKeown. MPLS-TE and MPLS VPNs with OpenFlow. ACM New York, NY, USA 2011.

[15] Saurav Das, Ali Reza Sharafat, Guru Parulkar, Nick McKeown. MPLS with a Simple OPEN Control Plane. Stanford University, CA, USA 2011.

[16] Marouen Mechtri†, Ines Houidi, Wajdi Louati, Djamal Zeghlache. SDN for Inter Cloud Networking. Institut Mines-Telecom, Evry, France 2013.

[17] Vasileios Kotronis, Xenofontas Dimitropoulos, Bernhard Ager. Outsourcing the Routing Control Logic:Better Internet Routing Based on SDN Principles. ETH Zürich, Zürich, Schweiz 2012.

[18] Martin Suchara, Dahai Xu, Robert Doverspike, David Johnson, Jennifer Rexford. Network Architecture for Joint Failure Recovery and Traffic Engineering. ACM New York, NY, USA 2011.

[19] J. Rexford and J. Feigenbaum. Incrementally-Deployable Security for Interdomain Routing. In CATCH '09. IEEE, 2009.

# Kapitel 5

# IT Security Checks für Behörden und Industrie

*Lukas Müller*

*Aufgrund der stetigen technischen Weiterentwicklung und Steigerung der Nutzung von digitalen Diensten und Verfahren bedarf es einer komplexen Absicherung der Informationswerte. Der Aufbau, Erhalt und Schutz der Informationssicherheit ist somit Kernelement für den Fortbestand einer Institution. Neben der Steigerung und dem Erhalt der Effizienz ist die Informationssicherheit außerdem für viele Kunden und Partner ein wichtiges Aushängeschild und damit kooperationsentscheidend. Diese Faktoren spielen nicht nur eine immense Rolle für Industrie und Unternehmen jeglicher Größe sondern auch für staatliche Behörden. Umso wichtiger ist eine verständliche, einfache, sichere und effektive Anwendung der Normen und Gesetze.*

## Inhaltsverzeichnis

## 5.1 Vorwort

Ziel dieser Seminararbeit ist die Einführung in das Thema der Informationssicherheits-Managementsysteme (ISMS) und Cyber-Sicherheits-Checks. Als Grundlage für die Betrachtungen wird zuerst ein Überblick über Normen und Richtlinien gegeben. Im Anschluss daran wird ein sogenannter Cyber-Sicherheits-Check an einem realem Beispiel durchgeführt. Die Tests auf Grundlage der Normen und Richtlinien zu verglichen und ins Verhältnis zu setzen muss auf ein Minimum beschränkt werden, da viele dieser Tests nicht frei zugänglich sind. Der Schwerpunkt der Arbeit liegt in der Bewertung der Effektivität des durchgeführten Tests im Vergleich zur Anwendung der Normen.

Dieser Sachverhalt wird durch das folgende Zitat aus der ISO 27000 unterstrichen.

> „In einer vernetzten Welt stellen Informationen und zugehörige Prozesse, Systeme und Netzwerke entscheidende Wirtschaftsgüter dar. Institutionen und ihre Informationssysteme und Netzwerke sind mit Sicherheitsbedrohungen aus einer Vielfalt von Quellen konfrontiert, einschließlich von computergestütztem Betrug, Spionage, Sabotage, Vandalismus, Feuer und Überschwemmungen. Schäden an Informations-systemen und Netzwerken, die durch Schadcode, Computer-Hacking, und Denial-of-Service-Attacken verursacht werden, sind häufiger, ehrgeiziger und immer raffinierter geworden.
> `[...]`
> Wenn Institutionen die ISMS-Normenfamilie übernehmen, können sie ihre Fähigkeit, einheitliche und gegenseitig erkennbare Prinzipien der Informationssicherheit anzuwenden, Geschäftspartnern und anderen interessierten Dritten unter Beweis stellen.“[1]

Ein ISMS ist demnach heutzutage wichtiger denn je, für jede Größe und Art einer Institution.

Besonderer Dank ist der Firma Muster GmbH, insbesondere Herrn Dipl.-Ing. T. Knorr, auszusprechen. Durch deren Hilfe die Vergleiche an einem bodenständigem, mittelständigem Unternehmen in einen realen Bezug gesetzt werden konnten.

## 5.2 Einleitung

Für Unternehmen und Behörden jeder Größe ist die Sicherstellung ihrer Werte (insbesondere ihrer Informationswerte), für Fortbestand sowie Effektivität, von grundlegender Bedeutung. Durch die Verlagerung von Prozessen in den digitalen Raum wird die Sicherheit der IT-Infrastruktur zum Kernfaktor für Industrie und Behörden.

Um hierzu eine Grundsicherheit (im BSI Grundschutz als akzeptables Sicherheitsniveau einer Institution beschrieben) zu gewährleisten stehen verschiedene Wege offen. Die hierbei theoretische Ebene bilden die Normen und Richtlinien, wie die ISO 27000 Reihe oder das BSI Grundschutz Dokument. Als anwendungsbezogene Ebene stellen verschiedene Unternehmen Tests nach den theoretischen Grundlagen zum Angebot.

Die wichtigsten Eigenschaften einer Institution, die es in diesem Zusammenhang zu schützen und zu sichern gilt, sind:

- das Sammeln, Verarbeiten, Speichern und Übermitteln von Informationen und
- zugehörige Prozesse, Systeme, Netzwerke und Personen, die für die Erreichung ihrer Ziele notwendig sind.

Diese Eigenschaften müssen nicht nur gegen Bedrohungen, wie Angriffe geschützt werden, sondern auch gegen Fehler, Naturereignisse und Schwachstellen. Die zur Verfügung stehenden Informationssicherheits-Maßnahmen müssen dabei bestmöglich im Verhältnis zu den verbundenen Risiken betrachtet werden, um die Effizienz der Institution aufrecht erhalten zu können.
Aufgrund von Bedrohungen, durch die die Werte einer Institution in Gefahr geraten, bedürfen die Werte einem gewissen Schutz.
Da sich die Bedrohungslage und das Risiko ständig ändern können, bedarf es einer ständigen Überwachung und Bewertung der Wirksamkeit der angewendete Maßnahmen und Verfahren. Gegebenenfalls müssen mögliche Informationssicherheits-Risiken neu identifiziert werden und angemessene Maßnahmen implementiert werden.

> „Diese koordinierten Tätigkeiten, die die Umsetzung geeigneter Maßnahmen und die Behandlung von unakzeptablen Informationssicherheits-Risiken steuern, werden allgemein als Bestandteile des Informationssicherheitsmanagement bezeichnet.“[1]

Die damit verbundenen Aufgaben zur Erreichung der Informationssicherheit sollten innerhalb einer Institution durch eigene Leitlinien festgelegt werden.

Dabei ist es wichtig, dass diese durch die Stakeholder bzw. die Geschäftsführung unterstützt und durchgesetzt werden, um die Akzeptanz in allen Geschäftsbereichen zu schaffen.

## 5.3 Normen und Richtlinien für Informations- und IT-Sicherheit

### 5.3.1 ISO 27000 Reihe

Die ISO Normen Reihe 27000 umfasst über 30 Teilgebiete. Im Wesentlichen werden hier Sicherheitsstrategien angesprochen die nicht ausschließlich IT-spezifisch orientiert sind, sondern auf Informationssicherheit jeglicher Art abzielen.
Die Abgrenzung von Informationssicherheit zur reinen IT-Sicherheit wird durch das nachstehende Zitat verdeutlicht.

> „Informationssicherheit hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.“[9]

Im Mittelpunkt der Betrachtung steht in den Teilen, ISO 27001 ... ISO 27007 ein Modell zur Einführung und zum Erhalt eines Informations-Managementsystem (kurz ISMS). Die ISO Teile 27011 ... 27799 befassen sich mit branchenspezifischen Richtlinien. Mithilfe eines ISMS, das die Vorgaben der ISO 27001 erfüllt, kann ein Unternehmen oder eine Behörde, jeglicher Größe, eigene Rahmenbedingungen für die Sicherheit ihrer Informationswerte erstellen und umsetzen. Die dabei selbst entwickelten Leitlinien sind somit genau auf die Institution und deren konkrete Ansprüchen abgestimmt.

Mithilfe eines ISMS wird ein Modell geschaffen zur Einführung, Umsetzung, Betrieb, Überwachung, Überprüfung, Pflege und Verbesserung von Maßnahmen und Richtlinien zum Schutz von Informationswerten.

Die ISMS-Normenfamilie umfasst in Ihren wesentlichen Bestandteilen:

- Anforderungen an ein ISMS und die damit verbundene Zertifizierung;
- direkte und detaillierte Anleitungen und Interpretationen sowohl für die Implementierung eines ISMS als auch für die übergeordnete Plan-Do-Check-Act-Prozesse;
- branchenspezifische Richtlinien;
- Konformitätsprüfungen für ISMS.

Institutionen müssen zur Sicherung ihrer Werte die Informationssicherheits-Risiken und die dazugehörigen implementierten Maßnahmen ständig auf Wirksamkeit überprüfen und ggf. anpassen. Die wichtigsten Merkmale für Informationssicherheit sind hierbei Vertraulichkeit, Verfügbarkeit und Integrität der Informationswerte.
Basis für ein ISMS ist eine Anforderungsanalyse, hierzu sollte eine Risikoeinschätzung (als Teil des Risikomanagements) erfolgen, die auf das Risikoakzeptanzniveau der Institution abgestimmt ist, um weiterhin in der Lage zu sein die Ziele der Institution zu verfolgen und erreichen zu können.
Die Anforderungsanalyse muss, möglichst vollständig, in allen Bereichen einer Institution durchgeführt werden. Dabei sollte der Grundstein, ein Bewusstsein für die Notwendigkeit der Informationssicherheit innerhalb der Institution, geschaffen werden. Hierbei sollte auf die Bedürfnisse, Interessen und Verpflichtungen der Geschäftsführung und Stakeholder eingegangen und diese einbezogen werden.

> „Ohne die Bereitschaft, ohne das Vorleben und ohne das aktive Mitwirken der Geschäftsleitung sowie ohne die Freigabe ausreichender personeller wie zeitlicher Ressourcen ist die Einführung der ISO27001 von Tag 1 an zum Scheitern verurteilt.“[19]

Resultierenden Maßnahmen und Konzepte werden mit Hilfe eines ISMS organisiert. Hierzu sollten relevante Informationssicherheits-Maßnahmen möglichst nahtlos in die Geschäftsprozesse integriert werden.
Aufgrund der Komplexität und der sich ändernden Anforderungen bedarf ein ISMS einer geeigneten Management Struktur, diese kann je nach Größe der Institution von einzelnen Personen bis hin zu Personengruppen zusammengesetzt werden.

Die wichtigsten Schritte auf dem Weg zum ISMS, gegeben und präzise zusammengefasst durch die ISO 27000:

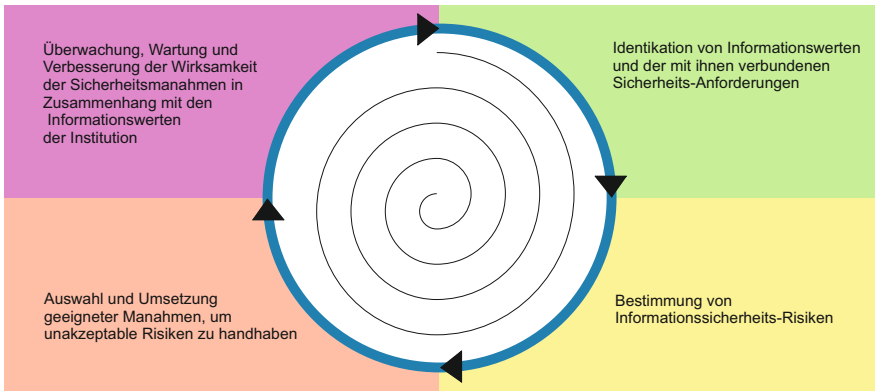


Abbildung 5.1: Schritte zum ISMS nach ISO 27000

Wie auf 5.1 zu sehen ist sind die Schritte jedoch keinesfalls nur einmal zu durchlaufen, sie sind vielmehr als sich wiederholende Arbeitsschritte zu verstehen um die Wirksamkeit eines ISMS sicherzustellen.

Die ISO 27000 gibt ein Beispiel für kritische Erfolgsfaktoren für ein ISMS. Diese Faktoren sollten zur erfolgreichen Implementierung eines ISMS in einer Institution vorhanden und berücksichtigt werden.

> **„a)** eine an die Ziele angepasste Informationssicherheits-Leitlinie, mit Zielsetzungen und Tätigkeiten;
>
> **b)** ein Ansatz und Rahmenwerk für die Planung, Umsetzung, Überwachung, Wartung und Verbesserung der Informationssicherheit in Übereinstimmung mit der Unternehmenskultur;
>
> **c)** erkennbare Unterstützung und Engagement seitens aller Managementebenen, insbesondere der Unternehmensspitze;
>
> **d)** ein Einvernehmen über die Anforderungen an den Schutz von Informationswerten, das durch die Anwendung eines Informationssicherheits-Risikomanagements erzielt wird;
>
> **e)** ein nachhaltiges Bewusstsein für Informationssicherheit, Schulungs- und Fortbildungsprogramme, bei denen alle Mitarbeiter und andere betroffene Parteien über ihre Verpflichtungen im Bereich der Informationssicherheit nach den Leitlinien und Normen zur Informationssicherheit informiert werden und motiviert werden, entsprechend zu handeln;
>
> **f)** ein leistungsfähiger Prozess zur Handhabung von Informationssicherheits-Vorfällen;
>
> **g)** ein leistungsfähiger Ansatz zum Business Continuity-Management; und
>
> **h)** ein Messsystem, das genutzt wird, um die Leistungsfähigkeit des Informationssicherheitsmanagements zu bewerten und Verbesserungsvorschläge zurück zu melden.“[1]

### Aufbau der ISMS-Normenfamilie

**ISO 27001** liefert die wesentlichen Anforderungen an ein ISMS (siehe Abbildung 5.2).
Auf Grundlage dieser Norm kann eine Institution ihre Konformität des ISMS auditieren und zertifizieren lassen. Dazu muss eine Institution die Referenz-Maßnahmenziele und Maßnahmen aus Anhang A der ISO 27001 [2] abdecken, diese beschreiben allgemeine Verwaltungs- und Sicherheitsprozesse eines ISMS, sie geben kaum Aufschluss über die technischen Details um auf Institutionen jeglicher Größe, Typ und Geschäftsfeld angewendet werden zu können.

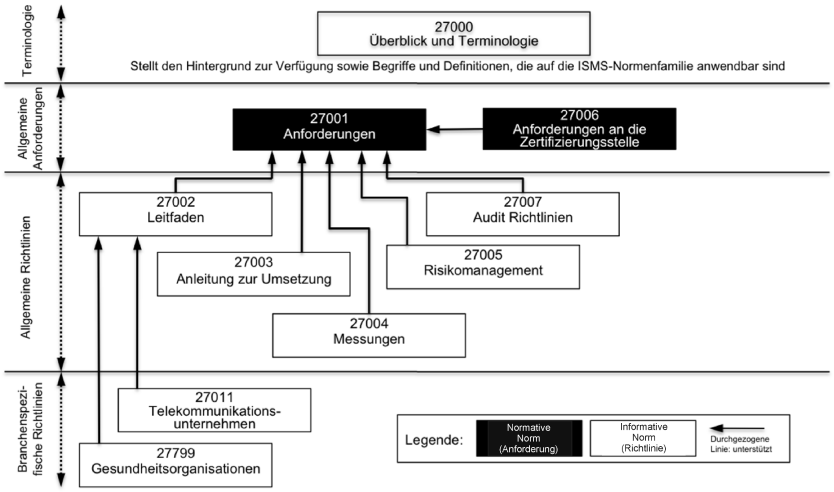


Abbildung 5.2: Übersicht der ISO 27000 Reihe/ ISMS-Normenfamilie [1]

Um die Konformität mit der IEC/ ISO 27001 [2] zu erreichen, müssen die folgenden Punkte (und deren Unterpunkte) innerhalb der Institution geplant, festgelegt, implementiert, beachtet, demonstriert, kontrolliert, ausgewertet und festgehalten werden:

- Kontext der Organisation
- Führung
- Planung
- Unterstützung
- Einsatz
- Leistungsauswertung
- Verbesserung

**ISO 27002** liefert mögliche Maßnahmen um Risiken zu handhaben, sie sind leicht auf die Größe und Komplexität verschiedener Institution anpassbar (siehe Abbildung 5.2). Sie enthält 14 Abschnitte über Sicherheitsmaßnahmen mit 35 Hauptkategorien der Sicherheit und 113 Sicherheitsmaßnahmen

Die dabei aufgelisteten Sicherheitsmaßnahmen (mit Hauptkategorien):

- Sicherheitsleitlinien (Managementausrichtung zur Informationssicherheit)
- Organisation der Informationssicherheit (Interne Organisation, Mobilgeräte und Telearbeit)

- Personalsicherheit (Vor der Anstellung, Während der Anstellung, Beendigung und Wechsel der Anstellung)
- Management von organisationseigenen Werten (Verantwortung für organisationseigene Werte, Klassifizierung von Informationen, Handhabung von Speicher- und Aufzeichnungsmedien)
- Zugriffskontrolle (Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle, Benutzerverwaltung, Benutzerverantwortung, Kontrolle des Zugangs zu Systemen und Anwendungen)
- Kryptographie (Kryptographische Maßnahmen)
- Schutz vor physischem Zugang und Umwelteinflüssen (Sicherheitsbereiche, Sicherheit von Betriebsmitteln)
- Betriebssicherheit (Betriebsverfahren und Zuständigkeiten, Schutz vor Malware, Backup, Protokollierung und Überwachung, Kontrolle von Betriebssoftware, Technisches Schwachstellenmanagement, Auswirkungen von Audits auf Informationssysteme)
- Sicherheit in der Kommunikation (Netzwerksicherheitsmanagement, Informationsübertragung)
- Anschaffung, Entwicklung und Instandhaltung von Systemen (Sicherheitsanforderungen für Informationssysteme, Sicherheit in Entwicklungs- und Unterstützungsprozessen, Prüfdaten)
- Lieferantenbeziehungen (Informationssicherheit bei Lieferantenbeziehungen, Management der Dienstleistungserbringung durch Lieferanten)
- Management von Informationssicherheitsvorfällen (Management von Informationssicherheitsvorfällen und Verbesserungen)
- Informationssicherheitsaspekte des Betriebskontinuitätsmanagements (Aufrechterhaltung der Informationssicherheit, Redundanzen)
- Richtlinienkonformität(Einhaltung gesetzlicher und vertraglicher Anforderungen, Informationssicherheitsprüfungen)

Kosten und Aufwendungen zur Implementierung der verschiedenen Sicherheitsmaßnahmen müssen gegen die Kosten beim Eintreten von Sicherheitsproblemen oder -vorfällen betrachtet werden. Diese Risikobewertung hilft dabei geeignete Maßnahmen zu identifizieren und zu priorisieren um ausgewählte Sicherheitsmaßnahmen zu implementieren.

**Folgende Normen-Teile**
Die darauf folgenden Normen-Teile (siehe Abbildung 5.2) bauen im wesentlichen auf die ISO 27001 und 27002 auf und spezifizieren diese. Hierbei werden Vorgehensweisen detailliert aufgeführt und beschrieben.

### 5.3.2 BSI IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt ein Grundschutz Dokument zur Verfügung mit dessen Hilfe Institutionen eine Basis für Informationssicherheit schaffen können. Das Hauptaugenmerk des BSI IT-Grundschutz liegt in der Erhöhung der IT-Sicherheit für alle Anwender. Hierzu stellt das BSI verschiedene Mittel zur Verfügung, als erstes sollten hier die BSI-Standards erwähnt werden. Ein weiteres wichtiges Hilfsmittel sind die IT-Grundschutz-Kataloge.

#### BSI-Standards

Die Optimierung des Sicherheitsmanagements und Einführung eines ISMS, kann oftmals die Informationssicherheit effektiver und nachhaltiger verbessern als Investition in Sicherheitstechnik. Außerdem haben einige, dadurch eingeführte, Änderungen auch einen positiven Effekt auf andere Arbeitsbereiche. Die damit die Nachhaltigkeit steigert und somit die gesamte Produktivität der Institution. Dies wird besonders im BSI-Standard 100-1 hervorgehoben.

> „Als positive Nebeneffekte sind eine höhere Arbeitsqualität, Steigerung des Kundenvertrauens, Optimierung der IT-Landschaft und organisatorischer Abläufe sowie die Nutzung von Synergieeffekten durch bessere Integration des Informationssicherheitsmanagements in bestehende Strukturen zu erwarten.“[9]

Der Grundstein für Sicherheit liegt in der systematischen Herangehensweise an die Problematik und erst in zweiter Gewichtung an technischen Maßnahmen.
Die BSI-Standards richten sich in erster Linie an alle die Verantwortung im Bereich IT übernehmen, somit mit der Informationssicherheit/ IT-Sicherheit einer Institution betraut sind.
Das BSI bietet die Möglichkeit Institutionen nach Ihren Standards zu Zertifizieren, diese beinhaltet dabei immer eine offizielle ISO-Zertifizierung nach ISO 27001. Die BSI-Standards helfen den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrund-Informationen und Beispielen, und geben so mehr Details als die ISO Normen.

Im folgenden werden die BSI-Standards 100-1 und 100-2, die für die Thematik der ISMS besonders wichtig sind angesprochen und ein minimaler Abriss derer gegeben. Auf die darüber hinaus existieren BSI-Standards 100-3 (Risikoanalyse auf der Basis von IT-Grundschutz) und 100-4 (Notfallmanagement),entfällt eine genauere Betrachtung aufgrund der zu großen Spezialisierung ,siehe Abbildung 5.3.

**BSI-Standard 100-1** beschreibt im wesentlichen die Planung, Entwicklung, Überwachung, Verbesserung und den Erhalt eines ISMS. Hierbei wird Schritt für Schritt in den wichtigsten Punkten beschrieben wie dies erreicht wird.
Der Standard des BSI ist vollständig kompatibel zur IEC/ ISO 27001, er wurde erstellt, um einige Teilgebiete der Norm näher betrachten zu können.

**BSI-Standard 100-2** beschreibt die Vorgehensweise um möglichst effizient ein gutes Sicherheitsniveau mit Hilfe eines ISMS und der IT-Grundschutz-Kataloge zu erreichen. Hierzu werden, im Gegensatz zu den ISO Normen, sehr konkrete Hinweise, Beispiele und Hintergrund-Informationen für eine Umsetzung gegeben.
Durch die Beachtung der Vorgaben kann ein angemessenes und ausreichendes Sicherheitsniveau für "den normalen Schutzbedarfërreicht werden.
Der BSI-Standard 100-2 gibt zum Beispiel genaueren Aufschluss über die Organisation des Sicherheitskonzeptes als die ISO Normen, dies wird besonders deutlich im Aufgabenfeld für einen möglichen Verantwortlichen für Informationssicherheit, die trefflichsten Bezeichnungen für diese Position sind Chief Security Officer (CSO) oder Chief Information Security Officer (CISO) im Gegensatz zu IT-Sicherheitsbeauftragter. Im Standard werden für viele relevanten Positionen, Personen und Teams Aufgaben, Anforderungen, Zuständigkeiten und weitere Eigenschaften genau beschrieben.

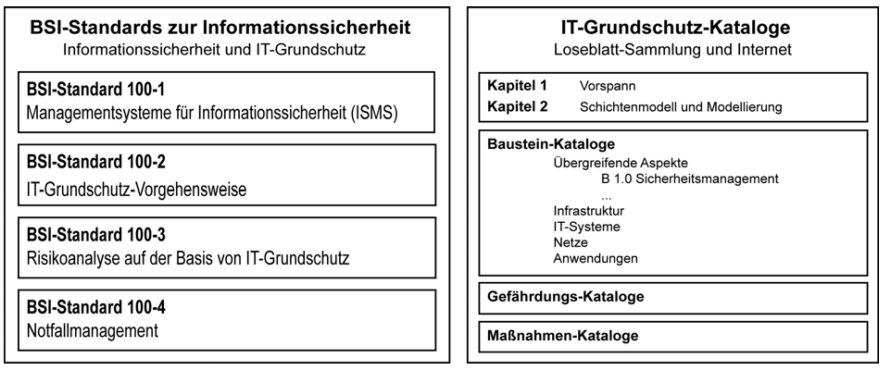


Abbildung 5.3: Übersicht über BSI-Publikationen zum Sicherheitsmanagement [9]

### IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge geben konkrete technische Maßnahmen zur praktischen Implementierung des ISMS und zum Aufbau eines angemessenen Sicherheitsniveaus an. Ihre Bausteine sind modular aufgebaut.
Zielsetzung des IT-Grundschutz ist die Reduzierung des Aufwandes im Informationssicherheitsprozess, dies wird durch Bündelung und Wiederverwendung von Vorgehensweisen zur Verbesserung der Informationssicher-

heit erreicht. IT-Grundschutz-Kataloge geben Standard-Gefährdungen und -Sicherheitsmaßnahmen für viele reale und häufig auftretende Problematiken an, um so Sicherheitskonzepte möglichst effizient erstellen und prüfen zu können.
Die Kataloge werden fortwährend an den Stand der Technik angepasst und sind somit aktueller als die BSI-Standards, die derzeit aktuelle Version der BSI-Standards ist von 2008 und im Vergleich dazu die Kataloge von 2013.
Der Aufbau der Kataloge beruht auf der gründlichen Betrachtung und Auswertung der folgenden Bausteine, die in fünf Schichten gegliedert sind (5.4) und auf ca. 4000 Seiten näher beschrieben werden.

Bausteine nach IT-Grundschutz-Katalog:

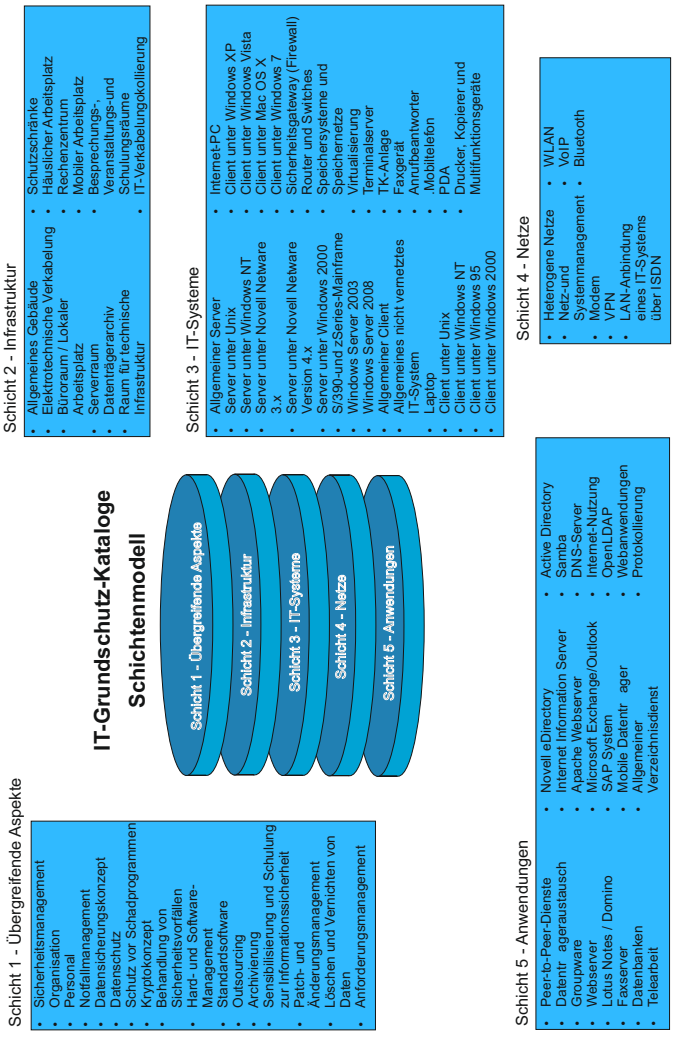


Abbildung 5.4: IT-Grundschutz-Katalog - Schichtenmodell

Neben den Baustein (-katalogen) werden in den IT-Grundschutz-Katalogen noch die Gefährdungskataloge und die Maßnahmenkataloge angegeben, die einen Großteil des Dokumentes ausmachen, siehe Abbildung 5.3.
Die Gefährdungskataloge geben Aufschluss über mögliche Gefährdungen für eine Institution, die hier beschriebenen Sachverhalte sind sehr umfassend und

reichen von Naturkatastrophen bis zu Sabotage. Die Maßnahmenkataloge geben beispielhaft Maßnahmen zur Kompensierung der Gefährdungen, auch hier wird sehr Umfangreich und detailliert beschrieben, von Infrastruktur-Maßnahmen bis Notfallvorsorge.

Zur Einführung und zum Betrieb eines ISMS ist die Umsetzung des BSI-Standard 100-2 und die Grundschutz-Kataloge hilfreich, Sie geben klaren und genauen Aufschluss über mögliche Maßnahmen und Planung.
Aufgrund des enormen Umfanges der Dokumente des BSI ist eine Einarbeitung hier viel Aufwendiger als die Einarbeitung in die ISO Normen. Die Beispiele und weiteren Ausführungen des BSI sind zwar anschaulich, jedoch für eine gute IT-Abteilung nichts neues und erhöhen damit den Einarbeitungs- und Bearbeitungsaufwand in nicht angemessener und nicht wirtschaftlicher Weise.

Aus SZuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz"[12] und "Vergleich von ISO/IEC 27033-1 und IT-Grundschutz"[13] geht auch hervor das die weiterführenden Teile der Normen durch die BSI Dokumente nahezu vollständig abgedeckt werden.

**ISO 27000 und 27001 vs. BSI-Standard 100-1** Aufgrund der Tatsache das der BSI-Standard in der Version 2008 aktuell ist, und die ISO Normen in der Version von 2013 (2014), kann es sein, das die Änderungen in den Normen Teilen gravierend sind, die Normen nun auch Anwender freundlicher, gegenüber dem Zustand von 2008, geworden sind.
Bei den BSI-Standards wurde versucht eine einfachere Formulierung und Betrachtungsweise zu schaffen, dadurch wurde leider die Übersichtlichkeit und Kompaktheit gegenüber der ISO Normen etwas in Mitleidenschaft gezogen. Ich konnte keine größere oder bessere Anwenderfreundlichkeit in dem BSI-Standards gegenüber der Normen feststellen, im Gegenteil, die Normen weisen sogar eine höhere Informationsdichte auf. Außerdem benutzt der BSI-Standards bestimmte Terminologien schwammig und ungenauer als die ISO Normen.

### 5.3.3 Framework for Improving Critical Infrastructure Cybersecurity

Aufgrund der großen Relevanz der Cybersecurity in behördlichen wie auch wirtschaftlichen Sektoren hat der Präsident der Vereinigten Staaten von Amerika zur Verdeutlichung die Executive Order 13636 Improving Critical Infrastructure Cybersecurityim Februar 2013 erlassen.
Im Februar 2014 wurde daraufhin das "Framework for Improving Critical Infrastructure Cybersecurity"[14] veröffentlicht.

Das Cybersecurity Framework besteht aus drei Teilen, dem Framework Core, Framework Profile und den Framework Implementation Tiers.

> „The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.“[14]

Das Framework ist ähnlich wie der BSI Grundschutz auf verschiedene Größen von Institutionen skalierbar und anpassbar an die besonderen Bedürfnisse einer speziellen Institution, die gesamte Problematik wird in einfacher Sprache beschrieben. Es wird ein relativ großer Spielraum zur Identifizierung, Planung und Umsetzung von geeigneten Maßnahmen und Organisationsstrukturen gegeben. Die Anwendung des Framework ist für Unternehmen freiwillig und soll deren Anfälligkeit gegenüber Cybersecurity Risiken möglichst kosteneffektiv verkleinern.
Die im Framework angesprochenen Methoden und Vorgehensweisen beziehen sich auf existierende Standards, wie die ISO 27000 Reihe, Control Objectives for Information and Related Technology (COBIT) oder ANSI/ISA-62443.

**Der Framework Core** spricht fünf Funktionen an, diese ist die Einteilung mit der geringsten Spezialisierung:

- **Identify** - Eigenschaften und Prozesse die es zu identifizieren gilt und deren Notwendigkeit es zu verbreiten gilt
- **Protect** - Erstellen und Implementieren von angemessenen Maßnahmen für Werte die es zu schützen gilt

- **Detect** - Erstellen und Implementieren von angemessenen Maßnahmen für Fehler und Gefahren die es zu identifizieren gilt
- **Respond** - Erstellen und Implementieren von angemessenen Maßnahmen für Vorkommnisse/ Ëventsäuf die es zu handeln gilt
- **Recover** - Erstellen und Implementieren von angemessenen Maßnahmen zum Umgang während und nach einem Ëvent"die es anzuwenden, zu verbessern und zu bewerten gilt.

Ein Event bezeichnet ein Ereignis der Cybersecurity das möglicherweise Auswirkungen auf die Tätigkeiten einer Institution hat, sowie Auswirkungen auf das Öffentlichkeitsansehen der Institution.

Die oben angesprochenen Funktionen werden weiter in Kategorien eingeteilt, sie sind Gruppen ähnlichen Charakters, die eine Betrachtung bezüglich Cybersecurity benötigen. Jede Kategorie wird in Unterkategorien eingeteilt in der technische oder organisatorische Maßnahmen angesprochen werden und mit anderen gültigen und gängigen Standards referenziert werden. Es werden jedoch keine Beispiele oder Hilfen zur Implementierung im Cybersecurity Framework gegeben.

**Die Framework Implementation Tiers** schaffen einen Überblick zur Einordnung einer Organisation hinsichtlich Cybersecurity:

- **Tier 1: Partial** - keine Formalisierung und feste Richtlinien einer Organisation bezüglich Cybersecurity
- **Tier 2: Risk Informed** - Notwendigkeit von der Leitungsebene der Organisation anerkannt, nicht flächendeckend innerhalb der Organisation angewendet
- **Tier 3: Repeatable** - Maßnahmen zur Cybersecurity und zum dazugehörigen Risikomanagement sind formell vorhanden und werden angewendet.
- **Tier 4: Adaptive** - Maßnahmen zur Cybersecurity und zum dazugehörigen Risikomanagement werden zusätzlich überwacht, angepasst und verbessert

**Die Framework Profile** geben Organisationen eine Möglichkeit um Ihre Ziele, der Cybersecurity, möglichst effektiv zu erreichen und zu vergleichen. Die Framework Profile können auch dazu verwendet werden, um den Ist-Zustand oder den angestrebten Zustand für Cybersecurity zu beschreiben.

Aufgrund der Größe und Komplexität vieler Organisationen können verschiedene Profile für unterschiedliche Komponenten und individuelle Bedürfnisse erstellt werden.

**Einführung oder Verbesserung der Cybersecurity** beschreibt Schritte einer Organisation zur Anwendung des Framework, um ein Cybersecurity Programm einzuführen oder ein bestehendes zu verbessern.

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan

Das "Framework for Improving Critical Infrastructure Cybersecurity"baut im wesentlichen auf die Normen Reihe ISO 27000 auf, es ist ähnlich wie vom BSI Grundschutz auf eine einfache und effektive Implementierung ausgelegt. Aufgrund der fehlenden Beispiele und konkreten Maßnahmen ist es nicht direkt anwendbar, diese müssen erst selbst identifiziert, bewertet und ausgewählt werden.
Im Framework werden nur IT-Spezifische Themen angesprochen, das Ziel der Informationssicherheit wie sie ein ISMS zu schaffen versucht kann somit nicht in gleichem Umfang wie durch Anwendung der ISO 27000 Reihe oder des BSI Grundschutz erreicht werden.

