Bachelorarbeit

Katrin Scholz

Entwicklung einer Methodik zur Sicherheitsanalyse von Datenkommunikationssystemen

Fachbereich Elektrotechnik und Informatik
Department of Electrical Engineering and Computer Science

Katrin Scholz

Entwicklung einer Methodik zur Sicherheitsanalyse von Datenkommunikationssystemen

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang Technische Informatik
am Fachbereich Elektrotechnik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr.-Ing Martin Hübner
Zweitgutachter : Prof. Dr.rer.nat. Gunter Klemke

Abgegeben am 10.Dezember 2004

Katrin Scholz

Thema der Bachelorarbeit

Entwicklung einer Methodik zur Sicherheitsanalyse von Datenkommunikationssystemen

Stichworte

IT-Sicherheit, Sicherheitsanalyse, Bedrohungsanalyse, Schwachstellenanalyse

Kurzzusammenfassung

Ziel dieser Arbeit ist es, eine Methodik für die Sicherheitsanalyse von Datenkommunikationssystemen zu entwickeln. Es soll eine strukturierte Vorgehensweise dargestellt werden, mit deren Hilfe diese Analyse erfolgreich durchgeführt werden kann. Sie soll auf andere Systeme anwendbar und an den jeweiligen Entwicklungsstand des Systems anpassbar sein. Dies wird dadurch erreicht, dass Methoden für die Sicherheitsanalyse vorgestellt und Einsatzbereiche umrissen werden.

Katrin Scholz

Title of the paper

Development of a methodology for analysis of security of data communication systems

Keywords

Information security, security analysis, analysis of threats, analysis of critical points

Abstract

Object of this dissertation is to develop a methodology applicable for the analysis of security of data communication systems. A structured proceeding shall be described that grants a successful analysis. The proceeding shall be applicable for other systems and depend upon the regarding state of development. This target is obtained by introducing methods for the analysis of security and determination of the fields of application.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Motivation

Über 220 Mio. Benutzer sind inzwischen, laut dem Internet Systems Consortium [isc], weltweit an das Internet angeschlossen. Selbst wenn 99,9% davon friedliche Anwender wären, so verblieben immer noch 220.000 Hacker und anderweitig spezialisierte Angreifer.

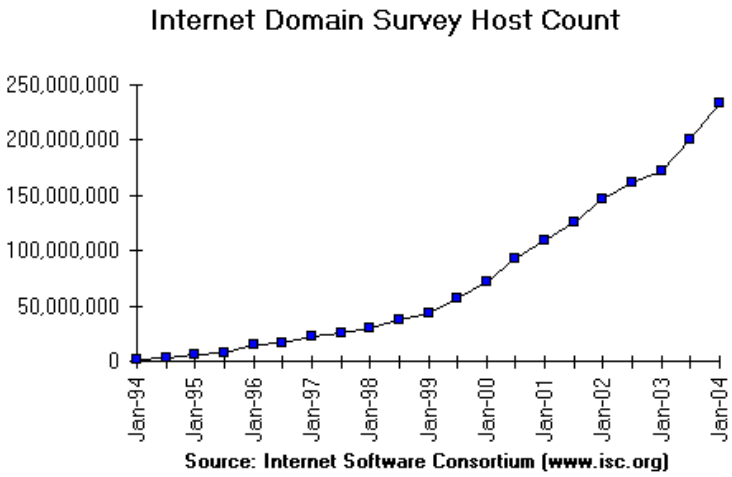


Abbildung 1: Anstieg der Internetnutzerzahlen [isc]

Die Motivation dieser Angreifer ist unterschiedlicher Art, so Othmar Kyas in seinem Buch „Sicherheit im Internet“ [OKya]. Hacker arbeiten unter einer Art Ehrenkodex und verfolgen das Ziel Schwachstellen bei der Sicherung von Systemen und dem Schutz von Daten aufzudecken. Die übrigen Angreifer bewegen unterschiedliche Gründe Systeme anzugreifen. Hierzu zählen finanzielle oder politische Gründe, aber auch Industrie- und Geheimdienst-Spionage, Unwissenheit oder Konkurrenzkampf. Die Angreifer möchten sich durch das Eindringen in die Systeme Wettbewerbsvorteile verschaffen oder, wie zum Beispiel bei den Geheimdiensten, zum Schutz der Staatsbürger vor Verbrechen und Terrorismus wirken. Im Internet hat jedermann Zugriff auf Hackertools, so dass sich jeder als Hacker versuchen kann. Vielen der Menschen, die diese Tools einfach mal ausprobieren, wissen gar nicht, dass derartige Tools zu großen Schäden führen können.

Schäden, welche hierbei entstehen können, lassen sich, laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) [bsigshb], typischerweise in die Bereiche informelle Selbstbestimmung, persönliche Unversehrtheit, Verstoß gegen Gesetze, Verträge und Vorschriften und andere Auswirkungen einordnen.

Die informelle Selbstbestimmung kann beeinträchtigt werden durch eine unzulässige Erhebung, Weitergabe und Kenntnisnahme von personenbezogenen Daten. Als personenbezogene Daten gelten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Welche Daten für welche Dauer von wem erfasst und abgespeichert werden dürfen, hängt von der Einwilligung der jeweiligen Person ab. Eine Erfassung und Weitergabe von personenbezogenen Daten ist jedoch ohne eine Einwilligung der betroffenen Person gänzlich untersagt. Hierzu zählt auch, wenn die Daten für einen anderen als den vorgesehenen Zweck verwendet werden. Personenbezogene Daten dürfen außerdem bei der Verarbeitung und Übertragung nicht verfälscht werden.

Eine Beeinträchtigung der persönlichen Unversehrtheit tritt dann ein, wenn einer Person eine Schädigung, Invalidität oder gar der Tod durch IT-Anwendungen oder Systeme droht. Dieses wäre zum Beispiel der Fall, wenn medizinische Überwachungs- oder Diagnosegeräte fehlerhaft arbeiten, ein Flugkontrollrechner oder ein Verkehrsleitsystem ausfällt.

Vorschriften und Verträge müssen eingehalten werden, hierzu zählen Verwaltungsvorschriften, Verordnungen und Dienstvorschriften, aber auch Dienstleistungsverträge im Bereich der Datenverarbeitung und Verträge zur Wartung von Betriebsgeheimnissen. Zu den Vertragsvereinbarungen gehört unter anderem die Festlegung der Ausfallzeit.

In Abbildung 3 sind die Verluste durch die jährliche Ausfallszeiten, welche im Zusammenhang mit der Verfügbarkeit von Systemen stehen, im Bereich E-commerce und Finanzdienstleister aufgeführt. Es ist deutlich erkennbar, welche Auswirkungen die Ausfallzeit auf die Verluste haben. Wer eine hohe Verfügbarkeit garantiert und diese auch einhält, kann seine Verluste gering halten – hierzu ist unter anderem eine zuverlässige Sicherheitsarchitektur erforderlich.

Verfüg-barkeit in %	jährliche Ausfallzeit	durchschnittliche Verluste in USD		eingesetzte Methoden
		E-Commerce	Finanz-Dienstleister	
99,9999	30 Sec	950	54.000	proprietäres, fehlertolerantes System
99,999	5 Min	9.500	540.000	Selbstheilung, Wan Clustering
99,99	52 Min	98.000	5,6 Mio	LAN-Clustering, synchrone Replikation
99,9	9 Std	988.750	56 Mio	asynchrone Replikation
99,5	44 Std	5 Mio	280 Mio	Datentresor
99	88 Std	10 Mio	560 Mio	Zurückfahren auf Checkpoint
95	18 Tage	50 Mio	3 Mrd	Off-/ Online Backup

Quelle: Veritas

Abbildung 2: Auswirkungen der Verfügbarkeit und der Ausfallzeit auf die Verluste [beko]

Die wichtigsten für die IT-Sicherheit relevanten Gesetze sind:

- Das Grundgesetz:
  Da die Würde des Menschen unantastbar ist, wie im Artikel 1 Abs. 1 des Grundgesetzes [GG] zu lesen ist, darf sie auch durch die Informationstechnik nicht angetastet werden. Ebenso verhält es sich mit dem Recht auf freie Entfaltung der Persönlichkeit und dem Brief-, Post- und Fernmeldegeheimnis. Eine Einschränkung gibt es hierbei jedoch, „... dem Schutze der freiheitlich demokratischen Grundordnung oder des Tatbestandes oder der Sicherung des Bundes und der Länder ...“[1]. Das bedeutet, dass der Staat und somit die Behörden in gewissen Bereichen hiervon ausgenommen sind, beispielsweise beim Verkehrsdelikten.

- Das Volkszählungsurteil:
  Die im Grundgesetz verankerten Punkte sind auch in das Volkszählungsurteil eingeflossen, sie werden jedoch im Bereich der informellen Selbstbestimmung eingeschränkt.
  Hier heißt es: „… Sie bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss, ...“ so Norbert Pohlmann in seinem Buch „Der IT-Sicherheitsleitfaden“ [NPoh]. Weiter führt er aus, „... dass bei der Regelung der Gesetzgeber den Grundsatz der Verhältnismäßigkeit zu beachten hat. Auch hat der Gesetzgeber organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken“. Wenn also ein Mitarbeiter sein Unternehmen dazu nutzt um Material zu verbreiten, welches die Würde anderer verletzt, so kann der Geschädigte ihn verklagen. Hierzu zählt auch, wenn der Ruf eines Unternehmens geschädigt würde. Aber auch das Post- und Fernmeldegeheimnis muss in einem Unternehmen gewahrt bleiben. Es darf also theoretisch kein Mitarbeiter die Post, welche zum Beispiel an einen Administrator gerichtet ist, öffnen. In dem Volkszählurteil wurde dieses jedoch eingeschränkt, so dass berechtigte Stellen zur Abwehr drohender Gefahren diese einsehen können.

- Das Bundesdatenschutzgesetz:
  „Das Bundesdatenschutzgesetz soll dazu beitragen, ... das Grundrecht auf informationelle Selbstbestimmung zu verwirklichen ...“, so das Bundesministerium des Inneren [bund]. Es entspricht der europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995, die für den ganzen Europäischen Wirtschaftsraum einheitliche Datenschutzstandards gesetzt

[1] Artikel 10 GG, Brief-, Post- und Fernmeldegeheimnis [GG]

hat ...“[2]. Dieses Gesetz gilt, solange es nicht durch ein Gesetz auf Landesebene spezieller geregelt wird.

Das Ziel des Datenschutzes ist es den Einzelnen davor zu schützen, dass er durch den Umgang, also Erhebung, Verarbeitung oder Nutzung, mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Im Bundesdatenschutzgesetz [bund] ist hierfür ein Datenschutzbeauftragter vorgesehen. Der Datenschutzbeauftragte hat die Aufgabe, die Ausführungen des Bundesdatenschutzgesetzes in Unternehmen sicherzustellen.
Die Gesetze auf Landesebene haben Vorrang vor den Gesetzen auf Bundesebene, wenn diese genauer auf den Sachverhalt eingehen. Die Landesverfassungen beschäftigen sich unter anderem mit dem Datenschutz, den Umweltdaten und den Datenschutzbeauftragten. Im weitesten Sinne kann man also sagen, dass sie das Recht zum Schutz der persönlichen Daten auf Landesebene regeln.

- Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste:
  Im Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste des Deutschen Bundestages
  [iid] wird den Unternehmen vorgeschrieben bei rechtsgültigen Handlungen auf rein digitalem Weg elektronische Signaturen zu verwenden.
  Zweck des Gesetzes zur digitalen Signatur ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

- Das Urheberrechtsgesetz und das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft:
  Unternehmen, welche Mediadaten verarbeiten, müssen sich mit dem Urheberrechtsgesetz und dem Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft auseinandersetzen, so steht es im Bundesgesetzblatt Jahrgang 2003 vom 12. September 2003 [wiki]. Es umfasst das Vervielfältigungsrecht und das Verbreitungsrecht für „Werken der Literatur, Wissenschaft und Kunst (...)“. Verstöße im privaten, gewerblichen, entgeltlichen

[2] [bfd]

und unentgeltlichen Bereich sind in diesen Gesetzen geregelt sowie das Kopieren, Anbieten und Verbreiten. Im Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft ist festgelegt, dass die Umgehung von Kopierschutzsystemen verboten ist und Privatkopien nur dann erlaubt sind, wenn „eine nicht offensichtlich rechtswidrig hergestellte Vorlage“ verwendet wird. Die Verantwortlichen haften auf Schadensersatz sowie nach den Regeln des Strafrechts.

Volker Hammer unterscheidet in seinem Buch „Die 2. Dimension der IT-Sicherheit“ zwischen dem direkten Schaden und dem Folgeschaden [VHam]. Direkte Schäden wären Wiederbeschaffungskosten, Wiederherstellungs- oder Reparationskosten, diese kann man genau einschätzen. Der Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit zieht immer Folgeschäden mit sich, wie zum Beispiel Stillstandskosten, Auswirkungen auf andere Systemkomponenten, Image-, Konkurrenzfähigkeits- und Vertrauensverlust und Anspruchskosten. Dieses sind die entscheidenen Faktoren bei der Bemessung des Ausmaßes des kompletten Schadens.

Im Haftungsrecht ist eindeutig geregelt wer bei Schäden haftet. Im Skript „Technisches Risikomanagement“ der Fachhochschule beider Basel [fhbb] steht hierzu folgendes:
„Wer Schäden geltend machen will, muss eindeutig und überprüfbar nachweisen:

- Den Schaden nach Umfang und Inhalt
- Den Fehler des Schaden verursachenden Produktes
- Den Zusammenhang zwischen Fehler und Schaden

Sind diese Voraussetzungen alle erfüllt, hat der Hersteller oder Vertreiber zu beweisen, dass er in seinem Verantwortungsbereich alles ihm technisch Mögliche und wirtschaftlich Zumutbare getan hat, um Entstehen und Wirksamwerden dieses Fehlers zu vermeiden.
Wenn die Sorgfaltspflicht nicht nachgewiesen werden kann, geht der Schaden zu Lasten des Beweispflichtigen, führt zur Haftung und verpflichtet zum Schadensersatz.“

Wird eine IT-Straftat entdeckt, so ist der Verantwortliche entweder persönlich oder als Repräsentant des Unternehmens dem Vorwurf einer Straftat ausgesetzt, so Robert Niemeier der Heussen Rechtsanwaltschafts GmbH [suco]. Für die IT-Sicherheit ist rein rechtlich die Unternehmensleitung verantwortlich, da sie zu entscheiden hat, welche technischen und organisatorischen Maßnahmen erforderlich sind. Sie kann die Aufgabe aber auch an einen entsprechend ausgebildeten und verantwortungsbewussten Mitarbeiter delegieren. Dieser Mitarbeiter kann dann ebenfalls bei einer Straftat zur Verantwortung gezogen werden. Der Verantwortliche muss gegebenenfalls mit seinem

Privatvermögen für den Schaden aufkommen. Die Versicherung kann im Fall von fahrlässigem handeln in der IT-Sicherheit ihre Leistung verweigern. Doch auch wenn es nicht zu finanziellem Schaden kommt, so muss das entsprechende Unternehmen mindestens mit einem Imageverlust rechnen.

Um die Sicherheit des Systems eines Unternehmens zu überprüfen und möglichst viele der genannten Schäden auszuschließen, gibt es unterschiedliche Methoden. Bedrohungen und Schwachstellen müssen aufgedeckt und behoben werden. Auf Grund der vielen unterschiedlichen Rechnerkonfigurationen, Betriebssysteme und Anwendungen gibt es jedoch kein Patentrezept oder gar eine fertige Lösung für einen 100 % sicheren Schutz von IT-Systemen, der gespeicherten Daten sowie der Kommunikationswege.