## 5.4 Test und Checks

### Angebot verschiedener Tests

Auf dem freien Markt ist eine große Vielfalt an verschiedenen Tests anzutreffen, hierzu gehören zum Beispiel:

- Allianz für Cybersicherheit - Leitfaden für Cybersicherheit
- Microsoft Security Health Check

Weitere Anbieter von Cybersecurity Checks sind zum Beispiel:

- IABG
- DESAG
- procilon.de (i-doit Test)
- mgn-computing.de
- securepoint.de

Diese Tests werden meist durch unabhängige Unternehmen durchgeführt, die Bewertung der Cybersicherheit geschieht meist durch einen Vertreter des anbietenden Unternehmens im Hause des Auftraggebers. Aufgrund der umfangreichen und vielseitigen einzusehenden Dokumente, Tests und Maßnahmen dauert eine solche Überprüfung meist mehrere Tage bis mehrere Wochen und ist damit sehr kostenintensiv.

**Leitfaden für Cybersicherheit** der Allianz für Cybersicherheit (Initiative des BSI, ISACA (Information Systems Audit and Control Association) Germany Chapter e.V. und Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)) bietet eine kostenlose Möglichkeit einen grundlegenden Sicherheitstest mit qualifiziertem eigenem Personal durchzuführen.
Darüber hinaus existiert auch ein Angebot einer offiziellen Bewertung durch externe Bewerter.
Cyber-Sicherheits-Checks können auch angewendet werden, wenn kein vollständiges ISMS oder abgeschlossener Sicherheitsprozess vorhanden ist und bieten somit eine einfache Möglichkeit die eigene IT-Sicherheit zu testen.

Die zu beurteilenden Eigenschaften der Sicherheit bei einem Cyber-Sicherheits-Checks der Allianz für Cybersicherheit:

- Absicherung von Netzübergängen
- Abwehr von Schadprogrammen
- Inventarisierung der IT-Systeme
- Vermeidung von offenen Sicherheitslücken
- Sichere Interaktion mit dem Internet
- Logdatenerfassung und –auswertung
- Sicherstellung eines aktuellen Informationsstands
- Bewältigung von Sicherheitsvorfällen
- Sichere Authentisierung
- Gewährleistung der Verfügbarkeit notwendiger Ressourcen
- Durchführung nutzerorientierter Maßnahmen
- Sichere Nutzung Sozialer Netzwerke
- Durchführung von Penetrationstests

Diese Maßnahmen werden noch einmal in Basismaßnahmen spezialisiert und unterteilt, eine genauere Beschreibung findet sich im Dokument "Basismaßnahmen der Cyber-Sicherheit"[16].
Die Betrachtung erfolgt immer in Unterteilung in die drei Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität, diese bildet die Cyber-Sicherheits-Exposition.
Cyber-Sicherheits-Checks der Allianz für Cybersicherheit betrachtet damit nur IT-Sicherheitsfaktoren, allerdings weist diese Betrachtung auch einige Lücken in diesem Bereich auf (siehe 5.5).

### Zertifizierung

Darüber hinaus besteht natürlich die Möglichkeit der offiziellen Zertifizierung nach ISO 27001 durch eine unabhängige Zertifizierungsstelle oder der Zertifizierung nach BSI Grundschutz (enthält ein ISO 27001 Zertifikat).
Ein richtig implementiertes ISMS bietet ausreichend Schutz gegen Cyberangriffe und andere Gefahren, es werden neben den IT spezifischen Sicherheitsvorkehrungen auch die allgemeineren und gesamt betrachtet wichtigeren Informationssicherheitsmaßnahmen beachtet. Es kann mit Hilfe der richtigen Dokumentation und wenig Aufwand auch als Cyber Security Check angesehen werden.
Der Cyber-Sicherheits-Check der Allianz für Cyber-Sicherheit beschreibt, im Bezug zu den Informationssicherheitsmaßnahmen, folgendes:

> „Nicht relevant sind alle Aspekte, die physischen Zugang zu IT Systemen betreffen bzw. Aspekte, die sich mit der physischen Sicherheit (Brandschutz, Einbruchsschutz etc.) beschäftigen.“[15]

Somit ist auch hier gezeigt das eine Zertifizierung nach ISO 27001 oder BSI Grundschutz mehr erfasst und mehr beurteilt als ein einfacher Cyber-Sicherheits-Check.

### Umfang im Vergleich

Die angesprochenen Tests sind, bis auf den Cyber-Sicherheits-Checks der Allianz für Cybersicherheit nicht frei zugänglich. Deshalb muss eine genauere Betrachtung und direkte Gegenüberstellung entfallen.

### Einhalten der Normen und Vollständigkeit der Tests

Fast alle Anbieter beziehen sich bei Ihren Tests auf die ISO 27001 oder zusätzlich andere Teilen der ISO 27000 Reihe, somit ist auch anzunehmen das diese eingehalten werden.
Aufgrund des nichtöffentlichen Zuganges zu den Tests, ist eine Bewertung hinsichtlich Umfang und Vollständigkeit zur ISO 27000 und 27001 nicht in vollem Umfang möglich.
Der Cyber-Sicherheits-Check der Allianz für Cybersicherheit erfüllt viele Kriterien der ISO 27001, da er allerdings nur auf IT-Sicherheit ausgelegt ist, wie die meisten Cyber-Security-Checks, nicht auf vollständige Informationssicherheit in allen Facetten, ist der Umfang kleiner als der der ISO 27001.
Nichts desto trotz bietet er die Möglichkeit mit relativ wenig Aufwand die rudimentäre Basis für IT-Sicherheit zu überprüfen und Schwachstellen aufzuzeigen (siehe 5.8.2).

## 5.5 Durchführung eines Cyber Security Checks

Im Verlauf dieser Seminararbeit wurde der Leitfaden-Cyber-Sicherheits-Check auf die Muster GmbH angewendet.

Dazu wurde zuerst eine Cyber-Sicherheits-Exposition durchgeführt, dabei wurden die Werte für Vertraulichkeit (sehr hoch), Verfügbarkeit (hoch) und Integrität (sehr hoch) ermittelt.
Die Einstufung "sehr Hoch" für Vertraulichkeit und Integrität kommen aufgrund der hohen Spezialisierung, der enormen Entwicklungsarbeit und dem damit verbundenen Geheimhaltungsgrad zustande. Der Wert "hoch" im Bereich Verfügbarkeit basiert auf der bereits erfolgreichen Abwehr von Angriffen.
Positiv kommt hinzu, dass die Transparenz "gering" eingestuft werden kann.
Im Anhang A (5.8.1) befindet sich die erstellte Cyber-Sicherheits-Exposition.

Auf Grundlage dieser Cyber-Sicherheits-Exposition wurden die Maßnahmen und dazugehörigen Basismaßnahmen für die IT-Landschaft bei der Muster GmbH bewertet (gemäß [15] und [16]).
Um dem Leitfaden Cyber-Sicherheits-Check [15] gerecht zu werden wurde die beschriebene Vorgehensweise zur Durchführung eines Cyber-Sicherheits-Checks sinngemäß eingehalten und mit einem Beurteilungsbericht abgeschlossen (5.8.2).

Trotz der Tatsche das bei diesem Cyber-Sicherheits-Check SSchwerwiegende Sicherheitsmängel"festgestellt wurden, sind die wichtigsten technischen Maßnahmen für Cyber-Sicherheit implementiert.
Die Mängel bezogen sich hauptsächlich auf das Fehlen zielgruppenorientierter, regelmäßiger Sensibilisierung für die Gefahren eines Cyber- Angriffs oder Schulung hinsichtlich des korrekten Verhaltens für alle Mitarbeiter und das Fehlen von verbindlichen Vorgaben (Social Media Guidelines) für Soziale Netzwerke.
Diese Mängel stellen grundsätzlich eine Gefahr für das Unternehmen dar, können allerdings innerhalb kurzer Zeit mittels geeigneten Leitlinien abgestellt werden.

Darüber hinaus konnten weitere kleinere "Mängel"gefunden werden (beziehungsweise sind diese bereits bekannt gewesen) die durch den Cyber-Sicherheits-Check der Allianz für Cyber-Sicherheit nicht abgedeckt werden. Diese Mängel fallen jedoch nicht ausschließlich unter den Bereich der (nicht betrachteten) Informationssicherheit sondern Teilweise auch in den Bereich der IT-Sicherheit.

Im Zusammenhang mit der IT-Sicherheit werden keine Maßnahmen für Endgerät Richtlinien insbesondere für MULTI USB Devices (Erkennung von bestimmten USB Geräten, je nach USB-ID zum Beispiel Freischaltung nur für Massenspeichermedien) vorgeschrieben. Des weiteren werden nicht direkt Maßnahmen zu Network Access Control wie der IEEE 802.1X Standard oder MAC Filterung angesprochen, auch eine Festplattenverschlüsselung oder "Remote-Löschfunkton"für besonders diebstahlgefährdete Geräte wie Laptops von Außendienst Mitarbeitern wird nicht gefordert.
Zu den nicht betrachteten Punkten bezüglich Informationssicherheit im Cyber-Sicherheits-Check zählt zum Beispiel, dass keine Regelungen und Maßnahmen bezüglich Richtlinien für BYOD (Bring Your Own Device)-Policy und generell mitgebrachten Geräten gefordert werden.

Dies verdeutlicht noch einmal die Tatsache dass der Cyber-Sicherheits-Check nur IT-Sicherheit prüft und nicht die Informationssicherheit und dabei nur die rudimentäre Basis für IT-Sicherheit.

## 5.6 Anwendung auf die Industrie

Durch Kapitel 5.5 konnte festgestellt und gezeigt werden, dass der Cyber-Sicherheits-Check der Allianz für Cyber-Sicherheit für eine gut funktionierende IT-Abteilung keine größere Hürde darstellt und selbst schwerwiegende Mängel innerhalb kurzer Zeit abgestellt werden können.

Da der Umfang äbgespecktërscheint und der geringe Umfang nachgewiesen wurde (siehe 5.5) wäre eine genauere Orientierung an der ISO 27001 oder am BSI Grundschutz hilfreich. Denn nur dadurch kann eine genaue und flächendeckende Beurteilung der Informationssicherheit erfolgen.

Um die Bedeutung der ISO 27001 zu verdeutlichen wurden die Maßnahmenziele und Maßnahmen aus Anhang A der ISO 27001 auf die Muster GmbH angewendet. Die Aufstellung befindet sich in Anhang C (5.8.3), auf weitere Ausführungen und Begründungen der Bewertung und Einstufung wird aufgrund von Datenschutzrechtlichen Gründen verzichtet.
Hierdurch kann gezeigt werden, dass der Umfang der ISO 27001, wie erwartet, (fast) vollständig alle Teilgebiete für Informationssicherheit abdeckt.
Die festgestellten Mängel können weitestgehend auf organisatorische Gründe und Entscheidungen des Management zurückgeführt werden. In den meisten Teilgebieten der IT-Sicherheit werden schon zur Zeit instinktiv die richtigen Entscheidungen bezüglich der ISMS Vorgaben getroffen, jedoch sind diese meist nicht schriftlich vom Management der Geschäftsführung angeordnet und können so nicht effektiv allen Mitarbeitern verpflichtend vorgeschrieben werden. Im Bereich der Informationssicherheit bedürfen die Vorgaben und Leitlinien durch die Führungsebene noch einiges mehr an Reglementierung um auch hier auf sehr hohem Niveau agieren zu können.
Ein möglicher Versuch diese Mängel abzustellen würde in erster Konsequenz darin bestehen die vorhandenen Richtlinien in adäquate Leitlinien umzuwandeln, zu erweitern und zu pflegen. Aufgrund der Tragweite und dem Arbeitsaufwand derartiger Entscheidungen könnte ein geeignetes Projektteam zur Implementierung und Pflege eines ISMS in den Geschäftsalltag von der Muster GmbH integriert werden.

Die Überprüfung auf die Maßnahmenziele und Maßnahmen aus Anhang A der ISO 27001 ist nur geringfügig aufwendiger wie die Anwendung des Cyber-Sicherheits-Check der Allianz für Cyber-Sicherheit und bietet dafür eine weitaus größere Aussagefähigkeit für die IT-Sicherheit und besonders für die Informationssicherheit.
Diese Aussage wurde auch von der Muster GmbH bestätigt, der große Umfang und die Vielfältigkeit der in der ISO Norm 27001 angesprochenen Punkte macht diese zur idealen Grundlage für einen eigenen Cyber-Sicherheits-Check.

## 5.7 Zusammenfassung und Folgerungen

Vorteil der Realisierung eines ISMS liegt neben der Senkung von Informationssicherheits-Risiken, bzw. deren Wahrscheinlichkeit und Auswirkungen, vor allem im genauen Auseinandersetzen mit der Thematik. Dadurch wird die Akzeptanz der Leitlinien sowie das Vertrauen von Partnern stark erhöht und gleichzeitig eine akzeptable Grundvoraussetzungen für Cyber-Sicherheit geschaffen.

Um eine Grundlage für Cyber-Sicherheit zu schaffen müssen alle Beteiligten an einem Strang ziehen, ein kritisches Problem kann zum Beispiel entstehen, wenn sich Geschäftsführung oder Stakeholder nicht ausreichend über die Risiken der Informationssicherheit klar sind.

> „Ein erfolgreiches Informationssicherheits-Managementsystem erfordert die Mitarbeit aller Mitarbeiter einer Organisation.“[3]

Die unabdingbare Notwendigkeit jeder Institution, sich in der heutigen Zeit, mit der Thematik der Informationssicherheit (Cyber-Sicherheit) in angemessener Weise auseinanderzusetzen muss jedem Mitglied der Leitungsebene, jedem Arbeitnehmer/ Mitarbeiter, jedem User und jedem Partner klar sein. Das dafür notwendige Verständnis muss gefördert, aktualisiert und erhöht werden.
Cyber-Sicherheit ist und wird es immer bleiben, ein kritischer Erfolgsfaktor für eine Institution.

> „Die trotzdem in vielen Unternehmen immer noch verbreitete Einstellung „Bisher ist ja auch nichts passiert“ kann daher schnell zu ernsthaften Problemen führen.“[15]

Darüber hinaus ist jedoch zu beachten das eine 100 %-ige Absicherung für Informationen und insbesondere auch für IT, nicht erreicht werden kann.
Das Problem ist wie ein Grenzwertproblem zu betrachten, man kann sich an die völlige Sicherheit herantasten, wird Sie jedoch nie erreichen. Interessant ist dabei auch, dass ab einem gewissen Punkt die Änderungen bezüglich steigender Sicherheit so marginal sind das Sie auf keinen Fall im Verhältnis zu den verursachten Kosten stehen.
Ab einem gewissen Punkt haben die zusätzlichen Kosten sogar kaum noch Effekt auf die Sicherheit.
Dies wird auch durch die Grafik (5.5) verdeutlicht.

Ich empfehle zur theoretischen Verdeutlichung und Einarbeitung, in die Thematik der Cyber-Sicherheit im Hinblick auf ein ISMS, die Anwendung der ISO Normen 27000 Reihe gegenüber den BSI-Standards. Allerdings können zur Umsetzung, der BSI-Standard 100-2 und die Grundschutz-Kataloge,

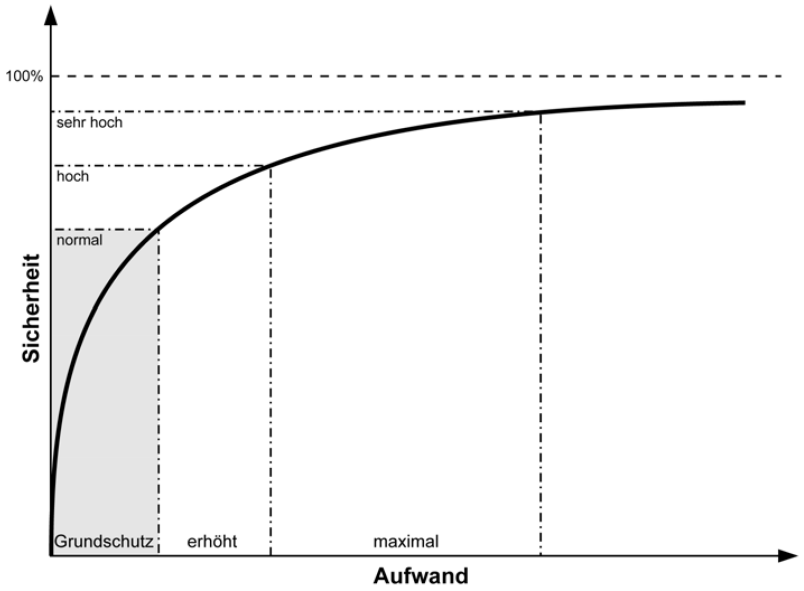


Abbildung 5.5: Aufwand-Nutzen-Relation für Informationssicherheit [10]

sehr hilfreich sein.

Die Implementierung eines ISMS wird einer Institution nicht ”von Heute auf Morgen”gelingen, der Weg zur Informationssicherheit muss wohl geplant und langfristig gesehen werden. Ein ISMS sollte den laufenden Prozess nicht negativ Beeinflussen oder verlangsamen. In erster Linie gilt der Grundsatz je größer das Risiko und dessen Auswirkungen desto schneller und intensiver muss man sich mit dem Problem auseinandersetzen.

## 5.8 Anhang

### 5.8.1 Anhang A - Cyber-Sicherheits-Exposition

Cyber-Sicherheits-Exposition nach dem Cyber-Sicherheits-Checks der Allianz für Cybersicherheit angewendet auf die Muster GmbH, siehe [15]und [17].

Cyber-Sicherheits-Exposition

| Kriterium | Vertraulichkeit | Verfügbarkeit | Integrität |
|---|---|---|---|
| Wert der Daten und Prozesse | 4 | 1 | 4 |
| | der Daten ist sehr hoch einzustufen ,da Forschung betrieben wird, Geheim eingestufte Dokumente von Kooperationspartner verwendet werden und Informationen verarbeitet werden die der Staatlichen Kontrolle unterliegen | ist normal, da bei einem Ausfall wichtiger Prozesse die Arbeit nicht vollständig zum erliegen kommen kann | der Daten ist sehr hoch einzustufen ,da Forschung betrieben wird, Geheim eingestufte Dokumente von Kooperationspartner verwendet werden und Informationen verarbeitet werden die der Staatlichen Kontrolle unterliegen |
| Attraktivität für Angreifer | 4 | 1 | 4 |
| | ist Aufgrund der hohen Spezialisierung, Sicherheitseinstufung und damit verbundenem Wert sehr hoch | für Angreifer "normal" interessant da wenig monetärer Schaden verursacht werden kann | ist Aufgrund der hohen Spezialisierung, Sicherheitseinstufung und damit verbundenem Wert sehr hoch |
| Art der Angreifer | 5 | 2 | 5 |
| | Interesse staatl. Akteure | Aufgrund des geringen mögl Schadens maximal durch Kleinkriminelle ausgenutzt | Interesse staatl. Akteure |
| Zielgerichtetheit des Angriffs | 5 | 1 | 5 |
| | gezielter Angriff denkbar | nur Flächenangriff denkbar da gezielter Angriff zu wenig Nutzen hätte | gezielter Angriff denkbar |
| Angriffe in der Vergangenheit | 1 | 3 | 1 |
| | keine direkten Angriffe bekannt | versuchter Angriff erfolgreich abgewehrt | keine direkten Angriffe bekannt |
| Transparenz | -1 | -1 | -1 |
| | Tranzparenz für möglichen Angreifer gering gehalten, keine Informationen die relevant sind sind verfügbar | | |

| Cyber-Sicherheits-Exposition | Vertraulichkeit | Verfügbarkeit | Integrität |
|---|---|---|---|
| | 4 | 2 | 4 |
| | sehr hoch | hoch | sehr hoch |

### 5.8.2 Anhang B - Beurteilungsbericht

Beurteilungsbericht nach dem Cyber-Sicherheits-Checks der Allianz für Cybersicherheit angewendet auf die Muster GmbH, siehe [15]und [16].

**Beurteilungsbericht**

**zum**

# Cyber-Sicherheits-Check

**der**

## Muster GmbH

**August 2014**

## 1. Rahmendaten

| | |
|---|---|
| Beurteilungsgegenstand | Cyber-Sicherheits-Check bei der Muster GmbH |
| Beurteiler | Herr Lukas Müller (UniBw M) |
| Ansprechpartner | Herr T. Knorr |
| Anlass | Durchführung eines Cyber-Sicherheits-Check im Rahmen einer Seminararbeit des Forschungszentrum Cyber Defence (CODE) an der Universität der Bundeswehr München |
| Grundlagen und Anforderungen | 1) Leitfaden Cyber-Sicherheits-Check (Version 1.0)<br>2) Verbindliche Liste der Maßnahmenziele (Version 1.0) |
| Zeitlicher Ablauf | Vor-Ort-Beurteilung: 12.08.14<br>Berichtsübergabe: 13.08.14 |
| Verteiler | Herr T. Knorr<br>Mit Bitte um Weiterleitung an die Geschäftsführung von Muster GmbH |

| | |
|---|---|
| Datei | Beurteilungsbericht.docx |
| Druckdatum | 13.08.14 |
| Dokumentenstatus | freigegeben |

## 2. Management Summary

Der Cyber-Sicherheits-Check soll Unternehmen und Behörden einen Überblick über den Status der Cyber-Sicherheit in einer Institution geben und die Verantwortung anhand konkreter Empfehlungen dabei unterstützen, festgestellte Sicherheitsmängel abzustellen.

### 2.1 Cyber-Sicherheits-Exposition

Auf Basis der vorgelegten Dokumente und gesammelten Informationen wurde für die Muster GmbH folgende Cyber-Sicherheits-Exposition festgestellt:

| | Vertraulichkeit | Verfügbarkeit | Integrität |
|---|---|---|---|
| Cyber-Sicherheits-Exposition | sehr hoch | hoch | sehr hoch |

Die Einstufung einer sehr hohen Cyber-Sicherheits-Exposition im Schutzziel „Vertraulichkeit“ und Integrität resultiert maßgeblich aus dem hohen Grad der Spezialisierung, dem enormen Aufwand im Entwicklungsbereich und dem in großen Teilen verbundene Geheimhaltungsgrad von Informationswerten. Die Gefährdungslage beinhaltet auch professionelle Angriffe und staatliche Akteure.
Das Schutzziel Verfügbarkeit wurde hoch eingestuft, da bereits Angriffe auf diesen Bereich erfolgreich abgewehrt wurden.

## 2.2 Cyber-Sicherheits-Status

Die Ergebnisse des Cyber-Sicherheits-Checks sind in der nachfolgenden Tabelle dargestellt und geben den Status der Cyber-Sicherheit bei Muster GmbH je Maßnahmenziel wieder. Die Bewertungsergebnisse der einzelnen Maßnahmen werden in Kapitel 3 näher erläutert.

Grundsätzlich ist zu bemerken, dass im Rahmen des Cyber-Sicherheits-Checks bei Muster GmbH in zwei Maßnahmenziel schwer-wiegende Sicherheitsmängel festgestellt werden konnten.

Insbesondere wurden im Maßnahmenziel K „Durchführung nutzerorientierter Maßnahmen“ schwerwiegende Sicherheitsmängel festgestellt. Diese beruhen auf der Tatsache, dass weder entsprechende Richtlinien/ Konzepte noch Prozesse zur ausreichenden Sensibilisierung der Mitarbeiter im Umgang mit hochsensiblen Daten etabliert sind. Da dies jedoch im Hinblick auf die sehr hohe Cyber-Sicherheits-Exposition im Schutzziel „Vertraulichkeit“ und „Integrität“ dringend notwendig erscheint, erfolgt hier eine Bewertung als „schwerwiegender Sicherheitsmangel“.

Darüber hinaus wurden im Maßnahmenziel L „Sichere Nutzung Sozialer Netzwerke“ ein „schwerwiegender Sicherheitsmangel“ festgestellt. Hier ist zu bemängeln das keine verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile des Beschäftigten in Sozialen Netzwerken existieren, auch die Sensibilisierung der Mitarbeiter hinsichtlich der Risiken und des korrekten Verhaltens in Sozialen Netzwerken, in regelmäßigen Abständen fehlt.
Im Hinblick auf die sehr hohe Cyber-Sicherheits-Exposition im Schutzziel „Vertraulichkeit“ und „Integrität“ wurde die Bewertung als „schwerwiegender Sicherheitsmangel“ eingestuft.

| Maßnahmenziel | Bewertet | Ergebnis | |
|---|---|---|---|
| A) Absicherung von Netzübergängen | Ja | Keine Mängel festgestellt | |
| B) Abwehr von Schadprogrammen | Ja | Keine Mängel festgestellt | |
| C) Inventarisierung der IT-Systeme | Ja | Keine Mängel festgestellt | |
| D) Vermeidung von offenen Sicherheitslücken | Ja | Keine Mängel festgestellt | |
| E) Sichere Interaktion mit dem Internet | Ja | Keine Mängel festgestellt | |
| F) Logdatenerfassung und –auswertung | Ja | Keine Mängel festgestellt | |
| G) Sicherstellung eines aktuellen Informationsstands | Ja | Keine Mängel festgestellt | |
| H) Bewältigung von Sicherheitsvorfällen | Ja | Keine Mängel festgestellt | |
| I) Sichere Authentisierung | Ja | Keine Mängel festgestellt | |
| J) Gewährleistung der Verfügbarkeit notwendiger Ressourcen | Ja | Keine Mängel festgestellt | |
| K) Durchführung nutzerorientierter Maßnahmen | Ja | Schwerwiegende Sicherheitsmängel festgestellt | |
| L) Sichere Nutzung Sozialer Netzwerke | Ja | Schwerwiegende Sicherheitsmängel festgestellt | |
| M) Durchführung von Penetrationstests | Ja | Keine Mängel festgestellt | |

## 3. Detaillierte Bewertungsergebnisse

| | |
|---|---|
| **Maßnahmenziel** | A - Absicherung von Netzübergängen |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | B - Abwehr von Schadprogrammen |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | C - Inventarisierung der IT-Systeme |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | D - Vermeidung von offenen Sicherheitslücken |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | E - Sichere Interaktion mit dem Internet |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | F - Logdatenerfassung und –auswertung |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | G - Sicherstellung eines aktuellen Informationsstands |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | H - Bewältigung von Sicherheitsvorfällen |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | I - Sichere Authentisierung |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | J - Gewährleistung der Verfügbarkeit notwendiger Ressourcen |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |
| / | |

| | |
|---|---|
| **Maßnahmenziel** | K - Durchführung nutzerorientierter Maßnahmen |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |

**Schwerwiegender Sicherheitsmangel:**

Es erfolgt keine zielgruppenorientierte, regelmäßige Sensibilisierung für die Gefahren eines Cyber- Angriffs oder Schulung hinsichtlich des korrekten Verhaltens.

**Empfehlung:**

Alle Mitarbeiter sollten eine zielgruppenorientierte, regelmäßige Sensibilisierung für die Gefahren eines Cyber- Angriffs und Schulung zum korrekten Verhalten erhalten, der Verantwortungsbereich eines jeden Mittarbeiters sollte ihm selbst und den anderen Mitarbeitern klar sein.

| | |
|---|---|
| **Maßnahmenziel** | L - Sichere Nutzung Sozialer Netzwerke |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |

**Schwerwiegender Sicherheitsmangel:**

Hier ist zu bemängeln das keine verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile des Beschäftigten in Sozialen Netzwerken existieren, auch die Sensibilisierung der Mitarbeiter hinsichtlich der Risiken und des korrekten Verhaltens in Sozialen Netzwerken, in regelmäßigen Abständen fehlt.

**Empfehlung:**

Es sollten verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile des Beschäftigten in Sozialen Netzwerken erstellt werden, auch die Sensibilisierung der Mitarbeiter hinsichtlich der Risiken und des korrekten Verhaltens in Sozialen Netzwerken sollte erfolgen.

| | |
|---|---|
| **Maßnahmenziel** | M - Durchführung von Penetrationstests |
| **Ergebnis** | Keine Mängel festgestellt |
| **Ansprechpartner** | Herr Knorr |
| **Stichproben** | vorgelegte Dokumente und gesammelte Informationen |

/

_____

13.08.14, Lukas Müller

### 5.8.3 Anhang C - Maßnahmenziele und Maßnahmen nach ISO 27001

Maßnahmenziele und Maßnahmen nach ISO 27001 angewendet auf die Muster GmbH, siehe [2].

Referenzmaßnahmen und Ziele für eine Zertifizierung nach ISO 27001, siehe Anhang A DIN/ ISO 27001

| | | Maßnahme | Bewertung/Status |
|---|---|---|---|
| **Sicherheitsleitlinien** | | | |
| **Vorgaben der Leitung zur Informationssicherheit**<br>Ziel: Bereitstellung von Vorgaben und Unterstützung seitens der Leitung für die Informationssicherheit nach geschäftlichen Anforderungen und den geltenden Gesetzen und Vorschriften. | Informationssicherheitsleitlinien | Ein Satz Informationssicherheitsleitlinien ist festzulegen, von der Leitung zu genehmigen, zu veröffentlichen und den Mitarbeitern sowie relevanten externen Parteien bekanntzumachen. | |
| | Prüfung der Informations-sicherheitsleitlinien | Die Informationssicherheitsleitlinien müssen in planmäßigen Abständen oder jeweils nach erheblichen Änderungen geprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind. | |
| **Organisation der Informationssicherheit** | | | |
| **Interne Organisation**<br>Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann. | Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit | Alle Zuständigkeiten im Bereich der Informationssicherheit müssen festgelegt und zugeordnet werden. | |
| | Kontakt zu Behörden | Es sind angemessene Kontakte zu relevanten Behörden zu pflegen. | |
| | Kontakt mit Interessenvertretungen | Es sind angemessene Kontakte zu Interessenvertretungen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden zu pflegen. | |
| | Informationssicherheit im Projektmanagement | Die Informationssicherheit muss ungeachtet der Art des Projekts auch im Projektmanagement berücksichtigt werden. | |
| | Aufgabentrennung | Miteinander in Konflikt stehende Aufgaben und Zuständigkeitsbereiche müssen getrennt werden, um das Risiko unautorisierter oder versehentlicher Änderung oder missbräuchlicher Anwendung der Werte der Organisation zu verringern. | |
| **Mobilgeräte und Telearbeit**<br>Ziel: Sicherstellung der Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten | Leitlinie zu Mobilgeräten | Es müssen eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz vor den Risiken durch die Nutzung von Mobilgeräten eingesetzt werden. | |

| | | | |
|---|---|---|---|
| | Telearbeit | Es müssen eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen festgelegt werden, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden. | |
| **Sicherheit des Personals** | | | |
| **Vor der Einstellung**<br>Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann. | Überprüfung | Prüfungen des Hintergrunds von Bewerbern müssen im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Informationen und den wahrgenommenen Risiken stehen. | |
| | Arbeitsvertragsklauseln | Im Rahmen ihrer vertraglichen Verpflichtung müssen Mitarbeiter den Arbeitsvertragsklauseln in ihrem Arbeitsvertrag, mit denen ihre eigenen Pflichten und die Pflichten der Organisation im Bereich der Informationssicherheit festgelegt werden, zustimmen und sie unterzeichnen. | |
| **Während der Anstellung**<br>Ziel: Sicherstellung, dass Mitarbeiter und externe Benutzer ihre Pflichten bezüglich der Informationssicherheit kennen und ihnen nachkommen. | Verantwortung des Managements | Das Management muss alle Mitarbeiter und externen Benutzer dazu anhalten, Sicherheitsmaßnahmen entsprechend den festgelegten Leitlinien und Verfahren der Organisation anzuwenden. | |
| | Bewusstsein, Ausbildung und Schulung für Informationssicherheit | Alle Mitarbeiter der Organisation sowie, falls relevant, externe Benutzer müssen ein Programm zur Sensibilisierung für Informationssicherheit sowie entsprechende Aus- und Weiterbildung und Schulungen durchlaufen und regelmäßig bezüglich der Leitlinien und Verfahren der Organisation, die für ihre berufliche Funktion relevant sind, auf dem neuesten Stand gehalten werden. | |
| | Disziplinarverfahren | Es muss ein formales und offiziell bekanntgegebenes Disziplinarverfahren eingeleitet werden, in dessen Rahmen Maßnahmen gegen Mitarbeiter verhängt werden können, die gegen Informationssicherheitsvorschriften verstoßen haben. | |
| **Beendigung und Wechsel der Anstellung**<br>Ziel: Schutz der Interessen der Organisation bei einem Wechsel oder der Beendigung der Anstellung | Zuständigkeiten bei Beendigung oder Wechsel der Anstellung | Zuständigkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Wechsel der Anstellung gültig bleiben, müssen definiert, dem Mitarbeiter oder externen Benutzer mitgeteilt und durchgesetzt werden. | |

| Wertemanagement | | | |
|---|---|---|---|
| **Verantwortung für Werte**<br>Ziel: Erreichen und Erhaltung eines angemessenen Schutzes der Werte der Organisation | Inventar der Werte | Werte, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, müssen ermittelt werden, und von diesen Anlagen ist ein Inventar zu erstellen und zu pflegen. | |
| | Eigentum von Werten | Für im Inventar geführte Werte muss es Eigentümer geben. | |
| | Zulässiger Gebrauch von Werten | Es müssen Regeln für den zulässigen gebrauch von Informationen und Werten, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, aufgestellt, dokumentiert und implementiert werden. | |
| **Klassifizierung von Informationen**<br>Ziel: Sicherstellung, dass Informationen eine angemessene Schutzstufe entsprechend ihrer Bedeutung für die Organisation zugeteilt bekommen. | Klassifizierung von Informationen | Informationen sind nach ihrem Wert, gesetzlichen Anforderungen, Vertraulichkeit und Betriebswichtigkeit zu klassifizieren. | |
| | Kennzeichnung von Informationen | Ein angemessener Satz Verfahren zur Kennzeichnung von Informationen ist entsprechend dem von der Organisation eingesetzten Plan zur Einstufung von Informationen zu entwickeln und zu implementieren. | |
| | Umgang mit Werten | Verfahren für den Umgang mit Werten sind entsprechend dem von der Organisation eingesetzten Plan zur Einstufung von Informationen zu entwickeln und zu implementieren. | |
| | Rückgabe von Werten | Alle Mitarbeiter und externen Benutzer müssen sämtliche Werte der Organisation zurückgeben, die sich bei Auslauf ihrer Anstellung oder ihres Vertrags noch in Ihrem Besitz befinden. | |
| **Umgang mit Medien**<br>Ziel: Verhinderung von unerlaubter Veröffentlichung, Veränderung, Entnahme oder Zerstörung von Informationen, die auf Medien gespeichert sind. | Verwaltung von Wechselmedien | Es sind Verfahren für die Verwaltung von Wechselmedien entsprechend dem von der Organisation eingesetzten Plan zur Klassifizierung von Informationen zu implementieren. | |
| | Entsorgung von Medien | Medien müssen sicher und unter Anwendung formaler Verfahrensanweisungen entsorgt werden, wenn sie nicht mehr benötigt werden. | |
| | Physische Weitergabe von Medien | Medien, auf denen Informationen gespeichert sind, müssen vor unautorisiertem Zugriff, missbräuchlicher Verwendung oder Verfälschung während des Transports geschützt werden. | |