Der Zusammenhang von Bedrohungen, die auf eine IT-Infrastrukur wirken, deren Verfügbarkeit, Vertraulichkeit und Integrität und die daraus folgenden Auswirkungen werden in der Abbildung 2 verdeutlicht:

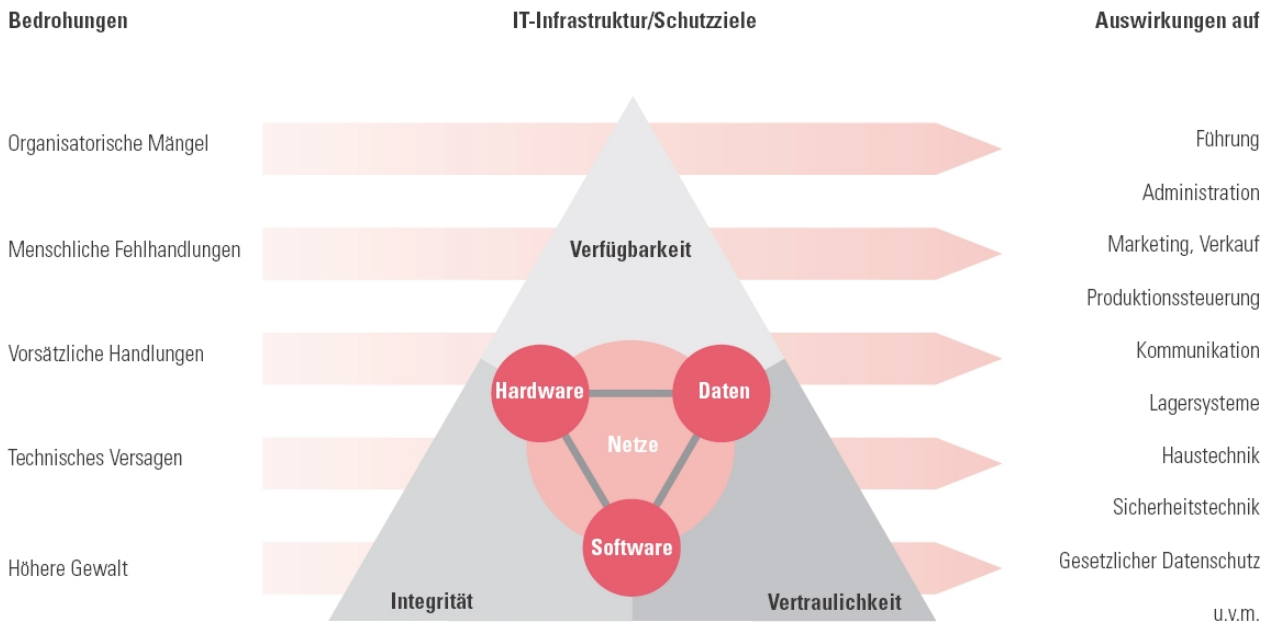


Abbildung 3: Auswirkungen der Bedrohungen [bhit]

Doch was bedeutet Sicherheit? Im englischsprachigen Raum gibt es für Sicherheit die drei Begriffe ‚safty', ‚security' und ‚protection'. Rolf Opplinger hat sie wie folgt definiert [ROpp]:
Safty - die Funktionssicherheit befasst sich mit der Korrektheit und Zuverlässigkeit des Systems. Es soll unterbunden werden, dass ein System unzulässige Zustände annimmt.
Security - die Informationssicherheit ist ein Begriff dafür, dass kein unautorisierter Nutzer Informationsveränderungen vornehmen oder einen Informationsgewinn aus dem System ziehen kann.
Protection - die Datensicherheit befasst sich mit dem Schutz vor Datenverlust.

Das klassische Problem der IT-Sicherheit ist die Geheimhaltung vertraulicher Daten über Zugriffschutz, Sicherstellung der Systemintegrität und Verfügbarkeit bis hin zum Schutz vor Naturkatastrophen und Terroranschlägen.

1.2 Zielsetzung

Ziel dieser Arbeit ist es, eine Methodik für die Sicherheitsanalyse von Datenkommunikations-systemen zu entwickeln. Es soll eine strukturierte Vorgehensweise dargestellt werden, mit deren Hilfe diese Analyse erfolgreich durchgeführt werden kann. Sie soll auf andere Systeme anwendbar und an den jeweiligen Entwicklungsstand des Systems anpassbar sein. Dies wird dadurch erreicht, dass Methoden für die Sicherheitsanalyse vorgestellt und Einsatzbereiche umrissen werden.

Durch eine Kombination von unterschiedlichen Normen und Standards sollen Möglichkeiten und Anregungen gegeben werden, wie eine Sicherheitsanalyse, bezogen auf Daten, Schnittstellen und Kommunikationsverbindungen, effektiv durchgeführt und auch erweitert werden kann.

Diese Analyse kann zum Zeitpunkt der Entwicklung stattfinden, aber auch zur Überprüfung eines bestehenden Systems. Sinnvoller ist es jedoch, diese Analyse während der Entwicklungsphase durchzuführen, so dass von vornherein alle Sicherheitsaspekte überdacht, entwickelt und implementiert werden können. Bei einer Analyse nach der Entwicklungsphase ist es schwerer und komplizierter Schwachstellen zu beheben, da bestehende Strukturen geändert und neu eingegliedert werden müssen, ohne dass es zu Folgefehlern im Rest des Systems kommt.

1.3 Gliederung der Arbeit

Die IT-Sicherheit ist ein sehr weitläufiges Themengebiet. In der Einleitung wird der Themenkomplex daher eingegrenzt.

Die Grundlagen für den Entwurf der Methodik und der Durchführung der Analyse werden in Kapitel 2 und 3 gelegt. Schwerpunkt dieser Kapitel ist es, Normen und Methoden vorzustellen, welche für eine Sicherheitsanalyse, Bedrohungs- und Schwachstellenanalyse eingesetzt werden. Es wird herausgearbeitet, worin die Unterschiede der verschiedenen Normen und Methoden liegen.

Die Erläuterung des Entwurfs dieser Methodik erfolgt im 4. Kapitel. Hier wird die genaue Vorgehensweise dargestellt, ebenso wie der Einsatz von Normen und Methoden. Auch Methoden, welche im Kapitel der Durchführung keinen Einsatz finden, sind hier am entsprechenden Einsatzort erläutert, so dass sie bei größeren und weiterentwickelten Systemen eingesetzt werden können.

Im 5. Kapitel wird das Beispielsystem, anhand dessen die Analyse durchgeführt wird, vorgestellt. Dieses System befindet sich am Anfang seiner Entwicklung und es sind noch relativ wenig Systemdetails bekannt. Dies hat Vor- und Nachteile. Einerseits können viele Schwachstellen aufgedeckt werden, andererseits können, auf Grund des frühen Entwicklungsstadiums des Systems, leider nur wenige der vorgestellten Methoden im Kapitel der Durchführung wirklich eingesetzt werden.

Die Durchführung der Sicherheitsanalyse im Kapitel 6 setzt das im Kapitel 5 erläuterte Verfahren zur Sicherheitsanalyse um. Für die Analyse selbst wird das in Kapitel 4 vorgestellte Beispielsystem verwendet. Eine Festlegung der Schutzmaßnahmen hat beim Beispielsystem nicht stattgefunden, es wurden jedoch Empfehlungen ausgesprochen.

Im Kapitel 7 folgt eine Zusammenfassung der Ergebnisse, Schlussfolgerungen und ein Ausblick auf die Zukunft.

1.4 Einordnung der Arbeit

Um die Sicherheit eines Systems bzw. eines Unternehmens zu gewährleisten muss es ein IT-Sicherheitsmanagement geben. Ein solches IT-Sicherheitsmanagement umfasst neben den Maßnahmen im technischen Bereich auch eine Sicherheitspolitik und -kultur, Sicherheitsstrukturen im Management als auch im Bereich der Mitarbeiter eines Unternehmens.

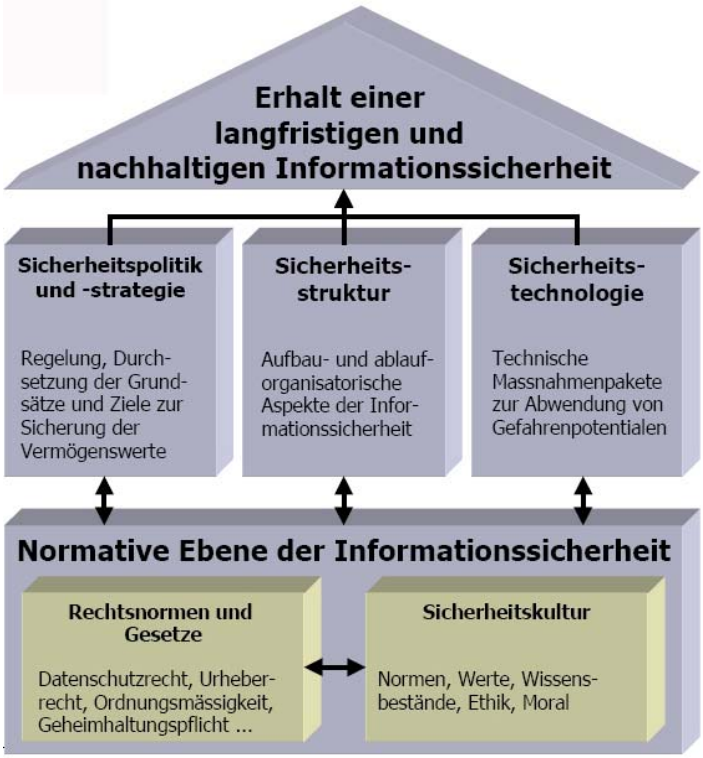


Abbildung 4: Erhalt der Informationssicherheit [ifida]

Die, für die Sicherstellung der IT-Sicherheit entscheidenden, Normen beschäftigen sich mit unterschiedlichen Bereichen der Informationssicherheit. Dies wird ausführlicher im Kapitel der Normen und Standards erläutert.

Diese Arbeit befasst sich ausschließlich mit den technischen Aspekten der IT-Sicherheit, der Sicherheitstechnologie, welche den produkt- und systemspezifischen Bereich betreffen. Zwar werden in Ansätzen auch die anderen Bereiche angesprochen, jedoch nicht vertieft betrachtet.

2 Normen und Standards

Wie schon im vorhergehenden Kapitel angesprochen befassen sich die Normen mit unterschiedlichen Ansätzen und Schwerpunkten für ein IT-Sicherheitsmanagement.

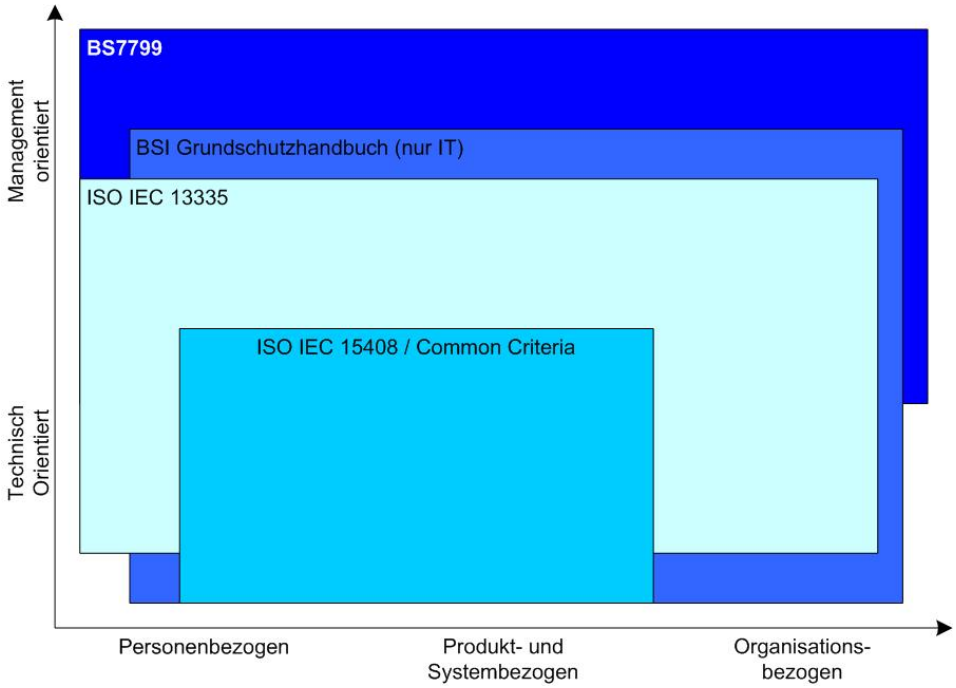


Abbildung 5: Ansätze von Normen [bfd] [ini]

Es gibt eine Reihe von Standards und Regelwerken, die Anleitungen für ein effektives IT-Sicherheitsmanagement bieten. Man unterscheidet technisch- und managementorientierte Ansätze, welche personenbezogene, produkt- und systembezogene oder organisationsbezogene Maßnahmen beinhalten. Die BS 7799-2 und das IT-Grundschutzhandbuch bieten zudem noch ein Zertifizierungsverfahren, mit dem die erfolgreiche Umsetzung der geforderten Maßnahmen nach innen und außen dokumentiert werden kann. In der Studie zu ISO-Normungsaktivitäten ISO/BPM des BSI sind einige Standards kurz und verständlich angerissen. [bsiiso]

Die ISO IEC 15408, das IT-Grundschutzhandbuch, die ISO/IEC TR 13335 und die Norm BS7799 werden hier vorgestellt. Es gibt jedoch noch viele weitere Standards, unter anderem:

- Die „COBIT – Control objectives for information and related technology“, welche hauptsächlich im technischen und produktbezogenen Bereich wirkt
- Die IT Infrastructure Library, welche eine Sammlung von Bücher zum Thema IT-Service Management ist
- Die ISO/IEC TC68, welche im Bereich des Bank und Management System ansässig ist

- Das Österreichische IT-Sicherheitshandbuch, welches weitgehend vom IT-Sicherheitshandbuch des BSI abgeleitet ist
- Die OECD Guidlines, welche sich zum Ziel setzen, eine IT-Sicherheitskultur zu schaffen und ein Bewußtsein für Sicherheit zu schaffen
- Das FIPS, ein Krisenkatalog zur Bewertung von Kryptosystemen
- Das Orange Book (TCSEC), ein erster Klassifikationskatalog für Sicherheit, herausgegeben vom amerikanischen Verteidigungsministerium

Ein Grossteil dieser Normen und Standards hat eine gemeinsame Historie, so dass sich einige der Themengebiete überschneiden und ergänzen. Ein Ausschnitt hiervon ist in der unteren Abbildung dargestellt.