| Zugriffskontrolle | | | |
|---|---|---|---|
| **Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle**<br>Ziel: Beschränkung des Zugriffs auf Informationen und informationsverarbeitenden Einrichtungen | Zugriffskontrollleitlinie | Eine Zugriffskontrollleitlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen zu erstellen, zu dokumentieren und zu prüfen. | |
| | Leitlinie zur Nutzung von Netzwerkdiensten | Benutzer dürfen ausschließlich auf denjenigen Netzwerken und Netzwerkdiensten Zugriff erhalten, zu deren Nutzung sie ausdrücklich autorisiert wurden. | |
| **Benutzerverwaltung**<br>Ziel: Sicherstellung des Zugriffs ausschließlich für autorisierte Benutzer und Verhinderung von nicht autorisierten Zugriffen auf Systeme und Dienste. | An- und Abmeldung von Benutzern | Es muss ein formales Verfahren für die An- und Abmeldung von Benutzern implementiert werden, mit dem allen Arten von Benutzern der Zugriff auf Systeme und Dienste gewährt und wieder entzogen werden kann. | |
| | Verwaltung von Sonderrechten | Die Zuteilung und Nutzung von Sonderzugriffsrechten muss eingeschränkt und kontrolliert werden. | |
| | Verwaltung geheimer Authentisierungs-informationen von Benutzern | Die Zuordnung von geheimen Authentisierungsinformationen muss über einen formalen Verwaltungsprozess kontrolliert werden. | |
| | Prüfung von Zugriffsberechtigungen der Benutzer | Werteeigentümer müssen die Zugriffsberechtigungen der Benutzer in regelmäßigen Abständen prüfen. | |
| | Entzug oder Anpassung von Zugriffsberechtigungen | Die Zugriffsberechtigungen aller Mitarbeiter und externen Benutzer zu Informationen und informationsverarbeitenden Einrichtungen müssen nach Auslauf der Anstellung oder des Vertrags entzogen bzw. bei einem Wechsel der Anstellung entsprechend angepasst werden. | |
| **Benutzerverantwortung**<br>Ziel: Übertragung der Verantwortung für den Schutz der Authentisierungsinformationen auf die Benutzer | Verwendung von geheimen Authentisierungs-informationen | Von den Benutzern muss verlangt werden, die sicherheitsrelevanten Praktiken der Organisation zur Verwendung von geheimen Authentisierungsinformationen zu befolgen. | |
| **Kontrolle des Zugriffs auf Systeme und Anwendungen**<br>Ziel: Verhinderung des unautorisierten Zugriffs auf Systeme und Anwendungen | Beschränkung des Zugriffs auf Informationen | Der Zugriff auf Funktionen von Informations- und Anwendungssystemen muss entsprechend der Zugriffskontrollleitlinie beschränkt werden. | |
| | Sichere Anmeldeverfahren | Der Zugriff auf Systeme und Anwendungen muss über ein sicheres Anmeldeverfahren kontrolliert werden, wenn dies nach der Zugriffskontrollleitlinie erforderlich ist. | |

| | | | |
|---|---|---|---|
| | Kennwortmanagementsystem | Kennwortmanagementsysteme müssen interaktiv sein und starke Kennwörter erfordern. | |
| | Verwendung von Dienstprogrammen mit Sonderberechtigungen | Die Verwendung von Dienstprogrammen, mit denen sich u. U. System- und Anwendungskontrollen umgehen lassen, muss beschränkt und streng kontrolliert werden. | |
| | Kontrolle des Zugriffs auf Software-Quellcode | Der Zugriff auf den Software-Quellcode muss beschränkt werden. | |
| **Kryptographie** | | | |
| **Kryptographische Maßnahmen**<br>Ziel: Sicherstellung der ordnungsnachen und wirksamen Verwendung von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen | Leitlinie zur Nutzung von kryptographischen Maßnahmen | Eine Leitlinie zur Verwendung von kryptographischen Maßnahmen für den Schutz von Informationen ist zu entwickeln und zu implementieren. | |
| | Verwaltung von Schlüsseln | Eine Leitlinie zur Verwendung, zum Schutz und zur Gültigkeitsdauer von kryptographischen Schlüsseln ist zu entwickeln und über deren gesamten Nutzungsdauer hinweg umzusetzen. | |
| **Schutz vor physischem Zugang und Umwelteinflüssen** | | | |
| **Sicherheitsbereiche**<br>Ziel: Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung. | Physische Sicherheitszone | Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitszonen festzulegen und zu verwenden. | |
| | Physische Zugangskontrolle | Sicherheitsbereiche müssen durch angemessene Zugriffskontrollen geschützt werden, durch die sichergestellt ist, dass nur autorisiertes Personal Zugriff hat. | |
| | Sicherung von Zweigstellen, Räumen und Anlagen | Es sind physische Sicherungsvorkehrungen für Niederlassungen, Räume und Anlagen zu konzipieren und anzuwenden. | |
| | Schutz vor externen und umweltbedingten Bedrohungen | Es sind physische Schutzvorkehrungen gegen Naturkatastrophen, vorsätzliche Angriffe oder Unfälle zu konzipieren und anzuwenden. | |
| | Arbeit in Sicherheitsbereichen | Es sind physische Schutzvorkehrungen und Richtlinien für die Arbeit in Sicherheitsbereichen zu konzipieren und anzuwenden. | |

| | | | |
|---|---|---|---|
| | Anlieferungs- und Ladezonen | Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich unautorisierte Personen Zugang zu den Betriebsgebäuden verschaffen könnten, müssen kontrolliert und nach Möglichkeit von informationsverarbeitenden Einrichtungen isoliert werden, um unautorisierten Zugriff zu verhindern. | |
| **Betriebsmittel**<br>Ziel: Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation | Platzierung und Schutz von Betriebsmitteln | Betriebsmittel sind so zu platzieren und zu schützen, dass Risiken durch Umweltbedrohungen und Gefährdungen sowie Möglichkeiten für den unautorisierten Zugriff verringert werden. | |
| | Versorgungseinrichtungen | Betriebsmittel müssen vor Stromausfällen und anderen Betriebsunterbrechungen durch Ausfälle von Versorgungseinrichtungen geschützt werden. | |
| | Sicherheit der Verkabelung | Stromversorgungs- und Telekommunikationskabel, die zur Übertragung von Daten oder zur Unterstützung von Informationsdiensten verwendet werden, sind vor dem Abfangen der Daten sowie vor Beeinträchtigung oder Beschädigung zu schützen. | |
| | Instandhaltung von Gerätschaften | Gerätschaften müssen ordnungsnach instand gehalten und gepflegt werden, um ihre Verfügbarkeit und Integrität sicherzustellen. | |
| | Entfernung von Werten | Ausstattung, Informationen oder Software dürfen nicht ohne vorherige Autorisierung vom Standort entfernt werden. | |
| | Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude | Sicherheitsvorkehrungen werden unter Berücksichtigung der diversen Risiken bei Arbeiten außerhalb der Betriebsgebäude der Organisation auch auf Werte außerhalb des Standorts angewandt. | |
| | Sichere Entsorgung oder Wiederverwendung von Betriebsmitteln | Alle Geräte, die Speichermedien enthalten, müssen vor ihrer Entsorgung oder Wiederverwendung überprüft werden, um sicherzustellen, dass vertrauliche Daten und lizenzierte Software entfernt oder sicher überschrieben wurden. | |
| | Unbeaufsichtigte Benutzerausstattung | Benutzer müssen sicherstellen, dass unbeaufsichtigte Ausstattung angemessen geschützt ist. | |
| | Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms | Der Grundsatz des aufgeräumten Schreibtisches für Papiere und Wechselmedien sowie des leeren Bildschirms für informationsverarbeitende Einrichtungen muss Anwendung finden. | |

| Betriebssicherheit | | | |
|---|---|---|---|
| **Betriebsverfahren und Zuständigkeiten**<br>Ziel: Sicherstellung des ordnungsnahen und sicheren Betriebs von Vorrichtungen zur Verarbeitung von Informationen | Dokumentierte Betriebsverfahren | Die Betriebsverfahren müssen dokumentiert und allen Benutzern zugänglich gemacht werden, die sie benötigen. | |
| | Änderungsmanagement | Änderungen an der Organisation, an Geschäftsprozessen, an Datenverarbeitungseinrichtungen und an Systemen sind zu kontrollieren. | |
| | Kapazitätsmanagement | Die Ressourcennutzung muss überwacht und abgestimmt werden, und es sind Prognosen zu zukünftigen Kapazitätsanforderungen zu erstellen, um ausreichende Systemleistung sicherzustellen. | |
| | Trennung von Entwicklungs-, Test- und Betriebsumgebungen | Entwicklungs-, Test- und Betriebsumgebungen sind zu trennen, um das Risiko unautorisierter Zugriffe oder unautorisierter Änderungen an der Betriebsumgebung zu verringern. | |
| **Schutz vor Malware**<br>Ziel: Sicherstellung, dass Daten und Datenverarbeitungseinrichtungen vor Malware geschützt sind | Kontrollmaßnahmen gegen Malware | Es sind Erkennungs-, Präventions- und Wiederherstellungs-maßnahmen zum Schutz vor Malware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer zu implementieren. | |
| **Datensicherungen**<br>Ziel: Schutz vor Datenverlust | Datensicherungen | Es sind Sicherungskopien von Daten und Software sowie System-Images anzufertigen und regelmäßig entsprechend der vereinbarten Sicherungsleitlinie zu prüfen. | |
| **Protokollierung und Überwachung**<br>Ziel: Aufzeichnung von Ereignissen und Generierung von Beweismaterial | Ereignisprotokollierung | Es sind Ereignisprotokolle anzufertigen, aufzubewahren und regelmäßig zu prüfen, in denen Aktivitäten der Benutzer, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet werden. | |
| | Schutz von Protokoll-informationen | Protokollierungseinrichtungen und Protokollinformationen müssen vor Manipulation und unbefugtem Zugriff geschützt werden. | |
| | Administrator- und Betreiberprotokolle | Es sind Protokolle der Aktivitäten von Systemadministratoren und Systembetreibern anzufertigen, zu schützen und regelmäßig zu prüfen. | |
| | Zeitsynchronisation | Die Uhren aller relevanten Datenverarbeitungssysteme innerhalb einer Organisation oder einer Sicherheitsdomäne müssen auf eine einzelne Referenz-Zeitquelle synchronisiert werden. | |
| **Kontrolle von Software im Betrieb**<br>Ziel: Sicherstellung der Integrität von Systemen im Betrieb | Installation von Software auf Systemen im Betrieb | Es sind Verfahren zur Kontrolle der Installation von Software auf betriebsrelevanten Systemen zu implementieren. | |

| | | | |
|---|---|---|---|
| **Management technischer Schwachstellen**<br>Ziel: Verhinderung einer Ausnutzung technischer Schwachstellen | Management technischer Schwachstellen | Informationen über technische Schwachstellen von verwendeten Informationssystemen müssen rechtzeitig eingeholt werden, die Anfälligkeit der Organisation für eine Ausnutzung solcher Schwachstellen ist zu bewerten, und es müssen angemessene Maßnahmen für den Umgang mit dem damit einhergehenden Risiko ergriffen werden. | |
| | Beschränkungen der Software-Installation | Für Software-Installationen durch Benutzer müssen Regeln festgelegt und implementiert werden. | |
| **Auswirkungen von Audits auf Informationssysteme**<br>Ziel: Minimierung der Auswirkungen von Audit-Aktivitäten auf Systeme im Betrieb | Kontrollen für Audits von Informationssystemen | Audit-Anforderungen und -Aktivitäten im Zusammenhang mit betriebsrelevanten Systemen müssen sorgfältig geplant und vereinbart werden, um Unterbrechungen der Geschäftsabläufe zu minimieren. | |
| **Sicherheit in der Kommunikation** | | | |
| **Netzwerksicherheitsmanagement**<br>Ziel: Sicherstellung des Schutzes von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen | Netzwerkkontrollen | Netzwerke müssen verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen. | |
| | Sicherheit von Netzwerkdiensten | Es müssen Sicherheitsmechanismen, Service-Level und Anforderungen für die Verwaltung aller Netzwerkdienste ermittelt und in Verträge über Netzwerkdienste aufgenommen werden, und zwar unabhängig davon, ob diese Dienste intern erbracht oder ausgelagert werden. | |
| | Trennung in Netzwerken | Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzwerken voneinander getrennt gehalten werden. | |
| **Informationsübertragung**<br>Ziel: Wahrung der Sicherheit von Informationen, die innerhalb einer Organisation oder im Austausch mit einer externen Stelle übertragen werden. | Leitlinien und Verfahren für die Informationsübertragung | Es müssen formale Leitlinien, Verfahren und Kontroll-maßnahmen in Kraft sein, mit denen die Informations-übertragung über alle Arten von Kommunikationseinrichtungen geschützt wird. | |
| | Vereinbarungen zur Informationsübertragung | Es muss Vereinbarungen für die sichere Übertragung von geschäftlichen Informationen zwischen der Organisation und externen Parteien geben. | |
| | Elektronische Nachrichtenübermittlung | Informationen in elektronischen Nachrichten müssen angemessen geschützt werden. | |
| | Vertraulichkeits- oder Geheimhaltungs-vereinbarungen | Entsprechend den Bedürfnissen der Organisation in Bezug auf den Schutz von Informationen müssen Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen ermittelt, regelmäßig geprüft und dokumentiert werden. | |

| Anschaffung, Entwicklung und Instandhaltung von Systemen | | | |
|---|---|---|---|
| **Sicherheitsanforderungen für Informationssysteme**<br>Ziel: Sicherstellung, dass Sicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Dies beinhaltet insbesondere spezifische Sicherheitsanforderungen für Informationssysteme, mit denen Dienste über öffentliche Netze bereitgestellt werden. | Analyse und Spezifikation von Sicherheitsanforderungen | Die Anforderungen für Kontrollen der Informationssicherheit müssen in den Angaben zu den geschäftlichen und technischen Anforderungen für neue Informationssysteme oder Verbesserungen an bestehenden Informationssystemen enthalten sein, und darin müssen alle relevanten Kriterien wie die gesamte Nutzungsdauer oder ggf. die Verfügbarkeit der Anwendung über öffentliche Netze berücksichtigt sein. | |
| | Sicherung von Anwendungsdiensten in öffentlichen Netzen | Informationen im Zusammenhang mit Anwendungsdiensten, die über öffentliche Netze übertragen werden, müssen gegen betrügerische Aktivitäten, Vertragsstreitigkeiten, unberechtigte Veröffentlichung oder Veränderung geschützt werden. | |
| | Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten | Informationen, die im Zuge von Transaktionen im Zusammenhang mit Anwendungsdiensten übertragen werden, müssen geschützt werden, um unvollständigen Übertragungen und Fehlleitungen sowie unautorisierten Offenlegungen, Vervielfältigungen oder wiederholten Wiedergaben von Nachrichten vorzubeugen. | |
| **Sicherheit in Entwicklungs- und Unterstützungsprozessen**<br>Ziel: Sicherstellung, dass Informationssicherheit im Rahmen des Entwicklungszyklus von Informationssystemen konzipiert und implementiert wird | Leitlinie für sichere Entwicklung | Es müssen Regeln für die Entwicklung von Software und Systemen festgelegt und bei Entwicklungen innerhalb der Organisation angewandt werden. | |
| | Änderungskontrollverfahren | Die Umsetzung von Änderungen muss einem formalen Änderungskontrollverfahren unterliegen. | |
| | Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform | Bei einem Wechsel der Betriebsplattform müssen geschäftskritische Anwendungen geprüft und getestet werden, um sicherzustellen, dass keine negativen Auswirkungen auf die Betriebstätigkeit oder die Sicherheit der Organisation gibt. | |

| | | | |
|---|---|---|---|
| | Beschränkung von Änderungen an Software-Paketen | Von Änderungen an Software-Paketen ist abzuraten. Falls doch Änderungen vorgenommen werden, müssen diese auf das Notwendige beschränkt sein und in jedem Fall streng kontrolliert werden. | |
| | Systementwicklungsverfahren | Es sind Grundsätze für die Entwicklung sicherer Systeme festzulegen, zu dokumentieren, aufrechtzuerhalten und bei jedem Systementwicklungsvorhaben anzuwenden. | |
| | Sichere Entwicklungsumgebung | Organisationen müssen eine sichere Entwicklungsumgebung für Systementwicklungen und Integrationsvorhaben, die den gesamten Zyklus der Systementwicklung abdeckt, herstellen und angemessen schützen. | |
| | Ausgelagerte Entwicklung | Die Organisation muss ausgelagerte Systementwicklungs-tätigkeiten beaufsichtigen und überwachen. | |
| | Systemsicherheitsprüfungen | Während der Entwicklung müssen die Sicherheits-vorkehrungen auf Funktion geprüft werden. | |
| | Systemabnahmeprüfung | Für neue Informationssysteme, Upgrades und neue Versionen sind Abnahmeprüfungsprogramme und dazugehörige Kriterien festzulegen. | |
| **Prüfdaten**<br>Ziel: Sicherstellung des Schutzes von zu Prüfzwecken verwendeten Daten | Schutz von Prüfdaten | Prüfdaten müssen sorgfältig ausgewählt, geschützt und kontrolliert werden. | |
| **Lieferantenbeziehungen** | | | |
| **Sicherheit in Lieferantenbeziehungen**<br>Ziel: Sicherstellung des Schutzes der für Lieferanten zugänglichen Informationen des Unternehmens | Informationssicherheitsleitlinie für Lieferantenbeziehungen | Die Informationssicherheitsanforderungen zurr Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Informationen oder informationsverarbeitende Einrichtungen der Organisation sind zu dokumentieren. | |
| | Sicherheitsthemen in Lieferantenverträgen | Mit jedem Lieferanten, der u. U. Zugriff auf Informationen der Organisation hat, sie verarbeitet, speichert, weitergibt oder IT-Infrastrukturkomponenten dafür bereitstellt, müssen jeweils alle relevanten Informationssicherheitsanforderungen festgelegt und vereinbart werden. | |
| | IKT-Lieferkette | Vereinbarungen mit Lieferanten müssen Anforderungen für den Umgang mit Informationssicherheitsrisiken im Zusammenhang mit der Dienstleistungs- und Produkt-lieferkette im Bereich der Informations- und Kommunikations-technologie enthalten. | |

| | | | |
|---|---|---|---|
| **Management der Dienstleistungserbringung durch Lieferanten**<br>Ziel: Aufrechterhaltung einer vereinbarten Informationssicherheitsstufe und Dienstleistungserbringung im Einklang mit Lieferantenverträgen | Überwachung und Prüfung von Lieferantendienst-leistungen | Organisationen müssen die Dienstleistungserbringung durch Lieferanten regelmäßig überwachen, prüfen und auditieren. | |
| | Management von Änderungen an Lieferantendienstleistungen | Änderungen an der Erbringung von Dienstleistungen durch Lieferanten einschließlich der Pflege und Verbesserung bestehender Informationssicherheitsleitlinien, -verfahren und -kontrollen müssen unter Berücksichtigung der Betriebswichtigkeit der betroffenen geschäftlichen Informationen, Systeme und Prozesse sowie einer erneuten Risikobewertung verwaltet werden. | |
| **Management von Informationssicherheitsvorfällen** | | | |
| **Management von Informationssicherheitsvorfällen und Verbesserungen**<br>Ziel: Sicherstellung einer konsistenten und wirksamen Strategie für das Management von Informationssicherheitsvorfällen einschließlich Benachrichtigung über Sicherheitsvorfälle und Schwachstellen | Zuständigkeiten und Verfahren | Zuständigkeiten und Verfahren für das Management sind festzulegen, damit schnell, effektiv und koordiniert auf Informationssicherheitsvorfälle reagiert werden kann. | |
| | Meldung von Informations-sicherheitsereignissen | Informationssicherheitsereignisse müssen so schnell wie möglich über geeignete Management-Kanäle gemeldet werden. | |
| | Meldung von Informations-sicherheitsschwachstellen | Mitarbeiter und externe Parteien, die die Informationssysteme und -dienste der Organisation nutzen, müssen dazu aufgefordert werden, jegliche beobachteten oder vermuteten Informationssicherheitsschwachstellen in Systemen oder Diensten festzuhalten und zu melden. | |
| | Bewertung und Einstufung von Informations-sicherheitsereignissen | Informationssicherheitsereignisse sind zu bewerten, und es muss darüber entschieden werden, ob sie als Informationssicherheitsvorfälle eingestuft werden. | |
| | Reaktion auf Informationssicherheitsvorfälle | Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden. | |

| | | | |
|---|---|---|---|
| | Erkenntnisse aus Informations-sicherheitsvorfällen | Aus der Analyse und Lösung von Informationssicherheits-vorfällen gewonnene Erkenntnisse müssen dazu genutzt werden, die Auftretenswahrscheinlichkeit oder die Auswirkun-gen zukünftiger Vorfälle zu verringern. | |
| | Sammeln von Beweismaterial | Die Organisation muss Verfahren für die Ermittlung, Sammlung, Aneignung und Aufbewahrung von Informationen, die als Beweismaterial dienen können, festlegen und anwenden. | |
| **Informationssicherheitsaspekte des Business Continuity Management** | | | |
| **Kontinuität der Informationssicherheit**<br>Ziel: Die Kontinuität der Informationssicherheit muss Teil des Business Continuity Management (BCM) der Organisation sein, so dass sichergestellt ist, dass Informationen jederzeit geschützt sind und die Organisation auf negative Ereignisse vorbereitet ist. | Planung der Kontinuität der Informationssicherheit | Die Organisation muss ihre Anforderungen für die Informationssicherheit und für die Aufrechterhaltung des Informationssicherheitsmanagements auch in schwierigen Situationen wie z. B. während einer Krise oder Katastrophe festlegen. | |
| | Implementierung der Kontinuität der Informations-sicherheit | Die Organisation muss Prozesse, Verfahren und Kontroll-maßnahmen festlegen, dokumentieren, implementieren und aufrechterhalten, um das erforderliche Maß an Kontinuität der Informationssicherheit in einer schwierigen Situation sicherstellen zu können. | |
| | Überprüfung, Überarbeitung und Auswertung der Kontinuität der Informations-sicherheit | Die Organisation muss die festgelegten und implementierten Kontrollmaßnahmen für die Kontinuität der Informations-sicherheit in regelmäßigen Abständen überprüfen, um sicherzustellen, dass sie gültig und auch in schwierigen Situationen wirksam sind. | |
| **Redundanzen**<br>Ziel: Sicherstellung der Verfügbarkeit von informationsverarbeitenden Einrichtungen | Verfügbarkeit von informationsverarbeitenden Einrichtungen | Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die Einhaltung der Verfüg-barkeitsanforderungen implementiert werden. | |

| Richtlinienkonformität | | | |
|---|---|---|---|
| **Informationssicherheitsprüfungen**<br>Ziel: Sicherstellung, dass Informationssicherheitsvorkehrungen entsprechend den Leitlinien und Verfahren der Organisation implementiert und angewandt werden. | Unabhängige Prüfung der Informationssicherheit | Die Strategie der Organisation für das Management der Informationssicherheit und deren Implementierung (d. h. Kontrollziele und -maßnahmen, Leitlinien, Prozesse und Verfahren zur Informationssicherheit) müssen in planmäßigen Abständen oder jeweils bei erheblichen Änderungen an der Implementierung von Sicherheitsvorkehrungen durch eine unabhängige Stelle geprüft werden. | |
| | Einhaltung der Sicherheitsleitlinien und -normen | Vorgesetzte müssen regelmäßig die Konformität der Informationsverarbeitung und der Verfahren in ihrem Zuständigkeitsbereich mit den jeweils anwendbaren Sicherheitsleitlinien, Normen und jeglichen sonstigen Sicherheitsanforderungen prüfen. | |
| | Inspektion der Technik auf Richtlinienkonformität | Informationssysteme müssen regelmäßig auf Konformität mit den Informationssicherheitsleitlinien und -normen der Organisation geprüft werden. | |
| **Einhaltung gesetzlicher und vertraglicher Anforderungen**<br>Ziel: Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit sowie gegen jegliche Sicherheitsanforderungen | Ermittlung anwendbarer gesetzlicher und vertraglicher Anforderungen | Alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen sowie die Strategie der Organisation zur Erfüllung dieser Anforderungen müssen für jedes Informationssystem sowie für die Organisation ausdrücklich ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden. | |
| | Rechte an geistigem Eigentum | Es sind angemessene Verfahren zu implementieren, mit denen die Einhaltung gesetzlicher, amtlicher und vertraglicher Anforderungen zur Verwendung von Material, an dem möglicherweise Schutzrechte bestehen, sowie von urheber-rechtlich geschützten Software-Produkten sichergestellt wird. | |
| | Schutz dokumentierter Informationen | Aufzeichnungen sind nach gesetzlichen, amtlichen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unautorisiertem Zugriff und unautorisierter Freigabe zu schützen. | |
| | Privatsphäre und Schutz von personenbezogenen Informationen | Die Privatsphäre sowie der Schutz von personenbezogenen Informationen müssen entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertrags-bestimmungen sichergestellt werden. | |
| | Regulierung kryptographischer Kontrollmaßnahmen | Kryptographische Kontrollmaßnahmen müssen unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt werden. | |

## 5.9 Glossar

nach ISO 27000 [1]

**Wert**
alles, was für die Institution von Wert ist
ANMERKUNG Es gibt viele Arten von Werten, einschließlich:

**a)** Informationen;

**b)** Software, z. B. Computerprogramme;

**c)** materielle Werte, z. B. Computer;

**d)** Dienstleistungen;

**e)** Menschen und ihren Qualifikationen, Fähigkeiten und Erfahrung; und

**f)** immaterielle Werte, z. B. Reputation und Image

**Angriff**
Versuch, einen Wert zu zerstören, offen zu legen, zu verändern, unbrauchbar zu machen, zu stehlen oder nicht autorisierten Zugriff auf ihn zu erlangen oder ihn ohne Berechtigung zu nutzen.

**Informationswert**
Wissen oder Daten, die von Wert für die Institution sind

**Bedrohung**
möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden des Systems oder der Institution führen kann

**Maßnahme**
Mittel zum Management von Risiken, einschließlich von Leitlinien, Verfahren, Richtlinien, Methoden oder Organisationsstrukturen, die verwaltender, technischer, leitender oder gesetzlicher Natur sein können ANMERKUNG Der Begriff „Maßnahme“ wird auch als Synonym für „Sicherheitsmaßnahme“ oder „Gegenmaßnahme“ benutzt

**Maßnahmenziel**
Beschreibung, was durch die Umsetzung von Maßnahmen als Ergebnis erreicht werden soll

**Korrekturmaßnahme**
Maßnahme zur Beseitigung der Ursache eines erkannten Fehlers oder einer anderen erkannten unerwünschten Situation [ISO 9000:2005]

**Effizienz**
Beziehung zwischen den erzielten Ergebnissen und dem Grad der Nutzung der Ressourcen

**Informationswert**
Wissen oder Daten, die von Wert für die Institution sind

**Informationssicherheit**
Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen ANMERKUNG Zusätzlich können auch andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit einbezogen werden

**Richtlinie**
Empfehlung dessen, was an Umsetzung erwartet wird, um ein Ziel zu erreichen

**Leitlinie**
vom Management formell ausgedrückte Gesamtintention und -richtung

**Risiko**
Kombination aus der Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen [ISO/IEC Guide 73:2002]

**Risikoeinschätzung**
gesamter Prozess der Risikoanalyse und Risikobewertung [ISO/IEC Guide 73:2002]

**Risikoakzeptanz**
Entscheidung, ein Risiko zu akzeptieren [ISO/IEC Guide 73:2002]

**Risikoanalyse**
systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des Risikos [ISO/IEC Guide 73:2002] ANMERKUNG Die Risikoanalyse bildet die Grundlage der Risikobewertung, Risikobehandlung und Risikoakzeptanz

**Zugriffskontrolle**
Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt

**Zurechenbarkeit**
Verantwortung einer Einheit für ihre Handlungen und Entscheidungen

**Authentisierung**
Sicherstellung, dass die von einer Einheit behauptete Eigenschaft korrekt ist

**Authentizität**
Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt

**Verfügbarkeit**
Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein

**Business Continuity**
Prozesse und/oder Verfahren, die der Sicherstellung eines kontinuierlichen Geschäftsbetriebs dienen

**Vertraulichkeit**
Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

**Wirksamkeit**
Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden [ISO 9000:2005]

**Ereignis**
Auftreten von ungewöhnlichen Umständen [ISO/IEC Guide 73:2002]

**Informationssicherheits-Ereignis**
erkanntes Auftreten eines System-, Service- oder Netzwerkzustands, der einen möglichen Verstoß gegen die Leitlinie zur Informationssicherheit, das Versagen von Maßnahmen oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt

**Informationssicherheits-Vorfall**
einzelnes oder eine Reihe von unerwünschten oder unerwarteten Informationssicherheits-Ereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird

**Management von Informationssicherheits-Vorfällen**
Prozesse der Entdeckung, Berichterstattung, Bewertung von, Reaktion auf, Behandlung von und des Lernens aus Informationssicherheits-Vorfällen

**Informationssicherheitsmanagementsystem (ISMS)**
Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt

**Informationssicherheits-Risiko**
Möglichkeit, dass eine vorhandene Bedrohung die eine Schwachstelle eines Wertes oder einer Gruppe von Werten ausnutzt und dadurch der Institution Schaden zufügen könnte

**Integrität**
Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten

**Managementsystem**
Rahmenwerk von Leitlinien, Verfahren, Richtlinien und den zugehörigen Ressourcen, um die Ziele der Institution zu erreichen

**Vorbeugungsmaßnahme**
Maßnahme zur Beseitigung der Ursache eines möglichen Fehlers oder einer anderen möglichen unerwünschten Situation [ISO 9000:2005]

**Verfahren**
festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen [ISO 9000:2005]

**Prozess**
Satz von in Wechselbeziehung oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt [ISO 9000:2005]

**Aufzeichnung**
Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt [ISO 9000:2005]

**Verlässlichkeit**
Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

**Risikokommunikation**
Austausch oder gemeinsame Nutzung von Informationen über Risiken zwischen Entscheidungsträgern und anderen Stakeholdern [ISO/IEC Guide 73:2002]

**Risikokriterien**
Bezugsrahmen für die Einschätzung der Bedeutung eines Risikos [ISO/IEC Guide 73:2002]

**Risikobestimmung**
Tätigkeit, bei der der Wahrscheinlichkeit und den Auswirkungen eines Risikos Werte zugeordnet werden [ISO/IEC Guide 73:2002]

**Risikobewertung**
Prozess, in dem das eingeschätzte Risiko mit den festgelegten Risikokriterien verglichen wird, um die Bedeutung des Risikos zu bestimmen [ISO/IEC Guide 73:2002]

**Risikomanagement**
koordinierte Tätigkeit zur Leitung und Kontrolle einer Institution in Bezug auf Risiken [ISO/IEC Guide 73:2002] ANMERKUNG Risikomanagement beinhaltet normalerweise Risikoeinschätzung, Risikobehandlung, Risikoakzeptanz , Risikokommunikation, Risikoüberwachung und Risikoüberprüfung.

**Risikobehandlung**
Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos [ISO/IEC Guide 73:2002]

**Erklärung zur Anwendbarkeit**
Dokument, das die Maßnahmenziele und Maßnahmen beschreibt, die für das ISMS einer Institution relevant und anwendbar sind

**Schwachstelle**
Schwäche eines Werts oder einer Maßnahme, die von einer Bedrohung ausgenutzt werden kann

**Plan-Do-Check-Act-Prozess**
Der prozessorientierte Ansatz für ein ISMS, der in der ISMS-Normenfamilie dargelegt wird, basiert auf dem Regelkreis, der in den ISO-Normen für Managementsysteme zugrunde gelegt wird und der unter der Bezeichnung „Plan-Do-Check-Act-Prozess“ („Planen, Durchführen, Prüfen, Handeln“) bzw. „PDCA-Prozess“ bekannt ist.

**a)** Planen — lege Ziele fest und erstelle Pläne (analysiere die Situation der Institution, lege übergreifende Ziele fest, lege Vorgaben fest und entwickle Pläne, um sie zu erreichen);

**b)** Durchführen — setze Pläne um (tu, was geplant war);

**c)** Prüfen — erfasse Ergebnisse (messe/überwache, in welchem Maße die Ergebnisse den geplanten Zielen entsprechen); und

**d)** Handeln — korrigiere und verbessere die Tätigkeiten (lerne aus Fehlern, wie die Tätigkeiten verbessert und bessere Ergebnisse erzielt werden können).

**Stakeholder**
(engl. ‚Teilhaber‘) bezeichnet eine Person oder Gruppe, die ein berechtigtes Interesse am Verlauf oder Ergebnis eines Prozesses oder Projektes hat. Es zählen hierzu unter anderem die Eigentümer, Manager, Mitarbeiter, Lieferanten, Kunden aber auch die Gesellschaft und der Staat. Siehe hierzu auch Projektbeteiligten nach DIN 69901-5.

# Literaturverzeichnis


[1] DIN ISO/IEC 27000. *Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2009).* DIN Deutsches Institut für Normung e. V., Beuth Verlag GmbH, Juli 2011. April 2014

[2] DIN ISO/IEC 27001 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC DIS 27001:2013) April 2014

[3] DIN ISO/IEC 27002 Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management (ISO/IEC FDIS 27002:2013) April 2014

[4] ISO/IEC 27003, Information security management system implementation guidance

[5] ISO/IEC 27004, Information security management — Measurement

[6] ISO/IEC 27005:2008, Information security risk management

[7] ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems

[8] ISO/IEC 27007, Guidelines for information security management systems auditing

[9] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Mai 2008, www.bsi.bund.de

[10] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008, www.bsi.bund.de

[11] IT-Grundschutz-Kataloge - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[12] Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand 12. Ergänzungslieferung

[13] Vergleich von ISO/IEC 27033-1 und IT-Grundschutz, Stefan Lenzhofer, April 2009

[14] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014, http://www.nist.gov/cyberframework/

[15] Leitfaden Cyber-Sicherheits-Check, BSI

[16] BSI-Veröffentlichungen zur Cyber-Sicherheit, Basismaßnahmen der Cyber-Sicherheit

[17] BSI, EMPFEHLUNG: MANAGEMENT, Cyber-Sicherheits-Exposition

[18] Checkliste Netzwerksicherheit, Rohde und Schwarz SIT GmbH, 9.2013 – Version 1.2

[19] Ein Informationssicherheitsmanagementsystem nach ISO27001:2013, complimant AG, 16. Januar 2014, Version 2.0

[20] Microsoft, DATA SHEET Security Health Check, www.microsoft.com/premiersupport

[21] Microsoft Services Catalogue, Australia and New Zealand, August 2009

# Kapitel 6

# IT-Sicherheitsmanagement vs. interne Sicherheitsbedrohungen

*Caroline Wölkert*

*In dieser Seminararbeit geht es um interne Sicherheitsbedrohungen und wie IT-Sicherheitsmanagement dagegen eingesetzt werden kann. Dabei soll zuerst einmal geklärt werden, was IT-Sicherheitsmanagement ist. Dann geht es um Innentäter und die Möglichkeiten einem Unternehmen von innen zu schaden. Welche Ursachen gibt es für solche Angriffe, wie können diese aussehen und welche Wege können sie nehmen? Danach wird ein Blick auf mögliche Maßnahmen geworfen, die Rahmen des IT-Sicherheitsmanagements ergriffen werden können, um diesen Gefahren zu begegnen. Es folgt eine kurzer Überblick über Werkzeuge und Verfahren, welche die technische Umsetzung ermöglichen sollen. Im Anschluss daran werden die am Anfang ausgearbeiteten Kanäle aus dem Unternehmen noch einmal beleuchtet und ein Lösungsansatz dafür aufgestellt. Schließlich gibt es noch ein kurzes Fazit, in dem auch die Frage behandelt wird, ob ein Unternehmen alle Kraft in die Abwehr von internen Sicherheitsbedrohungen investieren sollte.*

# Inhaltsverzeichnis

## 6.1 Motivation

Mit wachsender Bedeutung von IT-Systemen steigen die Anforderungen an die IT-Sicherheit und den Schutz von Daten. Befragt man IT-Führungskräfte, was ihre größte Sorge in Bezug auf die Sicherheit in ihren Unternehmen ist, so stellt sich oft heraus, dass für sie Insider-Bedrohungen eine große Rolle spielen. Dies ist vor allem bei Unternehmen in der Forschung und Entwicklung der Fall, für die zeitlicher Vorsprung vor der Konkurrenz eine wichtige Rolle spielt. Gerade mittelständische Unternehmen werden in besonderem Maße von Wirtschaftsspionage und Ausspähung, aber auch Erpressung bedroht [2]. Das Motiv dafür ist in vielen Fällen finanzieller Natur. Aber auch Sabotage und der Versuch der Einflussnahme haben in den letzten Jahren für die Angreifer an Bedeutung gewonnen [2].


Abbildung 6.1: Globale Untersuchung von Datenlecks im Jahre 2013 durch INFOWATCH [1]

Fast alle Firmen haben heute ihr eigenes IT-Sicherheitsmanagement. In speziellen IT-Abteilungen werden Regeln und Verfahren aufgestellt um möglichst gut für die Datensicherheit in ihrem Unternehmen zu sorgen. Dabei werden die Informationstechniker zunehmend in die Rolle einer Art Firmenpolizei gedrängt [3]. Für viele Chefs stellen interne Bedrohungen die größte Herausforderung für die Firmensicherheit dar. Das beste IT-Sicherheitsmanagement nützt nicht viel, wenn der Mensch in dem System nicht verlässlich ist.
Der Mensch ist in der Informationstechnik der am ehesten fehlerhafte und störbare Faktor, der außerdem auch noch am schwersten zu kontrollieren ist [4].

Wie also soll man sich vor diesen Bedrohungen schützen? Was tun, wenn der Angreifer in den eigenen Reihen sitzt? Damit beschäftigt sich diese Seminararbeit.

## 6.2 Einleitung

### 6.2.1 IT-Sicherheitsmanagement

Zuerst einmal muss die Frage geklärt werden, was IT-Sicherheitsmanagement überhaupt bedeutet. Laut [5] beschreibt die IT-Sicherheit Strategien, Vorgehensweisen und technische Maßnahmen, die Kommunikation zurechenbar gestalten. Des Weiteren sollen unerlaubte Zugriffe, ungewollte Veränderungen, Diebstahl oder physische Beschädigungen von Informationssystemen und den darin enthaltenen Informationen vermieden werden. Es gibt immer wieder neue Bedrohungen für Informationssysteme. Zum Schutz dieser Systeme muss man sich immer nach den aktuellen Gegebenheiten richten und die unterschiedlichsten Maßnahmen ergreifen um diese Gefahren abzuwehren. IT-Sicherheit ist also kein statischer, sondern ein dynamischer Prozess. Damit ein Unternehmen diesen Prozess steuern kann, benötigt es ein IT-Sicherheitsmanagement. Dazu werden zunächst einmal Sicherheitsziele für das jeweilige Unternehmen aufgestellt. Sicherheitsziele können auf den ersten Blick ganz unterschiedlich aussehen. In Abhängigkeit von den verschiedenen Anwendungsszenarien können sich zum Beispiel folgende Ziele ergeben [6]:

**Banken**:

- Schutz vor vorsätzlicher oder unbeabsichtigter Modifikation von Transaktionen
- Zuverlässige und nicht manipulierbare Identifikation von Kunden
- Schutz persönlicher Identifikationsnummern vor Offenlegung
- Schutz persönlicher Kundendaten

**Verwaltung**:

- Schutz vor Offenlegung sensitiver Informationen
- Realisierung elektronischer Signaturen für Verwaltungsdokumente

**Öffentlicher Netzbetreiber**:

- Beschränkung des Zugriffs auf Managementfunktionen des Netzes nur für autorisierte Betriebskräfte
- Schutz der Verfügbarkeit angebotener Dienste
- Gewährleistung einer konkreten und manipulationssicheren Abrechnung von Dienstnutzungen

- Schutz persönlicher Kundendaten

**Unternehmens- und private Netze**:

- Schutz der Vertraulichkeit von ausgetauschten Daten
- Sicherstellung der Authentizität von Nachrichten

**Alle Netze**:

- Schutz vor externen Eindringlingen

Im Allgemeinen kann man diese Sicherheitsziele aber zusammenfassen. Es handelt sich hier um **Vertraulichkeit**, **Datenintegrität**, **Zurechenbarkeit**, **Verfügbarkeit** und **kontrollierten Zugriff** (Abbildung 6.2).

| | Technische Bedrohungen | | | | | | |
|---|---|---|---|---|---|---|---|
| **Technische Sicherheits-ziele** | Maske-rade | Abhören | Autori-sierungs-verletzung | Verlust oder Modifikation von Information | Fälschen von Information | Abstreiten von Ereignissen | Sabotage (z.B. durch Überlast) |
| Vertraulichkeit | x | x | x | | | | |
| Datenintegrität | x | | x | x | x | | |
| Zurechenbarkeit | x | | x | x | | x | |
| Verfügbarkeit | x | | x | x | | | x |
| Kontrollierter Zugriff | x | | x | | x | | |

Abbildung 6.2: Technische Sicherheitsziele und wie sie bedroht werden

Darauf aufbauend können nun die Sicherheitsmaßnahmen geplant werden. Hierfür eignet sich als nicht unternehmensspezifische Grundlage zum Beispiel der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der an das jeweilige Unternehmen angepasst werden muss. Jede so aufgestellte Maßnahme sollte bewertet werden. Je nachdem, wie gut sie für die aktuelle Bedrohungslage geeignet ist, muss dann über ihren Einsatz entschieden werden. Wenn man sich dafür entscheidet sie einzusetzen, muss selbstverständlich auch ihre Wirkung überwacht werden. Nur so kann man ein möglichst hohes Sicherheitsniveau erreichen. Diese Vorgehensweise wird zum Beispiel im weit verbreiteten Standard ISO/IEC 27001 (IT-Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen) angewendet (Abbildung 6.3).

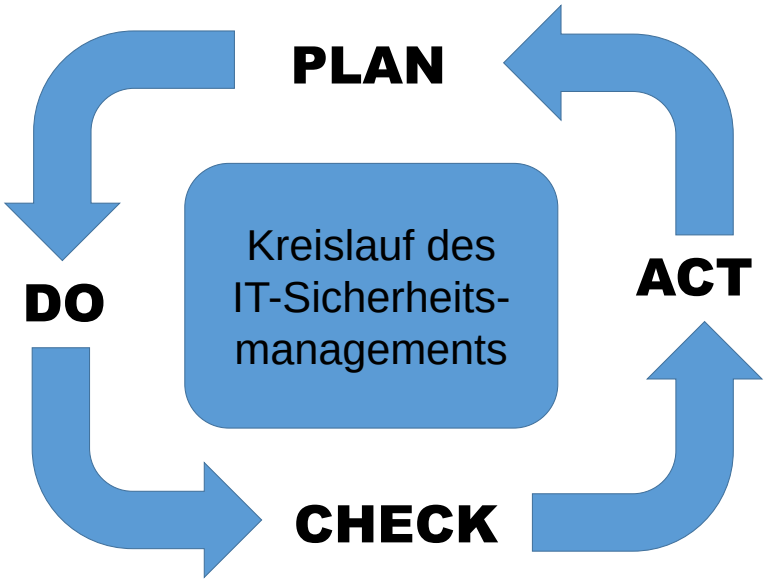


Abbildung 6.3: ISO/IEC 27001

Eine 100 prozentige Sicherheit wird es nie geben. Im IT-Sicherheitsmanagement kommt es deshalb darauf an, immer wieder Risiken anhand der sich stetig ändernden Lage abzuschätzen, Schwachstellen und Sicherheitslücken zu finden und in geeigneter Weise zu schließen.

## 6.3 Innentäter und Kanäle

### 6.3.1 Ursachen und Gründe

Um die Problematik der internen Sicherheitsbedrohungen untersuchen zu können müssen erst einmal deren Ursachen ergründet werden. Warum verletzen Mitarbeiter überhaupt die Sicherheitsrichtlinien ihrer Firmen?

In manchen Fällen mag es einfach nur **Unwissenheit** sein. Es kommt ein neuer Mitarbeiter und dieser wird schlecht in seinen neuen Arbeitsplatz und in die dort geltenden Bestimmungen und Richtlinien eingewiesen. Jetzt könnte man vielleicht sagen, dass die Grundlagen der IT-Sicherheit jedem bekannt sein müssten. Doch man kann nicht voraussetzen, dass alle Mitarbeiter einer Organisation die grundlegenden Prinzipien der IT-Sicherheit verstehen. Im Gegenteil, viel mehr muss angenommen werden, dass sie überhaupt nichts zu dem Thema wissen [7].

Auch **Fahrlässigkeit** und Bequemlichkeit spielen im Umgang mit Sicherheitsrichtlinien eine entscheidende Rolle. Wer kennt nicht die leidige Suche nach einem sicheren Passwort. Gern genommene Kandidaten sind "Passw0rd", oder "Passwort123"[8]. Es ist durchaus menschlich, dass es schwer fällt sich lange und komplizierte Passwörter zu merken. Laut einer Umfrage vom Bundesamt für Sicherheit in der Informationstechnik (BSI[1]) wählen deshalb viele Menschen Namen, Orte und Lebensdaten, die sie sich leicht merken können (Abbildung 6.4). Doch auch die Forderung nach komplexen Passwörtern löst das Problem nicht. Gerade wenn ein Anwender ständig gezwungen ist, sein Passwort zu ändern, neigt er dazu sich dieses aufzuschreiben [7]. Durch diese Fahrlässigkeiten macht man es Angreifern sehr leicht.

Ein weiteres Motiv für Verstöße gegen Sicherheitsrichtlinien könnte auch **Eitelkeit** sein [9]. Mitarbeiter berichten gern in aller Öffentlichkeit oder in offenen Newsgroups von den Errungenschaften ihrer Firma und ihren Vertriebserfolgen. So wollen sie Aufmerksamkeit und Anerkennung für ihren Beruf erhaschen und verbreiten ganz nebenbei Interna, die eigentlich nicht für jedermann Ohren bestimmt sind.

Das BSI weist auch auf die Möglichkeit hin, dass Mitarbeiter durch **Whistleblowing** (vgl. Wikileaks) auf Missstände aufmerksam machen wollen[10]. Sie bringen dann (geheime) Informationen an die Öffentlichkeit und wollen so ihr Unternehmen zu Erklärungen und zum Handeln zwingen.

Verfassungsschutz-Präsident Hans-Georg Maaßen zeigt einen weiteren wichtigen Aspekt auf: **Unzufriedenheit** [9]. Tritt diese dann auch noch in Verbindung mit (externen) finanziellen Anreizen auf, kann es sehr schnell gefährlich werden. Gegeben sei ein Firmennetz, in dem 100 technisch versierte

[1] www.BSI.de


Abbildung 6.4: BSI-Studie: Wie wählen Sie Ihr Passwort normalerweise aus?

Mitarbeiter arbeiten [8]. Wegen finanziellen Schwierigkeiten müssen 20 Mitarbeiter entlassen werden. Wie wahrscheinlich ist es, dass ein Mitarbeiter sich an dem Unternehmen rächen will? Er könnte Server lahm legen, oder seinen Marktwert steigern, indem er Daten für die Konkurrenz stiehlt. Gerade bei Unternehmen in der Forschung und Entwicklung spielt ein zeitlicher Vorsprung zur Konkurrenz eine wichtige Rolle. Umso besser werden hier natürlich Informationen bezahlt, die das eigene Unternehmen befähigen könnten, ein Produkt schneller und günstiger auf den Markt zu bringen. Unzufriedene oder gar frustrierte Angestellte neigen eher als zufriedene Mitarbeiter dazu, Firmengeheimnisse weiterzugeben, oder den eigenen Betrieb zu sabotieren. Ein gekündigter, oder unzufriedener, oder vielleicht *nur* schlecht bezahlter Mitarbeiter der Konkurrenz ist der ideale Angriffspunkt [11]. Er kann auf relevante Daten zugreifen ohne technische Zugriffsbeschränkungen umgehen zu müssen. So kann über ihn von außen Spionage oder gar Sabotage betrieben werden, ohne technische Kniffe anzuwenden und selbst Spuren im System zu hinterlassen. Was könnte einen frustrierten Mitarbeiter mehr befriedigen, als sich an seinem Unternehmen zu rächen und zeitgleich von der Konkurrenz noch gut bezahlt zu werden?

Neben der Unzufriedenheit im Beruf können aber auch belastende Privatumstände, wie Kredite oder Affären, Mitarbeiter in die Fänge der Konkurrenz treiben. Diese Umstände kann man heutzutage sehr leicht zwischen den Zeilen (oder ganz offen) in sozialen Netzwerken erfahren. So macht sich der eine oder andere Angestellte leicht **erpressbar**.

Angriffe aus den eigenen Reihen kann eine Firewall oft nicht entdecken. Wie kann man sich also vor solchen Attacken schützen?

### 6.3.2 Mögliche Angriffe

Um Angriffe entdecken zu können, muss bekannt sein, wie ein Angriff überhaupt aussehen kann. Das BSI unterscheidet hier drei mögliche Angriffsarten[10]:

- Datendiebstahl (Spionage) bzw. Verlust von Daten (Data Leakage)
- Vorbereitung von Folgeangriffen durch Social Engineering
- Sabotage

#### Spionage und Datenverlust

Hat ein Täter Zugriff auf Datenserver, Datenträger oder ganze IT-Systeme, so kann er elektronische Daten entwenden. Aber auch physikalische Dokumente, wie Ausdrucke oder handschriftliches dürfen nicht außer Acht gelassen werden.

#### Social Engineering

Durch soziale Kontakte innerhalb der Firma kann ein Täter herausfinden, wer Ansprechpartner für welche Bereiche ist. Außerdem kann er so erfahren, wie für ihn eigentlich uninteressante Prozesse genau ablaufen. Er könnte beispielsweise an Baupläne oder Rezepte kommen, für die er keine Rechte hat. Zu dem könnte er andere Mitarbeiter dazu missbrauchen fremde Software zu installieren, oder Konfigurationen zu ändern. Möglich wäre auch ein Szenario, in dem ein Täter über seine Kollegen an Schlüssel und Passwörter gelangt.

#### Sabotage

Ist dem Täter Spionage nicht genug, so könnte er auch dazu übergehen, das System zu schädigen. Das kann auf mehrere Arten geschehen. Beispielsweise könnte er Schadsoftware installieren, oder Steuerkomponenten manipulieren.

### 6.3.3 Informationskanäle

Um gegen Sicherheitslücken vorgehen zu können, muss man zuallererst die Wege detektieren, die Angreifer nutzen können.
Informationen können über mehrere Kanäle aus dem Unternehmen fließen. Neben den üblichen Verdächtigen, den **externen Speichermedien** (USB-Sticks, CDs, DVDs, Mobiltelefonen, Festplatten, Speicherkarten, usw.) und **internetbasierten Wegen** (E-Mails, Instandmessager, Peer-to-Peer Netzwerke, usw.), spielen auch **Drucker**, die **Entsorgung von Speichermedien** und die **Datensicherung** von Unternehmen eine wichtige Rolle (vgl. [11])(Abbildung 6.5).

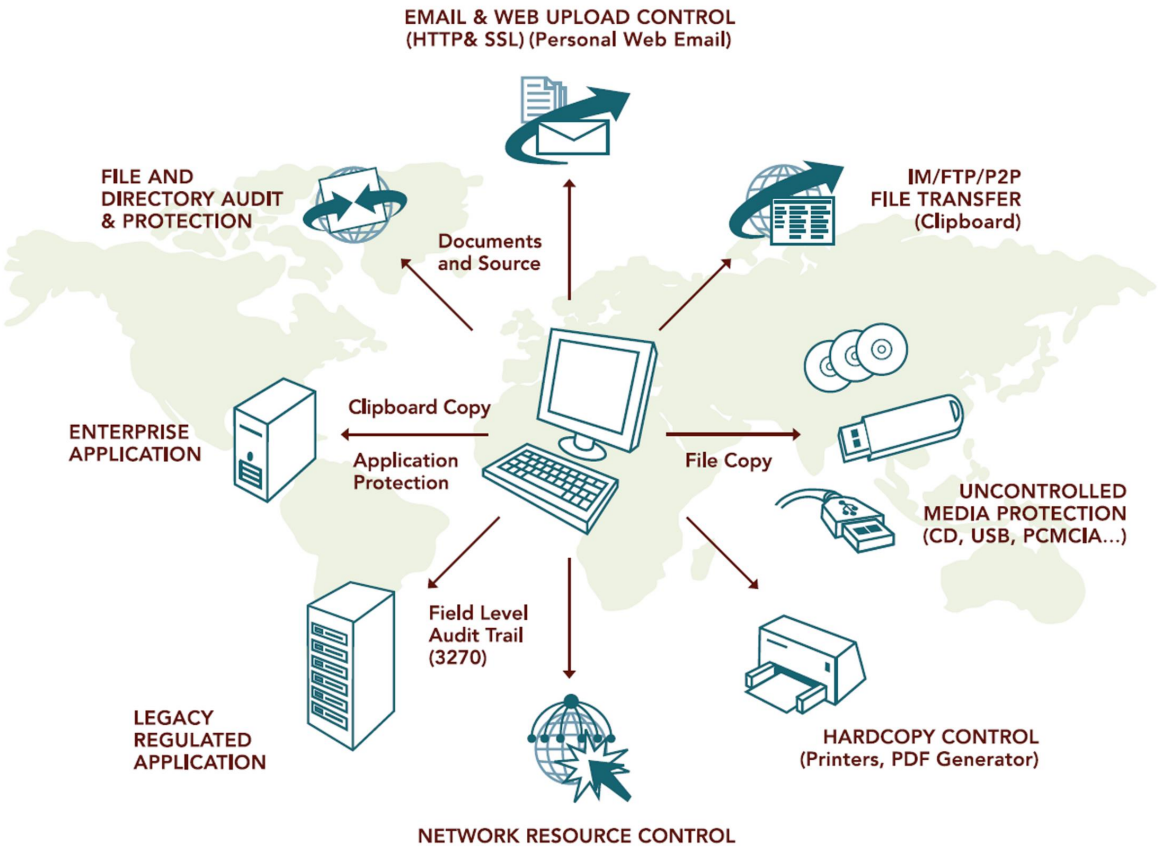


Abbildung 6.5: Datenkanäle aus dem Unternehmen[11]

#### Externe Speichermedien

Die klassischen externen Speichermedien sind USB-Sticks, externe Festplatten, Speicherkarten, MP3-Player, CDs und DVDs. Wie schnell kann man auf sie sogar sehr große Datenmengen verschieben und einfach in der Tasche mitnehmen. Die Gefahr des Datendiebstahls mit externen Speichermedien ist dementsprechend hoch einzustufen (vgl. [11]).

### Internetbasierte Wege

Die Datenmenge, die auf internetbasierten Wegen transportiert werden kann, ist zwar deutlich kleiner als bei externen Speichermedien, trotzdem ist die Gefahr hoch, dass Daten über diese Kanäle (E-Mail, Instant Messenger, Peer-to-Peer Netzwerke, Clouds) das Firmennetz verlassen. E-Mails sind eine weit verbreitete Art Daten auszutauschen. Sie werden in beinahe allen Bereichen verwendet und stehen so fast jedem Mitarbeiter zur Verfügung. E-Mails grundsätzlich zu verbieten ist daher kaum möglich. Auch Instand Messeger könnten für den Datentransfer genutzt werden. Einmal installiert sind sie oft leicht zu bedienen. Dabei sind die Informationen nicht nur dadurch gefährdet, dass sie bei einem unberechtigten Empfänger landen. Viele Messenger verschlüsseln die übertragenen Daten auch nicht. Somit können sie auch während des Transportes unverschlüsselt mitgelesen werden.
Etwas größere Datenmengen können über Tauschbörsen und Clouds transportiert werden. Allerdings ist die Handhabung von Tauschbörsen oft nicht so einfach, wie die der Messenger-Dienste. Meist benötigt man spezielle Software und muss große Dateien in kleinere Pakete aufteilen. Die neue Entwicklung von Internetspeichern und das steigende Angebot an Clouds (zum Teil in Terabyte-Größe) bieten Mitarbeitern eine schnelle und einfache Möglichkeit Unternehmensdaten außerhalb des Firmennetzes zu speichern. Der Zugang kann über Browser, Apps oder andere Programm erfolgen. Fortschreitende technische Entwicklungen und immer größere Bandbreiten erfordern es des Kanal Internet immer wieder neu in den Fokus zu rücken.

### Drucker

Bei heutigen Datenmengen denkt man vielleicht nicht mehr sofort an die Möglichkeit, diese in gedruckter Form zu transportieren. Aber auch das ist durchaus ein Kanal, den ein Angreifer nutzen kann. Abhängig davon, wie umfangreich die Datenmenge ist, kann man die Gefährdung einstufen. Geht es um Größenordnungen, die nicht druckbar sind, ist sie vernachlässigbar. Neben physischen Druckern darf man aber auch den Bildschirmdruck und die virtuellen Drucker nicht vergessen. Mit diesen lassen sich Daten leicht umwandeln und entwenden( vgl. [11]).

### Entsorgung von Speichermedien

Früher oder später müssen Unternehmen ihre Hardware austauschen, weil sie veraltet oder schlicht und ergreifend kaputt ist. Falls sich auf auszutauschenden Speichermedien relevante Informationen befinden, könnten diese bei der unbedachten Entsorgung in den falschen Händen landen( vgl. [11]).

**Datensicherung**

Datensicherung findet heute in fast jedem Unternehmen statt. Dabei sollten die Daten möglichst räumlich getrennt vom Sicherungsort lagern, um bei Katastrophen wie Bränden oder Überschwemmungen nicht auch verloren zu gehen. Prinzipiell eine sehr gute Idee. Gefährlich kann es allerdings werden, wenn die Daten unverschlüsselt gelagert und transportiert werden. Hier besteht dann das gleiche Risiko wie bei externen Speichermedien. Ein Angreifer kann einfach und schnell große Datenmengen entwenden und diese ohne Aufwand sofort verwenden.

## 6.4 Maßnahmen

### 6.4.1 Firmenpolicies

In dem fortwährenden Prozess des IT-Sicherheitsmanagements einer Firma ist es sehr wichtig Vorgaben und Verfahren anzupassen und gut zu dokumentieren. Damit kann den Mitarbeitern eine gewisse Sicherheit im Umgang mit Firmeninterna gegeben werden.
Firmenpolicies regeln was im Umgang mit Daten erlaubt oder verboten ist. Beispielsweise können hier Gegenstände wie Kameras oder Mobiltelefone verboten, oder Richtlinien für den Umgang mit unbekannten Daten festgehalten werden [11].
Auch externe Mitarbeiter sollten zum Einhalten der Firmenpolicies verpflichtet werden [10]. Aber eine reine Dokumentation der Regeln und Policies reicht nicht aus. Das ganze muss auch kontrollierbar und vollstreckbar sein. Schließlich helfen alle Belehrungen, Schulungen und Regeln nichts, wenn man sie nicht überwacht und gegebenenfalls abwandelt und anpasst [7].

### 6.4.2 Organisatorische Maßnahmen

Beruhen die Verstöße gegen IT-Sicherheitsrichtlinien allein auf Unwissenheit oder Fahrlässigkeit, so können sie oft leicht behoben werden. Es sollte auf jeden Fall dafür Sorgen getragen werden, dass Mitarbeiter gut eingewiesen, belehrt und aufgeklärt werden. Des Weiteren können zu besonders heiklen Themen und Bereichen extra Schulungen angeboten werden, die dem Angestellten klar machen, wie wichtig sein Verhalten und seine Vorsicht auf dem Gebiet sind. Gesunder Menschenverstand ist hier sehr wichtig. Der muss aber auch entsprechend sensibilisiert werden [12]. Eine einmalige Schulung reicht dafür meist nicht aus.
Um dem Phänomen des Whistleblowings vorzubeugen, sollte es in jedem Unternehmen eine interne Möglichkeit geben, auf Missstände aufmerksam zu machen[10]. Außerdem empfiehlt das BSI[10] ein Vier-Augen-Prinzip für wichtige Steuerprozesse. Natürlich gibt es überall schwarze Schafe. Man wird niemals *ausschließlich* zuverlässige Angestellte haben. Aber ein Unternehmen sollte stets darauf achten, dass in "den gefährdeten Bereichen, wo sie ihre Kronjuwelen hüten", nur zuverlässige Mitarbeiter eingesetzt werden [9].
Die Bundeswehr beispielsweise überprüft den Hintergrund von Soldaten, die sicherheitsrelevante Dienstposten bekommen sollen. Dabei gibt es drei Sicherheitsstufen(Ü1, Ü2, Ü3), die sich durch die Tiefe der Überprüfung unterscheiden. Besteht der Soldat die Ü1, so bekommt er Zugang zu vertraulich eingestuften Daten. Geheime Daten darf er bei bestandener Ü2 einsehen und streng geheime Daten bleiben den Soldaten mit bestandener Ü3 vorbehalten.

### 6.4.3 Klassifizieren von Daten

Um Daten technisch schützen zu können müssen sie klassifiziert, also in unterschiedliche Vertraulichkeitsstufen eingeteilt werden. Die Klassifikation kann individuell passieren. Zum Beispiel kann eine Unterscheidung in **offen**, **vertraulich**, **geheim** und **streng geheim** stattfinden. So könnten alle Daten, die für Werbung und Pressearbeit genutzt werden in die Vertraulichkeitsstufe offen eingeordnet werden. Als vertraulich eingestufte Daten sind hingegen schon nicht mehr für die Öffentlichkeit gedacht. Daten aus der Stufe geheim sind nicht nur nicht für die Öffentlichkeit gedacht, sondern können bei Offenlegung erheblichen Schaden anrichten. Streng geheim wäre in diesem System die höchste Vertraulichkeitsstufe. Diese Daten können in den falschen Händen schwere Schäden anrichten.
Um Daten sauber klassifizieren zu können muss es möglichst präzise Kriterien geben, die wenig Interpretationsspielraum lassen (vgl. [11] Abschnitt 3.1).

### 6.4.4 Sicherheitsstrategien

Es gibt zwei Sicherheitsstrategien um Unternehmensdaten zu schützen:
**Zugriffskontroll-** und **Informationsflussstrategien**. [11]

#### Zugriffskontrollstrategiene

Durch Zugriffskontrollstrategien wird der Zugang zu Daten eingeschränkt. Damit wird zwar nicht primär der Datenfluss verhindert, aber für die Datensicherheit ist es wichtig, dass nicht jeder Nutzer Zugriff auf *alle* verfügbaren Informationen hat [11].
Ein zentrales Modell der Zugriffskontrolle ist das Konzept des sogenannten Referenzmonitors [6](Abbildung 6.6).

Der Referenzmonitor hat die Aufgabe, für die ihm vorgelegten Zugriffsanfragen anhand der vorher definierten Sicherheitsrichtlinien zu entscheiden, ob der Zugriff gestattet ist, oder nicht. Das Konzept des Referenzmonitors wird in realen Systemen durch einen Zugriffskontrollmechanismus (Access Control Mechanism) implementiert.
Man kann die Kontrollmechanismen in drei Kategorien einteilen [6]:

- Wahlfreie Zugriffskontrolle (Discretionary Access Control)
- Verbindliche Zugriffskontrolle (Mandotory Access Control)
- Rollenbasierte Zugriffskontrolle (Role Based Access Control)

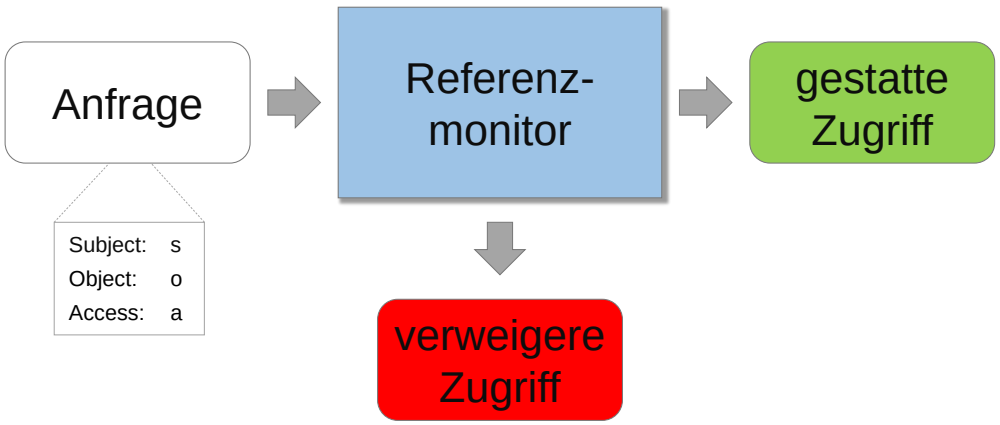


Abbildung 6.6: Konzept des Referenzmonitors[6]

Bei der **wahlfreien Zugriffskontrolle** kann der *Eigentümer* eines Objektes eigenständig über die Zugriffserlaubnis anderer Subjekte entscheiden. Er ist selbst für den Schutz verantwortlich [13].
Die **verbindliche Zugriffskontrolle** bezeichnet alle Vorgänge, die Zugriffsanfragen im Sinne einer zentral festgelegten Menge von Regeln vermittelt [6].
Eine jüngere Entwicklung, welche die beiden anderen Ansätze ergänzt ist die **rollenbasierte Zugriffskontrolle**. Bei diesem Verfahren bekommt jeder Nutzer eine (oder mehrere) konkrete Rolle. Daran ist geknüpft, ob ein Subjekt dieser Rolle mit einer spezifischen Methode auf ein Objekt zugreifen darf, oder nicht. Die Entscheidung wird also nicht mehr auf Grund des Subjekts, sondern auf Grund der Rolle getroffen, die das Subjekt wahrnimmt. Dies vereinfacht die Rechteverwaltung, da man nun nicht mehr jedes Subjekt verwalten muss, sondern nur noch Regeln für Rollen bestimmen muss und diese dann dynamisch dem Subjekt zuweisen kann [6].

Das **Bell-LaPadula Modell**
Das Bell-LaPadula Modell, das hier beispielhaft erklärt werden soll, basiert auf einem dynamischen Zugriffsmatrixmodell. Die Zugriffsrechte werden durch universelle Rechte (*read-only*, *append*, *execute*, *read-write*, *control*) vorgeschrieben (vgl.[14] Abschnitt 6.2.4). *Read-only* berechtigt lediglich zum Lesen eines Objektes. *Append* erlaubt Daten an ein bereits vorhandenes Objekt anzufügen. Um eine ausführbare Datei zu starten benötigt man das *execute*-Recht. Lese- und Schreibzugriff erlaubt das *read-write*-Recht und durch *control* kann man Rechte vergeben bzw. zurücknehmen.
Des Weiteren wird eine geordnete Menge an Sicherheitsklassen erstellt. In diese Sicherheitsklassen werden alle Subjekte und Objekte eingeordnet. Somit ergeben sich unterschiedliche Vertraulichkeitsstufen. Jedes

Element einer Sicherheitsstufe bekommt ein Paar, bestehend aus einer Sicherheitsmarke und einer Menge von Sicherheitskategorien, zugewiesen. Ein Subjekt bekommt eine Sicherheitsstufe (Clearance) und jedes Objekt eine Sicherheitsklassifikation (Classification). Die Clearance eines Subjekts gibt die höchste Classification an, die es einsehen darf.
Im Bell LaPadula Modell gibt es zwei grundlegende Regeln: die **Simple Security Property** und die ***-Property**(Abbildung 6.7).

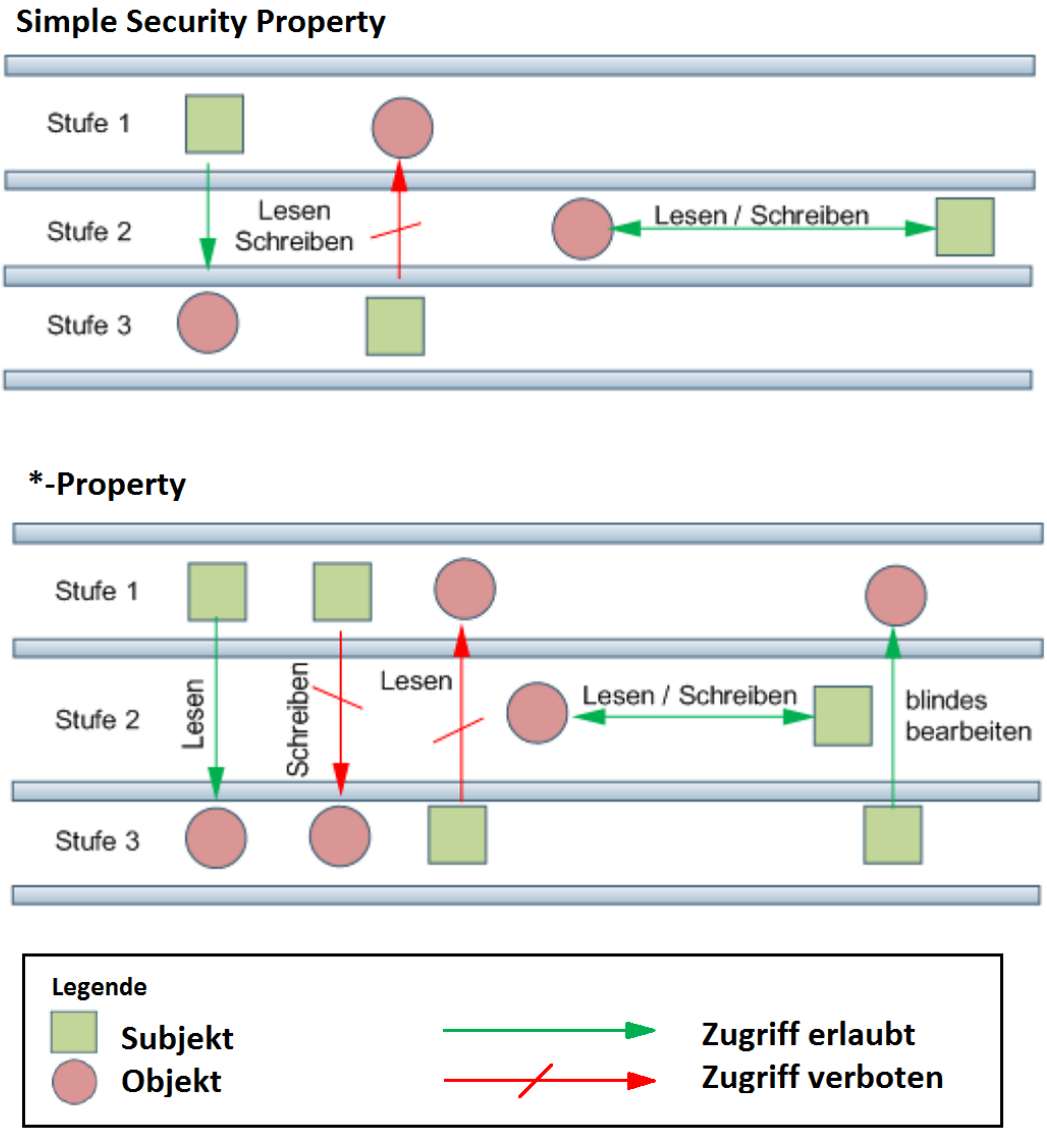


Abbildung 6.7: Die Simple Security Property und die *-Property[11]

Durch die Simple Security Property wird ein Lesen von Objekten einer höheren Sicherheitsstufe verhindert (*No-Read-Up Policy*). Trotzdem ist eine Überführung von einer höheren Sicherheitsstufe in eine niedrigere immer noch möglich (vgl.[11]). So kann beispielsweise ein Mitarbeiter ein Dokument einfach in einer niedrigeren Sicherheitsstufe erstellen, um so den Umgang (aber auch den Missbrauch) zu vereinfachen. Diese Si-

cherheitslücke wird durch die *-Property geschlossen. Durch diese Regel kann man Objekte nicht mehr in eine niedrigere Geheimhaltungsstufe überführen (*No-Write-Down Policy*). Folglich kann ein Subjekt nur noch Objekte für seine oder eine höhere Stufe erstellen. Das hat allerdings zur Folge, dass ein Subjekt ein Objekt einer höheren Sicherheitsstufe erstellen kann und diese im Anschluss selbst nicht mehr lesen kann (Simple Security Property). Damit ist die Datenintegrität nicht mehr gegeben. Erstellt zum Beispiel ein Mitarbeiter ein Objekt mit wichtigen Informationen für seinen Vorgesetzten (in einer höheren Ebene), so kann er selbst dieses Objekt nicht mehr einsehen. Er kann das Objekt aber immer noch ändern. Dabei ist er durch die No-Read-Up Policy gewissermaßen blind. Trotzdem kann er so Informationen in höheren Sicherheitsstufen verfälschen. Das Bell-LaPadula Modell garantiert also lediglich die Vertraulichkeit von Daten, nicht aber deren Integrität (vgl.[11]).