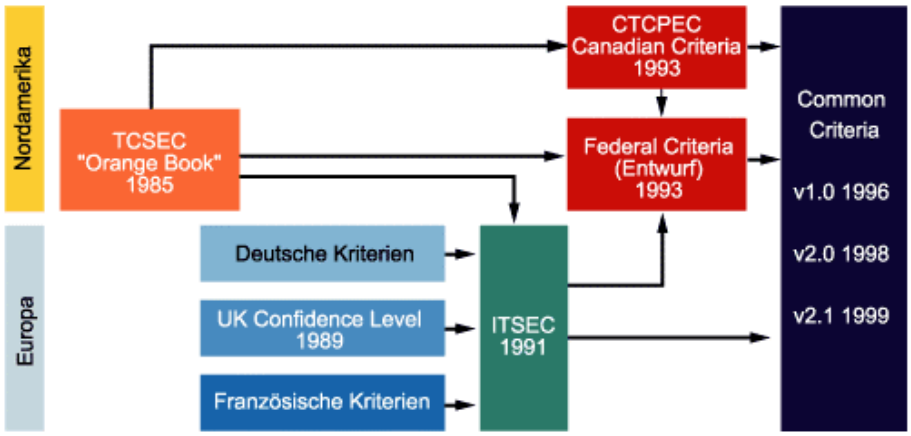
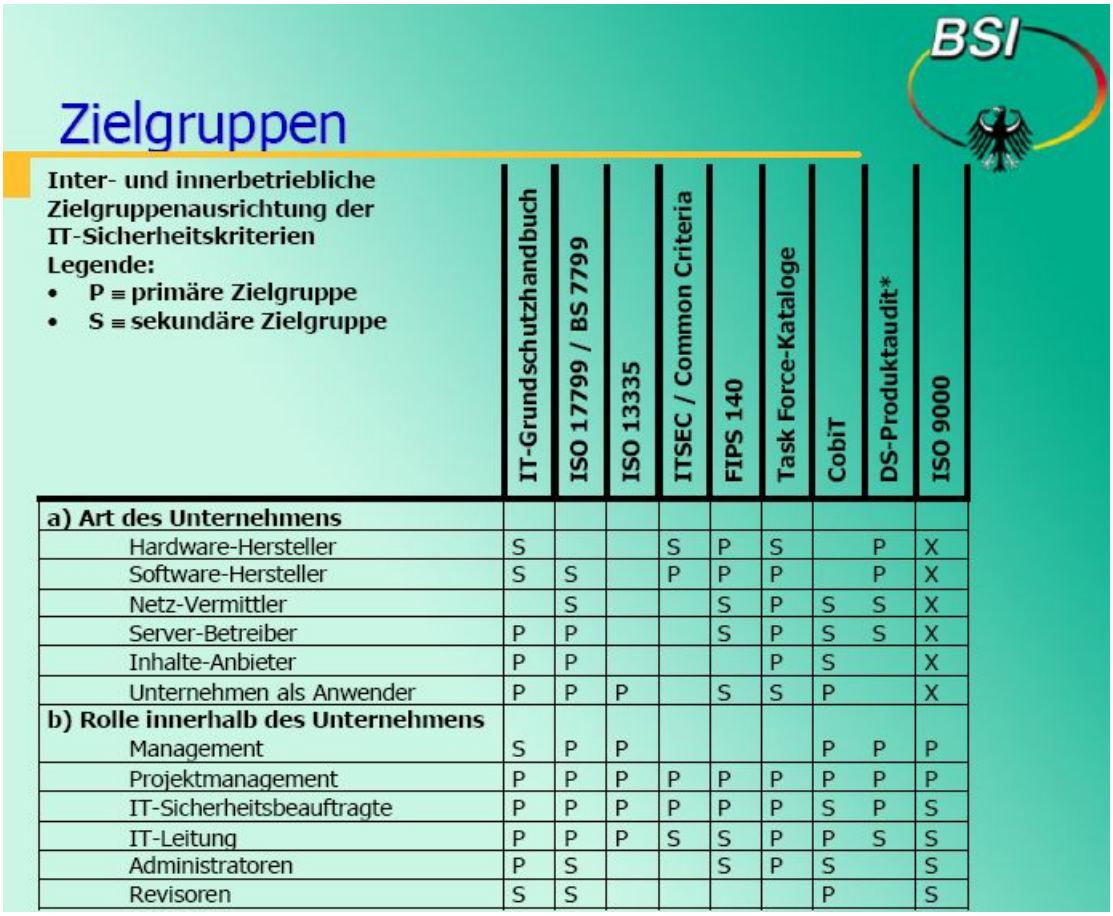


Abbildung 6: Historische Entwicklung der Normen [comp]

Als Kriterien für die Auswahl einer bestimmten Norm werden von Dr. Niggemann vom BSI[decu] folgende genannt:

- Die Zielsetzung und die Zielgruppen
- Vorgehensweise
- Skalierbarkeit und Aktualisierbarkeit
- Angestrebtes Sicherheitsniveau
- Anwendbarkeit und Kosten



Zielgruppen

Inter- und innerbetriebliche Zielgruppenausrichtung der IT-Sicherheitskriterien
Legende:
- **P ≡ primäre Zielgruppe**
- **S ≡ sekundäre Zielgruppe**

	IT-Grundschutzhandbuch	ISO 17799 / BS 7799	ISO 13335	ITSEC / Common Criteria	FIPS 140	Task Force-Kataloge	CobiT	DS-Produktaudit*	ISO 9000
a) Art des Unternehmens									
Hardware-Hersteller	S			S	P	S		P	X
Software-Hersteller	S	S		P	P	P		P	X
Netz-Vermittler		S			S	P	S	S	X
Server-Betreiber	P	P			S	P	S	S	X
Inhalte-Anbieter	P	P				P	S		X
Unternehmen als Anwender	P	P	P		S	S	P		X
b) Rolle innerhalb des Unternehmens									
Management	S	P	P				P	P	P
Projektmanagement	P	P	P	P	P	P	P	P	P
IT-Sicherheitsbeauftragte	P	P	P	P	P	P	S	P	S
IT-Leitung	P	P	P	S	S	P	P	S	S
Administratoren	P	S			S	P	S		S
Revisoren	S	S					P		S

Abbildung 7: Zielgruppen der unterschiedlichen Normen [decu]

2.1 Common Criteria (ISO IEC 15408 oder ITSEC)

Die Common Criteria entstand 1996 als internationales Projekt unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, der Niederlande, der USA und Kanadas.
Ziel war, so der Diplom Informatiker Thomas Hungenberg [demo], die Weiterentwicklung und Harmonisierung der ITSEC, der TCSEC, des Orange Books der USA und der kanadischen Kriterien CTCPEC. Es sollten weltweit einheitliche Evaluierungskriterien zur Verfügung gestellt werden. Thomas Hungenberg [demo] und Claudia Eckert [CEck] erläuterten die historischen Eckdaten und Zusammenhänge, welche grafisch in der Abbildung 8 aufgearbeitet wurden.

Die Common Criteria bildet laut dem BSI [bsicc] für die Hersteller die Grundlage zur Sicherung der Qualität ihrer Produkte und stellt Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik dar. Die Vertrauenswürdigkeit von IT-Produkten und Systemen soll mit Hilfe dieser Richtlinie hergestellt werden. Sie ist nicht nur ein Kriterienkatalog, sondern bietet einen Überblick über alle möglichen Sicherheitsanforderungen, deren Zusammenhänge und Umsetzung.

Außerdem wird eine ausführliche Analyse sowohl in theoretischer als auch praktischer Form vorgestellt.

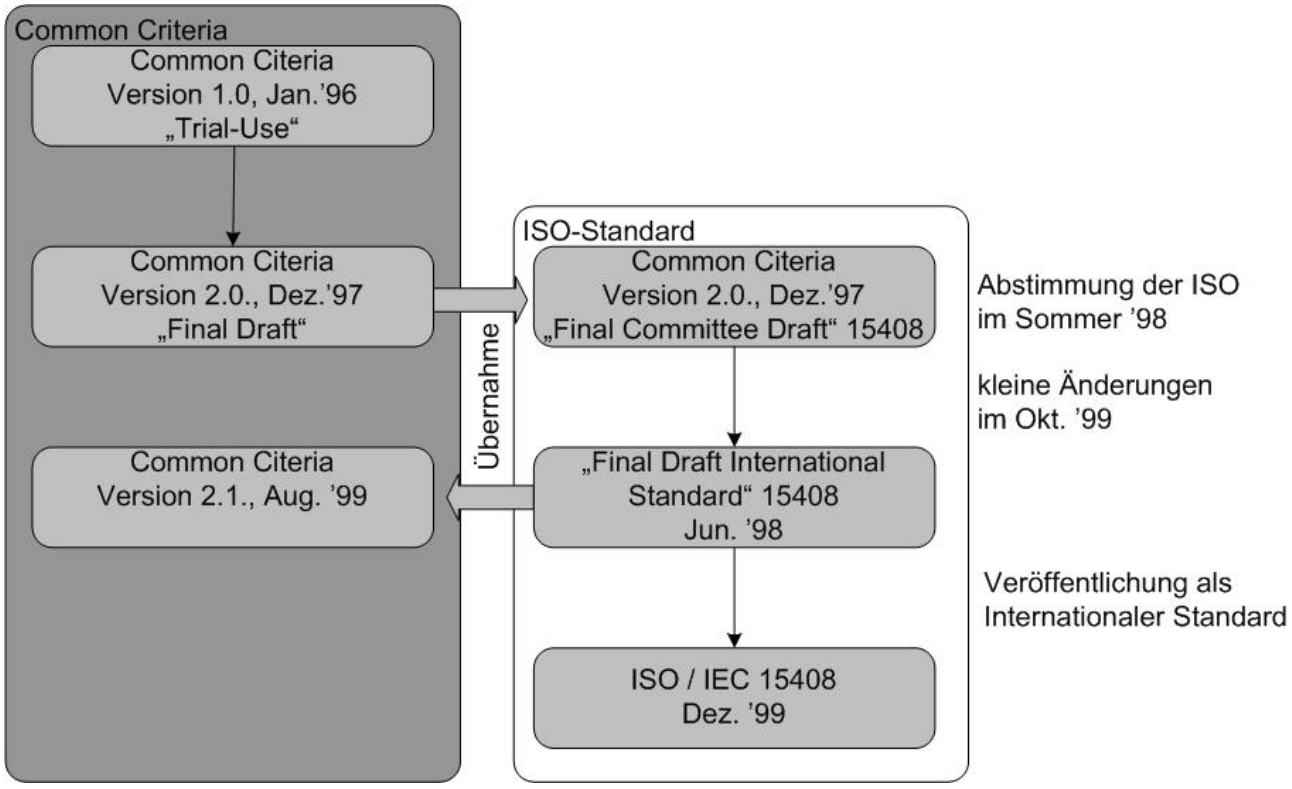


Abbildung 8: Entstehungsgeschichte der Common Criteria

Claudia Eckert umreißt die drei Teile wie folgt [CEck]. Der erste Teil befasst sich mit der Einführung, also den Grundlagen, den Geltungsbereichen, und dem allgemeinen Modell. Im zweiten Teil werden die funktionalen Sicherheitsanforderungen betrachtet. Ein umfangreicher Katalog mit Funktionsanforderungen ist inbegriffen, er dient als Empfehlung für die Beschreibung der Funktionalität des Systems. Im dritten Teil werden die Anforderungen an die Vertrauenswürdigkeit des Systems ermittelt.

2.2 ISO/IEC TR 13335 (ISO/IEC JTC 1/SC 27/WG1)

Die ISO IEC TR 13335 ist eine umfassende Sammlung von vier Normdokumenten zum Management von Informationssicherheit. Sie stellt den Ausgangspunkt für eine Reihe von Dokumenten im IT-Sicherheitsmanagement dar, wie etwa das Österreichische IT-Sicherheits-handbuch, das IT-Grundschutzhandbuch des BSI und die Norm BS 7799 sowie die Studie zu ISO-Normungsaktivitäten ISO/BPM des Bundesamtes für Sicherheit in der Informationstechnik (BSI). [bsiiso]

Die ISO IEC TR 13335 wurde ursprünglich in 5 Teilen entwickelt, die im Wesentlichen aufeinander aufbauen bzw. die vorherigen Teile verfeinern. Im Rahmen einer Überarbeitung wurden laut dem BSI [bsiiso] die Teile 1 und 2 jedoch zu einem gemeinsamen Teil 1 verschmolzen, so dass derzeit die folgende Struktur diskutiert wird:

- ISO IEC TR 13335-1 (1996/1997) beinhaltet die Vorgehensweisen auf Ebene des IT-Sicherheitsmanagements, zum Beispiel die Definition von Sicherheitszielen und Hilfsmittel zur Auswahl einer geeigneten Strategie zur IT-Sicherheit
- ISO IEC TR 13335-3 (1998) beinhaltet die Vorgehensweisen zur Ermittlung geeigneter IT-Sicherheitsmaßnahmen basierend auf der vorher gewählten Vorgehensstrategie. Im Rahmen dieses Dokuments werden verschiedene Ansätze beschrieben, z. B. der IT-Grundschutz-Ansatz und eine ausführliche Risikoanalyse
- ISO IEC TR 13335-4 (2000) beinhaltet zahlreiche Hilfsmittel zur Auswahl von Sicherheitsmaßnahmen, welche wieder abhängig von der zuvor gewählten Strategie zur IT-Sicherheit ist. Sie beinhaltet detaillierte Maßnahmenkataloge und deren Zuordnung im Rahmen eines einfachen Grundschutzes abhängig vom betrachteten IT-System, sowie darüber hinaus eines erweiterten Grundschutzes, welcher abhängig von bestehenden Sicherheitszielen und deren Bedrohungen ist
- ISO IEC TR 13335-5 (2001) beinhaltet die Vorgehensweisen zum Schutz vernetzter IT-Systeme

Die Schwächen dieser Vorgehensweise liegen vor allem in einer fehlerfreien Beschreibung der übergeordneten Prozesse des Managementsystems, der Betrachtung und Steuerung der notwendigen Ressourcen. Wenn man diese Methode für eine Sicherheitsanalyse wählt, muss man das System und auch das Unternehmen sehr gut kennen, da es ansonsten eventuell nicht ausreichend untersucht wird und Schwachstellen unentdeckt bleiben. Es muss also das gesamte Unternehmen in den Sicherheitsentwicklungsprozess mit eingebunden werden.

2.3 IT-Grundschutzhandbuch

Das IT-Grundschutzhandbuch enthält Standardsicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel für zahlreiche IT-Konfigurationen, die typischerweise im heutigen IT-Einsatz anzutreffen sind. Dieses Informationsangebot soll zur Lösung häufiger Sicherheitsprobleme dienen, die Anhebung des Sicherheitsniveaus von IT-Systemen unterstützen und die Erstellung von IT-Sicherheitskonzepten vereinfachen. Es enthält einen Maßnahmenkatalog, welcher über 600

Standard-IT-Sicherheitsmaßnahmen enthält, geht detailliert auf technische und organisatorische Aspekte ein und ist die Spezifikation für eine formale IT-Grundschutz-Zertifizierung.

2.4 Norm BS7799

Die Norm BS7799 ist eine Einführung in das systematische Management der Informationssicherheit in Organisationen, so Jörg Völker der Secorvo Security Consuling GmbH in seinem Überblick „BS 7799, Vom „Best Practice“ zum Standard“ [seco]. Die BS7799 bildet die Grundlage zur Identifikation und Beherrschung spezifischer IT-Risiken sowie zur Sicherstellung der benötigten Zuverlässigkeit von IT&T-Systemen. Sie stellt eine Systematik zur organisationsweiten Betrachtung der Informationssicherheit und zur Einführung eines umfassenden Sicherheitsmanagementsystems zur Verfügung. Sie ist unterteilt in zwei Teile, die in den folgenden Abschnitten erläutert sind.