Weitere Zugriffskontrollmodelle sind unter anderem das **BiBa-Modell** oder auch das **Chinese-Wall-Modell**(erklärt in [11]).

Um Zugriffskontrollen noch ein bisschen sicherer zu machen, empfiehlt das BSI[10] die Verwendung von Time-Out-Mechanismen und passwortgeschützten Bildschirmschonern. So kann ein Unberechtigter nicht einfach am Rechner eines anderen Mitarbeiters (mit möglicherweise mehr, oder anderen Rechten) arbeiten, während dieser gerade nicht am Arbeitsplatz ist.
Zugriffskontrollstrategien können also helfen zu reglementieren, wer wie und unter welchen Umständen auf welche Daten zugreifen kann. Das sichert die Datenvertraulichkeit. Doch wie bereits oben erwähnt, schützt das allein nicht vor ungewolltem Datenabfluss. Mit Zugriffskontrollen wird nur sichergestellt, dass kein unautorisierter Zugriff auf bestimmte Daten erfolgt, aber nicht, *was* mit den im Objekt enthaltenen Informationen geschehen darf. Angreifer, die legitimen Zugriff auf (vertrauliche) Daten besitzen, können also nur durch Zugriffskontrollen nicht gestoppt werden. Diese Sicherheitslücke sollen Informationsflussmodelle schließen. Sie sollen das Weitergeben der Daten durch Personen mit Zugriffsrechten verhindern. [11]

### Informationsflussstrategien

Bei der **Informationsflussstrategie** steht die *Informations*sicherheit im Vordergrund. Die Modelle beschreiben zulässige und unzulässige Informationskanäle zwischen Subjekten(vgl. [14] Abschnitt 6.3).

Das **Verbandsmodell**
Das Verbandsmodell, als ein Beispiel für Informationsflussmodelle verallgemeinert den oben beschriebenen Bell-LaPadula Ansatz. Das charakteristische am Verbandsmodell ist, dass Beschränkungen für den Informationsfluss unabhängig von den Objekten, welche die Informationen repräsentieren, festgelegt sind. Das bedeutet, dass es Vorschriften

für zulässige und unzulässige Informationskanäle gibt, die den Umgang mit Informationen reglementieren (vgl. [11]). In diesem Modell gibt es verschiedene Sicherheitsstufen. Genau wie im Bell-LaPadula Modell bekommen sowohl die Objekte, als auch die Subjekte eine Sicherheitsmarke. Daten können nur innerhalb einer Sicherheitsstufe oder aufwärts fließen. Stufenabwärts oder auch zwischen Stufen, für die keine Beziehung festgelegt wurde, dürfen keine Informationen ausgetauscht werden. Niedrig eingestufte Informationen können also unbeschränkt fließen (vgl. [14] Abschnitt 6.3). Es können auch einzelne abweichende Informationsflüsse definiert werden. Hieraus ergibt sich aber auch ein Nachteil des Modells. Für jede Sicherheitsstufe müssen die Informationsflüsse definiert werden. Um eine detaillierte Definition aufzustellen, müssen daher viele Sicherheitsstufen festgelegt werden. Dies hat einen hohen Verwaltungsaufwand zur Folge (vgl. [11]). Außerdem sind die Sicherheitsklassifikationen im Verbandsmodell relativ unflexibel. Im Allgemeinen findet eine statische Einstufung von Objekten und Subjekten zu einer Sicherheitsstufe statt. Niedrig eingestufte Subjekte haben oft so wenig Rechte, dass sie ohne Zugriff auf höher eingestufte Objekte nicht mehr vernünftig arbeiten können. Als einfache Lösung werden diese Subjekte dann folglich höher eingestuft als erlaubt und haben somit mehr Rechte, als ihnen eigentlich zustehen.

Weitere hier nicht näher erklärte Informationsflussmodelle sind beispielsweise das **Modell von Sutherland**[15] oder das **Restrictiveness-Modell**[16] von McCullough.

### 6.4.5 Kryptografie

Kryptografie sichert uns die **Vertraulichkeit**, **Integrität**, **Authentizität** und **Zurechenbarkeit** von Daten. Mit ihr kann man Daten ver- und entschlüsseln. Somit sind sie für Dritte nicht mehr im Klartext zu lesen. Das sichert die Vertraulichkeit von Informationen. Kryptografische Verfahren können außerdem zeigen, dass Daten nicht nachträglich verändert wurden. Das ist beispielsweise für Transaktionen sehr wichtig. So kann die Datenintegrität erhalten werden. Des Weiteren kann der Absender eindeutig identifiziert werden. So erhält man Aufschluss über seine Identität und es garantiert seine Authentizität. Außerdem sind Informationen somit eindeutig zurechenbar. Vor allem bei Datensicherung und -austausch sind kryptografische Verfahren dringend zu empfehlen. Hier sind Informationen am gefährdetsten. Unverschlüsselte vertrauliche Daten können in den falschen Händen großen Schaden anrichten. Durch Kryptografie kann diese Gefahr abgewendet werden.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI[2]) gibt einen Leitfaden zur Entwicklung eines Kryptokonzepts (M 2.161) heraus.

[2] www.BSI.de

Werden Zugriffs- und Informationsflussstrategien in einem Unternehmen implementiert, wichtige Daten verschlüsselt und durch organisatorische Maßnahmen dafür Sorge getragen, dass möglichst nur zuverlässige Leute Zugang zu den empfindlicheren Informationen in hohen Sicherheitsschichten haben, so macht man es internen Angreifern schon sehr schwer. Trotzdem kann man damit allein die Datenkanäle aus einem Unternehmen nicht schließen. Dafür müssen technische Werkzeuge eingesetzt werden.

## 6.5 Spezielle Werkzeuge und Verfahren

Im Folgenden sind verschiedene Systeme und Verfahren beschrieben, die dazu dienen können Sicherheitslücken zu erkennen und zu schließen.

### 6.5.1 Virenschutz

Um sich vor Sabotageangriffen durch Schadsoftware zu schützen, ist es unbedingt erforderlich eine Antivirensoftware auf seinem System zu installieren. Laut BSI[17] haben sich Programme, die IT-Systeme nach sämtlicher bekannter Schadsoftware durchsuchen, in der Vergangenheit am besten bewährt. Solche Software prüft beispielsweise bei jedem Datenzugriff und jeder eingehenden oder ausgehenden Mail, ob bekannte Viren vorhanden sind. Hierfür ist das Aktualisieren der Datenbank sehr wichtig. Nur so können auch neue Viren entdeckt werden.
Außerdem empfiehlt es sich regelmäßig das gesamte System zu überprüfen. So kann auch Schadsoftware gefunden werden, die beim letzten Zugriff noch nicht bekannt war.
Das BSI bietet eine Hilfestellung zur Auswahl eines geeigneten Viren-Schutzprogramms (M 2.157).

### 6.5.2 Digital Rights Management

Mit Digital Rights Management (DRM) kann die Nutzung von Daten kontrolliert werden. Es wurde ursprünglich erfunden, um unerlaubten Zugriff auf urheberrechtlich geschützte Dateien zu verhindern. Dabei ging es hauptsächlich um Video- und Audiodateien. Aber auch eBooks, PDFs oder Officedateien können mit DRM geschützt werden. Beispielsweise kann es bei einem PDF bewirken, dass Inhalte nicht kopiert oder gedruckt werden können, oder bei einem Video dafür sorgen, dass es höchstens drei Mal abspielbar ist (z.B. Online-Videothek)(vgl. [11]).
Der Vorteil dieses Verfahrens ist, dass geschützte Informationen nur auf Systemen verwendet werden können, die ein DRM einsetzen. Somit kann einer unautorisierten Nutzung vorgebeugt werden. DRM reglementiert jedoch nur den Zugriff auf Daten, nicht aber den Datenfluss (vgl. [11]).

### 6.5.3 Data Leakage Prevention

Data Leakage Prevention Systeme (DLP-Systeme) haben die Aufgabe Firmendaten vor ungewolltem Abfluss zu schützen. Es geht hierbei also nicht darum, das System zu schützen, sondern die darin enthaltenen sensiblen Daten. Dafür müssen sowohl technische als auch organisatorische Maßnahmen

getroffen werden. Es gibt host- und netzwerkbasierte Data Leakage Prevention Systeme.

#### Hostbasierte Data Leakage Prevention Systeme

Im hostbasierten DLP-System gibt es einen Softwareagent, der bestimmte Regeln im Umgang mit Daten überwacht und durchsetzt. Diese Regeln sind zentral auf einem Managementserver gespeichert. Auf jedem Client (Rechner, Notebook, usw.) des Systems befindet sich ein Agent. Er greift über eigene Kernelmodule in das Betriebssystem ein und kann so alle Systemvorgänge überwachen. Dazu gehört auch die Überwachung aller an den Rechner angeschlossenen Datenträger. Diese Überwachung nennt man auch Endpoint-Security (vgl. [11] Abschnitt 4.2). Hostbasierte DLP-Systeme sind meist das Mittel der Wahl, da sie mehr Kanäle überwachen können, als netzwerkbasierte.
Der Agent kann auf Verstöße gegen Regeln auf unterschiedliche Weisen reagieren. *Logging* sorgt beispielsweise dafür, dass Regelverstöße im System gesichert werden, um zu einem späteren Zeitpunkt noch ausgewertet werden zu können. Außerdem kann er eine *Warnung* speichern. Häufen sich diese Warnungen gibt es die Möglichkeit bei dem IT-Sicherheitsverantwortlichen einen *Alarm auszulösen*. Des Weiteren kann der Nutzer durch ein *Dialogfeld* auf seinen Verstoß aufmerksam gemacht werden. Nicht alle DLP-Systeme bieten auch alle der hier genannten Möglichkeiten. Aber jedes gute DLP-System sollte in der Lage sein eine *Blockierung des Datentransfers* auszulösen (vgl. [11] Abschnitt 4.1.2).

#### Netzwerkbasierte Data Leakage Prevention Systeme

Netzwerkbasierte DLP-Systeme durchsuchen den Netzwerkverkehr nach auffälligen Mustern. Sie können so das Netzwerk als Informationskanal überwachen. Andere Kanäle sind diesen Systemen verborgen. Der Nutzen ist laut [11] nur gering, da lediglich unverschlüsselte Inhalte überwacht werden können. Sobald die Informationen verschlüsselt sind greift das System nicht mehr. Anders als bei der hostbasierten Variante geht es hier nur um einen inhaltsbasierten Ansatz. Also müssen die Suchmuster für illegale Aktivitäten schon vorher bekannt sein. Die Erstellung von inhaltsbasierten Regeln ist sehr aufwändig. Somit steigt bei netzwerkbasierten DLP-Systemen der Administrationsaufwand im Vergleich zu hostbasierten DLP-Systemen an.

### 6.5.4 ADAMS - insider threat detection

Sieht man in den Nachrichten Berichte über Selbstmordattentäter oder Amokläufe, so kommt oft die Frage auf, wie das passieren konnte. Schaut

man sich dann den Hintergrund der Täter an, so ergibt sich meist ein eindeutiges Bild. Doch in der Regel erkennt man diese Auffälligkeiten erst im Nachhinein.
Hier setzt ADAMS (=Anomaly Detection at Multiple Scales) an. Es ist ein Verfahren, das dabei helfen soll Anomalien in großen Datenmengen zu erkennen. Das große Ziel ist es Auffälligkeiten zu erkennen und daraus abzuleiten, ob daraus zukünftig ein Zwischenfall entstehen könnte[18].
Das Projekt ADAMS wird von der Defense Advanced Research Projects Agency (DARPA) und dem Army Research Office finanziert. Ein Forscherteam (Oregon State University, University of Massachusetts, Carnegie Mellon University) versucht eine Software zu erstellen, die mit einer Reihe von Algorithmen die Onlineaktivitäten von Personen überwacht[19]. Dazu zählen E-Mail-Verkehr, Dateizugriffe und Sofortnachrichten. Die Datenmengen die dabei entstehen liegen im Terabyte- und Petabytebereich. Um dieses Volumen bearbeiten zu können braucht man leistungsfähige Algorithmen und Hochleistungsrechner. Zu erkennen was *normal* ist und was nicht ist eine große Herausforderung für die Forscher.

## 6.6 Kanalbasierte Lösungsansätze

### 6.6.1 Externe Speichermedien

Durch Vorkehrungen wie Zugriffskontroll- und Informationsflussstrategien allein lässt sich die Gefahr des Informationsabflusses über externe Speichermedien nicht eindämmen. Es müssen auch hardwaretechnische Maßnahmen ergriffen werden. An den physikalischen Schnittstellen (USB, SATA, usw.), die ein externes Medium benötigt, kann man sehr gut ansetzen. Entfernt oder deaktiviert man diese Schnittstellen, ist ein Datenfluss unmöglich. Somit kann man die möglichen Wege aus dem System zahlenmäßig beschränken.
[11] verweist auch auf die Möglichkeit der Nutzung von *Thin Clients*.
Thin Clients sind lediglich Schnittstellen für Mitarbeiter. Die eigentliche Datenverarbeitung und -sicherung passiert in Rechenzentren. Ein Mitarbeiter kann sich an jedem beliebigen Thin Client im Unternehmen schnell anmelden und greift wieder auf dieselben Daten zurück. So müssen und können (bei entsprechender Konfiguration) Daten nicht mehr extern gespeichert werden. Auf diese Weise ist es praktisch unmöglich, dass die Daten verloren gehen (vgl. [20]).

### 6.6.2 Internetbasierte Wege

Wie in 1.3.3 bereits angesprochen ist es nahezu unmöglich E-Mails in Unternehmen ganz zu verbieten. Um dafür Sorge zu tragen, dass trotzdem keine Daten illegal verschickt werden, stellen manche Firmen extra Mitarbeiter ein, die ausgehende E-Mails lesen. Allerdings geht das nur, wenn die Mails nicht verschlüsselt sind. Es besteht keine Kontrollmöglichkeit, wenn die Mails verschlüsselt sind (vgl. [11]). Sind die Mails nicht verschlüsselt, kann ein DLP-Agent sowohl den Inhalt, als auch die Klassifikation der Anhänge prüfen. So kann er entscheiden, ob der Versand der Mail erlaubt oder blockiert wird. Peer-to-Peer-Anwendungen und Instand Messenger können über Layer-7-Firewalls blockiert werden.

### 6.6.3 Drucker

Da Daten nicht nur in virtueller Form, sondern auch gedruckt aus dem Unternehmen entwendet werden können, müssen auch dagegen Vorkehrungen getroffen werden. Hier kann ein hostbasiertes Data-Leak-Prevention-System (DLP-System) helfen. Es kann überwachen, welche Daten gedruckt werden. Um entscheiden zu können, ob ein Druckauftrag rechtens ist, oder nicht, nutzt ein DLP-Agent die Klassifizierung der Daten [11].

### 6.6.4 Entsorgung von Speichermedien

In einem Unternehmen muss ab und an veraltete oder kaputte Hardware entsorgt werden. Sind alle Daten auf den ausgemusterten Datenträgern verschlüsselt, müssen keine weiteren Vorkehrungen getroffen werden. Wenn jemand diese Speichermedien in die Hand bekäme, könnte er damit ohne weiteres nichts anfangen[11]. Befinden sich darauf jedoch unverschlüsselte Daten, müssen die Datenträger vor dem Entsorgen für Angreifer unbrauchbar gemacht werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt einen *Überblick über Methoden zur Löschung und Vernichtung von Daten* zur Verfügung. Dieser Maßnahmenkatalog (M 2.433) hilft in Verbindung mit einer *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*(ebenfalls BSI, M 2.167) unter anderem bei der Vernichtung von sensiblen Daten auf Festplatten mit magnetischem Datenträger, Halbleiterfestplatten, optischen Datenträgern und flüchtigen und nichtflüchtigen Halbleiterspeichern.

### 6.6.5 Datensicherung

Die meist externe Lagerung der Daten, aber auch der Transport zum Sicherungsort kann gefährlich sein. Werden die Daten beispielsweise unverschlüsselt gelagert und transportiert, braucht ein Angreifer nur das Sicherungsmedium stehlen und besitzt dann sofort die unverschlüsselten Informationen. Hier kann einzig und allein die Kryptografie helfen[11]. Sollte der Dieb dann das Sicherungsmedium an sich nehmen, kann er die Daten nicht mehr ohne weiteres auslesen.

## 6.7 Fazit und Ausblick

Der wirtschaftliche Schaden, der jedes Jahr durch Innentäter angerichtet wird ist enorm. Dabei können die Ursachen ganz unterschiedlich gelagert sein und durch einfache Maßnahmen oft leicht behoben werden. Organisatorische und technische Maßnahmen ermöglichen es heute, Systeme vor äußeren, aber auch inneren Angriffen zu schützen. Interne Angreifer können erkannt und in ihrer kriminellen Arbeit gestört werden. Technische Hilfsmittel können dabei unterstützen die Sicherheitsziele Vertraulichkeit, Datenintegrität, Zurechenbarbeit, Verfügbarkeit und kontrollierten Zugriff so gut wie möglich zu erreichen.

Doch es sollte immer bedacht werden, je sicherer ein System gestaltet werden soll, je mehr Passwörter, Zugangsberechtigungen oder Sicherheitsebenen vor relevante Informationen geschaltet werden, desto schwieriger wird die Arbeit mit dem System. Zu viel Sicherheit kann dazu führen, dass Systeme nicht mehr effektiv genutzt werden können[5]. Ständiger technischer Fortschritt und gesellschaftliche Akzeptanz von kriminellen Gruppen (z.B. Anonymous) bedingen es technische Sicherheitssysteme weiterzuentwickeln, um entsprechenden Bedrohungen voraus zu sein.
Auch die beste Technik stößt irgendwann an ihre Grenzen. Das beste Sicherheitssystem wird nicht verhindern können, dass ein Mitarbeiter sich interessante Daten merkt oder gar einen Stift zur Hand nimmt und aufschreibt.
Ein Unternehmen sollte im eigenen Interesse, aber auch im Interesse seiner Angestellten und Kunden dafür Sorge tragen, dass Innentätern möglichst wenig Möglichkeiten zur Sabotage und Spionage bleiben. Aber die Hauptaufgabe des Unternehmens sollte dabei nicht aus den Augen verloren werden. Sicherheit engt immer auch ein. Zu viel Sicherheit kann eine lähmende Wirkung haben und so auch schaden. Bedrohungen müssen abgewehrt werden, aber nicht mit aller Kraft.

## 6.8 Glossar

**Abhören**
Eine Instanz liest eine Information, die eigentlich nicht für sie bestimmt ist. [6]

**Autorisierungsverletzung**
Eine Instanz nutzt Dienste oder Ressourcen, die sie eigentlich nicht nutzen sollte.

**Bedrohung**
Eine Bedohung in einem Kommunikationsnetz ist ein potentielles Ereignis beziehungsweise eine Reihe von Ereignissen, die zur Gefährdung eines oder mehrerer Sicherheitsziele führt. [6]

**Datenintegrität**
Es muss möglich sein, unbeabsichtigte oder vorsätzliche Datenänderungen zu erkennen. Hierfür muss der Urheber eindeutig und nicht manipulierbar identifizierbar sein [6]

**Datenleck** (vertrauliche Daten)
unter dem Datenleck (vertrauliche Daten) verstehen wir die Handlung bzw. Untätigkeit einer Person, die einen rechtmäßigen Zugang zu vertraulichen Information hat, die (die Handlung) den Verlust der Kontrolle der Information bzw. die Nichteinhaltung der Vertraulichkeit dieser Information zur Folge hat. [1]

**Denial-of-Service** (DoS)
siehe Sabotage

**IT-Sicherheit**
Strategien, Vorgehensweisen und technische Maßnahmen, die Kommunikation zurechenbar gestalten sowie den unerlaubten Zugriff, ungewollte Veränderungen, Diebstahl oder physische Beschädigungen von Informationssystemen und den darin enthaltenen Informationen vermeiden soll. [5]

**Informationsflussmodell**
Bei einem Informationsflussmodell steht die Informationssicherheit im Mittelpunkt. Die Modelle beschreiben zulässige und unzulässige Informationskanäle zwischen Subjekten. [14]

**Maskerade**
Eine Instanz gibt vor, die Identität einer anderen Instanz zu haben. [6]

**Objekt**
IT-Systeme speichern und verarbeiten Informationen. Die Information ist aber ein Abstraktum, das in Form von Daten bzw. Datenobjekten repräsentiert wird. Informationen und die Objekte, die sie repräsentieren, sind schützenswerte Güter eines Systems. [14]

**Sabotage**
Jede Aktion, die zum Ziel hat, die Verfügbarkeit oder korrekte Funktion von Diensten oder Systemen zu reduzieren. Im englischsprachigen Raum werden diese Angriffe mit dem Begriff Denial-of-Service (DoS) bezeichnet. [6]

**Sicherheitsrichtlinie**
Die Sicherheitsrichtlinie (Security Policy) eines Systems definiert die Bedingungen, unter denen Zugriffsanfragen von Subjekten, die mit spezifischen Aktionen auf bestimmte Objekte zugreifen möchten, durch die Referenzmonitor-Funktionalität des Systems entschieden und durchgesetzt werden. [6]

**Sicherheitsziele**
Im Allgemeinen können bei Kommunikationsnetzen die folgenden technischen Sicherheitsziele unterschieden werden: Vertraulichkeit (Confidentiality), Datenintegrität (Data Integrity), Zurechenbarkeit (Accountability), Verfügbarkeit (Availability), Kontrollierter Zugang (Controlled Access) [6]

**Spionage**
Tätigkeit für einen Auftraggeber oder Interessenten, besonders eine fremde Macht, zur Auskundschaftung militärischer, politischer oder wirtschaftlicher Geheimnisse.

**Subjekt**
Die Benutzer eines Systems und alle Objekte, die im Auftrag von Benutzern im System aktiv sein können, wie z.B. Prozesse, Server und Prozeduren, werden als die Subjekte eines Systems bezeichnet. [14]

**Verfügbarkeit**
Die in einem System realisierten Dienste sollen verfügbar sein und korrekt funktionieren. [6]

**Vertraulichkeit**
Übertragene oder gespeicherte Daten oder Details sollen nur berechtigten Instanzen bekannt werden. [6]

**Zugriff** (kontrollierter)
Nur autorisierte Instanzen sollen auf bestimmte Dienste und Daten zugreifen können. [6]

**Zugriffskontrollstrategie**
Eine Zugriffskontrollstrategie ist ein Entscheidungsverfahren, das angibt, ob ein Subjekt s in einer bestimmten Situation t eine Operation r auf einem Objekt o ausführen darf. [21]

**Zugriffskontrolle**
Der Begriff Zugriffskontrolle (Access Control) bezeichnet den Prozess der Vermittlung zwischen den Anfragen von Subjekten eines Systems auf bestimmte Objekte in einer spezifischen Art und Weise, das heißt mit einer spezifischen Aktion, zuzugreifen. Hierbei besteht die Hauptaufgabe der Zugriffskontrolle

darin, auf der Grundlage einer definierten Sicherheitsrichtlinie (Security Police) jeweils zu entscheiden, ob ein bestimmter Zugriff gestattet werden kann, und diese Entscheidung durchsetzt. [6]

**Zugriffskontrollsystem**
Das Zugriffskontrollsystem ist ein Teilsystem des Computersystems, das die Ausführung von Operationen auf im System enthaltene Objekte erlauben oder verbieten kann. Die Entscheidung des Zugriffskontrollsystems hängt dabei von der aktuellen Zugriffskontrollstrategie ab. [21]

**Zurechenbarkeit**
Es muss möglich sein, die für bestimmte Ereignisse verantwortliche Instanz zu identifizieren [6]

# Literaturverzeichnis


[1] Analysezentrum InfoWatch. *Globale Untersuchung von Datenlecks im Jahre 2013*, Analysezentrum InfoWatch, 2014.

[2] Bundesamt für Sicherheit in der Informationstechnik. *Fokus IT-Sicherheit*, Bonn Juli 2013.

[3] Buxton, Ima. *IT in der Verantwortungsfalle*, computerwoche, 13.04.2011.

[4] Dierstein, Rüdiger. *Sicherheit in der Informationstechnik*, Informatik-Spektrum, 2004.

[5] Laudon, Kenneth c., Laudon, Jane P., Schoder, Detlef. *Wirtschaftsinformatik - Eine Einführung*, Pearson Studium, München 2006.

[6] Schäfer, Günter. *Netzsicherheit, 2.,aktualisierte und erweiterte Auflage*, dpunkt.verlag GmbH, Heidelberg 2014.

[7] Beaver, Kevin. *Grundlagen der IT-Sicherheit, die Ihre Firma bereits kennen sollte*, searchsecurity.de.

[8] Linten,M. ,Schemberg,A. ,Surendorf,K.. *PC-Netzwerke, Das umfassende Handbuch*, Galileo Press, Bonn 2013.

[9] *Geheimdienst warnt vor frustrierten Angestellten*, Spiegel, 03.07.2014.

[10] Bundesamt für Sicherheit in der Informationstechnik. *Industrial Contol System Security - Innentäter*, 13.05.2013.

[11] Kasparick, Hannes. *Data Leakage Prevention*, Hagenberg 2008.

[12] *IT-Sicherheitstraining und interne Bedrohungen*, searchsecurity.de.

[13] Brüssau, K.. *Modellierung sicherheitskritischer Systeme mit UML*, Testbuch-Verlag, Hamburg 2005.

[14] Eckert, Claudia. *IT-Sicherheit, Konzepte - Verfahren - Protokolle*, Oldenbourg Wissenschaftsverlag GmbH, München 2012.

[15] Sutherland, D.. *A model of Information*, 9th National Computer Security Conference, September 1986.

[16] McCollough, D.. *A Hookup Theorem for Multilevel Security*, IEEE Transactions on Software Engineering, 1990.

[17] Bundesamt für Sicherheit in der Informationstechnik. *M 4.3 Einsatz von Viren-Schutzprogrammen*, 2013.

[18] Defense Advanced Research Projects Agency. *Anormaly Detection at Multiple Scales (ADAMS)*, 22.10.2010.

[19] Kenyon, Henry.*DARPA program seeks early detection of insider threats*, defensesystem.com 17.11.2011

[20] Handelsblatt. *Flexibler IT-Arbeitsplatz – Welche Computer-Lösung ist sicher und günstig?*, http://www.handelsblatt.com 28.08.2014.

[21] Stiemerling, Oliver, Won, Markus, Wulf, Volker. *WIRTSCHAFTSINFORMATIK, 42. Jg., Nr. 4*, Bonn 2000.

[22] Bitkom. *Kompass der IT-Sicherheitsstandards*, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2009.

[23] Rieger, Holger, Schoolman, Jürgen. *Praxishandbuch IT-Sicherheit*, Symposion Publishing GmbH, Düsseldorf 2005.

[24] Bundesamt für Sicherheit in der Informationstechnik. *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 29.12.2013

# Kapitel 7

# Kommunikationsstrukturen und Vorgehen von Hacktivisten

*Thomas Salwasser*

*Die Technologie schreitet immer weiter voran. Computer werden immer schneller, bekommen stets neue Funktionen und sind in der heutigen Welt nicht wegzudenken. Doch mit diesem Fortschritt steigt auch das Risiko, Opfer von Internetkriminalität zu werden. Diese Problematik rückt mehr und mehr in den Vordergrund für Unternehmen, Behörden, aber auch für den Privatnutzer. Denn es gibt mittlerweile unzählige Gruppierungen von Hackern mit unterschiedlichsten Interessen, die im Handumdrehen Sicherheitslücken aufspüren und diese ausnutzen, um an empfindliche Daten heran zu kommen. Einige von ihnen teilen ihre Vorhaben der Allgemeinheit mit, um Aufmerksamkeit von der Öffentlichkeit zu erhalten, andere agieren im Hintergrund. Doch wie kommunizieren Hacktivisten untereinander und mit der Welt? Welche Mittel und Wege nutzen sie, um ihr Ziel zu erreichen? Was wollen sie erreichen und für wen? Mit diesen Fragen werde ich mich in dieser Seminararbeit auseinandersetzen.*

# Inhaltsverzeichnis

## 7.1 Einleitung

> "Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist." [1]

Die Anzahl der heutzutage agierenden Hacktivisten ist enorm groß. Täglich geschehen Angriffe auf verschiedenste Institutionen und auch der normale Bürger ist im Internet einer ständigen Gefahr ausgesetzt, Opfer der Cyberkriminalität zu werden. Den wenigsten ist dabei bekannt, wie Hacktivisten dabei vorgehen und wie diese organisiert sind, weshalb viele Angriffe nicht einmal bemerkt werden oder erst dann, wenn der Angriff bereits erfolgreich war. Dazu bedienen sich solche Gruppierungen einer Vielzahl von Angriffstechniken, wie z.B. *SQL-Injections*, *Website defacement* oder *DoS-Attacken*. Angestrebte Ziele können politischer oder wirtschaftlicher Natur sein oder lediglich der Freude an der Zerstörung entstammen. Einige Gruppierungen streben nach Aufmerksamkeit und berichten auf Webseiten oder sozialen Netzwerken über deren Aktivitäten und den damit verbundenen Forderungen und Meinungen. Andere möchten nicht erkannt oder bemerkt werden, um im Verborgenen zuzuschlagen. Deshalb ist über viele Hacktivisten sehr wenig bekannt. Auch die Struktur ist von Gruppe zu Gruppe unterschiedlich. Während *Anonymous* keine hierarchischen Strukturen und keine festen Mitglieder hat, gibt es bei der *GNAA*(Gay Nigger Association of America) einen Präsidenten.

In dieser Seminararbeit werden zunächst die verschiedenen Arten von Hackern aufgeführt, sowie der Ursprung des Hacktivismus beschrieben. Außerdem wird eine mögliche Einteilung von Hackern in Gruppen dargelegt. Darauf folgt eine Beschreibung über die Vorgehensweisen von Hacktivisten in Kapitel 7.3. Die am häufigsten verwendeten Angriffsarten werden ebenfalls aufgelistet und erklärt. Das darauf folgende Kapitel beschäftigt sich mit einigen Medienwirksamen Gruppierungen der Hackerszene. Unter anderem werden hier Struktur, Kommunikation und Absichten der einzelnen Gruppen aufgezeigt. Zum Schluss wird ein Fazit aus dem Vorgehen und den Kommunikationsstrukturen von Hacktivisten gezogen und eine Zusammenfassung der Seminararbeit gegeben.

## 7.2 Hacker und Hacktivismus

### 7.2.1 Arten von Hackern

Zu Beginn der Computerisierung wurde der Begriff "Hacker" für Personen verwendet, die Freude an der Erstellung und Veränderung von Software oder Hardware haben. Im weiteren Verlauf wurden außergewöhnlich gute Programmierer und später Personen, die Videospiel-Piraterie betrieben haben, so genannt. Mittlerweile bezeichnet "Hacker" jemanden, der in Computersysteme eindringt. Nach letzterer Definition gilt es mehrere Typen von Hackern zu unterscheiden. [2]

**White Hat Hacker**
Dies sind Hacker, die nur die Sicherheit eines Systems überprüfen wollen, um konstruktiv an der Entwicklung von z.B. Software beizutragen. [3]

**Black Hat Hacker**
Das Komplement zu den White Hat Hackern sind die Black Hat Hacker. Diese sind die eigentlichen Piraten, die mit schädlichen Absichten in andere Computersysteme eindringen und können wiederum in mehrere Bereiche eingeteilt werden. So genannte *Crasher*, auch Script Kiddies genannt, sind User mit sehr wenig Erfahrung, die im Internet nach Programmen suchen, um anderen zu Schaden. *Phreakers* interessieren sich für das Hacken von Telefonleitungen, um Telefoniekosten zu umgehen oder Telefonleitungen zu stören. Eine weiterer Typ ist der *Carder*, welcher sich auf das Hacken von Chipkarten spezialisiert, insbesondere um Geldautomaten oder ähnliches zu knacken. Personen, die Programme entwickeln, mit deren Hilfe Computersysteme angegriffen, oder Kopierschütze umgangen werden sollen, werden *Cracker* genannt. [4]

**Grey Hat Hacker**
Grey Hat Hacker verstoßen möglicherweise gegen Gesetze, allerdings zum Erreichen eines höheren Ziels. Beispielsweise durch die Veröffentlichung von Sicherheitslücken, um ein Leugnen unmöglich zu machen und die Verantwortlichen dazu zu zwingen, diese zu beheben. Grey Hats zeichnen sich dadurch aus, dass sie nicht eindeutig als „gut“ oder „böse“ einzustufen sind. [5]

**Hacktivisten**
Der Begriff *Hacktivist* (Kofferwort, zusammengesetzt aus Hacker und Aktivist) erfuhr die erste Verwendung im Juli 2004 von Mitgliedern eines Hacker-Kollektivs namens *Omega*.[6] Diese auch Cyberprotestanten genannten Hacker sind keiner der oben genannten Gruppen direkt zuzuordnen, am ehesten

jedoch den Gray Hats. Ihre Motivation ist ideologischer bzw. politischer Natur. Sie nutzen das Internet und ihre Fähigkeiten und Kenntnisse in diesem Bereich, um zu protestieren, was zumeist Schäden für ihre Gegner zufolge hat. Der Schwerpunkt dieser Seminararbeit bezieht sich auf diesen Typ. [7]

### 7.2.2 Ursprung des Hacktivismus

Quellen zufolge ist der Begriff Hacktivismus 1995 zum ersten mal in einem Artikel über den Filmemacher Shu Lea Cheang verwendet worden. Ein Jahr später nutze eine amerikanische Hackergruppe namens *Cult of the Dead Cow (cDc)* [1] diesen Begriff in einem Online-Artikel. Anonymous ist ein Paradebeispiel für den Hacktivismus, der zunächst für das Eintreten von Idealen, insbesondere die Freiheit des Internets auf Basis des Internets stand. In den Jahren 2007 und 2008 bekam der Hacktivismus weltweite Aufmerksamkeit aufgrund von zwei Internetangriffen in Estland [2] und Georgien [3]. Diese hatten das Ausmaß eines Internetkrieges, begründen dennoch den pressewirksamen Beginn des Hacktivismus. [7]

### 7.2.3 Gruppen von Hacktivisten

Hacktivisten können ebenfalls in verschiedene Typen eingeteilt werden. Eine Möglichkeit ist die Einteilung in *Anonymous*, *Cyberoccupier* und *Internetkrieger*.