2.4.1 ISO/IEC 17799 (BS7799-1)

Die ISO IEC 17755 ist ein internationaler Standard, welcher die Zielsetzung der Informationssicherheit über die Erhaltung von Vertraulichkeit, Integrität und Verfügbarkeit definiert.
Er ist in zehn Themenbereiche gegliedert, wie die Netzagentur Nordrhein-Westfalen in ihrem Workshop „Einführung eines IT-Sicherheitsmanagements an Hochschulen“ ausführt [netz]. Es ist beschrieben, was die Normelemente eines Informations-Sicherheits-Management-System (ISMS) ausmachen sowie eine Sammlung von ca. 127 allgemein und praxiserprobten Sicherheitsanforderungen – die so genannten Baseline Controls.
Die zehn Themenbereiche sind die folgenden:

- Informationssicherheitspolitik
- Informationssicherheitsorganisation
- Klassifizierung und Überwachung der Anlagen und Bestände
- Personelle Sicherheit
- Physische und umgebensbezogene Sicherheit
- Rechner- und Netzverwaltung, Management der Kommunikation und des IT-Betriebes
- Systemzugriffskontrolle
- Entwicklung und Wartung
- Geschäftskontinuitätsplanung, Management des kontinuierlichen Geschäftsbetriebes
- Erfüllung der Verpflichtung

2.4.2 BS 7799-2

Die BS 7799-2 ist der britische Standard, welcher nie als ISO-Norm akzeptiert wurde. Trotzdem ist er von internationaler Bedeutung als Qualitätsinformations-Sicherheitssiegel. Er bildet eine solide Grundlage für Auditierung und Zertifizierung von IT-Systemen. Die BS 7799-2 befasst sich laut dem BSI [bsiiso] mit der Fragestellung nach dem Managementsystem. Es werden vier große Bereiche angesprochen:

- Das Informationssicherheitsmanagementsystem (ISMS)
- Die Verantwortung des Managements
- Das Management Review
- Die Verbesserung des ISMS

2.5 Zertifizierung

Laut dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik [bsigshb] ist die Vertrauenswürdigkeit von IT-Produkten ein entscheidendes Auswahlkriterium für deren Einsatz. Für IT-Verantwortliche ist es allerdings fast unmöglich, selbst die Sicherheitseigenschaften zu bewerten. Für den Hersteller hingegen ist es schwierig, glaubwürdig die Sicherheit seiner Produkte zu belegen, er ist auf Referenzen oder unabhängige Tests angewiesen.

Diesen Nachweis der vertrauenswürdigen Realisierung von IT-Produkten schaffen die Evaluierung und Zertifizierung. Beides erfolgt nach objektiven Kriterien, wie z. B. dem Common Criteria Standard oder durch neutrale Stellen wie dem BSI. Ziel der Zertifizierung ist es, IT-Produkte und -Systeme hinsichtlich ihrer Sicherheitseigenschaften transparent und vergleichbar zu bewerten.

3 Methoden zur Sicherheits- und Bedrohungsanalyse

3.1 Black-Box-Test

Als Black-Box-Test bezeichnet man eine Methode des Software Tests, so die Fraunhofer Gesellschaft [soko]. Diese Tests werden ohne Kenntnisse über die innere Funktionsweise des zu testenden Systems entwickelt. Ziel ist es, die Übereinstimmung eines Softwaresystems mit seiner Spezifikation zu überprüfen. Dieser Black-Box-Test hat mit dem in dieser Arbeit verwendeten Diagramm nur im Entferntesten etwas zu tun. Das Black-Box Diagramm stellt das System, ohne das Wissen um die innere Funktionsweise des Systems, optisch dar. Es dient aber weniger dem Softwaretest als zur Visualisierung von bekannten Sachverhalten.

3.2 Vorläufige Sicherheitsanalyse (PHA, preliminary hazard analysis)

Die vorläufige Sicherheitsanalyse, kurz PHA, wird für die Anforderungsanalyse eingesetzt sowie in der frühen Phase des Entwurfs. Das Ziel der PHA ist, sicherheitskritische Bereiche zu erkennen und erste Einschätzungen von Gefahren zu liefern, so die Frauenhofer Gesellschaft [soko]. Hinzu kommen Gefahrenkontrollen und entsprechende Handlungsweisen. Diese Methode ist wenig formal, denn sie besteht meist aus einem Brainstorming, welches auf den Erfahrungen der teilnehmenden Mitarbeiter basiert. Üblicherweise werden Checklisten erstellt.

3.3 Fehlerbaumanalyse (FTA)

Diese Methode wurde ursprünglich für Hardware Systeme entwickelt, sie wurde später aber auch in der Software Fehleranalyse angewendet, so die Fachhochschule beider Basel [fhbb].

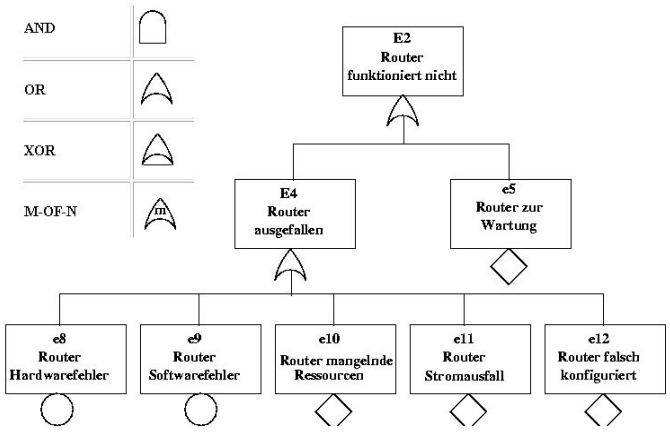


Abbildung 9: Beispiel einer Fehlerbaumanalyse anhand eines Routers [magd]

Der Fehlerbaum ist eine grafische Darstellung der logischen Zusammenhänge, die zu einem unerwünschten Ereignis führen. Das Ergebnis einer Fehlerbaumanalyse ist eine Erfassung und Darstellung von Ausfallkombinationen und Schwachstellen. Folgende Schritte sind für eine effektive Arbeit mit einem Fehlerbaum notwendig:

- Systemanalyse
- Schwachstellenanalyse und Feststellen der Bedrohungen
- Aufstellen eines Fehlerbaumes
- Auswertung des Fehlerbaumes
- Bewertung und Schlussfolgerungen

3.4 Ausfalleffektanalyse (FMEA)

Die Ausfalleffektanalyse soll das System hinsichtlich des Ausfalls einzelner Komponenten und sicherheitsrelevanter Aspekte untersuchen. Das Verfahren der Analyse ist weitgehend formalisiert, damit alle Untersuchungen systematisch und vollständig durchgeführt werden können, so die Fachhochschule beider Basel [fhbb]. Mit fortschreitender Detailplanung kann diese Analyse erweitert werden.

Für die Durchführung der Analyse ist ein Systemzustand festzulegen der als Ausgangssituation gilt. Alle Komponenten werden als intakt betrachtet. Sind mehrere Systemzustände wichtig, so sind für jeden Systemzustand jeweils getrennte Analysen durchzuführen. Das zu betrachtende System wird in Komponenten und Module unterteilt. Die Detaillierung hängt davon ab, wie umfangreich und genau die Analyse sein soll. Für jede dieser Komponenten wird ein Vordruck angefertigt, in dem die Ausfallarten, deren Auswirkungen auf das System und gegebenenfalls die Umgebung eingetragen und bewertet werden. Für die Ausfalleffektanalyse ist folgender Ablauf vorgesehen:

- Auflistung aller Komponenten
- Identifizierung aller Ausfallarten
- Bestimmung der Auswirkung auf das System
- Klassifizierung nach Gefahr und Auswirkung
- Ermittlung der Vorgehensweise zur Reduzierung der Ausfallhäufigkeit bzw. Fehlerreduzierung
- Ausfüllen des Vordruckes

Für die Fehlerbaumanalyse liefert die Ausfalleffektanalyse nützliche Vorabinformationen.

3.5 Ereignisbaumanalyse (ETA)

Diese Art der Analyse soll zur Beschreibung und Bewertung von Ereignisabläufen aller Art eingesetzt werden, vorzugsweise für die Störungs- und Schwachstellensuche. Ereignisabläufe lassen sich einfach und übersichtlich in Form eines Ereignisablaufdiagramms darstellen und analysieren. Die grafische Darstellung soll die logischen physikalischen und zeitlichen Zusammenhänge deutlich machen und zugleich ein Schema zur Berechnung der Wahrscheinlichkeit von Ereignisabläufen liefern, so Dr. Ing. Ralf Mock der Zürcher Fachhochschule [fhzheta].
Der Ereignisbaum und die Fehlerbaumanalyse ergänzen sich gegenseitig.

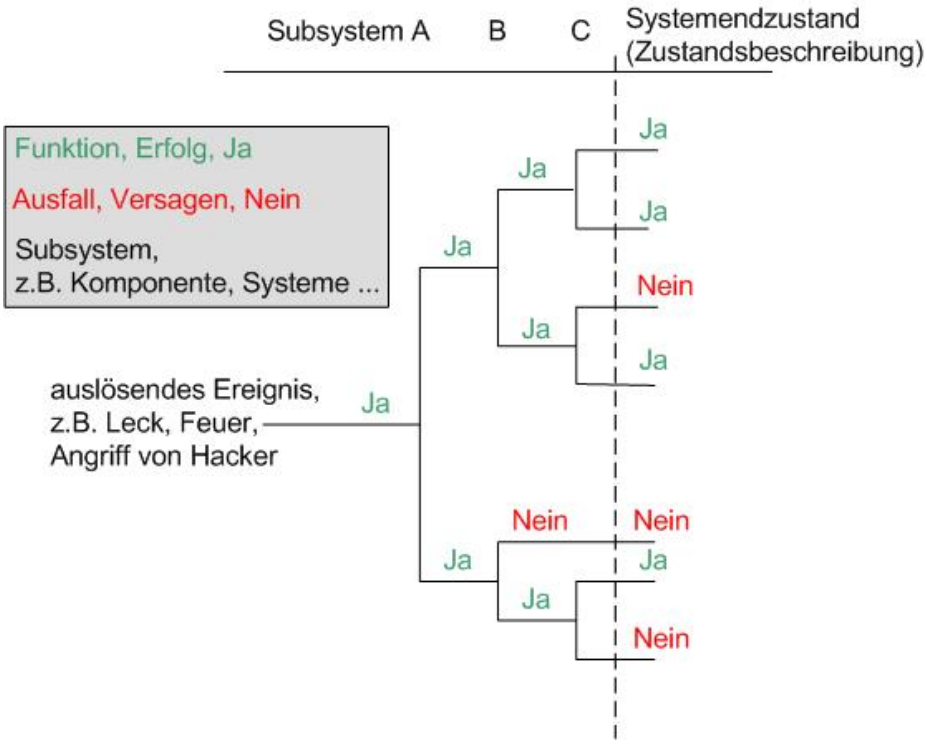


Abbildung 10: Prinzipieller Aufbau eines Ereignisbaumes [fhzheta]

3.6 Bedrohungsbaum

Durch den Einsatz von Bedrohungsbäumen können Gefahren grafisch dargestellt werden, so die Frauenhofer Gesellschaft [soko]. Die Blätter des Baums repräsentieren dabei die einzelnen potentiellen Angriffsmöglichkeiten.

Ein Bedrohungsbaum ist wie folgt aufgebaut:

- Die Wurzel definiert das Angriffsziel, d.h. eine mögliche Bedrohung des Systems.
- Die Kinder eines Knotens repräsentieren Zwischenziele, die zur Erreichung des Ziels des Vaterknotens beitragen.

Zur Verknüpfung können UND und ODER Knoten eingesetzt werden, also ähnlich dem Fehlerbaum. Die Pfade von den Blättern zur Wurzel beschreiben Angriffsschritte zum Erreichen des Angriffsziels.

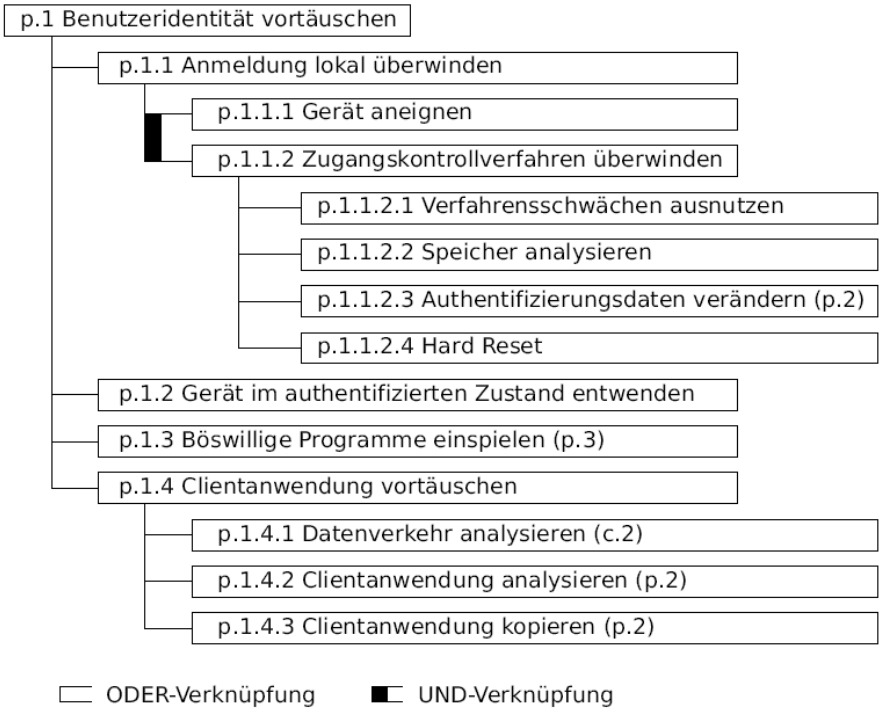


Abbildung 11: Beispiel für einen Bedrohungsbaum: Benutzeridentität vortäuschen [influe]

Vorteil eines Bedrohungsbaums ist die einfache Erkennung eines möglichen Angriffs durch die strukturierte Darstellung, sowie die einfache Erweiterbarkeit der Bäume. Hierdurch wird systematisches Arbeiten ermöglicht.

Nachteilig kann sich dagegen auswirken, dass der Baum mit zunehmender Größe immer komplexer und damit unüberschaubarer wird. Dadurch kann sich das Auffinden von bestimmten Pfaden als unnötig kompliziert erweisen oder einzelne Angriffsmöglichkeiten übersehen werden.

3.7 Bedrohungsmatrix

In einer Bedrohungsmatrix sind die Zeilen die Gefährdungsbereiche und die Spalten sind die potentiellen Auslöser von Bedrohungen.

	interne Benutzer	externe Benutzer	mobiler Code
interner Angriff	logische Bomben	Passwort knacken	Viren, Trojaner, Würmer
externer Angriff	Passwort ausspionieren	-	-
Verfübarkeit	Prozesse erzeugen	Denial of Service	Monopolisieren der CPU

Abbildung 12: Eine mögliche Bedrohungsmatrix [dakr]

Ein Nachteil bei der Erzeugung einer Bedrohungsmatrix sind die eingeschränkten Beschreibungsmöglichkeiten einer Matrix. Es ist zum Beispiel nicht möglich, den Ablauf einer möglichen Bedrohung in der Matrix darzustellen.

3.8 Ishikawa-Diagramm

Das Ishikawa-Diagramm, auch Ursache-Wirkung-Analyse oder Fischgräten Diagramm genannt, ist ein einfaches Hilfsmittel zur systematischen Ermittlung und übersichtlichen Darstellung von Systemzusammenhängen. Es dient der Visualisierung eines Problemlösungsprozesses. Das Problem wird an die Pfeilspitze geschrieben und die Einflussgrößen, Wirkungen und mögliche Ursachen zielen nun von oben und unten auf diesen Pfeil.

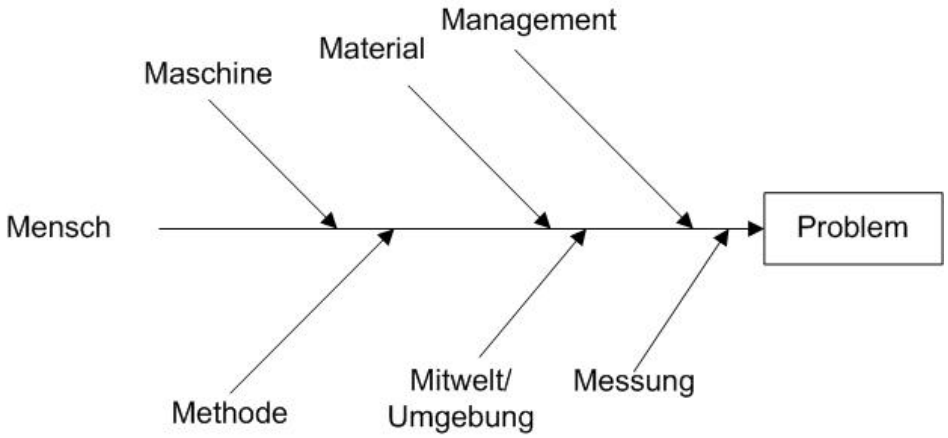


Abbildung 13: Ishikawa- Diagramm

Meist werden die Einflussgrößen den folgenden Rubriken unterteilt, so die Henning Peters & Peter Helbig Unternehmensberatung [pete]:

- Mensch, also alle Ursachen, die aus fehlender Erfahrung, Fähigkeiten, Kenntnisse, persönlichem Verhalten, Abneigungen, Einstellung zur Arbeit etc. entstanden sein könnten
- Maschine, also alle Ursachen, die durch Einrichtungen, Arbeitsplatzgestaltung, Maschinen, Werkzeuge und sonstige Betriebsmittel entstanden sein könnten
- Material, also alle Ursachen, die durch eingesetzte Materialien entstanden sein könnten
- Methode, also alle Ursachen, die durch Arbeitsabläufe, Organisationsstrukturen, Dienstanweisungen, Kontroll- und Genehmigungsverfahren entstanden sein könnten
- Mitwelt, also alle Ursachen, die durch externe Einflüsse wie Kundenverhalten, gesetzliche Vorschriften, Konkurrenzsituation, Arbeitsmarktsituation u. a. entstanden sein könnten
- Management, also alle Ursachen, die durch Unternehmensprinzipien oder Entscheidungen des Managements entstanden sein könnten
- Messung, also Ursachen welche durch Messeinrichtungen und damit verbundenen Messfehlern entstanden sein können

Sinnvoll und effektiv ist diese Methode jedoch nur in Teamarbeit anzuwenden. Eine vereinfachte Version ist in der Abbildung 13 dargestellt, hier sind die Ursachen auf die Rubriken reduziert.

3.9 HAZOP und SecHAZOP

Ziel des HAZOP-Verfahrens ist es, Gefahren und Probleme eines Systems systematisch zu untersuchen. Zur Ermittlung des Verhaltens aller relevanter Komponenten bzw. aller Kommunikationsverbindungen stellt man einen Systemplan auf.

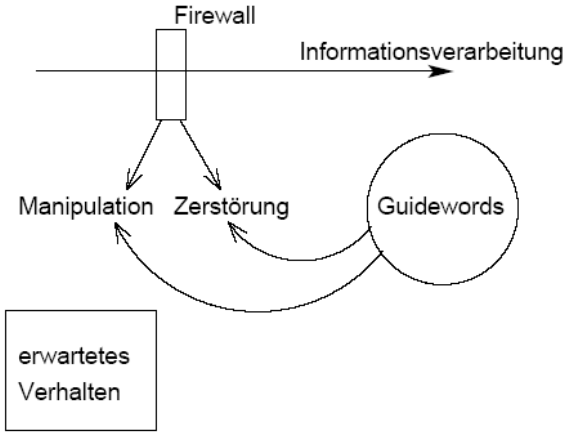


Abbildung 14: Systemplan [darm]

Die Eigenschaften der Komponenten werden als Attribute bezeichnet, hierzu zählen zum Beispiel die Manipulation oder die Zerstörung. Abweichungen werden in Form von Guidewords beschrieben. Diese sind beispielsweise technisches Versagen, ein Virus oder Insider.
Als Resultat der Ermittlung erzielt man dann eine solche Tabelle:

Attribut	der	Komponente	durch	Guidword
Manipulation		Firewall		Insider
				Techn. Versagen
				Virus
Zerstörung		Firewall		Insider
				Techn. Versagen
				Virus

Abbildung 15: Ermittlung der Bedrohung durch Kombination von Guidewords und Attribut angewendet auf eine Komponente [darm]

Die in der Tabelle eingetragenen Ausdrücke werden im Anschluss daraufhin untersucht, ob die Bedrohungen, welche als Attribute dargestellt sind, eintreten können und wenn ja, welche Auswirkungen dies haben kann. Je nachdem zu welchen Ergebnissen man kommt, muss im Anschluss entsprechend gehandelt werden. Dies wird in der Diplomarbeit von Anne-Kathrin Walter der Universität Bremen ausführlich beschrieben [darm].

Ebenso verhält es sich mit dem SecHAZOP Verfahren. Das HAZOP Verfahren wird auf den Einsatz in der Informationssicherheit übertragen. Da bei der Informationssicherheit Bedrohungen aufgedeckt werden sollen, sind die zu schützenden Informationen Ausgangspunkt der Analyse. Dementsprechend müssen die Guidewords angepasst werden.

Bewährt haben sich folgende Guidewords:

- kein
- mehr
- weniger
- ebenfalls
- Teil von
- umgekehrt
- anders als

Auch hier ergibt die Kombination von Attributen mit den Guidewords Fragen, welche von den beteiligten Mitarbeitern diskutiert werden müssen.

Hat man zum Beispiel das Attribut „Sicherer Speicher des Passworts auf dem Rechner“, so treten bei der Kombination folgende Fragen auf:
Kein – Ist das Passwort oder der Rechner anders geschützt?
Mehr – Gibt es zu viele Zugriffe?
Weniger – Ist der Schutz des Speichers zu schwach?
Ebenfalls – Profitieren Dritte von der Sicherung des Speichers?
Teil von – Ist der Schutz nur bedingt gegeben?
Umgekehrt – Kann der Schutz durch Manipulation oder einem Angriff außer Kraft gesetzt werden?
Anders als – Kann es passieren, dass der Speicher zwar sicher ist, aber durch Umgehen der Sicherheitsmaßnahmen Zugriff erlangt wird?

3.10 Functional Hazard Assessment (FHA)

Das Ziel dieser Methode ist, diejenigen Funktionen des Systems zu identifizieren, die zu Gefahren beitragen können. Diesen Funktionen werden daher entsprechenden Gefahrenstufen zugewiesen. Bei dieser Methode wird der Entwurf auf funktionaler Perspektive analysiert, so die Frauenhofer Gesellschaft [soko].

Die FHA erfordert Fachwissen, um sinnvolle Ergebnisse heraus zu bekommen. Die Ausgabedaten sind Tabellen, welche die Ergebnisdaten darstellen. Außerdem gibt es für jede Entwicklungsphase eine Beschreibung der jeweiligen Auswirkungen und empfohlene Gegenmaßnahmen. Als Gegenmaßnahmen werden häufig auch weitere Analysemethoden aufgeführt, wie in der Abbildung 16 dargestellt.
Für diese Analysemethode müssen alle Systemfunktionen sowie die möglichen Fehlerquellen und Schwachstellen bekannt sein.

System-funktion	**Fehlerbedingung (Beschreibung der Gefahr)**	**Betriebs-zustand**	**Auswirkungen der Fehlerbedingung auf das Flugzeug bzw. die Besatzung**	**Klassifizierung**	**Verweis auf das zugehörige Modell**	**Überprüfungs-methode**
Abbremsen des Flugzeugs am Boden	*1. Verlust der Abbremsfähigkeit*	*Lande-/ Startphase/ Rangieren*	*siehe unten*			
	1.a. Unangekündigter Verlust der Abbremsfähigkeit	Lande-/ Startphase	Besatzung kann Flugzeug nicht abbremsen, Flugzeug wird zu schnell und überschreitet die Landebahn	Katastrophal		Flugzeug-Fehlerbaum
	1.b. Angekündigter Verlust der Abbremsfähigkeit	Landephase	Besatzung fliegt geeigneten Flughafen an, benachrichtigt Notfallunterstützung am Boden und bereitet Insassen auf Landung mit Überschreitung der Landebahn vor	Gefährlich	Notlandungsmaßnahmen bei Verlust der Abbremsfähigkeit	Flugzeug-Fehlerbaum

Abbildung 16: Ausschnitt einer FHA anhand des Beispiels Abbremsen eines Flugzeugs [soko]

4 Entwurf der Methodik

Der Entwurf befasst sich mit der Analyse von Daten, Schnittstellen und Kommunikationsverbindungen. Hierzu wird das System im ersten Schritt vereinfacht, so dass nur die wesentlichen Systemkomponenten untersucht werden. Das bedeutet, dass alle für das System benötigten Komponenten in einfacher Form dargestellt werden. Es folgt die Systemanalyse. Ab diesem Punkt der Analyse wird zwischen Daten, Schnittstellen und Kommunikationsverbindungen unterschieden und diese unterschiedlich behandelt. Nachdem das System untersucht ist, wird eine Schwachstellen- und Bedrohungsanalyse durchgeführt, gefolgt von einem Soll-Ist Vergleich. Die Solldaten werden parallel zu der beschriebenen Analyse nach einer Anforderungsanalyse mit Hilfe des IT-Grundschutzhandbuches ermittelt. Sind die Differenzen geklärt so können die Schutzmaßnahmen ermittelt und die Empfehlungen ausgesprochen werden. Sind diese in das System eingearbeitet, muss es erneut überprüft werden. Die Analyse beginnt von neuem. Alle Änderungen müssen eingearbeitet und betrachtet werden, um zu sehen ob diese den erwünschten Effekt haben oder ob es weiterer Handlung bedarf. Dies betrifft sowohl den Ist- als auch den Soll-Bereich.

Für die Entwicklung der Methodik waren das IT-Grundschutzhandbuch und die ISO 13335 hilfreiche Anhaltspunkte. Der allgemeine Ablauf ist angelehnt an die ISO 13335, da in diesem Standard die Wechselwirkungen und Zusammenhänge des Schutzbedarfs, der Bedrohungen, der Schwachstellen und der unterschiedlichen Objekte und Komponenten hervorragend dargestellt sind. Bei der Durchführung der Analyse ist das IT-Grundschutzhandbuch unverzichtbar, da in ihm alle wichtigen Details, welche die Sicherheit eines Systems betreffen, beschrieben sind.

Die Common Criteria wurde nicht zu Hilfe genommen, da sie auf Grund der mnemotechnischen Bezeichnungen unübersichtlich wirkt und eine Einarbeitung notwendig ist. In Bezug auf die Gesetzeslage lieferte sie jedoch wichtige Informationen. Wer bereit ist, sich in die Common Criteria einzulesen, für den wird sie hilfreich im Bereich der Analyse sein. Die Inhalte sind dem IT-Grundschutzhandbuch ähnlich.

Als zu managementlastig stellte sich die ISO IEC 17799 heraus, daher wurde sie für die Systemanalyse des technischen Bereiches nicht hinzugezogen. Außerdem enthält die ISO IEC 17799, anders als das IT-Grundschutzhandbuch, nur übergreifende Anforderungen, also keine detaillierten Umsetzungshinweise.

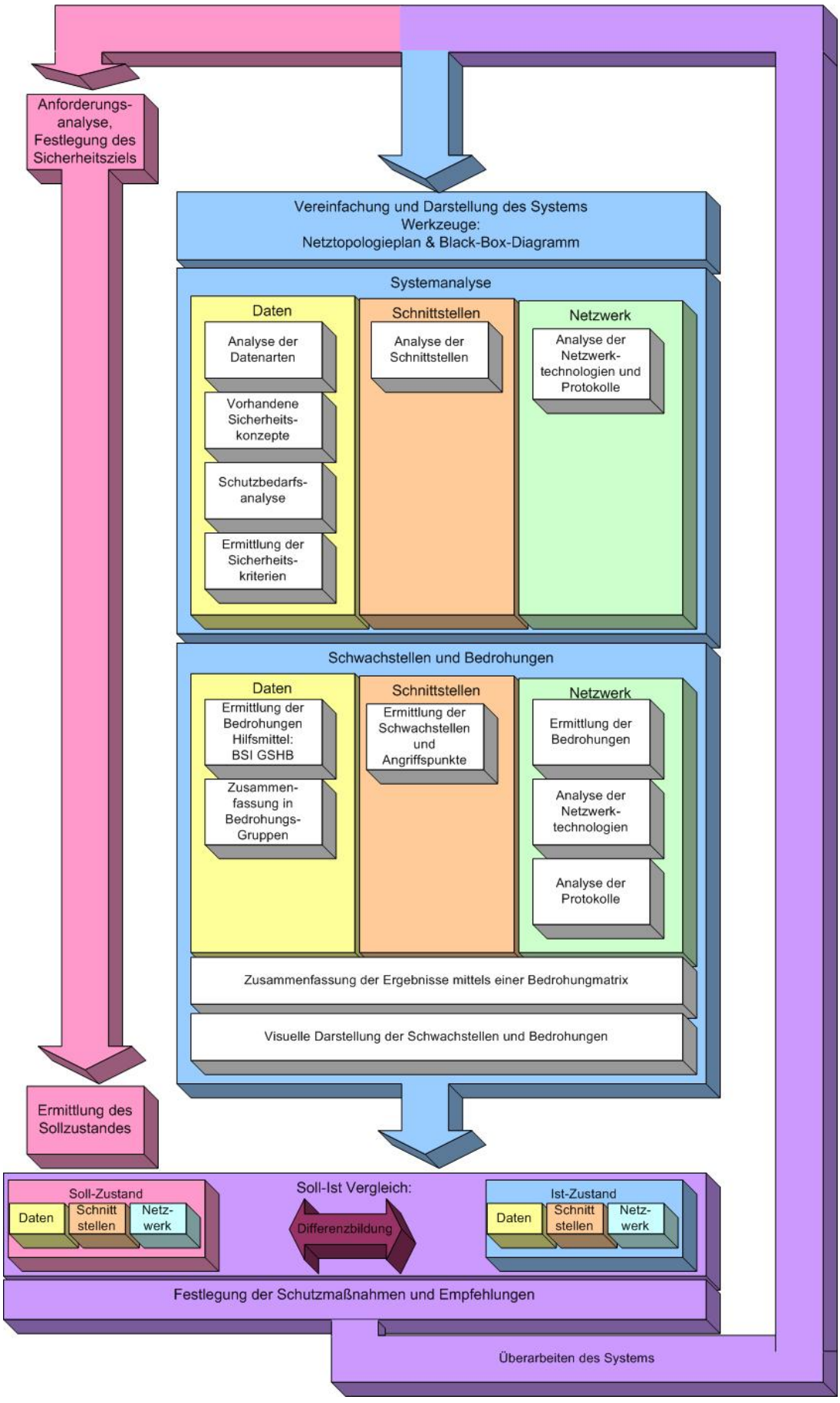


Abbildung 17: Ablauf der Analyse

4.1 Anforderungsanalyse

Bei der Anforderungsanalyse muss heraus gearbeitet werden, welche Sicherheitsanforderungen an welche Komponenten und Daten durch den Kunden gestellt werden. Dieses wird durch das Wissen der Entwickler und Spezialisten unterstützt und ergänzt. Sie stellt den Ausgangspunkt für die Festlegung des Soll-Zustandes dar.

Festzuhalten sind die Ergebnisse der Anforderungsanalyse in einem Pflichtenheft, in welchem alle Anforderungen präzise formuliert und mit Prioritäten versehen niedergeschrieben werden, so dass es zu keinerlei Missverständnissen kommen kann. Bei der Anforderungsanalyse müssen alle Verantwortlichen für dieses System, die Spezialisten sowie einige der betroffenen Mitarbeiter und der Kunde zusammen arbeiten. Alle Bedürfnisse und Anforderungen, welche an das System gestellt werden, werden so berücksichtigt. Damit alle Teilnehmer effizient an dem Projekt mitarbeiten können, ist es unbedingt notwenig, dass alle bis zu diesem Zeitpunkt bekannten Daten und Unterlagen des Systems jedem Teilnehmer vorliegen.