**1. Anonymous**
Anonymous ist die bekannteste hacktivistische Gruppierung. Mitglieder dieser stehen für ein freies Internet ein und nutzen unter anderem Hacks und den Diebstahl und die Veröffentlichung vertraulicher Informationen, um denjenigen zu schaden, die ihren Idealen im Wege stehen. Andererseits werden auch Angriffe durchgeführt, die einen scherzhaften, unpolitischen Hintergrund haben. [7]

**2. Cyberoccupier**
Aktivisten, die das Internet und soziale Netzwerke in erster Linie nutzen, um Beziehungen aufzubauen und Werbung sowie Informationen zu verbreiten werden Cyberoccupier genannt. Hierzu gehören auch die Internetdissidenten, die wie ihre Pendants im echten Leben die Legitimität der politischen Macht, der sie gehorchen sollen, nicht mehr anerkennen. Solche versuchen durch groß angelegte Aktionen im Internet in ihrem Land zum Beispiel die Demokratie zu stärken oder die Korruption zu bekämpfen. [7]

[1] siehe `http://w3.cultdeadcow.com/cms/about.html`
[2] siehe `http://www.golem.de/0903/65870.html`
[3] siehe `http://www.spiegel.de/netzwelt/web/hack-attacke-auf-georgien-ehrenamtliche-angriffe-a-572033.html`

**3. Internetkrieger**
Internetkrieger sind vor allem in Ländern mit totalitären Tendenzen anzutreffen. Diese sind selbst ernannte Patrioten, die sich zum Großteil zu Internetarmeen zusammenschließen. Solche Gruppen nutzen verschiedenste Tools, um Dissidenten zu attackieren. Des Weiteren gehört zu ihrem Repertoire das Website defacement (siehe Kapitel 7.3.3) als ihre wichtigste Waffe. Weiterhin unterstützen sie nationale und extremistische Bewegungen und behaupten, sie handeln dadurch im Namen ihrer Regierungen. Diese Behauptung konnte jedoch noch nicht überprüft werden. [7]

## 7.3 Vorgehensweisen

Wie bereits in der Einleitung erwähnt haben Hacker ein Repertoire an Vorgehensweisen, um ihre Ziele, die dem Systemnutzer nur selten bekannt sind, zu erreichen. Dazu werden Schwachstellen in Betriebssystemen, Software oder sogar Nutzer-Systemen ausgenutzt. Es finden jede Minute mehrere Angriffe auf jedes Computersystem statt, das mit dem Internet verbunden ist. Die Angriffsarten können in sechs Bereiche unterteilt werden.

### 7.3.1 Bereiche der Angriffsarten

#### Physikalischer Zugriff

Hier hat der Angreifer Zugang zu den Räumlichkeiten des Systems oder sogar zum System selbst. Der Täter kann hier einen Stromausfall verursachen, den Rechner herunterfahren, die Hardware beschädigen, Datenträger stehlen oder den Netzwerkverkehr mitverfolgen.

#### Unterbrechen von Kommunikationsvorgängen

Dieser Bereich umfasst Angriffe, bei denen der Hacker versucht, eine bereits existierende Sitzung zu manipulieren. Dies ermöglicht dem Angreifer das erlangen von Privilegien eines authentifizierten Nutzers oder das Manipulieren von Nachrichten. Eine der bekanntesten Methoden für solch einen Angriff ist das *Session Hijacking*[4], bei dem eine TCP-Session zwischen zwei Maschinen übernommen wird. Da eine Authentifizierung meist nur zu Beginn einer solchen Sitzung stattfindet, kann sich der Angreifende Zugang zu einer Maschine verschaffen. [8]

[4]siehe `http://www.imperva.com/Resources/Glossary?term=session_hijacking`

### Denial of Service(Dos)

Das Ziel dieses Angriffs ist es, den reibungslosen Ablauf eines Services durch Überlastung zu stören oder sogar temporär unnutzbar zu machen. Dies geschieht unter Ausnutzung von Schwachstellen im TCP/IP-Protokoll oder der Serversoftware. Werden dazu mehrere Systeme verwendet, z.B. mithilfe eines Botnets, wird von einer DDoS-Attacke(Distributed Denial of Service) gesprochen. DoS Angriffe gehören zu den effektivsten Angriffen, um Firmen oder Organisationen zu schaden. Durch die freie Verfügbarkeit von kostenlosen Werkzeugen die einen DoS ausführen, stieg die Anzahl solcher Angriffe in den letzten Jahren. Ein bekanntes und leicht zu bedienendes kostenloses Werkzeug ist *LOIC*(Low Orbit Ion Cannon)[5], welches auch von Anonymous mehrfach verwendet wurde. [8][9]

### Eindringen

Unter diese Kategorie fällt unter anderem das *Port Scanning*, in dem systematisch die Ports eines Computersystems durchleuchtet werden. Ein bekannter Port Scanner ist *Nmap*[6] Des Weiteren gehören auch Malware, wie Viren, Würmer und Trojaner, sowie das Erhöhen von Berechtigungen, dieser Angriffsart an. Für Letzteres werden Schwachstellen von Anwendungen ausgenutzt, indem vom Entwickler nicht vorgesehene Anfragen gesendet werden, die dem Angreifer Zugriff zum System ermöglichen können. So kann zum Beispiel durch das Senden großer Datenmengen ein Pufferüberlauf entstehen, wodurch Speicherbereiche überschrieben werden, die außerhalb des vorgesehenen Puffers liegen. [8]

### Social Engineering

In diesem Fall ist der Nutzer selbst die Schwachstelle. Hacker nutzen die Unvorsichtigkeit des Nutzers, um an kritische Daten wie Passwörter zu gelangen. Dies geschieht z.B. indem der Anhang einer E-Mail unvorsichtig geöffnet wird oder indem der Angreifende sich als Administrator einer Webseite ausgibt und vorgibt,die Zugangsdaten des Opfers zu benötigen. Zudem wird häufig das selbe Passwort auf mehreren Plattformen verwendet, sodass der Angreifer gleich Zugang zu vielen Accounts des Nutzers erhält. [8][10]

### Falltüren

Falltüren sind in einer Software verbaute Hintertüren, die es dem Entwickler später erlauben Zugriff zu dem System zu erhalten. Diese können auch von Unbefugten genutzt werden, um in das System einzudringen. [8]

[5]Download unter `http://sourceforge.net/projects/loic/`
[6]Download unter `http://nmap.org/download.html`

### 7.3.2 Generelles Vorgehen von Hackern

Auch wenn das Vorgehen von Hackern nicht immer dasselbe ist, gibt es dennoch Phasen, die jeder Angreifer durchläuft.

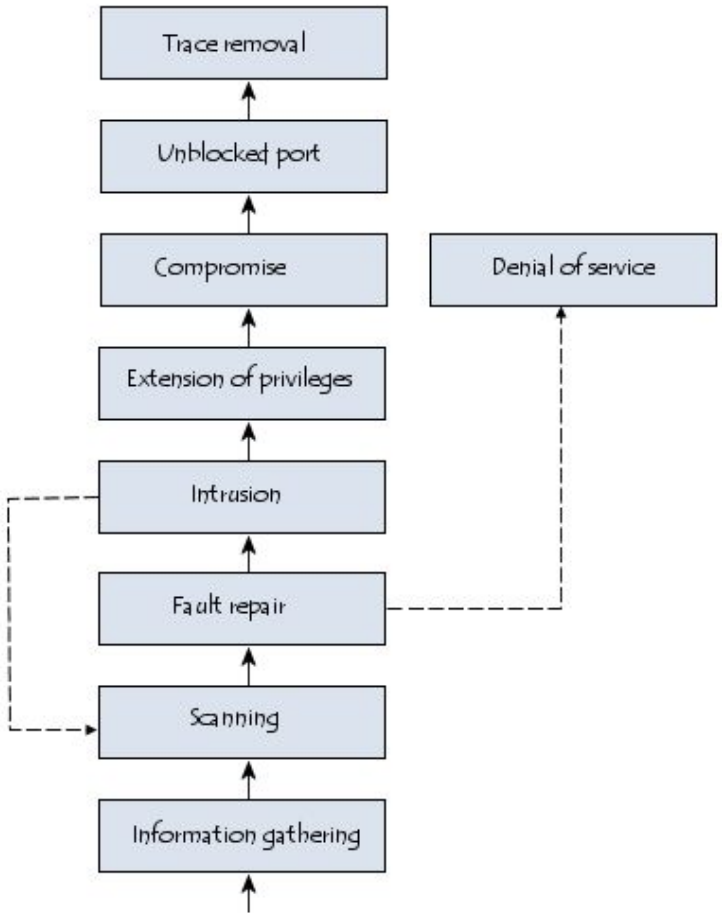


Abbildung 7.1: Phasen eines Angriffs[8]

**1. Informationsbeschaffung**

In der ersten Phase verschafft sich der Angreifer möglichst viele Informationen über die Rechnernetzarchitektur, Anwendungen und Betriebssysteme des Opfers, um ein passendes *Exploit*(Ausnutzung einer Schwachstelle) durchzuführen. Vor allem sind hier Informationen über die Adressierung des Rechnernetzes von besonderer Wichtigkeit. Das Erlangen solcher Informationen wird auch *Fingerprinting* genannt. Ziel ist es, IP-Adressierung, Domänenname, Netzwerkprotokolle, aktivierte Dienste, Serverarchitektur und ähnliches in Erfahrung zu bringen. Durch die Kenntnis des Domänennamens oder der IP Adresse eines der Rechner im Rechnernetz des Opfers ist es möglich in öffentlichen Datenbanken, wie `http://www.iana.net`, den Bereich der öffentlichen IP-Adressen des Zieles zu ermitteln, sowie dessen Unterteilung in

Unternetzwerke. Zudem gibt es Tools, wie Mimikatz[7] und WCE[8], die bei Windowsrechnern unter Anderem Passwörter und Kennungen in Klartext liefern können. Eine sehr einfache Methode ist außerdem das Nachforschen über Suchmaschinen, welche oftmals wichtige Informationen für einen erfolgreichen Angriff bereithalten. Um in das Zielsystem eindringen zu können, benötigt der Hacker Zugang zu gültigen Accounts. Eine weitere Möglichkeit dafür ist das *Social Engineering*, bei dem sich der Angreifer als jemand anderes ausgibt, um an Informationen über das System und möglicherweise sogar Passwörter zu kommen. Hierbei wird auf die Naivität der User des Systems spekuliert. Deshalb gilt auch allgemein, dass ein System so sicher ist, wie sein schwächstes Glied.
Eine andere Option ist das Überprüfen von Verzeichnissen, um Usernamen heraus zu finden. Messenger-Dienste oder der gemeinsame Dateizugriff bieten sich dafür an. Zusätzlich kann der Hacker Brute-Force-Angriffe ausführen, bei denen viele geläufige und naheliegende Passwörter nacheinander auf einer Account-Liste ausprobiert werden. Auch hierfür gibt es kostenlose Programme, wie den *BruteForcer*.[9] [11]

## 2. Scannen

Durch die Kenntnis der Netztopologie, kann der Hacker mithilfe eines *Scanners* wie z.B. Nmap(siehe 7.3.1), einem Netzwerktool, alle im Rechnernetz aktiven IP-Adressen, sowie offene Ports und sogar das Betriebssystem herauszufinden. Es gibt verschiedene Arten von Scannern. Einige, so genannte *passive mapper* ermitteln die Netzwerktopologie, falls diese vorher unbekannt war. Sie analysieren nicht, im Gegensatz zu anderen Scannern, empfangene Pakete und können dadurch nicht durch *Intrusion Detection Systeme*[10] entdeckt werden. Dies sind Programme, die unerlaubten Zugriff erkennen und auf diesen reagieren.
Weiterhin kann der Angreifer, nach dem Netzwerkscan Anfragen an laufende Dienste Senden, wodurch das Betriebssystem, der Server und dessen Version zurückgegeben werden können. Dieser Vorgang wird *Banner Grabbing* genannt.
Des Weiteren gibt es Programme, die eingegebene Tastenfolgen abfangen, wodurch Passwörter oder Ähnliches ermittelt werden können, so genannte *Keylogger*(z.B. Refog[11]). Eine weitere Methode ist, nachdem man die in 7.3.2 erwähnten Tools verwendet hat, das Abhören des TCP Ports 445, wodurch heraus gefunden werden kann, welche Rechner ein Windows Betriebssystem nutzen. Im Anschluss können per *SMB(Server Message Block)*[12], ei-

[7] Download unter `http://blog.gentilkiwi.com/mimikatz`
[8] Download unter `http://www.ampliasecurity.com/research/wcefaq.html`
[9] Download unter `http://www.chip.de/news/Brute-Force-Programm-Gratis-Download-knackt-Archive_62848723.html`
[10] siehe `http://www.google.com/patents/US6405318`
[11] Download unter `http://www.chip.de/downloads/Refog-Free-Keylogger_14493439.html`
[12] siehe `http://technet.microsoft.com/de-de/library/hh831795.aspx`

nem Kommunikationsprotokoll für Serverdienste, mögliche Netzlaufwerke abgefragt werden. [11]

### 3. Ausweitung von Rechten

Hat der Angreifer Zugang zum Rechnernetz erlangt, muss dieser sich erweiterte Rechte, zum Beispiel die eines *root*(Administrators), auf dem Rechner beschaffen. Eine Möglichkeit ist die Installation eines *Sniffers*[13], welcher den Datenverkehr abhören kann. Dabei erhofft sich der Hacker das Erlangen von Passwörtern und IDs von Nutzeraccounts mit mehr Rechten, im Idealfall die des Netzwerkadministrators. [11]

### 4. Kompromittierung

In diesem Abschnitt nutzt der Angreifer die Approbations-Beziehungen zwischen den Rechnern, um seine Handlungen auf möglichst alle Rechner auszuweiten. Durch das *Spoofing* übernimmt dieser die Identität des Nutzers und kann so in privilegierte Rechnernetze eindringen, zu denen der kompromittierte Rechner Zugriff hat. In einigen Fällen wünscht der Hacker nach dem Ausführen seines Angriffs noch einmal auf den von ihm kompromittierten Rechner zuzugreifen. In diesem Fall wird eine Anwendung installiert, die eine künstliche Sicherheitslücke erschafft. Solche Anwendungen werden *Backdoors* genannt. [11]

### 5. Verwischung von Spuren

In den meisten Fällen wünscht der Angreifer nicht, zurückverfolgt werden zu können. Deshalb muss er seine Spuren verwischen. Dies beinhaltet das Löschen der von ihm erzeugten Dateien und der Logdateien aller Rechner, auf die er zugegriffen hat. Logdateien sind eine Auflistung von durchgeführten Aktivitäten in einem Netzwerk oder Computer.[14] Wenn sich der Administrator zur selben Zeit anmeldet, wie der Hacker, kann dieser sehen, dass jemand in das System eingedrungen ist. Um dies zu verhindern gibt es *Rootkits*. Das sind Programme, die dem Administrator die Präsenz des Eindringenden und der von ihm installierten Schadsoftware vorenthalten. Einer der effektivsten Rootkit Angriffe geschah durch den Schadcode *Agent.BTZ*[15], der das United States Central Command Netzwerk infiziert hat. Es dauerte 14 Monate, diesen vollständig aus dem Netz zu entfernen. Viele spätere Cyberspionage Kampagnen, wie z.B. TURLA/SNAKE bauen auf dieser Software auf.

[13]Download unter `http://www.netstumbler.com/downloads/`

[14]siehe `http://www.itwissen.info/definition/lexikon/logfile-Log-Datei.html`

[15]siehe `http://www.kaspersky.com/de/about_kaspersky/news/allgemeine/2014/Cyberspionage-Kampagne_Turla_Snake_nutzt_bekannten_Schadcode_Agent_BTZ_als_Vorlage_`

Außerdem wird oft ein Proxy verwendet, um den Internetdatenverkehr über mehrere Knoten zu leiten. Ein Beispiel hierfür ist *TOR*(The Onion Router)[16], eine spezielle Routing Software speziell für diesen Zweck. [11][7]

### 7.3.3 Am häufigsten verwendete Angriffsarten

**SQL-Injection**
Bei der SQL-Injection werden Sicherheitslücken im Zusammenhang mit SQL-Datenbanken ausgenutzt, die durch mangelnde Maskierung oder Überprüfung von Metazeichen bei Benutzereingaben entstehen. Dadurch können Benutzereingaben und Ähnliches in den SQL-Interpreter gelangen und somit Funktionen ausgeführt werden. Dies ermöglicht dem Hacker das Ausspähen und Verändern von Daten, das Erlangen von Rootrechten, sowie Manipulation des Datenbank-Servers. [12]

**Denial of Service(DoS)**
Siehe 7.3

**Website Defacement**
Website Defacement ist ein Angriff, bei dem der Hacker sich administrative Rechte der angegriffenen Webseite aneignet, um dessen Inhalt oder Erscheinung zu verändern bzw., um den vorhandenen Inhalt durch eigenen, schadhaften zu ersetzen. So kann der Angreifer zum Beispiel in den Webserver eindringen und eine vorhandene Webseite durch eine vom Hacker erstellte ersetzen. [13]

**Strategic Web Compromise(swc) / Watering Hole**
Ein Angriff, bei dem eine stark frequentierte Webseite mit Malware infiziert wird, um so möglichst viele Besucher(einer bestimmten institution) zu infizieren. [14]

**Man In The Middle**
Hierbei hört der Hacker die Kommunikation zwischen zwei oder mehreren Gesprächspartnern ab und gibt sich daraufhin als ein beteiligtes Mitglied des Gespräches aus. Dadurch kann dieser das Gespräch manipulieren oder wichtige Informationen sammeln.

**Cross-Site Scripting**
Cross-Site Scripting (XSS) ist ein *Exploit*[17] durch das der Hacker Schadcode

[16]siehe `https://www.torproject.org/`

[17]Ein Exploit ist ein Computerprogramm oder Skript, welches Schwächen bzw. Fehlfunktionen eines anderen Computerprogramms ausnutzt. Siehe `http://www.people4.net/was-bedeutet-der-begriff-exploit`

in einen Link einer vermeintlich vertrauenswürdigen Quelle einfügt. Nutzt das Opfer den Link wird der Schadcode ebenfalls auf dessen Computer ausgeführt, was es dem Angreifer beispielsweise ermöglicht Informationen zu stehlen. [16]

**Inter-Protocol Exploitation**
Dieser Angriff nutzt eine Sicherheitslücke im Fundament zweier kommunizierender Protokolle aus, die im Internet verwendet werden(z.B. HTTP). Das Protokoll, das den Exploit kapselt, wird Trägerprotokoll, das Protokoll, dass das gefährdete Zielprogramm verwendet, Zielprotokoll genannt. Es wird ein Dienst angegriffen, der ein anderes Protokoll verwendet. Da die Spezifikationen des Zielprotokolls in den meisten Fällen einen Angriff dieser Art nicht in Betracht ziehen, ist dieser sehr effektiv. [17]

**Cross-Protocoll Scripting**
Cross-Protocol Scripting ist eine Kombination aus Cross-Site Scripting und Inter-Protocol Exploitation.

## 7.4 Hacktivistische Gruppierungen

Im Folgenden werden nur einige, pressewirksame Hacktivistengruppen genannt, um den Rahmen dieser Seminararbeit nicht zu überschreiten. Zu diesen Gruppen gehören Anonymous, AnonGhost, Backtrace Security, LulzSec, Derp(Trolling), GNAA, SEA, TeaM p0is0N, APT1, Hidden Lynx, Energetic Bear(cyber-burkut) und Putter Panda(MSUpdater).

### 7.4.1 Anonymous

Abbildung 7.2: Markenzeichen von Anonymous: Guy Fawkes Maske

Anonymous ist keine konkrete Gruppe, sondern eine Bewegung. Es wird auch vom Internetphänomen Anonymous gesprochen. Daraus ist zu folgern, dass es innerhalb dieser Bewegung keine feste Struktur gibt. Die Mitglieder(Anon) verbinden lose Ziele und Wertvorstellungen. So wird eine Gute Idee eines Anons von anderen weiterverbreitet und in die Tat umgesetzt. Dazu nutzt Anonymous hauptsächlich das Internet und damit einhergehend Hackerangriffe, aber auch Demonstrationen finden statt.

Die Motivation der Mitglieder ergibt sich aus dem Wunsch nach Redefreiheit und der Unabhängigkeit des Internets. Zudem ist Anonymous gegen

das Urheberrecht, Internetzensur und einige Organisationen, wie Scientology, staatliche Behörden und global agierende Konzerne. Besonderheiten der Bewegung finden sich schon zu Beginn ihrer Geschichte. Sie entstand aus dem bekannten Imageboard 4chan[18], in dem sich einige Mitglieder zusammen getan haben, da diese Spaß am hacken hatten. Mit der Zeit ergaben sich gemeinsame Ziele und Wertevorstellungen. Eine Maske, die den englischen Freiheitskämpfer Guy Fawkes abbildet, wurde zu ihrem Markenzeichen. Das Motto "We are Anonymous, We are Legion, We do not Forgive, We do not forget, expect us." soll den Zusammenhalt der Mitglieder stärken.
Eines der bekanntesten Projekte dieser Gruppierung war *Operation Payback*, das sich gegen die Schließung von *Pirate Bay*[19], einer Filesharing-Plattform, sowie gegen die Finanzblockaden von Wikileaks richtete. Regierungseinrichtungen, Handelsorganisationen, Einzelpersonen, Anwaltskanzleien und Finanzinstitutionen kamen durch DDoS Angriffe zu Schaden, darunter die Recording Industry Association of America (RIAA), die Motion Picture Association of America (MPAA), die US-Urheberrechtsbehörde sowie die Finanzfirmen Visa, Mastercard und Bank of America. Die Angriffe wurden über *IRC Chats*(Internet Relay Chat) koordiniert und mit dem Werkzeug LOIC durchgeführt. Das Projekt begann am 16. September 2010 und endete frühestens am zweiten Januar 2011. Mehrere Anonymous Anhänger wurden wegen Beteiligung an einer Verschwörung inhaftiert. [18]
Einige weitere bekannte Projekte von Anonymous sind Project Chanology, Operation Sony, Operation Zeta und viele mehr. Sie arbeiten auch mit dem Wiki-Leaks-Projekt zusammen. Untereinander kommunizieren die Mitglieder über Foren, soziale Netzwerke, insbesondere Twitter und IRC Chats. Die fünf wichtigsten Twitter-Accounts für aktuelle Informationen über Anonymous sind *AnonOps: Wir kämpfen für die Freiheit im Internet*, *AnonymousIRC: Wir sind die Botschafter von #AntiSec*, *YourAnonNews*, *AnonymousPress* und *Anon_Central: Anonymous-Operationen*. Wichtige Webseiten für Neuigkeiten der Bewegung sind *anonops.blogspot.com*, *youranonnews.tumblr.com*, *anoncentral.tumblr.com* und *anonnews.org*. Hierbei treten sie sehr anonym auf, sodass eine Rückverfolgung stark erschwert wird. Somit kann Anonymous auch keine favorisierte Angriffsart zugeordnet werden. [7] [20]

### 7.4.2 AnonGhost

Ein Ableger von Anonymous ist AnonGhost, der jedoch allein an Nebenprojekten des Kollektivs arbeitet. Bekannte Angriffe sind OpIsrael(Angriff auf israelische Webseiten) und OpNSA. OpIsrael richtete sich im April 2013 gegen die israelische Regierung und 39 israelische Webseiten fielen ihr zum Opfer. [22]

[18] siehe `http://www.4chan.org/`
[19] siehe `http://thepiratebay.se/`


Abbildung 7.3: Logo von AnonGhost

### 7.4.3 BackTrace Security

BackTrace Security ist eine Splittergruppe von Anonymous. Die Ziele einiger Mitglieder stimmten nicht mehr mit den politischen hacktivistischen Aktivitäten von Anonymous überein, weshalb sich diese Gruppe abgesondert hat. Eines der Ziele von BackTrace Security ist es, Anonymous momentane Stellung zu schwächen. Dazu veröffentlichten sie sogar einige Namen und Standorte von Anons. [23]

### 7.4.4 LulzSec

Abbildung 7.4: Logo von LulzSec

LulzSec, Abgeleitet von LOL(Laughing Out Loud) und Security ist, ähnlich wie Anonymous, eine lose Organisation und Splittergruppe von Anonymous, wobei sie im Kern sechs Mitglieder[20] hat. Hector Xavier Monsegur alias Sabu ist der Gründer und ehemaliger Sprecher von LulzSec. Die Mitglieder dieser Gruppierung operieren hauptsächlich wegen ihrer Freude am Chaos. Dennoch prangern sie Korruption und Rassismus insbesondere in Behörden an, sind gegen Unterdrückung durch die Sicherheitsindustrie und die Regierung, gegen Polizei, Firmen und das Militär. Diese Institutionen werden von dieser Gruppe hauptsächlich durch DDos Angriffe und SQL-Injections attackiert. Besonders bekannt sind der DDos Angriff auf die CIA und die *SQL-Injection* auf die Firma Sony. Weitere sehr bekannte Opfer von LulzSec waren InfraGard, der US-Senat, PBS und The Sun. Auch diese Gruppierung kommuniziert über Social Networks, speziell Twitter, und über ihre eigene Webseite. Am 19. Juli 2011 führten sie die Operation Anti-Security in Zusammenarbeit mit Anonymous aus. Die Operation wurde von Twittereinträgen der Hacker kommentiert. LulzSec ist zudem bekannt für die Veröffentlichung von Daten, zum Beispiel von der *SOCA*(Serious

[20]siehe `http://www.theregister.co.uk/2013/05/17/lulzsec_analysis/`

Organized Crime Agency) auf ihrer Webseite, sowie auf PirateBay. Sie wollen auf diese Weise den Internetnutzern zeigen, dass ihre Daten bei solchen Organisationen nicht sicher sind und durch illegale oder legale Zugriffe missbraucht werden können. Sabu wurde verhaftet und hat Informationen über Anonymous und LulzSec an das FBI weiter gegeben, woraufhin einige Hacktivisten beider Gruppierungen gefangen genommen wurden. [21]

### 7.4.5 Derp(Trolling)

Diese Gruppierung entstand 2011 und ihre Mitglieder nutzen Twitter, um DoS-Angriffe auf hoch frequentierte Seiten und Online Spiele zu koordinieren. Bekannt ist zum Beispiel die Reihe von Angriffen auf den Livestreamer Phantoml0rd bei mehreren Spieleplattformen, wie "League of Legends¨ und "World of Tanks". Anders, als Hacktivisten haben Mitglieder dieser Gruppe kein klares Motiv, sondern werden durch ihre Freude am Chaos tätig. [24]

### 7.4.6 GNAA


Abbildung 7.5: Logo der GNAA


Abbildung 7.6: Logo der Goatse Security

Die GNAA("Gay Nigger Association of America") ist eine hierarchisch aufgebaute Gruppe, die einen Präsidenten, derzeit "timecop¨, besitzt. GNAA ist eine Anti-blogging Internet-trolling Organisation. Der Name sei nicht rassistisch oder homophob zu interpretieren, sondern soll Verstörung auslösen und soziale Normen herausfordern. Die Mitglieder gründeten sogar eine Grey Hat Information Security Gruppe, "Goatse Security", die regelmäßig Sicherheitslücken von Programmen und Systemen aufdeckt und veröffentlicht. Bekannt ist die Veröffentlichung von ca. 114.000 E-Mail Adressen von IPad Nutzern. Die GNAA nutzt Angriffe, wie *Crapflooding*, dem Überfluten von Webblogs mit wiederkehrendem Text, *IRC-Chat-flooding*, Schockseiten, welche Malware enthalten, *Cross-Protocol Scripting* und veröffentlichen, wie bereits erwähnt, Schwachstellen in Software. [25] [26]


Abbildung 7.7: Logo der SEA

### 7.4.7 SEA

In Syrien werden Webseiten zensiert und Personen arrestiert, die diese besuchen. Die SEA (Syrian Electronic Army) unterstützen die syrische Regierung und Bashar Al-Assad. Angriffsziele sind politische Oppositionen, einschließlich Nachrichtenorganisationen und Menschenrechtsgruppen, sowie Twitter-Accounts. Die am häufigsten verwendeten Methoden der SEA sind *DDos-Angriffe* und *Website defacement*. Sie teilen ihre Pläne ebenfalls über Twitter und andere soziale Netzwerke der Öffentlichkeit mit und führen auf Diensten wie Facebook Spam Angriffe aus. [27]

### 7.4.8 TeaM p0is0N


Abbildung 7.8: Logo von Poisanon

TeaM p0is0n ist eine Gruppe von Hackern, die mit der ZHC(ZCompany Hacking Crew) zusammenarbeitet. Eine Kooperation mit Anonymous wurde unter dem Namen Poisanon geführt. Die bekannteste Zusammenarbeite mit Anonymous war die *Operation Robin Hood*. LulzSec stehen sie feindlich gegenüber, da diese unfähig und keine echten Hacker seien, aber dennoch viel Aufmerksamkeit erregen. Das TeaM p0is0n verbreitet unautorisierte Statusupdates auf Facebook, veröffentlicht Daten(z.B. über Tony Blair oder die NASA) und hackt Webseiten. Des Weiteren missbrauchen die Mitglieder Kreditkarten und übergeben die Gelder an Aktivisten. Die Ziele sind mit denen von Anonymous vereinbar und beide Gruppierungen verwenden die selben Kommunikationswege. [28]

### 7.4.9 APT1

APT1(Advanced Persistent Threat 1) ist eine chinesische Gruppierung, welche höchstwahrscheinlich von der chinesischen Regierung bezahlt wird, um Firmen und Organisationen im englischsprachigen Raum auszuspähen und an Informationen und Daten von wirtschaftlichem oder politischem Interesse zu gelangen. So wurden hunderte Terrabyte Daten von mindestens 141 Organisationen gestohlen, darunter auch eine Vorlage für ein Atomkraftwerk. Ihr Netzwerk von Computersystemen ist auf der ganzen Welt verteilt. Diese Organisation hat außerdem dutzende oder sogar hunderte Mitglieder, von denen fast nichts bekannt ist. [29] [30]

### 7.4.10 Hidden Lynx

Diese Gruppe von Auftrags-Hackern ist erstmals 2009 auf Aufmerksamkeit gestoßen. Ihre Hacks, insbesondere ihre *watering hole* Attacken, übertreffen zum Teil alle anderen wohl bekannten Gruppierungen. Die 50 bis 100 Mitglieder zeichnen sich durch technische Professionalität, Geschwindigkeit, Organisationstalent, Geduld und großen Einfallsreichtum aus. Ihre bevorzugten Ziele sind Banken, Rüstungsindustrie und Regierungsinstitutionen, wobei man ihre Organisation in zwei Teams aufteilen kann. Das so genannte *Team Moudoor*Team Moudoor ist für grobe Arbeiten zuständig und scheut keine Hilfsmittel, selbst wenn dadurch die Chance, dass die Gruppe aufgeklärt wird, sich erhöht. Das Andere Team, *Team Naid*, greift nur bestimmte Ziele an und ist viel geduldiger und geschickter. Zum Teil vergehen sogar Monate, bis ein Auftrag ausgeführt wird. Laut der Sicherheitsfirma Symantec agiert Hidden Lynx von China aus und für die richtige Menge Geld ist ihnen kein Aufwand zu hoch, um ihre Aufträge zu erfüllen. [31]

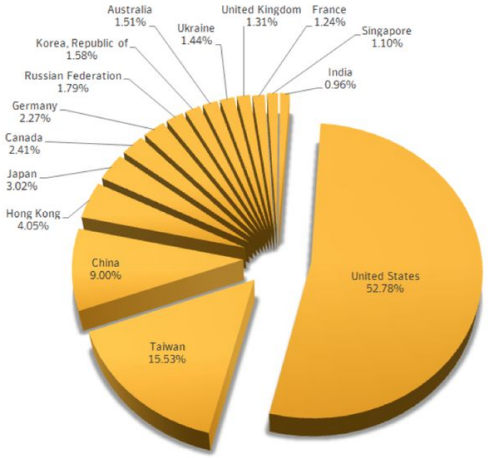


*Figure 2. Countries/regions targeted by the Hidden Lynx group since November 2011*

Abbildung 7.9

### 7.4.11 Energetic Bear(cyber-burkut)

Dies ist eine Gruppe, die dem CrowdStrike Report 2013[21] zufolge Spionage für die russische Regierung betreibt. Bewiesen konnte diese Hypothese jedoch noch nicht. Energetic Bear führt fokussiert Angriffe auf den Energiesektor aus und nutzt dazu vorzugsweise Watering-Hole Angriffe. Die gestohlenen Informationen in diesem Sektor können einem Staat unterschiedliche Vorteile erbringen. Weniger Kosten in Entwicklung und Forschung, effizientere Technologien, bis hin zum Lahmlegen der Energieversorgung anderer Nationen sind denkbar. Aber auch andere Ziele sind bereits Opfer dieser Gruppierung geworden. Es wird außerdem eine Verbindung zu APT1 vermutet, da die Taktiken, Techniken und Prozeduren denen von APT1 gleichen.
Cyber-burkut ist ebenfalls eine Gruppe, der man nachsagt, sie arbeite für die russische Föderation. Analysten von Wapack Lab[22] vermuten, dass Cyber-burkut eine low budget Operation, gerichtet an die ukrainische Bevölkerung, sei um die Meinung des Volkes zu manipulieren. Verstärkt werden DDoS-Angriffe genutzt. Außerdem ruft die Gruppierung die allgemeine Bevölkerung dazu auf, dem Cyberkrieg gegen die Ukraine beizutreten.

### 7.4.12 Putter Panda(MSUpdater)

Putter Panda oder auch MSUpdater genannt, agiert zumindest seit 2007 und spioniert als chinesische Gruppierung westliche Staaten aus. Vor allem stand die europäische Satelliten- und Raumfahrtindustrie und die amerikanische Verteidigung im Fokus. Exploits für populäre Anwendungen, wie Adobe Reader und Microsoft Office werden vorzugsweise von dieser Gruppe verwendet, um Schadsoftware per E-Mail an Nutzer zu übertragen. Crowdstrike entdeckte einen Zusammenhang zwischen Domänen, die von Putter Panda verwendet wurden und Email Adressen, die ”cpyy” beinhalten und konnte somit einige Informationen über die Angriffe und deren Akteure ermitteln. Das Kürzel ”cpyy” konnte somit dem Nicknamen einer möglicherweise für die Gruppe agierenden Person zugeordnet werden. Des Weiteren wurde ein verdächtiges Bürogebäude über Posts im sozialen Netzwerk Picasa[23] in den Fokus genommen, in dessen unmittelbarer Nähe große Satellitenschüsseln aufgestellt sind. Vorangegangene Indizien, sowie eine Überlappung der Organisationen Putter Panda und *Comment Panda* weisen darauf hin, dass beide Gruppen für die chinesische Regierung tätig sind. [33]

[21] siehe `http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf`

[22] siehe `http://wapacklabs.com/`

[23] siehe `http://picasa.google.de/intl/de/`

## 7.5 Zusammenfassung

### 7.5.1 Fazit

Es gibt verschiedenste Arten von Hackern mit den unterschiedlichsten Absichten. Wenn ihre Absichten bekannt sind, ist es leichter sich vor Angriffen zu schützen. Hacktivisten haben die Absicht Aufsehen zu erregen und ihre Meinung durch das Hacken von Andersdenkenden zum Ausdruck zu bringen. Sie geben ihre Pläne der Öffentlichkeit durch soziale Netzwerke, vor allem Twitter, preis, bevor sie zuschlagen. Somit können rechtzeitig Gegenmaßnahmen ergriffen werden, um größere Schäden zu vermeiden. Bei Hackergruppierungen, die für die Regierung arbeiten, aus wirtschaftlichen Gründen agieren oder lediglich Schaden anrichten wollen, kommt der Angriff zumeist überraschend und unangekündigt. Diese wollen nicht erkannt werden. In solchen Fällen muss das Vorgehen der Hacker analysiert werden um Rückschlüsse auf den Täter zu ziehen. Die vielen Angriffsmöglichkeiten und Vorgehensweisen ermöglichen im Idealfall das Wiedererkennen eines Angreifers. Dieser muss seine gestohlenen Daten sichern, zum Beispiel als crypted-ZIP an einen FTP-Server senden. Solche Aktionen hinterlassen Spuren, anhand derer man Unterschiede bei den Vorgehensweisen der einzelnen Gruppierungen erkennen kann. Den Feind zu kennen ermöglicht Absichten und Ziele des Täters festzustellen, weshalb die Zuordnung eine Kernkomponente der IT-Sicherheit ist.

### 7.5.2 Hackergruppen und wichtige Daten im Überblick

In der nachfolgenden Tabelle sind die in der Seminararbeit behandelten Hackergruppen und bekannte Informationen über diese aufgelistet. Bei Informationen, die nicht sicher zutreffen, befindet sich hinter diesen ein ”?” Symbol. Wurden keine Quellen bezüglich eines Tabelleneintrags gefunden, steht an dessen Stelle das Wort ”Unbekannt”.

| **Gruppe** | **Land** | **Kommunikation** | **Angriffsarten** | **Größte Projekte** |
|---|---|---|---|---|
| Anonymous | Weltweit | Twitter,IRC | Alle | OpPayback |
| AnonGhost | Weltweit | Twitter,IRC | Alle | OpIsrael |
| BackTrace Security | Weltweit | Unbekannt | Unbekannt | Unbekannt |
| LulzSec | Weltweit | Twitter,Webseite | DDos,SqlInjection | OpAntiSecurity |
| Derp(Trolling) | Weltweit | Twitter | DDos | Phantoml0rd |
| GNAA | Weltweit | Webseite | flooding | Unbekannt |
| SEA | Syrien | Twitter | DDos,WebsiteDefacement | Unbekannt |
| TeaM p0is0N | Weltweit | Twitter,IRC | Unbekannt | OpRobinHood |
| APT1 | China | Unbekannt | Unbekannt | Unbekannt |
| Hidden Lynx | China? | Unbekannt | WateringHole | Unbekannt |
| Energetic Bear | Russland? | Unbekannt | WateringHole | Unbekannt |
| Putter Panda | China | Unbekannt | Unbekannt | Unbekannt |

# Literaturverzeichnis


[1] Margaret Rouse (Juni 2007) : *hacktivism*, http://searchsecurity.techtarget.com/definition/hacktivism.

[2] Margaret Rouse (Oktober 2006) : *hacker*, http://searchsecurity.techtarget.com/definition/hacker.

[3] Margaret Rouse (Juni 2007) : *white hat*, http://searchsecurity.techtarget.com/definition/white-hat.

[4] Margaret Rouse (Juni 2007) : *black hat*, http://searchsecurity.techtarget.com/definition/black-hat.

[5] Margaret Rouse (Juni 2007) : *gray hat (or grey hat)*, http://searchsecurity.techtarget.com/definition/gray-hat.

[6] Michael Seemann (24. Januar 2013) : *Den Staat zu hacken, ist nicht genug*, http://www.zeit.de/digital/internet/2013-01/hacktivismus-ccc : Zeit Online.

[7] François Paget (2012) : *Hacktivismus - Das Internet ist das neue Medium für politische Stimmen*, http://www.mcafee.com/de/resources/white-papers/wp-hacktivism.pdf : McAfee Labs.

[8] *http://de.kioskea.net/contents/721-einfuhrung-zu-angriffen* , 2014.

[9] Pavitra Shandkhdhar (29. Oktober 2013) : *DOS Attacks and Free DOS Attacking Tools*, Infosec Institute

[10] Sarah Granger (18. Dezember 2001) : *Social Engineering Fundamentals, Part I: Hacker Tactics*, SecurityFocus.com.

[11] Jean-François PILLOU (September 2014) *Sicherheit - Methodologie einer Intrusion in ein Netzwerk*, http://de.kioskea.net/contents/726-sicherheit-methodologie-einer-intrusion-in-ein-netzwerk.

[12] Amirmohammad Sadeghian, Mazdak Zamani, Azizah Abd. Manaf (2013) : *A Taxonomy of SQL Injection Detection and Prevention Techniques*, International Conference on Informatics and Creative Multimedia.

[13] Sanehdeep Singh (26. Dezember 2012) : *Website Defacement Prevention (Part-I)*, http://www.symantec.com/connect/articles/website-defacement-prevention-part-i.

[14] Steven Adair, Ned Moran (15. Mai 2012) : *Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Results*, http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/.

[15] Oliver Wege (22. September 2011) : *Man-In-the-Middle*, http://www.secupedia.info/wiki/Man-In-the-Middle.

[16] Margaret Rouse (September 2010) : *cross-site scripting (XSS)*, http://searchsoftwarequality.techtarget.com/definition/cross-site-scripting.

[17] Wade Alcorn (05. März 2007) Inter-Protocol Exploitation `https://www.nccgroup.com/media/18511/inter-protocol_exploitation.pdf`.

[18] Friedhelm Greis (04. Oktober 2013) : *USA klagen 13 mutmaßliche Hacker von Anonymous an*, http://www.golem.de/news/operation-payback-usa-klagen-13-mutmassliche-hacker-von-anonymous-an-1310-101959.html

[19] Kaspersky Lab, *http://www.kaspersky.com*

[20] Ole Reissmann, Christian Stöcker, Konrad Lischka, *We are Anonymous: Die Maske des Protests - Wer sie sind, was sie antreibt, was sie wollen* , 2012.

[21] Christian Stöcker, Konrad Lischka, *http://www.spiegel.de/netzwelt/web/lulzsec-und-anonymous-fbi-hebt-beruechtigte-hackergruppe-aus-a-819716.html* , Spiegel, 2012.

[22] Nauman Ashraf (15. Januar 2013) : *Israeli websites hit by AnonGhost, #OpIsrael*, http://thehackerspost.com/2013/01/israeli-websites-hit-by-anonghost.html.

[23] Andy Greenberg (18. März 2011) : *Ex-Anonymous Hackers Plan To Out Group's Members*, http://www.forbes.com/sites/andygreenberg/2011/03/18/ex-anonymous-hackers-plan-to-out-groups-members/.

[24] (30. Dezember 2013) *Hacker Group DERP Target World of Warcraft, League of Legends, EA, And More*, http://www.gamebreaker.tv/news-main/hacker-group-derp-target-world-warcraft-league-legends-ea/.

[25] Fruzsina Eördögh (3. Dezember 2012) : *Trolling Group GNAA Claims "Brony" Culture Was Target of Today's Nasty Attack on Tumblr*, `http://www.slate.com/blogs/future_tense/2012/12/03/gnaa_tumblr_worm_trolling_group_says_it_was_targeting_bronies.html`.

[26] (12. August 2014) : *Gay Nigger Association of America*, `http://en.wikipedia.org/wiki/Gay_Nigger_Association_of_America#References`.

[27] SEA official website (3. September 2014) : http://sea.sy/index/en.

[28] Wikipedia (25. August 2014) : http://en.wikipedia.org/wiki/TeaMp0isoN.

[29] Mandiant Corporation : *APT1 - Exposing One of China's Cyber Espionage Units* `http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf`

[30] Carnegie Mellon University (Mai 2014) : *Investigating Advanced Persistent Threat 1 (APT1)* , http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=90426.

[31] Symantec Security Response (17. September 2013) : *Hidden Lynx – Professional Hackers for Hire* http://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire.

[32] Jeff Stutzman, Wapack Labs (10. Mai 2014) : *Red Sky Weekly: Energetic Bear, Cyber-burkut*, http://henrybasset.blogspot.de/2014/05/red-sky-weekly-energetic-bear-cyber.html.

[33] Nathaniel Hartley (09. Juni 2014) : *Hat-tribution to PLA Unit 61486*, http://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/index.html.

# Kapitel 8

# Netzwerksicherheit und -monitoring vs. Datenschutz

*Julian Petery*

## Inhaltsverzeichnis

## 8.1 Einleitung

In dieser Arbeit soll ein Überblick über die Problematik der Absicherung von Netzen, über Firewalls und Netzwerkmanagementtools und die daraus resultierenden Probleme im Bezug auf den Datenschutz gegeben werden.

Dazu wird zunächst ein beispielhaftes bestehendes Netz analysiert und Verbesserungsmöglichkeiten dafür präsentiert. Im Anschluss daran werden zwei Firewalls und Netzwerkmanagementtools vorgestellt. In einem weiteren Abschnitt wird die Rechtslage für Datenschutz in Deutschland und eine Möglichkeit der Umsetzung dargestellt. Verbunden wird dies mit der Betrachtung der Frage, inwieweit der Nutzer als Teil eines sicheren Netzes betrachtet werden muss. Dabei wird auch die private Nutzung des Internets und dienstlicher E-Mail-Adressen untersucht. Am Ende werden die einzelnen Abschnitte des Hauptteils zusammengefasst und bewertet sowie ein Ausblick auf weitere Problemstellungen gegeben.

## 8.2 Hauptteil

Gemäß [3] haben bereits über 80% der kleinen und mittelständischen Unternehmen in Deutschland Maßnahmen zum System- und Netzmanagement vollständig oder teilweise umgesetzt. Deshalb wird davon ausgegangen, dass Unternehmen in diesem Bereich ausreichend sensibilisiert sind. In der Studie wird daher nicht weiter auf die genauen Maßnahmen eingegangen. Diese sind allerdings in den Veröffentlichungen des BSI zu finden. Die Umsetzung der darauf aufbauenden Handlungsempfehlungen wird in den folgenden Abschnitten dargestellt, wobei bei der Betrachtung einzelner Komponenten nur auf Firewalls und Netzwerkmanagementtools eingegangen wird.

### 8.2.1 Analyse eines vorhandenen Netzes

In diesem Abschnitt wird zunächst eine beispielhafte Konzeption eines Firmennetzwerkes beschrieben, danach auf problematische Stellen hingewiesen und mögliche Lösungen vorgestellt.

Die Abbildung 8.1 stellt ein Firmennetzwerk dar, das über einen gewissen Zeitraum gewachsen und stets an neue Aufgaben angepasst wurde, ohne dabei einem ganzheitlichen Konzept zu folgen. So hat zunächst jeder Organisationsbereich ein Netz in eigener Verantwortung aufgebaut. Jedes Netz besteht aus den jeweiligen Client-Rechnern und einem File-Server für die in diesem Organisationsbereich benötigten Daten. Erst im Laufe der Zeit wurden diese einzelnen Organisationsbereiche miteinander verbunden und an das Internet angeschlossen. Dadurch kommt es zu Redundanzen, wie z.B. bei den Dokumentenservern.

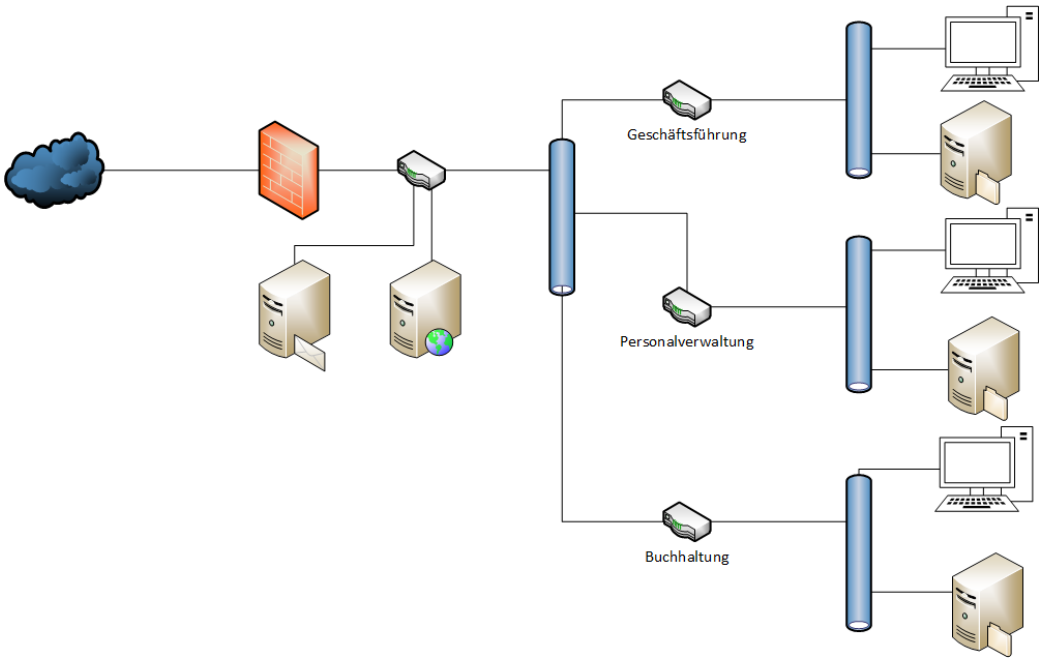


Abbildung 8.1: Gliederung des bestehenden Netzes

Als Vorgehensweise zur Verbesserung einer Netzwerkstruktur, insbesondere im Hinblick auf das Sicherheitsniveau, bietet der BSI Standard 100-2 [8] das in Abbildung 8.2 dargestellte Modell.

Im Rahmen der Informationstechnik (IT)-Strukturanalyse wird, wie in [2] und in [8] beschrieben, zunächst eine Komplexitätsreduzierung durch Gruppenbildung durchgeführt. Hierbei werden den einzelnen Endgeräten Funktionen zugewiesen, z.B. werden alle Clients von Geschäftsführungsmitgliedern oder alle File-Server zusammengefasst. Diese Gruppen ermöglichen die weitergehende Strukturierung des neu aufzustellenden Netzes.

Im nächsten Schritt erfolgt die Erhebung der IT-Systeme. Dabei werden die eingeteilten Gruppen genauer beschrieben, insbesondere werden Daten über das Betriebssystem, den Status (in Betrieb/außer Betrieb) und die Zugriffsrechte erhoben.
Danach werden die IT-Anwendungen und die zugehörigen Informationen erfasst. Dies geschieht nach [7]. Dabei werden alle Systeme auch in Hinblick ihres Bedarfes an Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert.Anhand dieser Klassifizierung kann im nächsten Schritt eine Schutzbedarfsfeststellung durchgeführt werden.
Die Schutzbedarfsfeststellung gliedert sich in 4 Schritte:

- Schutzbedarf der IT-Anwendungen
- Schutzbedarf der IT-Systeme
- Schutzbedarf der Übertragungsstrecken
- Schutzbedarf der IT-Räume

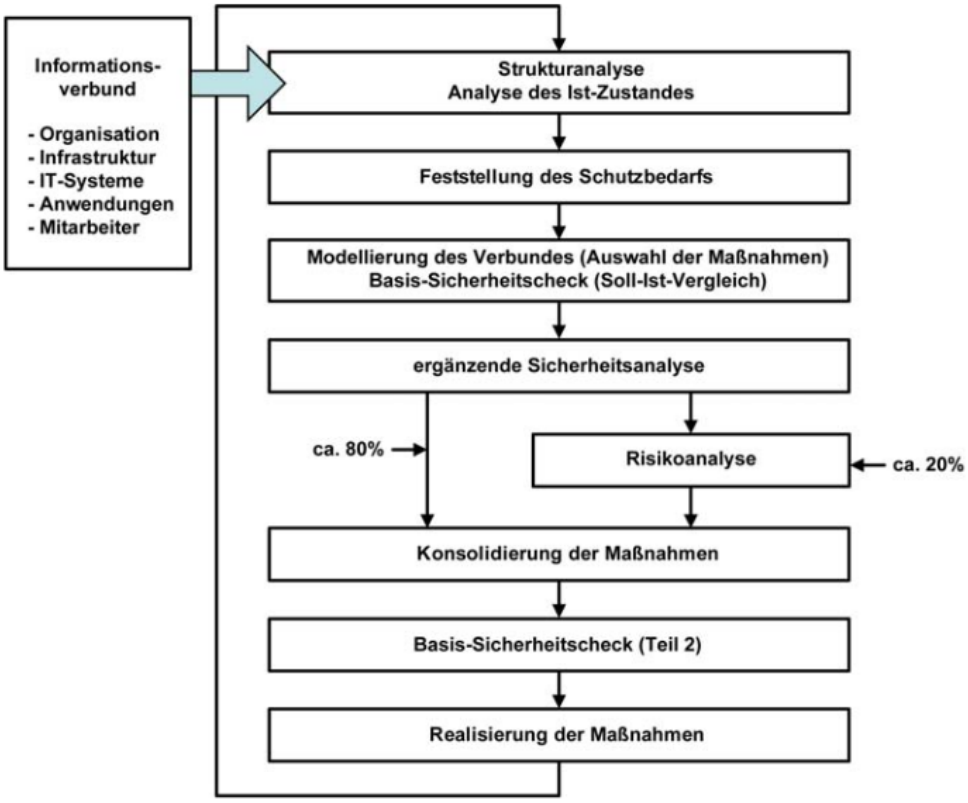


Abbildung 8.2: Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement

Nach dem BSI-Grundschutzhandbuch wird der Schutzbedarf in 3 Kategorien unterteilt:

- niedrig bis mittel
- hoch
- sehr hoch

Die Schutzbedarfsfeststellung untersucht in jedem Schritt den Schutzbedarf hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität. Die mögliche Höhe eines materiellen oder ideellen Schadens bestimmt letztendlich den Schutzbedarf. Mögliche Schadensszenarien sind:

- Verstoß gegen Gesetze, Vorschriften und Verträge
- Verstoß gegen Datenschutzbestimmungen
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung

- Negative Auswirkungen
- Finanzielle Auswirkungen [2]

Aus den gewonnenen Erkenntnissen hinsichtlich des Schutzbedarfes und der Verwendung einer jeden Komponente (Netzkomponente, Server, Client) werden notwendige Schutzmaßnahmen zielgerichtet ausgewählt. Die einzelnen Maßnahmen können aus dem BSI-Grundschutz entnommen werden, der hierzu eine Richtlinie bildet. Diese Maßnahmen werden dann in einem Anforderungskatalog zusammengefasst. Ein Auszug daraus besteht für den vorgestellten Fall aus den folgenden Punkten:

- *Abschottung des Managementnetzes* Damit soll erreicht werden, dass die sensiblen Informationen über den Zustand von Netzkomponenten nur von berechtigten Personen gelesen werden können. (M 2.146)
- *Abschottung der Server* Es sollen nur die Dienste der Server im Netz erreichbar sein, nicht aber die Administrationsschnittstellen. (M4.432)
- *Segmentierung des Netzes* Damit soll sichergestellt werden, dass Nutzer nur auf die Dienste zugreifen können, die für die Erfüllung ihrer Arbeit notwendig sind. (M5.77)
- *Trennung von Intranet und Internet* Nutzer sollen Dienste im Internet nicht direkt erreichen können, um einerseits die Struktur des Netzwerkes nach außen hin zu verschleiern und andererseits weniger Angriffsflächen zu bieten. (M 2.70)
- *Einrichtung eines Sicherheitsgateways* Sämtlicher ein- und ausgehender Verkehr soll überwacht werden, um das Eindringen von Schädlingen zu erschweren. (M 2.70)

Die Umsetzung dieser Maßnahmen richtet sich dabei nach der Höhe des Schutzbedarfes. Mögliche Mittel zum Schutz auf Netzwerkebene sind Firewalls. Gleichzeitig müssen zur effizienten Verwaltung von vielen Komponenten Informationen über den jeweiligen aktuellen Zustand zentral gesammelt, verarbeitet und dargestellt werden. Dies geschieht mit Hilfe von Netzwerkmanagementtools.
Im nachfolgenden Bild 8.3 ist eine mögliche Umsetzung der Verbesserungen dargestellt.

Diese Verbesserungen gliedern sich in:

- Einführung einer Demilitarized Zone (DMZ), in der sich der Webserver, das Mail-Gateway und ein Proxy für sonstigen Internetverkehr befindet. Dies dient dazu, den gesamten ein- und ausgehenden Verkehr überwachen und filtern zu können. Insbesondere die Filterung ist für das spätere Datenschutzkapitel relevant.

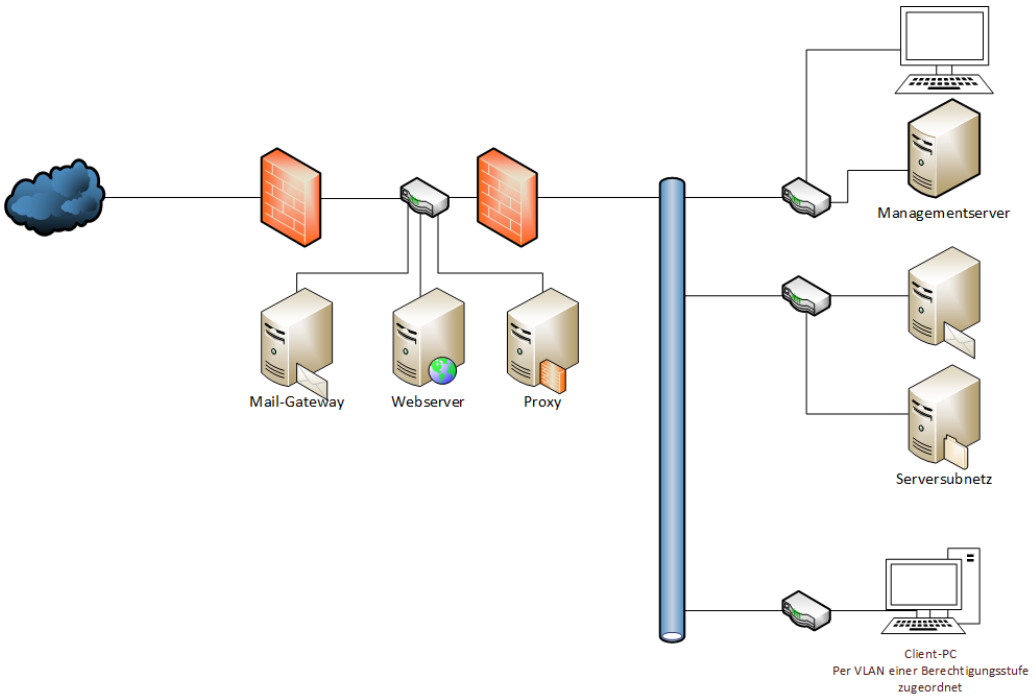


Abbildung 8.3: Gliederung des Netzes nach Reorganisation

- Einführung eines getrennten Management-Netzes. Dieses Netz besteht aus einem oder mehreren Management-Servern und zugehörigen Arbeitsplätzen. Es nimmt alle Statusinformationen der restlichen Komponenten auf und speichert diese.

- Zusammenfassung aller File-Server und Einrichtung eines Mail-Servers in einem Subnetz. Dieses Netzwerk gibt nur seine Dienste in das Intranet frei. Falls einzelne Dienste in das Internet weitergereicht werden sollen, geschieht dies über einen Proxy in der DMZ. Sämtliche Wartung muss innerhalb des Netzes geschehen.

- Zuordnung eines jeden Benutzers/Client-PC zu einer Berechtigungsstufe. Umsetzung der Trennung verschiedener Organisationsbereiche durch Virtual Local Area Network (VLAN).

### 8.2.2 Firewalls

Firewalls bilden die äußerste Verteidigungslinie eines Netzes. Sie arbeiten auf den International Organization for Standardization (ISO)-Schichten 3 und 4, wobei auch Schicht 7 bei modernen Firewalls zum Einsatz kommen kann. Es gibt verschiedene Kategorien: Paketfilter, Stateful Inspection, Proxyfilter und Contentfilter. Das BSI betrachtet in seinem Grundschutzkatalog nur statische und dynamische Paketfilter/Stateful Inspection[7]. Die statischen Paketfilter verwenden nur die Header-Daten eines jeden Paketes ohne auf den

Kontext bzw. andere Pakete zu achten. Der dynamische Paketfilter betrachtet diesen Kontext. Es wird dafür gespeichert, von welchen Endgerät über welchen Port/Protokoll zu welchem Ziel eine Verbindung aufgebaut wurde, damit Antwortpakete durchgelassen werden können. Dadurch ist es möglich, eine deutlich tiefer greifende Analyse der Datenflows durchzuführen.

### iptables/ufw

Das System, mit dem im Auslieferungszustand geringsten Funktionsumfang, ist in diesem Vergleich iptables. Da es aber seit Linux 2.4 in den Kernel integriert ist [1] und die Funktionalitäten (insbesondere die Netzwerksegmentierung und die Beschränkung von Diensten für einzelne Endgeräte) der anderen Produkte nachgebildet werden können, lohnt sich die Betrachtung dieses dynamischen Paketfilters mit einfachen Stateful-Inspection-Funktionen. Für jede Verbindung ist die Erstellung einer Regel notwendig, die das Verhalten der Firewall genau beschreibt. Der Administrator muss sich also zuerst überlegen, welches Gerät (oder Subnetz) auf welche Adressen über welche Ports zugreifen darf. Dabei wird er von iptables, nicht von Helfern unterstützt. Dies ist gleichzeitig einer der größten Nachteile des Systems, da dafür ein bestimmtes Wissen vorausgesetzt wird und Fehlkonfigurationen wahrscheinlicher werden.
Zur Unterstützung des Administrators bei der Konfiguration gibt es zahlreiche Programme. Als Beispiel sei hier ufw (uncomplicated firewall) genannt. Dieses Kommandozeilenprogramm gehört zum Standardprogramm der meisten Linux-Distributionen. Hiermit können mit einfachen Kommandos die zum Teil recht komplexen Regeln von iptables erstellt werden. Bei den vielen Diensten entfällt auch die Angabe des Ports, da dieser bereits gespeichert ist.

### Firewall-1/VPN-1

Die israelische Firma Check Point, die nach eigenen Angaben Marktführer ist, bietet unter dem Namen "Check Point Firewall Software Bladeëine Stateful Packet Inspection Firewall an. Es gilt als das Unternehmen, das die erste funktionierende Stateful Packet Inspection Firewall implementiert hat. Das BSI beurteilte in einer Studie aus dem Jahre 2001 [6] die zugrundeliegende Firewall-1 wie folgt:
"Vorteilhafte Eigenschaften:

- Die CheckPoint FireWall-1 lässt sich gut in ein umfassendes Netzwerk-Sicherheitsmanagement einbinden. So kann man mit der Administrationskonsole auch die Router und Switches verschiedener Hersteller konfigurieren und überwachen.

- Mit Gründung der Operational Security (OPSEC)-Initiative ist es Checkpoint gelungen, eine Reihe von Produktherstellern rund um die Firewall (angefangen von Clustering über Network Management bis hin zu Virus Checking) zur Unterstützung gemeinsamer Schnittstellen und Prinzipien zu gewinnen. Das macht die FireWall-1 für komplexe Umgebungen mit vielfältigen Anforderungen interessant.

- Die Version 4.0 der Firewall-1 wurde 1999 nach Information Technology Security Evaluation Criteria (ITSEC) E3 zertifiziert. Die aktuelle Produktversion ist auf Windows NT 4.0/SP 4 und zwei Netzwerkadaptern nach Common Criteria (CC) EAL2 zertifiziert (Zertifizierungsreport siehe http://niap.nist.gov/cc-scheme/CCentries/TTAP-CC-0006.html). Außerdem ist die Firewall-1 von International Computer Security Association (ICSA) (siehe auch Abschnitt 4.18, „Bedeutung der Zertifizierung“) zertifiziert.

Unvorteilhafte Eigenschaften:

- Proxy-Dienste werden von CheckPoint vernachlässigt. In den einschlägigen Listen [BugTraq, CERT, eSO] werden wiederholt Schwachstellen im Bereich der Stateful Inspection der Firewall-1 bekannt. Es stellt sich daher die Frage, ob diese Technik tatsächlich ein Application Gateway ersetzen kann. [1]

- Viele interessante Features sind nicht in der Standarddokumentation beschrieben und somit nur unter Mithilfe von Spezialisten nutzbar. So wird im Prinzip die Definition unterschiedlicher administrativer Rollen ermöglicht, womit auch die Trennung zwischen Administration und Revision durchgeführt werden kann. Leider geben die Handbücher darüber keine Auskunft.

- Defizite sind im Bereich des Verhaltens der Firewall bei partiellen Ausfällen und im fehlenden Integritätstest festzustellen.”

Mittlerweile ist diese Firewall eine Komponente in der Sicherheitssuite SSecurity Gateway Systems”. Diese läuft auf einem gehärteten Linux-System und bietet weitere Software-Blades für VPN, die Filterung des Internetverkehrs oder Anti-Spam. Das angesprochene Application Gateway wurde seit dieser Studie weiter ausgebaut und ist nun als gesonderte Produkte erhältlich (”Check Point Secure Web Gateway Applianceünd Äpplication Control Software Blade”). Dabei können einzelne Dienste und Seiten für bestimmte Nutzer(-gruppen) freigegeben werden und sogar per Secure Sockets Layer (SSL) verschlüsselte Kommunikationen untersucht werden.

[1] Mit der großen Verbreitung der FireWall-1 steigt die Wahrscheinlichkeit, dass zu diesem Produkt vermehrt Fehlermeldungen auftauchen.

Ein besonderes Modul stellt das Ïdentity Awareness Software Blade"dar. Darüber wird die Möglichkeit bereitgestellt, Nutzern auf der Basis von Identitäten, die aus Diensten wie Active Directory, Lightweight Directory Access Protocol (LDAP) oder Remote Authentication Dial-In User Service (RADIUS) gewonnen werden, Geräten oder Aufenthaltsorten Zugriff auf Netzwerkressourcen, Anwendungen oder Daten zu gewähren.[12]

**ipfire**

Vom Funktionsumfang und der Erweiterbarkeit vergleichbar mit der Sicherheitssuite von Check Point ist die Open-Source-Software IPFire. Auch diese basiert auf einem gehärteten Linux, in der momentanen Version auf der Grundlage von Linux from scratch. In der Grundversion sind bereits viele Funktionalitäten vorhanden, die über eine Firewall oder Router hinausgehen. Dazu zählen u.a. ein OpenVPN-Server, das Intrusion Detection System Snort mit der Erweiterung guardian oder ein Proxyserver mit Contentfilter. Zusätzlich lassen sich Add-ons über den integrierten Paketmanager installieren. Dadurch lässt sich das System mit weiteren Funktionalitäten nachrüsten, wie z.B. Datei-, Druck- und Mailserver, Virenscanner oder Netzwerkmanagementtools. Diese stellen unter Umständen Sicherheitsprobleme dar, da nicht ausgeschlossen werden kann, dass in diesen Sicherheitslücken vorhanden sind und ein Angreifer darüber Zugriff auf die Firewall erlangen kann.

Als Firewall kommt Endian Firewall zum Einsatz, die von der Südtiroler Firma Endian Srl betreut wird. Sie ist eine Stateful Paket Inspection Firewall, die auf das Linux Paketfilter-Framework netfilter aufbaut. Allerdings versteht diese Firma ihr Produkt als mehr als nur eine Firewall, deshalb hat sie neben Routerfunktionalitäten (es findet schon von Haus aus eine Trennung in rotes/unsicheres, grünes/sicheres, oranges/teilsicheres oder "demilitarisiertesünd blaues/teilsicheres, da drahtloses Netz statt) auch Funktionalitäten wie einen Virenscanner und einen Spamfilter eingebaut. Bedient wird die Endian Firewall normalerweise über eine Webschnittstelle, die damit ein graphisches Interface zur Verfügung stellt.

### 8.2.3 Netzwerkmanagementtools

Im Modul B 4.2 Netz- und Systemmanagement des Grundschutzkataloges des BSI [7] wird das Netzmanagement als "die Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung des effektiven Einsatzes eines Netzes [beschrieben]. Hierzu gehört beispielsweise die Überwachung der Netzkomponenten auf ihre korrekte Funktion, das Monitoring der Netzperformance und die zentrale Konfiguration der Netzkomponenten. Netzmanagement ist in erster Linie eine organisatorische Problemstellung, deren Lösung lediglich mit technischen Mitteln, einem Netzmanagementsystem, unterstützt werden

kann."
Zur Überwachung einzelner Komponenten ist es nötig, auf diesen sogenannte Agenten einzusetzen, die über ein Managementprotokoll, unter Umständen über Subagenten, mit dem Manager verbunden sind. Diese Protokolle können entweder die standardisierten Protokolle Simple Network Management Protocol (SNMP) und Common Management Information Protocol (CMIP) oder proprietäre herstellerspezifische Protokolle sein.

### Nagios

Das Netzwerkmanagementtool Nagios von Ethan Galstadt, der gleichzeitig die Firma Nagios Enterprises LLC zur Betreuung des Projekts führt, basiert auf einem Apache-Webserver. Ihr Vorteil liegt in der einfachen und Ressourcen sparenden Funktionsweise. Jede einzelne Überwachung besteht aus den folgenden Konfigurationsmöglichkeiten:

- *hosts:* Die zu überwachende Komponente, in der Regel definiert durch die IP-Adresse
- *services:* Der zu überwachende Dienst, z.B. Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) oder eine Eigenschaft der Komponente wie z.B. verfügbarer Speicherplatz, Auslastung oder interne Fehlermeldungen.
- *commandos:* Parameter, die zur Erlangung der gewünschten Informationen notwendig sind
- *contact:* Dieser Parameter beschreibt das Verhalten im Alarmfall

Da die Erstellung dieser Regeln ein fundiertes Wissen über den jeweiligen Dienst voraussetzt, gibt es zahlreiche Plug-Ins, die schon für den jeweiligen Dienst vorkonfiguriert sind - Zum Zeitpunkt dieser Arbeit sind es über 3300 [13]. Diese Plug-Ins sind eigenständige Programme, die über zwei Parameter mit dem Hauptprogramm kommunizieren. Der erste ist ein String, der im Webinterface und in den Benachrichtigungen veröffentlicht wird, der zweite ist eine Zahl, die die Werte 0 für ÖK", 1 für "Warning", 2 für "Criticalünd 3 für Ünknown"beinhalten kann. [11] Diese Programme können in jeder beliebigen Sprache - so lange sie auf einem Webserver ausgeführt werden kann - verfasst werden, verbreitet sind hierbei Perl, Python und auch Shell-Programme. Zusätzlich können diese Plug-Ins nicht nur einfache Regeln auswerten, sondern auch mit dem Dienst interagieren, um nicht nur prüfen zu können, ob ein Dienst erreichbar ist, sondern auch, ob der Dienst auf Nutzereingaben korrekt reagiert.

### Zenoss

Das Netzwerkmanagementtool Zenoss der Firma Zenoss Inc. ist ebenso eine Open-Source-Software, basiert allerdings auf Python und Java. Es stellt ebenfalls ein Webinterface zur Verfügung, welches allerdings für vielfältigere Aufgaben eingesetzt werden kann:

- *Gerätemanagement* In diesem Bereich werden alle Geräte, die im überwachten Netzwerk eingesetzt werden, in einer zentralen Datenbank gespeichert. Zusätzlich können alle Veränderungen an diesen gesichert werden. Der Administrator kann manuell Geräte eintragen oder diese selbstständig finden lassen, indem Routingtabellen zu Informationsgewinnung herangezogen werden. Zur Definition eines Gerätes können SNMP, Secure Shell (SSH) oder Ports eingesetzt werden.

- *Verfügbarkeits- und Performanceüberwachung* Zenoss setzt die Layer-3 Protokolle Internet Control Message Protocol (ICMP) und SNMP ein, um die Verfügbarkeit bzw. Erreichbarkeit der folgenden Geräte/Dienste zu ermitteln:

  - Netzwerkgeräte
  - TCP/IP Dienste und Ports
  - Erreichbarkeit von URLs
  - Windows-Dienste und Prozesse
  - Linux Prozesse

  Die aus den Routingtabellen gewonnenen Informationen über die Netztopologie ermöglichen es Zenoss, Folgefehler zu erkennen und dem Nutzer auszublenden. Gleichzeitig kann es dadurch einen Netzplan der überwachten Komponenten erstellen.
  Im Bereich der Performanceüberwachung kann Zenoss Statistiken über Dateisysteme, CPU-Last und Speicher-Gebrauch erstellen, sowie über Java Management Extensions (JMX) Java Anwendungen überwachen. Zusätzlich unterstützt es auch Plug-Ins für Nagios und Cacti. Beim Überschreiten eines definierten Schwellwertes kann es dann ein Ereignis auslösen.

- *Ereignismanagement* Neben den gerade erwähnten Statistiken können auch Logs sowie Alarmierungen über SNMP Ereignisse auslösen. Diese kann der Nutzer für seine Erfordernisse definieren und priorisieren. Das System unterstützt ihn dabei durch eine automatische Kategorisierung, Verhinderung von Mehrfachalarmen und eine Korrelation von Ereigniseintritten. Wie das System auf ein Ereignis reagieren soll, definiert der Administrator durch ein Regelwerk, in dem er festlegt, ob das System z.B. eine E-Mail schicken, ein Script ausführen oder auch nichts tun und nur den Vorfall aufzeichnen soll.