4.2 Vereinfachung des Systems

Um das System übersichtlicher zu gestalten wird es erst grafisch aufgearbeitet und im zweiten Schritt vereinfacht.

Mittels eines Netztopologieplans wird das Zusammenwirken des gesamte System, also alle Kommunikationsverbindungen, Server und Clients, grafisch dargestellt. Alle wichtigen Hardwarekomponenten werden hier erfasst und bezeichnet. Unklarheiten und Fehler bei der Kommunikation können so schon frühzeitig aufgedeckt werden. Vorteilhaft ist diese Art der Darstellung, da die vorhandenen Systemdetails visuell aufgearbeitet werden und somit für alle verständlich werden sollten. Ob die in der Anforderungsanalyse gestellten Forderungen schon erfüllt sind kann ebenfalls anhand des Netztopologieplanes überprüft werden.

Eine Darstellung in Form eines Black-Box Diagramms ist notwenig um die wichtigsten Komponenten übersichtlich darzustellen. Eine Zusammenfassung der Gruppen von Clients oder Servern, für die Übersichtlichkeit des Systems, ist vorgesehen. Dieses stellt eine Vereinfachung gegenüber dem Netztopologieplan dar. Die Hardwareseite wird, im Gegensatz zum Netztopologieplan, durch die Softwarekomponenten ergänzt, falls diese schon bekannt sind.

4.3 Systemanalyse

Ein IT-System, also auch das Beispielsystem, ist laut Rolf Opplinger [ROpp] drei Grundbedrohungen ausgesetzt: Der Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit.

Ein Verlust an **Vertraulichkeit** bedeutet, dass Unbefugte einen Informationsgewinn durch fehlende Sicherheitsmaßnahmen ziehen können und diese Informationen missbräuchlich verwendet werden können. Der Verlust an **Integrität** geht darüber hinaus, er bedeutet, dass die Daten modifiziert, also geändert oder verfälscht werden können. Wenn ein gewünschter Dienst nicht verfügbar ist, so spricht man vom Verlust der **Verfügbarkeit.** Auslöser kann ein Angreifer oder ein bestehender Fehler sein. Um diese drei Grundbedrohungen minimieren zu können, muss das System auf Schwachstellen untersucht werden. Dies ist jedoch erst möglich, wenn man das System, die Daten, die Schnittstellen und die Kommunikationsverbindungen genau kennt, dies erlangt man durch die Systemanalyse.

Die Unterlagen, welche bei der Anforderungsanalyse zusammengetragen wurden, also das Pflichtenheft sowie der Netztopologieplan und das Black Box Diagramm, sind notwendige Grundvoraussetzungen für die Durchführung der Systemanalyse. Use-Case-Diagramme, Anwendungsfalldiagramme und Beschreibungen, Kollaborationsdiagramme, Sequenzdiagramme und Zustandsdiagramme sind hilfreich bei der Analyse. Fehlende Daten müssen eingeholt und Fragen bezüglich des Systems mit den Verantwortlichen, Spezialisten und Mitarbeitern abgeklärt werden. Ziel dieser Analyse ist es eine vollständige Systembeschreibung zu erhalten. Zu diesem Zeitpunkt wird die Grenze der Sicherheitsanalyse und somit des zu analysierenden Systems abgesteckt.

Hat man ein Überblick über das bestehende System gewonnen und sich die Anforderungen verinnerlicht kann man das System in die Bereiche Daten, Schnittstellen und Kommunikationsverbindungen aufteilen. Dies ist notwendig, damit alle wichtigen Hard- und gegebenenfalls auch Softwarekomponenten erfasst und analysiert werden. Zwar kann es bei dieser Vorgehensweise zu Überschneidungen während der Analysephase kommen, es minimiert aber die Wahrscheinlichkeit einen wichtigen Aspekt zu übersehen. Spätestens während der Realisierungsphase werden diese Überschneidungen aber aufgehoben.

Die Systemanalyse der unterschiedlichen Daten ist die Grundlage der eigentlichen Analyse. Die Schnittstellen und Kommunikationsverbindungen müssen auf ihre Schwachstellen untersucht

werden um die ermittelten Daten zu schützen. Das Vorgehen ist wie folgt: Alle Daten werden zusammengetragen, aufgelistet und in einem Black-Box Diagramm dargestellt. Neben den Kommunikationsverbindungen, zwischen allen Hard- und Softwarekomponenten, werden die Daten eingetragen.

Daten gleichen Typs dürfen zu einem Oberbegriff zusammengefasst werden, wenn viele Daten gleichen Typs sind. Es muss jedoch eine Auflistung geben, in der die Zuordnung der Daten zu dem jeweiligen Oberbegriff stattfindet. Ohne diese Zusammenfassung ist eine Analyse zwar genauso möglich, bedeutet jedoch erheblich mehr Aufwand. Generell gilt aber, solange der Aufwand auf Grund großer Datenmengen nicht zu groß ist, sollte von einer Zusammenfassung abgesehen werden.

Wenn über die Kommunikationsverbindungen jeweils nur wenige Daten gesendet würden, wäre eine detaillierte Aufführung sinnvoll, denn hier wäre eine Zusammenfassung zu allgemein. Ein weiterer wichtiger Aspekt ist die Aktualisierung. Wenn sich während der Analyse heraus stellt, dass es weitere oder neue Datenarten gibt, so muss dieser Punkt der Analyse aktualisiert werden, um Schwachstellen auszuschließen.

Die Ermittlung bereits vorgesehener Sicherheitsstandards, für die unterschiedlichen Hard- und Softwarekomponenten, stellt einen weiteren Analysepunkt dar. Die Ergebnisse dieser Analyse werden der Übersicht halber in einer Tabelle niedergeschrieben. Diese Tabelle ist nach Komponente und Daten unterteilt und wird bei fortschreitender Analyse weiterverwendet, beispielsweise beim Soll-Ist Vergleich im Kapitel 6.6.

Hat man sich einen Überblick über das System verschafft, so folgt im Anschluss die Ermittlung der Schutzbedürftigkeit der Daten. Hierzu wird als erstes die Art der Grundbedrohung ermittelt und welche Daten im Einzelnen gefährdet sind.

Es muss überprüft werden, welche Gesetze eingehalten werden müssen und welche Auswirkung diese auf den Schutzbedarf der Daten haben. Mit diesem Wissen kann man ermitteln, welche Schäden bei welchen Daten auftreten können und daraus schlussfolgern, welcher Gefährdungsklasse die Daten zugeordnet werden müssen. Die Gefährdungsklassen sind denen des BSI identisch. Das Niederschreiben einer Begründung dieser Zuordnung ist sinnvoll, um im Nachhinein die Entscheidung für eine bestimmte Gefährdungsklasse nachvollziehen zu können und

um zu überprüfen, ob die in der Anforderungsanalyse gestellten Forderungen korrekt eingeflossen sind.

Der Bereich der Schnittstellen gewinnt erst in den folgenden Kapiteln an Bedeutung. Zum diesem Zeitpunkt der Analyse werden nur die Schnittstellenarten ermittelt, also ob es Nutzer- oder Datenaustauschschnittstellen sind. Bei Datenaustauschschnittstellen wird es zum Beispiel keine direkte Zugriffskontrolle geben, beispielsweise durch das Einführen einer Chipkarte, dies könnte aber bei einer Benutzerschnittstelle der Fall sein. Die Schnittstellen werden zur Verdeutlichung in das Black-Box Diagramm eingetragen und die durch die Daten hervorgerufene Gefährdungsklasse farblich gekennzeichnet.

Beim den Kommunikationsverbindungen werden die Übertragungstechnologien und Protokolle ermittelt und in einer Tabelle eingetragen. Gleichzeitig erfolgt eine Darstellung mittels Black-Box Diagramms. Wie auch schon bei den Schnittstellen werden die Gefährdungsklassen ermittelt, welche abhängig von der Gefährdungsklasse der zu übertragenden Daten sind. Die Gefährdungsklasse der Kommunikationsverbindung ist unabhängig davon, welche Sicherheit das Übertragungsmedium gewährleisten kann. Es besteht die Möglichkeit, während des weiteren Analyseverlaufs zu überprüfen, ob die Sicherheit des Übertragungsmediums ausreicht um die Daten einer bestimmten Gefährdungsklasse zu schützen.

Unterstützend könnte das SecHazop oder Hazop Verfahren eingesetzt werden. Hiermit werden Systemzusammenhänge dargestellt. Während der Schwachstellen und Bedrohungsanalyse ist es weiter einsetzbar, sie können ermittelt und eingezeichnet werden. Die Anwendung dieses Verfahren ist allerdings nur möglich, wenn der Entwicklungsstand relativ weit fortgeschritten ist und viele Hard- und Softwaredetails bekannt sind.

4.4 Schwachstellen und Bedrohungen

Zu den Schwachstellen in der IT-Sicherheit gehören Sicherheitsschwächen unter anderem des Gebäudes, des Unternehmens, in den Richtlinien, der Mitarbeiter, der verwendeten Protokolle und Technologien in der Hard- und Software oder auch Programmfehler. Schwachstellen können genutzt werden um gezielt oder unbeabsichtigt Schaden an einem Unternehmen oder an einem System zu verursachen. Durch diese Schwachstellen haben die Bedrohungen eine Chance, auf das System einzuwirken.

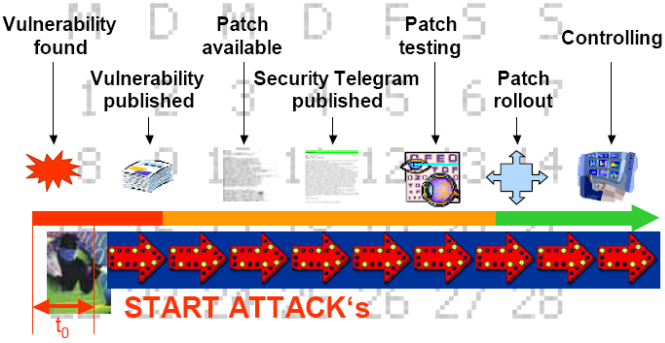


Abbildung 18: Zeitlicher Ablauf einer Sicherheitslücke [eday]

Auch wenn alle Schwachstellen aufgedeckt werden, wird es allerdings immer ein Restrisiko geben. Dieses Restrisiko wird durch neue Methoden oder unentdeckte Schwachstellen hervorgerufen. Daher ist es an diesem Punkt der Analyse besonders wichtig, dass möglichst viele der Spezialisten und Entwickler zusammenarbeiten.

Die Schwachstellenanalyse beginnt mit einem Brainstorming, welches mit Hilfe des IT-Grundbuchhandbuchs [bsigshb] die Bedrohungen, welche die Daten betreffen, ermittelt. Es werden die Daten in Bezug auf die Verfügbarkeit, die Integrität und die Vertraulichkeit untersucht. Im Anschluss werden diese Bedrohungen in fünf Klassen eingeteilt, organisatorische Mängel, menschliche Fehlhandlungen, Höhere Gewalt, vorsätzliches Handeln und technisches Versagen.

Die Schnittstellen sind ebenfalls Angriffen und Bedrohungen ausgesetzt. Das BSI Handbuch [bsigshb] ist auch in diesem Punkt hilfreich. Eine kurze Begründung verdeutlicht, aus welchen Beweggründen die Daten welcher Gefährdungsklasse zugeteilt werden. Hierdurch kann man später die Entscheidung für eine Gefährdungsklasse einfacher nachvollziehen. Diese Ergebnisse sind schriftlich zu fixieren.

Die Vorgehensweise im Bereich der Kommunikationsverbindungen ist identisch. Erweitert wird die Analyse dadurch, dass die Bedrohungen und Schwachstellen der Übertragungstechnologien und Protokolle in einer Tabelle zusammengefasst werden.

Eine Zusammenfassung der Erkenntnisse der drei vorangegangenen Unterkapitel folgt. Diese Erkenntnisse werden in einer Bedrohungsmatrix verewigt. Alle Systemkomponenten werden den jeweiligen Angreifern gegenübergestellt und die Klasse ermittelt, aus der diese Bedrohung stammt. Auf diesem Wege können die Maßnahmen ermittelt werden und an welchen Punkten angesetzt werden muss um die Hard- und Softwarekomponenten zu schützen. Visuell werden diese

Ansatzpunkte in einem Black-Box Diagramm dargestellt. Mittels Blitzen, welche mit Legenden versehen sind, werden die jeweiligen Bedrohungen angedeutet.

Es gibt noch weitere Methoden, welche während der Analyse angewendet werden könnten. Ein Bedrohungsbaum oder Fehlerbaum kann erzeugt und dann systematisch nach Schwachstellen behandelt werden. Dies ist allerdings nur möglich, wenn verhältnismäßig viele Systemdetails bekannt sind.

Auch das Ishikawa-Diagramm kann für die Bedrohungsanalyse eingesetzt werden. Dieses Diagramm ist dem Fehlerbaum recht ähnlich. Das Ishikawa-Diagramm ist ein einfaches Hilfsmittel zur systematischen Ermittlung und strukturierten, übersichtlichen Darstellung von Ursache-Wirkungs-Zusammenhängen. Dieses Diagramm kann allerdings nur eingesetzt werden, wenn einem die Auswirkungen der Bedrohungen bewusst sind.

Eine Gefahrenanalyse mit Hilfe der PHA-Methode wäre denkbar. Es werden die Bedrohungen, die Auswirkungen, der Schweregrad der Auswirkung, die Randbedingungen welche für das Eintreten der Bedrohung ausschlaggebend sind, die Häufigkeit des Eintretens und schließlich noch wie diese Gefahr vermieden werden könnte, ermittelt. Für diese Methode ist allerdings relativ viel Hintergrundwissen erforderlich. Oftmals sind einige der eben genannten Punkte zu diesem Zeitpunkt der Analyse noch nicht bekannt, so dass sich diese Methode wie ein roter Faden durch das komplette Analyseverfahren bis zur Realisierungsphase zieht. Es wäre eine Möglichkeit eine Übersicht zu bekommen, welche im Anschluss die Ergebnisse der gesamten Analyse in tabellarischer Form darstellt.

Die FHA-Methode wäre ebenfalls in diesem Kapitel einsetzbar, sie ist der PHA-Methode sehr ähnlich. Für diese Methode müssten laut Anne-Kathrin Walter [darm] folgende Attribute bekannt sein:

- Die jeweilige Systemfunktion
- Die Fehlerbedingung, also wann ein Fehler auftreten würde
- Der Zustand in dem sich das System befindet
- Die Auswirkungen des Fehlers
- Die Gefährdungsklasse
- Welche Komponente zuständig wäre für die Verhinderung eines Fehlers o.ä.
- Mit welcher Methode dieser Fehler dargestellt wurde, beispielsweise ein bestimmter Fehlerbaum

Wie schon die PHA-Methode würde sich diese Methode durch die gesamte Analyse ziehen. Gekoppelt wäre sie unter anderem mit den Fehlerbäumen. Diese Methode einzusetzen ist erst sinnvoll, wenn Software- und Funktionsdetails bekannt sind, so dass alle oben genannten Punkte bearbeitet werden können.

4.5 Ermittlung des Soll-Zustandes

Um den Soll-Ist-Vergleich durchführen zu können muss der Soll-Zustand ermittelt werden. Das IT-Grundschutzhandbuch [bsigshb] sieht folgende Regelungen für die IT-Sicherheit vor:

- Datensicherung
- Datenarchivierung
- Datenträgertransport
- Datenübertragung
- Datenträgervernichtung
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration, Zugriffs- und Zutrittsrechten
- Gebrauch von Passwörtern
- Zutrittsberechtigungen
- Zugangsberechtigungen
- Zugriffsberechtigungen
- Betriebsmittelverwaltung
- Kauf und Leasing von Hardware und Software
- Wartungs- und Reparaturarbeiten
- Software: Abnahme und Freigabe
- Software: Anwendungsentwicklung
- Datenschutz
- Schutz gegen Computer-Viren, (Virenschutzkonzept, Kryptokonzept, Schlüsselmanagement und Firewallkonzept)
- Revision
- Notfallvorsorge
- Vorgehensweise bei der Verletzung der Sicherheitspolitik

Um den Soll-Zustand zu ermitteln wird der Maßnahmenkatalog des BSI durchgegangen, die für das System relevanten Punkte zusammengetragen und diese den jeweiligen Systemkomponenten

zugeordnet. Dieses wird im Bereich der Daten, der Schnittstellen als auch der Kommunikationsverbindungen gemacht. Eine genaue Beschreibung der Maßnahmen erfolgt im Kapitel 6.7 „Festlegung der Schutzmaßnahmen und Empfehlungen“, da dieses Kapitel für die Entwickler bei der Weiterentwicklung des Systems von Bedeutung ist.

4.6 Soll-Ist-Vergleich

Nachdem alle Daten analysiert, Schnittstellen und Kommunikationsverbindungen überprüft sind, kann festgestellt werden, welche der Anforderungen nicht erfüllt sind. Mittels Differenzbildung des Soll- und des Ist-Zustands kann man sehen wo Handlungsbedarf ist. Dieses wird nacheinander bei den Daten, Schnittstellen und bei den Kommunikationsverbindungen durchgeführt. In der Zusammenfassung wird dann das Ergebnis der Differenzbildung niedergeschrieben, so dass die Überscheidungen, zu denen es notgedrungen kommt, wegfallen.

4.7 Empfehlung von Schutzmaßnahmen und für das weitere Vorgehen

Beim Soll-Ist-Vergleich hat sich herausgestellt wo Verbesserungen und Ergänzungen vorgenommen werden müssen. Jetzt müssen entsprechende Gegenmaßnahmen gefunden und realisiert werden. Um sicherzugehen, dass nichts vergessen wird oder neue Fehler eingebaut werden sollte diese Analyse nur im Team durchgeführt werden. Eine Wiederholung der kompletten Analyse nach einem Re-Design ist notwendig.

In diesem Kapitel sollten auch Maßnahmen, die über die Softwareentwicklung hinausgehen, wie zum Beispiel das Sicherheitskonzept, angesprochen werden. Parallel zu der Softwareentwicklung gibt es noch viele wichtige Details zu beachten. Unbedingt notwenig ist es sich zu diesem Zeitpunkt Gedanken über das weitere Vorgehen zu machen. Selbst wenn in diesem Kapitel nicht in die Feinheiten des Systementwurfs gegangen wird, so sollten dennoch Empfehlungen für das weitere Vorgehen angesprochen werden. Dies könnte beispielsweise die Aufstellung eines Konzeptes für einen bestimmten Bereich sein.

5 Das Beispielsystem

Ein Audio-Server bietet Mediadaten, welche die Plattenlabel zur Verfügung stellen, zum Verkauf an. Über einen Reseller können Endkunden diese Mediadaten beziehen. Ein Teil der Daten, etwa 95 %, befinden sich von Anfang an auf der Settop Box des Kunden oder werden über eine breitbandige Kommunikationsverbindung per Broadcast nachgeladen. Die Übertragung der gekauften Mediadaten, meist die restlichen 5 %, geschieht über eine schmalbandige Verbindung. Eine Übersicht bietet die Abbildung 17, der Netztopologieplan des Systems.

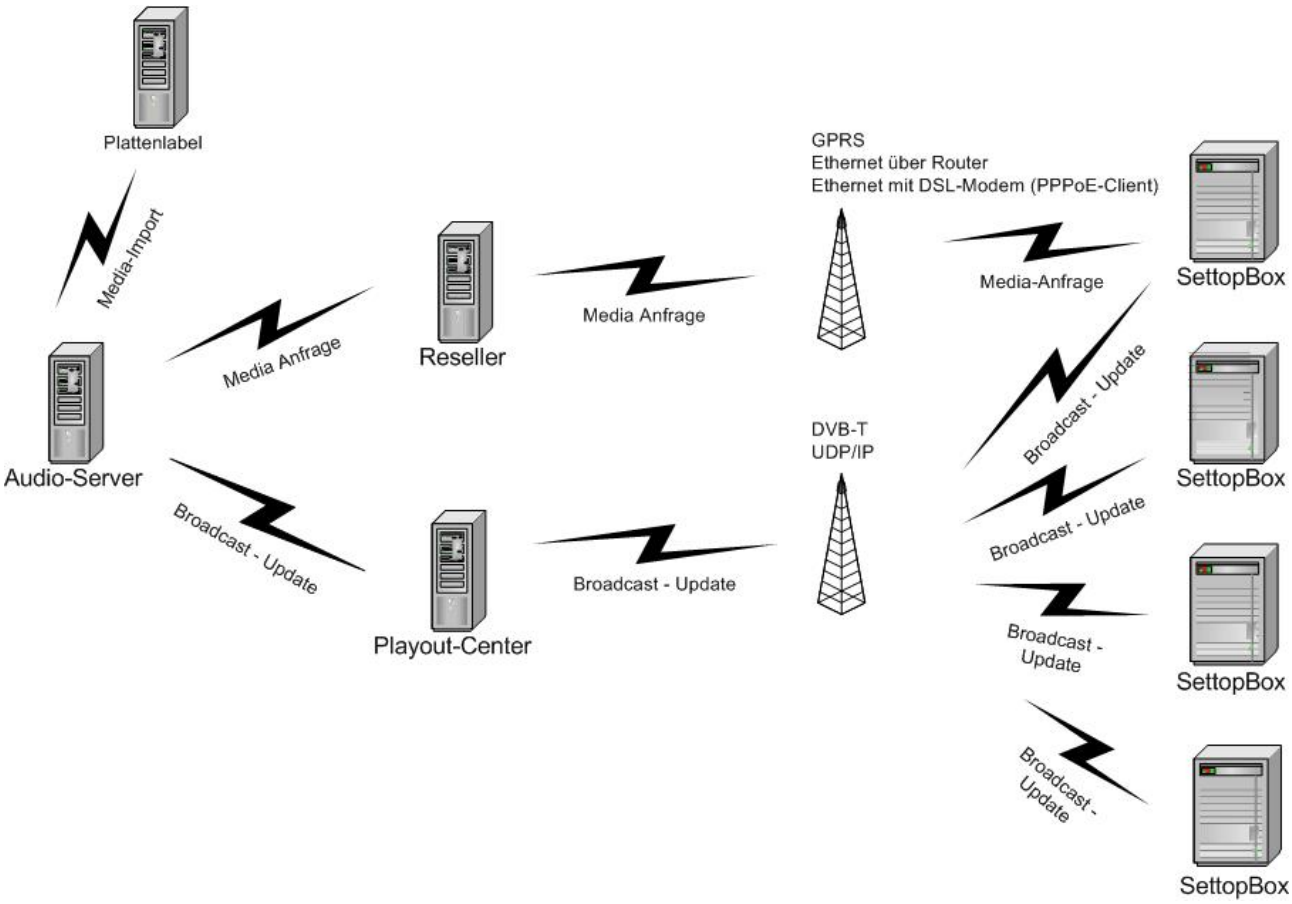


Abbildung 19: Netztopologieplan des Systems

5.1 Audio-Server

Der Audio Server ist für die Verteilung, Speicherung und Verarbeitung der Mediadaten zuständig. Über eine Benutzerschnittstelle können die Benutzerkonten und das Musikarchiv gepflegt werden. Der Import von Mediadaten geschieht über eine Schnittstelle zu den Plattenlabeln. Resellerkundendaten, DRM-Daten, Streaming Schlüssel, Kundeninformationen, Zugriffsrechte, Dateiformate und Wasserzeichen werden auf diesem Server in einer Verwaltung-Datenbank

gespeichert. Die Abrechnung der Mediadaten, gegenüber dem Reseller, geschieht auf diesem Server. Damit alle Daten vor unerlaubten Zugriffen geschützt sind, muss sich jeder Benutzer authentifizieren bevor er auf das System zugreift. Mittels einer Rechtekontrolle wird überprüft ob es ihm erlaubt ist, auf das System und die jeweiligen Daten zuzugreifen. Um die Daten bei der Übertragung zu schützen werden sie mit Hilfe von Schlüsseln, welche hier erzeugt und in einer Schlüsseldatenbank gelagert werden, verschlüsselt.

5.2 Playout Center

Das Playout Center steht mittels DVB-T in Verbindung mit den Clients. Seine Aufgabe ist es per Broadcast die Mediadaten, welche nur teilweise oder noch gar nicht vorhanden sind, zu übertragen und dann auf den Settop Boxen abzuspeichern. Mit Hilfe der Steuerungsdaten des DVB-Streaming Planers wird die Sendereihenfolge der Mediadaten ermittelt.

Die Kommunikation zum Reseller geschieht über eine VPN-Kopplung. Zu den Settop Boxen ist die Kommunikation nur einseitig, es können also nur Daten zu den Boxen übertragen werden. Hier sind die Protokolle UDP/IP und SSL vorgesehen.

5.3 Reseller

Über den Reseller werden die Mediadaten angefordert und übertragen. Er rechnet die erfolgreich übertragenen und gekauften Mediadaten mit dem Endkunden ab. Alle Verkaufsprozesse und Verbindungen werden protokolliert, so dass im Fehlerfall nachvollzogen werden kann, wo der Fehler auftrat und der Ausgangs-Systemzustand wiederhergestellt werden kann. Beim Reseller werden die Kunden verwaltet, also sowohl die Kundendaten, als auch die Rechnungsdaten und Besitzverhältnisse des Kunden. Der DVB-Streaming Planer, welcher den Ablauf der Kommunikation und die Übertragung der Mediadaten regelt, befindet sich beim Reseller.
Über jeweils ein Interface kommuniziert der Reseller über eine geschützte Verbindung mit dem Audio-Server und den Settop Boxen. Die Kommunikation zu den Settop-Boxen geschieht über GPRS, Ethernet über Router oder Ethernet mit DSL-Modem (PPPoE-Client). Als Protokoll ist SSL vorgesehen.

5.4 Settop Box

Die Settop Box ist Eigentum des Kunden. Auf ihr befinden sich Teile von Mediadaten, komplette Mediadaten welche gekauft wurden, sowie die Authentifikationsdaten, Wasserzeichen und Schlüssel des Endkunden. Hier werden Mediadaten bei Bedarf entschlüsselt und in einem Media-Archiv gespeichert. Mittels eines Watchdogs wird die Festplattenkapazität überprüft und bei Bedarf Daten gelöscht. Jede Settop Box beinhaltet außerdem einen Audioplayer und CD Brenner. Via Interface kommuniziert die Settop Box mit dem Reseller. Über dieses Interface werden fehlende Mediadaten bei Kauf eines Titels bestellt und übermittelt, aber auch die Protokollierung des Kaufs geschieht auf diesem Wege.

6 Durchführung der Analyse

Die Analyse wird anhand des im Kapitel 5 vorgestellten Beispielsystems durchgeführt. Der Entwicklungsstand des Systems ist wenig fortgeschritten, reicht jedoch aus um die wesentlichen Merkmale der Analyse darzustellen.

6.1 Anforderungsanalyse

Es soll ein Medienübertragungssystem entwickelt werden, bei dem die wirtschaftlichen Interessen der Plattenlabel und die Sicherheit des Systems gewährleistet sind.

Die Medienübertragung soll einerseits über eine breitbandige, anderseits über eine schmalbandige Kommunikationsverbindung geschehen. Die Mediadaten werden in 5 % und 95 % Blöcke aufgeteilt. Die 95 % Blöcke werden vorab auf die Settop Boxen geladen, dieses geschieht über die breitbandige Verbindung. Alternativ wäre es auch mittels CD denkbar. Die restlichen 5 % werden beim Kauf eines Titels über eine schmalbandige Kommunikationsverbindung nachgeladen.

Dieses Splitten der Mediadaten ist notwenig, da die Plattenlabel nicht ihre kompletten Mediadaten aus der Hand geben werden. Ein Grund hierfür ist, dass ein Schutzmechanismus der Mediadaten beispielsweise von unautorisierten Hackern geknackt werden könnte und somit alle Mediadaten, welche sich auf der Festplatte der Settop Box befinden, zur freien Verfügung stehen würden. Dies wäre es riesiger Verlust für die Plattenfirmen und anderseits, durch rechtliche Schritte, auch für die entwickelnde Firma.

Besonderen Schutz muss den Mediadaten, welche dem Urheberrecht unterliegen, und den Endkundendaten, da sie die persönlichen Daten des Kunden sind, zukommen. Die Gesetzgebung schreibt vor, dass diese persönlichen Daten zu schützen sind, ansonsten kann es zu Schadensersatzforderungen durch die Endkunden kommen. Bei den Resellerdaten und Daten, welche die Geschäftsbeziehungen zwischen dem Audio-Server Betreiber und dem Reseller wiedergeben, handelt es sich nicht um persönliche Daten von Kunden, sondern um Firmendaten. Hier ist der Schutzbedarf geringer als bei den Endkundendaten.

Ausgeschlossen werden sollen Schäden durch vorsätzliches Handeln, also beispielsweise Ausspähen, Zerstören und Löschen von Daten durch Hacker oder Schäden, welche durch fehlende

Schutzmechanismen entstehen. Es sollen keine Daten durch unautorisierte Personen eingesehen oder geändert werden oder das System außer Kraft gesetzt werden können.

6.2 Vereinfachung des Systems

6.2.1 Netztopologieplan

Im Netztopologieplan sind alle bekannten Server, Kommunikationsverbindungen und verschiedene Typen von Settop Boxen, also Clients, aufgeführt. Alle bekannten Daten bzw. möglichen Anfragen sind eingetragen, so dass sie für die spätere Analyse nur übernommen werden müssen. Im Laufe der Analyse kann sich dieser Netztopologieplan noch verfeinern, denn alle Änderungen, welche vorgenommen werden, müssen auch in diesem Netztopologieplan vorgenommen werden.

Es sind nur so viele Reseller, Playout Center, Plattenlabel, Audio-Server und Settop Boxen, wie für das Verständnis notwendig, eingezeichnet, auch wenn es in der Realität mehr sind. Somit wird das Zusammenwirken deutlich und das System bleibt übersichtlich und leicht verständlich.