- *Erstellung von System-Berichten* In diesen Berichten werden Informationen aus dem Gerätemanagement, der Verfügbarkeits- und Performanceüberwachung, dem Ereignismanagement und der Benutzerverwaltung zusammengeführt. Dadurch kann der Auslöser für ein bestimmtes Ereignis durch den menschlichen Betrachter leichter gefunden werden.

- *Benutzer- und Alarmierungsverwaltung* Zenoss erlaubt es, verschiedene Benutzerkonten mit verschiedenen Zugriffsrechten anzulegen. Diese können auch im Alarmierungsfall einzeln angesprochen werden, so dass nur die Personen über Ereignisse informiert werden, die diese Information auch benötigen.[9]

### 8.2.4 Datenschutz

In der Studie [3] wurde festgestellt, dass 50% der deutschen kleinen und mittelständischen Unternehmen die private Nutzung des Internets und/oder E-Mails vollständig oder zumindest teilweise (wie z.B. außerhalb der Kernarbeitszeiten) gestatten. Die Problemstellungen, die sich hieraus ergeben, und mögliche Lösungen werden in den folgenden Abschnitten dargestellt.

#### Rechtslage

Die relevanten Quellen für diesen Aspekt sind der §88 des Telekommunikationsgesetz (TKG) und das Bundesdatenschutzgesetz (BDSG).
In §88 TKG wird das Fernmeldegeheimnis festgelegt. Es besagt, dass der Inhalt und die beteiligten Personen einer Verbindung und auch die näheren Umstände erfolgloser Verbindungsversuche dem Fernmeldegeheimnis unterliegen. Der Dienstanbieter darf diese Informationen nur im erforderlichen Maß zur Erbringung der Leistung und dem Schutz seiner technischen Systeme verwenden, d.h. alles was nicht erforderlich ist, darf gar nicht erst erfasst werden.

Gemäß §9 des BDSG haben "Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, [...] die Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes [...] zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."Personenbezogene Daten sind hierbei nach §3 Abs. 1 BDSG Ëinzelangaben, über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Besondere Arten sind hierbei Ängaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben"(§3 Abs. 9 BDSG).

Betroffene Personen haben nach dem BDSG und den Landesdatenschutzgesetzen die folgenden Rechte:

- *Recht auf Auskunft* Welche Daten sind vorhanden? Woher kommen diese? Warum werden diese gespeichert?
- *Recht auf Berichtigung* Wenn falsche Daten gespeichert wurden, müssen diese richtiggestellt werden können.
- *Recht auf Sperrung* Wenn sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt und der Betroffene die Richtigkeit anfechtet, müssen diese Daten für die Verarbeitung gesperrt werden.
- *Recht auf Löschung* Wenn Daten unrechtmäßig erhoben wurden, die Speicherung dieser unzulässig ist oder sie nicht mehr benötigt werden, müssen die Daten gelöscht werden. Wenn ein triftiger Grund (gesetzliche Fristen, schutzwürdige Interessen des Betroffenen oder unverhältnismäßiger Aufwand) gegen die Löschung besteht, werden die Daten nur gesperrt, bis dieser Grund wegfällt.
- *Recht auf Widerspruch gegen die Datenverarbeitung* Wenn die persönlichen Umstände des Betroffenen gegen die Verarbeitung sprechen, dürfen die Daten nicht verarbeitet werden, falls dies nicht durch eine Vorschrift oder Gesetz verlangt wird.
- *Recht auf Schadensersatz* Wenn Daten unzulässig oder unrichtig erhoben, verarbeitet oder benutzt wurden, darf der Betroffene Schadensersatz fordern.

**Umsetzung**

In der Umsetzung ist insbesondere der §9 des BDSG relevant. Aus ihm folgt die Pflicht, Maßnahmen zu treffen, die dem Schutz persönlicher Daten dienen [4]. In der Anlage dazu sind acht Kontrollziele (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Einhaltung der Zweckbestimmung) für die technischen und organisatorischen Maßnahmen vorgegeben.
Im BSI-Grundschutz werden im Baustein B1.5 Datenschutz die Maßnahmen M2.501 bis M2.515, sowie M2.110 für Datenschutzaspekte in der Planung, Konzeption, Umsetzung und im Betrieb vorgestellt.

- *Planung und Konzeption*
  - *M2.501 Datenschutzmanagement* Vorstellung des Prozesses, der zur Umsetzung der gesetzlichen Anforderungen des Datenschutzes notwendig ist. Dieser Datenschutzprozess ist ein zyklischer Prozess, der aus den Phasen Soll-Ist-Abgleich, Umsetzung fehlender Maßnahmen und Aufrechterhaltung des Datenschutzes im laufenden Betrieb besteht.

  - *M2.502 Regelung der Verantwortlichkeiten im Bereich Datenschutz* In dieser Maßnahme wird die Funktion eines betrieblichen bzw. behördlichen Datenschutzbeauftragten vorgestellt. Insbesondere wird darauf eingegangen, welche Qualifikationen dieser haben muss, mit welchen anderen Funktionen dieses Amt zusammengelegt werden darf und welche Rechte und Pflichten ihm zugestanden werden sollten.
  - *M2.503 Aspekte eines Datenschutzkonzeptes* Hier ist eine Aufzählung möglicher Aspekte zu finden, die bei der Erstellung eines Datenschutzkonzeptes relevant sind. Diese Punkte können dazu dienen, dass alle Bereiche und Vorgänge einer Institution/Firma in diesem Konzept abgedeckt werden.
  - *M2.504 Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten* Als Voraussetzung für die Verarbeitung personenbezogener Daten muss zunächst geprüft werden, ob dies zulässig und erforderlich ist, ob die Daten für einen bestimmten oder besonderen Zweck verwendet werden und ob eine Vorabkontrolle notwendig ist.
  - *M2.505 Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten* Diese Maßnahme beschäftigt sich mit den oben aufgeführten acht Kontrollzielen und wie man diese umsetzen kann.

- *Umsetzung*

  - *M2.506 Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten* Bevor Personen personenbezogene Daten verarbeiten dürfen, müssen diese über die Wahrung des Datengeheimnisses unterrichtet bzw. dazu verpflichtet werden.
  - *M2.507 Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten* Die Wahrung der oben aufgeführten Rechte betroffener Personen muss gewährleistet werden.
  - *M2.508 Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten* Es muss ein Verfahren zur Erstellung eines Verzeichnisses aller eingesetzten Hardware und Software zur Verarbeitung personenbezogener Daten sowie der Verfahren bei der Bearbeitung und Erhebung dieser existieren.
  - *M2.509 Datenschutzrechtliche Freigabe* Vor dem Einsatz von Software und IT-Verfahren müssen diese geprüft werden, u.a. im Bezug auf den Datenschutz. Dies kann mit anonymisierten oder unter bestimmten Umständen auch nicht-anonymisierten Daten erfolgen. In diesem Modul werden die Bedingungen und das Vorgehen beim Einsatz dieser beschrieben.

  - *M2.510 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten* Wenn anderen Stellen (z.B. bei einem elektronischen Grundbuch Notaren, Banken und Versicherungen) automatisiert Zugriff auf personenbezogene Daten gewährt wird, sind bestimmte Aspekte zu beachten, insbesondere, dass gespeichert wird, wer wann darauf zugegriffen hat, und dass ausreichende Maßnahmen gegen unbefugten Zugriff getroffen wurden.
  - *M2.511 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten* Wenn die Verarbeitung personenbezogener Daten ausgelagert wird, bleibt dennoch der Auftraggeber für die Einhaltung des Datenschutzes verantwortlich.
  - *M2.512 Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten* Wenn personenbezogene Daten nicht durch eine Maske, die nur bestimmte Zugriffe erlaubt, sondern durch frei wählbare Attribute abgefragt werden können, ist zu verhindern, dass dadurch unzulässige Ergebnisse (wie z.B. detaillierte Profile) erzielt werden können.

- *Betrieb*

  - *M2.110 Datenschutzaspekte bei der Protokollierung* Hier wird aufgeführt, was auf jeden Fall protokolliert werden sollte und welche Daten u.U. nur selektiv geloggt werden müssen. Zusätzlich werden Empfehlungen zu Aufbewahrungsdauer und anderen technischen und organisatorischen Rahmenbedingungen ausgesprochen.
  - *M2.513 Dokumentation der datenschutzrechtlichen Zulässigkeit* Jegliche Soft- und Hardware, die zur Verarbeitung personenbezogener Daten eingesetzt wird, muss auf ihre Datenschutzkonformität geprüft werden. Die Ergebnisse sind festzuhalten.
  - *M2.514 Aufrechterhaltung des Datenschutzes im laufenden Betrieb* IT-Revision, die die Ordnungsmäßigkeit der Datenverarbeitung überwacht, und Datenschutzkontrolle, die die Einhaltung der datenschutzrechtlichen Anforderungen kontrolliert, arbeiten miteinander zusammen, um die Speicherung von Protokolldaten möglichst kurz zu halten und Missbrauch frühzeitig aufzudecken.
  - *M2.515 Datenschutzgerechte Löschung/Vernichtung* Beim Aussondern von Datenträgern ist sicherzustellen, dass keine Informationen von diesen mehr gelesen werden können. Dies kann durch mehrmaliges Überschreiben, mechanische oder thermische Zerstörung oder magnetische Durchflutung geschehen.

### Beispiel Firewall und Netzwerkmanagementtools

Nachdem im vorherigen Teil der Datenschutz und seine Umsetzung abstrakt betrachtet wurden, soll hier beispielhaft die Umsetzung an den vorher be-

sprochenen Netzkomponenten Firewall und Netzwerkmanagementtools dargestellt werden.

Zunächst gilt es zu klären, ob an diesen Stellen überhaupt personenbezogene Daten erhoben werden bzw. ob diese unter das TKG fallen. Firewalls sind hierbei besonders durch das Fernmeldegeheimnis betroffen, da sie an jeder Kommunikation beteiligt sind. Beide vorgestellten Firewalls sind Stateful Inspection Firewalls, d.h. sie speichern für einen gewissen Zeitraum, von welchem Rechner welche Verbindung nach außen aufgebaut werden soll. Diese Daten sind sowohl für die Erbringung der Leistung als auch für die Absicherung der technischen Systeme notwendig und dürfen somit nach TKG erhoben werden. Die Daten können aber Rückschlüsse auf die persönlichen Verhältnisse eines Nutzers gestatten, sobald dieser Verbindungen außerhalb der dienstlichen Notwendigkeit aufbaut. Dieses Thema wird insbesondere dann relevant, sobald die private Nutzung des Internets erlaubt wird. Da die Regeln, die bei Stateful Inspection Firewalls zur Annahme der Antworten erstellt werden, per default ziemlich lange gespeichert werden - bei iptables sind fünf Tage der Standardwert für TCP-Verbindungen, die nicht abgebaut wurden -, kommen hierbei datenschutzrechtliche Aspekte ins Spiel. In der Abbildung 8.4 ist eine beispielhafte Übersicht, die aus der Endian Firewall stammt, dargestellt. Zu erkennen sind der lokale Rechner mit Port, der Zielrechner mit Port, über den der aufgerufene Dienst erkennbar ist, das Protokoll und wie lange die jeweilige Verbindung noch gespeichert wird. Es muss also sichergestellt werden, dass - nicht nur aus diesem Grund - kein Unberechtigter Zugriff auf die Firewall erhält. Gleichzeitig sollte auch der Datenschutzbeauftragte und damit auch jeder Mitarbeiter über diese Tatsache informiert werden.

Netzwerkmanagementtools hingegen sind in der Regel nicht an der Kommunikation beteiligt und fallen somit nicht unter das Fernmeldegeheimnis. Allerdings können hier andere personenbezogene Daten entstehen, z.B. könnte festgestellt werden, ob ein Rechner während einer Gewerkschaftssitzung benutzt wird oder wie häufig Arbeitspausen eingelegt werden. Zugleich ist hier auch die Speicherung für die Datenschutzproblematik relevant, da aus diesen Protokolldateien Zuverlässigkeitsaussagen gewonnen werden können, wenn sie über einen längeren Zeitraum vorliegen. Deshalb sollte zunächst geprüft werden, ob überhaupt jedes Endgerät überwacht werden sollte bzw. ob gerade solche sensiblen Daten von diesem erhoben werden müssen. So könnte zum Beispiel ein Rechner nicht regelmäßig nach seinem Betriebszustand gefragt werden, sondern dieser erhält die Möglichkeit, Fehlermeldungen selbstständig abzusetzen. Dabei ist allerdings abzuwägen, ob das damit verbundene Risiko, dass ein Ausfall nicht erkannt wird, zu akzeptieren ist. Bei Arbeitsplatzrechnern kann dies aber der Fall sein, wenn bei diesen eine gewisse Ausfallzeit akzeptabel ist und der Mitarbeiter die Fehlermeldung über einen anderen Kanal absetzen kann. Auf jeden Fall ist auch hier der Datenschutzbeauftragte in die Planung einzubeziehen und anschließend jeder Mitarbeiter über die Umsetzung zu informieren.

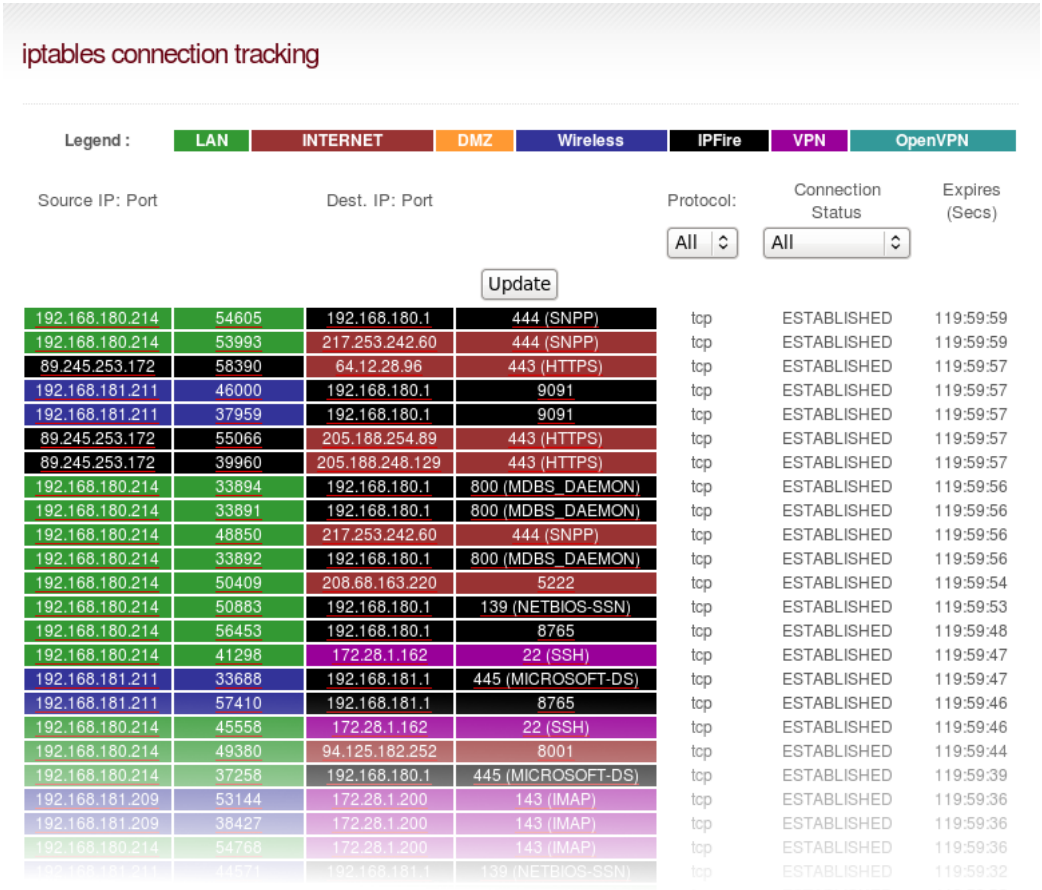


Abbildung 8.4: Übersicht über momentan aufgebaute Verbindungen

Eine weitere Problematik bei der Überwachung von Netzen kann entstehen, wenn in einem drahtlosen Netz gespeichert wird, wann welches Gerät in welche Funkzelle eingeloggt war. Cisco bietet hierfür eine Anwendung "Cisco Wireless Location Appliance", die die Aufenthaltsorte und dadurch den Bewegungsverlauf von drahtlosen Geräten speichert und sowohl graphisch darstellen als auch in Extensible Markup Language (XML) exportieren kann. Die Vorteile liegen darin, dass dadurch bestimmte Bereiche und Geräte überwacht werden können und beim Betreten bzw. Verlassen von vorher definierten Gebieten Alarm ausgelöst werden kann. Da dadurch Bewegungsprofile von Mitarbeitern erstellt werden können, ist der Einsatz als problematisch zu bewerten. Der Datenschutzbeauftragte ist hier auf jeden Fall vor der Einführung zu konsultieren. Der Einsatz kann jedoch durch eine Betriebsvereinbarung gestattet werden. Schwieriger wird es allerdings, wenn dadurch auch Geräte überwacht werden, die nicht Mitarbeitern zuzuordnen sind, wie z.B. Kunden oder Besuchern. Diese sind vor der Nutzung zu informieren und aufzuklären.

### 8.2.5 Sicherheitsrisiko Mitarbeiter

Im Jahr 2013 veröffentlichte das BSI seinen Cyber Security Report [10], in welchem unter anderem auch Unternehmen nach den Gefahrenquellen für die IT-Sicherheit in ihrem Unternehmen gefragt wurden. 57% der Unternehmen gaben dabei an, dass Mitarbeiter, die leichtfertig mit Daten umgehen und Sicherheitsstandards umgehen, eine große oder sehr große Gefahr darstellen. Zusätzlich fürchten 36% der Unternehmen Datenmissbrauch, z.B. durch unerlaubte Weitergabe von Daten durch Mitarbeiter des Unternehmens. Der erste Punkt nimmt mit der Größe des Unternehmens zu. So sind es bei Unternehmen, die zwischen 50 und 100 Mitarbeiter haben, 48%, während Unternehmen mit über 1000 Mitarbeitern schon zu 68% den leichtfertigen Umgang mit Daten fürchten.

Deshalb soll nun im Folgenden auf zwei Aspekte der "menschlichenSSeite der Netzwerksicherheit eingegangen werden, wobei hier auch stets noch eine Brücke zum vorhergehenden Aspekt des Datenschutzes geschlagen wird.

#### Private Nutzung des Internets

Laut der bereits erwähnten Studie [3] gestatten über die Hälfte der kleinen und mittelständischen Unternehmen in Deutschland die private Nutzung des Internets. Einschränkungen beschränken sich auf die Nutzungszeiten und Filterlisten, die den Zugriff auf bestimmte Seiten verbieten. Damit wird nur ein Aspekt der Problematik betrachtet, nämlich der der Produktivität der Mitarbeiter in einem Unternehmen. Dadurch lässt sich allerdings noch nicht der Abfluss von Daten durch Mitarbeiter verhindern. Dafür bietet sich ein zweigleisiges Vorgehen an, zum einen durch die technische Absicherung durch den Einsatz von Contentfiltern, die innerhalb des Datenstromes nach Schlüsselwörtern suchen und gegebenenfalls diese Verbindung trennen, und zum anderen durch die Schulung der Mitarbeiter. Gerade dieser Aspekt ist besonders wichtig, da der Abfluss von Daten nicht nur über das Internet sondern auch über andere, schwerer kontrollierbare Kanäle stattfindet.

Das BSI empfiehlt hierfür in der Maßnahme M2.198 die Schulung der Mitarbeiter, damit diese Zwischenfälle frühzeitig erkennen und eigenverantwortlich sinnvolle Maßnahmen ergreifen können. Dabei soll zunächst eine Information der Mitarbeiter über die Grundprinzipien der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit), das Sicherheitskonzept der Institution und die Umsetzung davon in den Sicherheitsrichtlinien stattfinden. Dabei ist allerdings darauf zu achten, dass nicht alle Details enthüllt werden, damit der Mitarbeiter die Kenntnis über diese nicht dazu nutzen kann, um Sicherheitseinrichtungen zu umgehen. Anschließend sollen Mittel gefunden werden, um auch im Alltag stets auf die Thematik hinzuweisen, z.B. durch Plakate in der Kantine. Notwendig für den Erfolg ist vor allem, dass die Vorgesetzten und andere Mitarbeiter an der Umsetzung mitwirken. So

könnten z.B. die Vorgesetzten selbst auch intern nur verschlüsselte E-Mails verschicken und damit eine Vorbildfunktion einnehmen.

Je mehr Ressourcen in diesen Bereich investiert werden, desto weniger dringlich ist die Einführung technischer Gegenmaßnahmen, wie es ein Contentfilter sein kann. Dieser ist auch aus Datenschutzsicht recht problematisch, da hier jede Kommunikation nach Schlüsselwörtern abgesucht wird und anhand dieser Rückschlüsse auf besonders schützenswerte personenbezogene Daten, wie z.B. den Gesundheitszustand, möglich sind.

**Private E-Mails**

Ein besonderer Fall der Internetnutzung ist die Verwendung eines dienstlichen E-Mail-Accounts für private Zwecke. Interessant dafür ist das Urteil des Landgerichts Berlin-Brandenburg vom 16. Februar 2011 (Az. 4 Sa 2132/10). Darin stellt das Gericht fest:
"1. Ein Arbeitgeber wird nicht allein dadurch zum Dienstanbieter i. S. d. Telekommunikationsgesetzes, dass er seinen Beschäftigten gestattet, einen dienstlichen E-Mail-Account auch privat zu nutzen.

2. Belassen die Beschäftigten bei Nutzung des Arbeitsplatzrechners die eingehenden E-Mails im Posteingang bzw. die versendeten im Postausgang, so unterliegt der Zugriff des Arbeitgebers auf diese Daten nicht den rechtlichen Beschränkungen des Fernmeldegeheimnisses.-[5]

In der Begründung spricht das Gericht davon, dass §88 TKG hier keine Anwendung finden kann, da der Übertragungsvorgang in dem Moment zu Ende ist, in dem die E-Mail beim Empfänger angekommen ist. Ein Postfach, in dem eingegangene oder versandte E-Mails gespeichert werden, unterliegt somit nicht dem Fernmeldegeheimnis.

Allerdings darf das Unternehmen als privat gekennzeichnete E-Mails nicht öffnen oder lesen, soweit dies klar erkennbar ist. Dies ist nach Ansicht des Gerichts dadurch gegeben, dass im Betreff das Schlagwort "privat"benutzt wird.

Ansonsten gelten für die E-Mail-Nutzung die gleichen Richtlinien wie für die Internetnutzung im Allgemeinen.

## 8.3 Bewertung

In diesem Abschnitt werden zunächst die vorgestellten Netzkomponenten miteinander verglichen und bewertet, danach der Datenschutz im Unternehmen. Bewertungskriterien für die Netzkomponenten sind:

- *Benutzerfreundlichkeit* Unter diesem Begriff wird die Erfahrung des Benutzers bei der Bedienung verstanden.
- *Wartungsfreundlichkeit* Weiter als die Benutzerfreundlichkeit geht die Wartungsfreundlichkeit, hier finden vor allem die Möglichkeiten zur Administration Einfluss.
- *Versorgung mit Updates* Gerade bei Software, die an sicherheitsrelevanten Stellen eingesetzt wird, ist es notwendig, dass schnellstmöglich auf Sicherheitslücken reagiert wird.
- *Dokumentation* Es ist einerseits wichtig, dass die Schnittstellen genau beschrieben und offengelegt sind, da Netzkomponenten niemals getrennt von anderen Systemen eingesetzt werden. Andererseits muss auch sichergestellt werden, dass der Administrator über die Möglichkeiten der Software informiert ist, da Fehlkonfigurationen hier besonders schwerwiegende Folgen haben können.
- *Ressourcenbedarf* Hier wird betrachtet, wie die Systemvoraussetzungen für ein solches System sind, da geringere Anforderungen einfachere Systeme erlauben, aber auch bei einem erhöhten Datenaufkommen noch mit einem vertretbaren Aufwand eingesetzt werden können.

Als erstes werden die Suites Security Gateway Systems mit Firewall-1/VPN-1, IPFire und iptables/ufw betrachtet. Im Hinblick auf die Wartungsfreundlichkeit liegt Firewall-1/VPN-1 vorne, da dies ein kommerzielles Produkt ist, welches über eine graphische Oberfläche einzurichten ist. Auf einem ähnlichen Niveau liegt auch die Endian Firewall von IPFire, da auch sie eine Weboberfläche zur Verfügung stellt, die Administration der zugrundeliegenden Distribution erfolgt aber über Kommandozeile, es sei denn ein Add-on stellt eine eigene Oberfläche zur Verfügung. Hingegen ist iptables/ufw nur über die Kommandozeile bedienbar.
Auch in der Benutzerfreundlichkeit zeichnet sich die Firewall-1/VPN-1 durch eine graphische Oberfläche aus, die für weniger gut ausgebildete Nutzer eine geringere Hemmschwelle darstellt. Die Bedienbarkeit über den Browser erleichtert auch die Bedienung der Endian Firewall, da hierüber Statistiken eingesehen und Regeln bearbeitet werden können. Die Kommandozeile hingegen bedarf einer gewissen Einarbeitungszeit.
Bei der Versorgung mit Updates hat jedes Produkt gewisse Vor- und Nachteile. Da die Firewall-1/VPN-1 ein kommerzielles Produkt ist, werden solange regelmäßig und häufig Updates zur Verfügung gestellt, wie das Produkt vom Hersteller betreut wird. Allerdings sind diese mit Kosten verbunden. Da iptables/ufw ein Open-Source-Projekt ist, werden die Updates von der Community bereitgestellt und sind daher nicht vorhersagbar, auch wenn sie standardmäßig im Kernel verankert sind und daher von gewissen Firmen auch betreut werden. IPFire nimmt dabei eine Mittelstellung ein, da die Firewall zwar auch von einer Firma betreut wird, diese aber im Ruf steht, Updates für die freie Version nur verspätet oder teilweise auch gar nicht

zur Verfügung zu stellen. Die restliche Software von dieser Suite ist dabei auch von ähnlichen Problemen betroffen, so dass sich hier keine einheitliche Aussage über das Gesamtsystem treffen lässt.
Firewall-1/VPN-1 wurde von einer israelischen Firma selbst entwickelt und dokumentiert nur die Schnittstellen zu anderen Produkten. Dagegen ist iptables/ufw und Endian Firewall als Open-Source-Projekt komplett offengelegt und für jeden im Quelltext zugänglich. Deshalb können hier mehr Personen nach Schwachstellen suchen. Die Zusammenarbeit mit den Nutzern ist bei Open-Source-Projekten ein essentieller Bestandteil der Produktkultur.
Da die Firewall-1/VPN-1 in eine größere Sicherheitssuite eingebettet ist, benötigt sie naturgemäß mehr Ressourcen (Speicherplatz, Rechenleistung, Bandbreite). Bei IPFire sind vor allem die Add-ons für die Dimensionierung des Systems ausschlaggebend, das Grundsystem läuft bereits auf Systemen wie dem Raspberry Pi. Im Gegensatz dazu ist iptables/ufw ein spezialisiertes und auf das Notwendigste beschränktes Programm, das auch auf den kleinsten Systemen arbeitet.

Für kommerzielle Nutzer in großen Unternehmen mit einer kleinen IT-Abteilung ist insbesondere aufgrund der Benutzerfreundlichkeit Firewall-1/VPN-1 zu empfehlen, während Privatanwender mit IT-Kenntnissen mit iptables/ufw ein kosteneffizientes Produkt finden können. Mittelgroße Unternehmen oder Privatanwender mit erweiterten Kenntnissen können mit IPFire die Funktionalitäten einer teuren Software kostenlos zur Verfügung stellen. Eine Übersicht über die verschiedenen Produkte ist in der Tabelle 8.1 zu finden. Die Skala geht hierbei von ⊕ für eine gute Bewertung in dieser Kategorie über ◯ zu ⊖ bei einem schlechten Abschneiden.

Tabelle 8.1: Übersicht über die vorgestellten Firewalls

| | Firewall-1/VPN-1 | IPFire | iptables/ufw |
|---|---|---|---|
| Wartungsfreundlichkeit | ⊕ | ◯ (Endian Firewall: ⊕) | ⊖ |
| Benutzerfreundlichkeit | ⊕ | ◯ (Endian Firewall: ⊕) | ⊖ |
| Versorgung mit Updates | ⊕ | ◯ | ⊕ |
| Dokumentation | ⊖ | ⊕ | ⊕ |
| Ressourcenbedarf | ⊖ | ◯ | ⊕ |

Bei den Netzmanagementtools Nagios und Zenoss treffen zwei Opensourcetools auf einander. Beide stellen dem Nutzer graphische Oberflächen zur Verfügung. Allerdings benötigt Nagios bei der Erstellung der Regeln einen externen Editor, um Textdateien zu bearbeiten. Im Gegensatz dazu werden bei Zenoss die Regeln auf der graphischen Oberfläche erstellt.
Auch bei der Wartungsfreundlichkeit zeichnet sich Zenoss durch seine graphische Oberfläche aus, da hier alle Einstellungsmöglichkeiten gebündelt sind, während der Administrator bei Nagios Konfigurationsdateien bearbeiten muss.

Da beide Projekte Opensource sind, sind beide der Gnade der Community ausgeliefert. Hinter beiden stehen allerdings die Firmen Nagios Enterprices LLC und Zenoss Inc., wodurch die Updates hauptsächlich von der jeweiligen Firma gestellt werden.
Durch die Betreuung über eine Firma kommen auch die kostenfreien Versionen der beiden Produkte in den Genuss der Dokumentation der kommerziellen Produkte. Während Zenoss in Python geschrieben ist und somit direkt in ausführbarem Code vorliegt, benötigt Nagios den Apache-Webserver. Dies kann Zenoss einen Performancevorteil bringen. Eine Übersicht über die verschiedenen Produkte ist in der Tabelle 8.2 zu finden. Die Skala geht hierbei von ⊕ für eine gute Bewertung in dieser Kategorie über ◯ zu ⊖ bei einem schlechten Abschneiden.

Tabelle 8.2: Übersicht über die vorgestellten Netzwerkmanagementtools

| | Nagios | Zenoss |
|---|---|---|
| Wartungsfreundlichkeit | ◯ | ⊕ |
| Benutzerfreundlichkeit | ⊕ | ⊕ |
| Versorgung mit Updates | ◯ | ◯ |
| Dokumentation | ⊕ | ⊕ |
| Ressourcenbedarf | ◯ | ⊕ |

Der Sinn des Datenschutzes liegt im Schutz des einzelnen Mitarbeiters vor einem unberechtigten Zugriff auf seine personenbezogenen Daten. Das Problem ist allerdings, dass diese Daten im Betrieb anfallen oder sogar für den Betrieb eines Netzwerkes notwendig sind. Gleichzeitig ist es für einen Administrator interessant, Daten über sein Netzwerk möglichst lange zu speichern, um die Ursachen etwaiger Probleme genau rekonstruieren zu können. Für die Lösung dieser Problematik ist der Administrator auf die Zusammenarbeit mit dem Datenschutzbeauftragten angewiesen. Diese Zusammenarbeit kann in einer betrieblichen Vereinbarung festgehalten werden, bei deren Erstellung auch der Betriebsrat zu beteiligen ist. In einer solchen Vereinbarung wird geregelt, welche Daten wie lange gespeichert werden dürfen.

## 8.4 Fazit und Ausblick

In dieser Arbeit wurde zunächst ein Netzwerk vorgestellt, dessen Erstellung keinen gesamtheitlichen Konzept gefolgt war. Zu seiner Verbesserung wurde das Vorgehensmodell zur Erstellung einer Sicherheitskonzeption im Informationssicherheitsmanagement gemäß BSI Standard 100-2 beschrieben und angewendet. In dieser Anwendung kamen ausgewählte Bausteine des BSI-Grundschutzes zum Tragen. Im Anschluss daran wurden die Netzkomponenten Firewall und Netzwerkmanagement beschrieben und drei bzw. zwei Produkte in jeder Kategorie dargestellt. Die Firewalls sind Firewall-1/VPN-1,

Endian Firewall und iptables/ufw. Zwei Systeme der ersten Produktgruppe sind Bestandteile einer größeren Sicherheitssuite. Die beiden Netzwerkmanagementtools sind Nagios und Zenoss. Danach wurde in einem weiteren Kapitel die Problematik des Datenschutzes geschildert. Zunächst wurden die rechtlichen Rahmenbedingungen vorgestellt. Relevant ist hierfür vor allem der §88 des Telekommunikationsgesetzes und das Bundesdatenschutzgesetz. Daraus folgern sich bestimmte Rechte, die beschrieben wurden. Die Umsetzung dieser gesetzlichen Vorgaben wurde anhand der Maßnahmen, die im BSI-Grundschutz aufgeführt sind, dargestellt. Die Anwendung dieser Maßnahmen auf die Problematik Firewalls und Netzwerkmangementtools wurde im Anschluss geschildert. In einem weiteren Abschnitt wurde auf das Sicherheitsrisiko durch Mitarbeiter eingegangen, insbesonders auf die Problematik der privaten Nutzung des Internets und der privaten Nutzung geschäftlicher E-Mail-Adressen. Dabei wurde auch auf die Datenschutzproblematik eingegangen. In einer Bewertung wurden zunächst die Firewalls und Netzwerkmangementtools miteinander verglichen.
Weitere Arbeiten könnten sich mit weiteren Produkten aus den Bereichen Firewall (ipcop, zentyal) und Netzwerkmanagement (zabix, cacti) sowie anderen Bausteinen eines Netzwerkes befassen.

# Literaturverzeichnis


[1] BSI - Bundesamt für Sicherheit in der Informationstechnik. *Konzeption von Sicherheitsgateways*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 29.12.2013

[2] Netzwerk emsländischer IT-Leiter "DE-IT-EmslandArbeitskreis IT-Sicherheit. *IT-Sicherheitsleitfaden für mittelständicher Unternehmen*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 29.12.2013

[3] BSI - Bundesamt für Sicherheit in der Informationstechnik. *Studie zur IT-Sicherheitin kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 29.12.2013

[4] BSI - Bundesamt für Sicherheit in der Informationstechnik. *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 06.01.2014

[5] LAG Berlin-Brandenburg. *Az. 4 Sa 2132/10*, verfügbar auf `http://openjur.de/u/168249.html`, abgerufen am 06.01.2014

[6] BSI - Bundesamt für Sicherheit in der Informationstechnik. *BSI Firewall Studie II*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 06.01.2014

[7] BSI - Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz-Kataloge*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 06.01.2014

[8] BSI - Bundesamt für Sicherheit in der Informationstechnik. *BSI- Standard 100-2 - IT Grundschutzvorgehensweise*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 06.01.2014

[9] Michael Badger. *Zenoss Core Network and System Monitoring*, Packt Publishing, Birmingham, 2008

[10] BSI - Bundesamt für Sicherheit in der Informationstechnik. *Cyber Security Report 2013*, verfügbar auf `https://www.bsi.bund.de/`, abgerufen am 01.02.2014

[11] Götz Rieger. *Netzwerk unter Kontrolle – Netzwerküberwachung mit Nagios*, c't 3/06, S. 206

[12] Check Point Software Technologies Ltd.. *Identity Awareness Software Blade*, verfügbar auf `http://www.checkpoint.com/products/identity-awareness-software-blade/`, abgerufen am 16.02.2014

[13] Nagios Enterprises, verfügbar auf `http://exchange.nagios.org/directory`, abgerufen am 16.02.2014

[14] Cisco Systems Inc.. *Cisco Wireless Location Appliance*, verfügbar auf `http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-location-appliance/product_data_sheet0900aecd80293728.html`, abgerufen am 16.02.2014