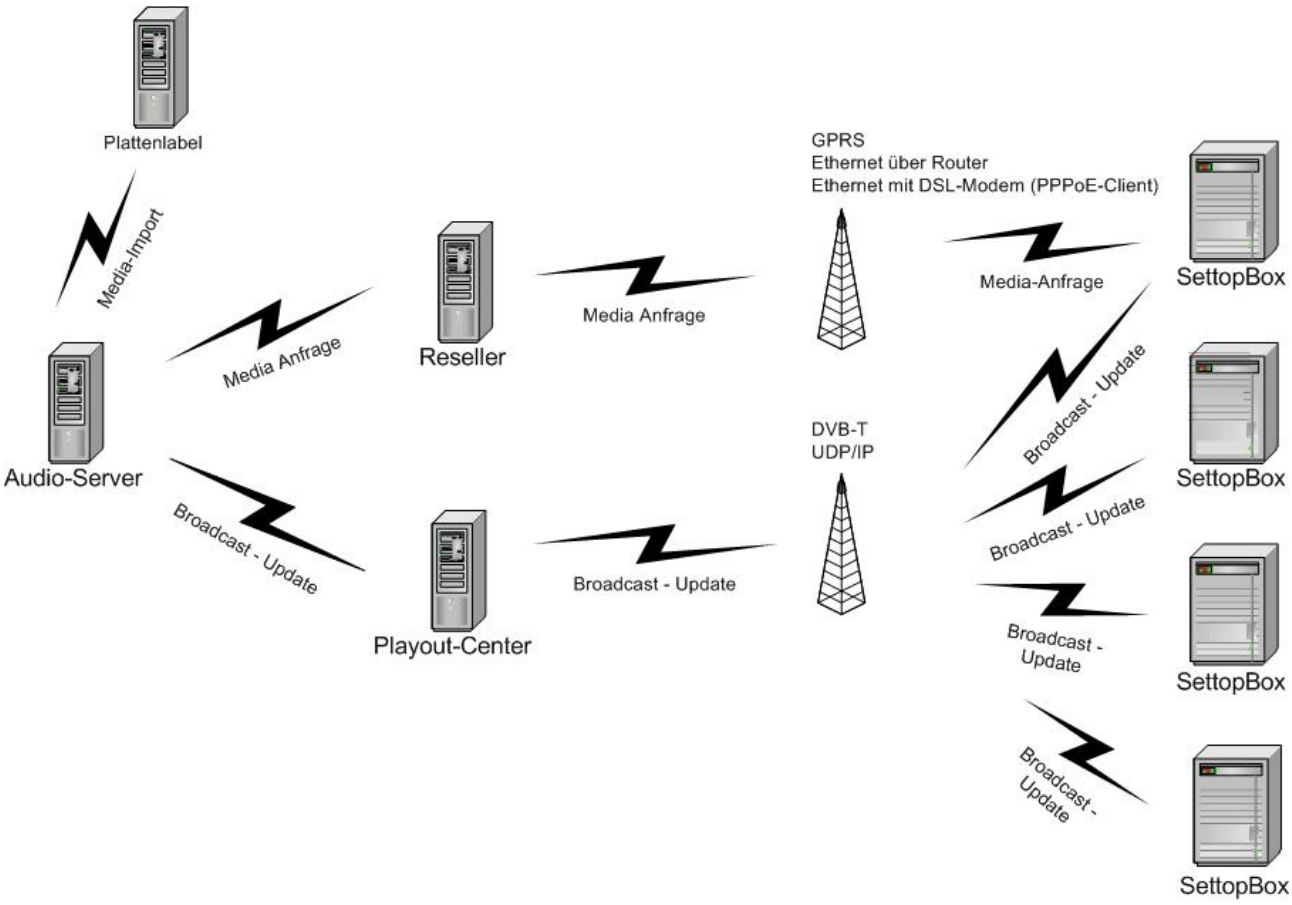


Abbildung 20: Netztopologieplan des Beispielsystems

6.2.2 Black-Box Diagramm

Alle Komponenten werden mittels eines Black-Box Diagramms dargestellt. Eine Zusammenfassung gleicher Komponenten ist notwendig, dadurch gewinnt das System an Übersichtlichkeit. Schnittstellen, Kommunikationsübertragungssysteme, Server und Clients werden eingetragen und bezeichnet.

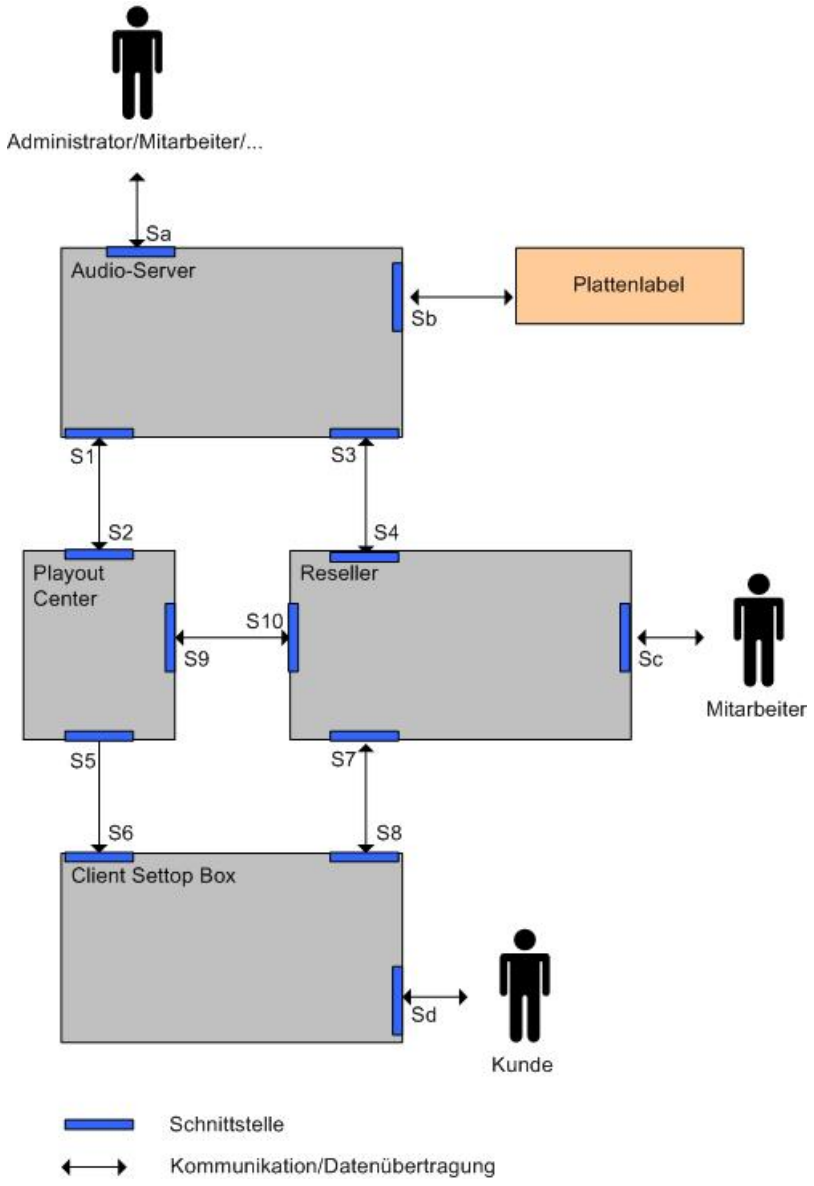


Abbildung 21: Black-Box Diagramm des Bespielsystems

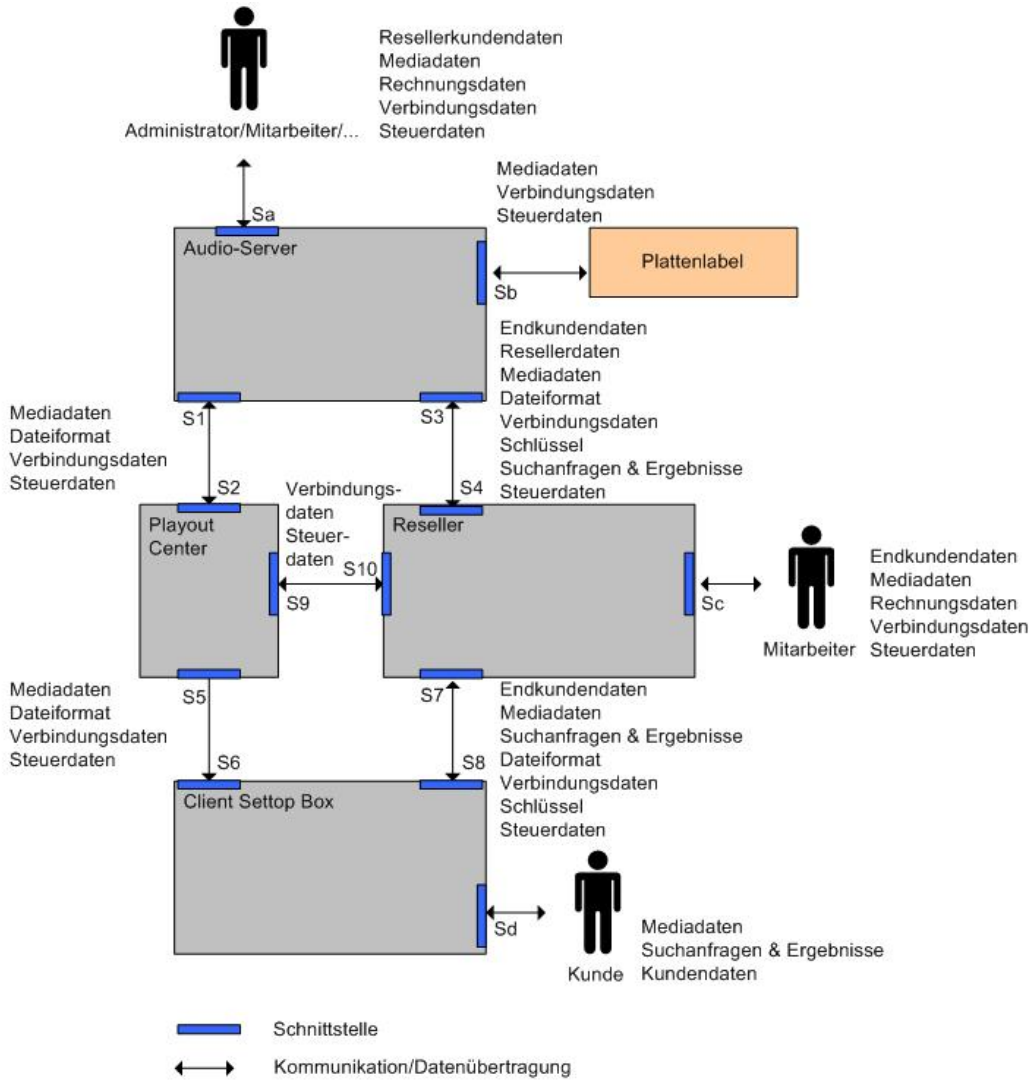
6.3 Systemanalyse

Daten, Schnittstellen und Kommunikationsverbindungen des Systems sind zu diesem Zeitpunkt der Entwicklung noch nicht voll ausgereift, dass ist aber nicht von Nachteil. Im Kapitel 6.7 „Feststellung der Schutzmaßnahmen und Empfehlungen“ werden in diesem Fall Empfehlungen für

das weitere Vorgehen ausgesprochen, so dass ein unausgereiftes System durch die bis dahin erworbenen Kenntnis mit den nötigen Sicherheitsmaßnahmen weiterentwickelt werden kann.

6.3.1 Daten

Die Daten wurden gemäß ihres Typs einem Oberbegriff zugeordnet. Eine Erläuterung dieser Zusammenfassung steht unterhalb des Black-Box Diagramms. An den Kommunikations-verbindungen sind die bekannten Daten, in Form des Oberbegriffs, eingetragen.



Resellerkundendaten: Kundeninformationen, Zahlungsmodalitäten, Zugriffsrechte, abrufbare Dateiformate
Mediadaten: TitelID, Priorität, Metadaten, Mediadateien(komplett und zerhackt)
DRM-Daten (Wasserzeichendaten): Wasserzeichen, komplette Kundendaten des Endkundens
Endkundendaten: Name, Wohnort, Kundennummer, EndkundenId, Zahlungsmodalitäten
Schlüssel
Verbindungsdaten: BoxIP, diverse IP-Adressen
Steuerdaten: Priorität, Playlist, Befehle
XML-Daten
Geschäftsbeziehungen

Abbildung 22: Systemanalyse, Analyse der vorhandenen Datentypen

Nachdem die Datentypen bekannt sind, kann analysiert werden, welche Sicherheitskonzepte das System bis zum derzeitigen Zeitpunkt schützen. Der Ist-Zustand wird festgestellt.

Ist-Zustand	Audio-Server
Resellerkundendaten	• Zugriffsrechte werden bei der Schnittstelle Sa und S1 überprüft
Mediadaten	• Zugriffsrechte werden bei der Schnittstelle Sa und S1 überprüft • Wasserzeichen des Resellers • Verschlüsselung der Übertragung mit Blowfish
DRM Daten	• Zugriffsrechte werden bei der Schnittstelle Sa und S1 überprüft
Endkundendaten	
Schlüssel	• Zugriffsrechte werden bei der Schnittstelle Sa und S1 überprüft
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Ist-Zustand	Playout Center
Resellerkundendaten	
Mediadaten	
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Ist-Zustand	Reseller
Resellerkundendaten	
Mediadaten	
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Ist-Zustand	Settop Box
Resellerkundendaten	
Mediadaten	• Verschlüsselung der Daten während der Übertragung • Wasserzeichen des Endkunden
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Der nächste Schritt ist festzustellen in welchen Bereichen die Sicherheit beeinträchtigt werden könnte.

	Verfügbarkeit	Integrität	Vertraulichkeit
Resellerkundendaten		x	x
Mediadaten		x	x
DRM-Daten		x	x
Endkundendaten		x	x
Schlüssel	x	x	x
Verbindungsdaten	x		
Steuerdaten	x		
XML-Daten (Sucheanfragen & Ergebnisse)	x		
Geschäftsbeziehungen		x	x

Die Einteilung der Daten in Gefährdungsklassen erfolgt mit Hilfe des IT-Grundschutzhandbuches [bsigshb]. Dort sind die Schutzbedarfskategorien wie folgt gegliedert.

Schutzbedarfskategorien	
"niedrig bis mittel"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Abbildung 23: Schutzbedarfskategorien [bsigshb]

Die Gefährdung der Daten erfolgt durch Beeinträchtigung der Vertraulichkeit, der Integrität oder der Verfügbarkeit.

In der Tabelle sollte, neben der Begründung, auch niedergeschrieben werden, wodurch welche Schäden auftreten könnten. Auch hier dürfen wieder die Oberbegriffe der Daten verwendet werden. Die Begründung sollte die in der Anforderungsanalyse gestellten Forderungen enthalten, können aber auch ergänzt werden.

	Gefährdungs-klasse	Schaden durch	Begründung
Reseller-kundendaten	hoch	Verstoß gegen Gesetze/Vorschriften/Verträge Beeinträchtigung des informationellen Selbstbestimmungsrechts negative Außenwirkung finanzielle Auswirkungen	Es handelt es sich um Firmendaten, nicht um Endkundendaten. Die Persönlichkeit eines Menschen ist nicht gefährdet, daher sehe ich die Gefährdung der Daten zwar als hoch an, aber nicht als sehr hoch.
Mediadaten	sehr hoch	Verstoß gegen Gesetze/Vorschriften/Verträge Beeinträchtigung der Aufgabenerfüllung negative Außenwirkung finanzielle Auswirkungen	Mediadaten unterliegen dem Urheberschutz. Daher können Plattenlabel Rechtsansprüche gegenüber der Herstellerfirma geltend machen, wenn Unbefugte ungehindert oder auch nur „aus versehen“ an nicht gekaufte Mediadaten gelangen.
DRM-Daten	sehr hoch	Verstoß gegen Gesetze/Vorschriften/Verträge Beeinträchtigung des informationellen Selbstbestimmungsrechts negative Außenwirkung finanzielle Auswirkungen	In Verbindung mit den DRM-Daten stehen unter anderem Endkundendaten. Werden diese verfälscht, eingesehen oder gehen verloren kann die betroffene Person, wenn sie es heraus bekommt, auf Grund des Datenschutzgesetzes eine Anklage gegen die Firma erheben.
Endkunden-daten	sehr hoch	Verstoß gegen Gesetze/Vorschriften/Verträge Beeinträchtigung des informationellen Selbstbestimmungsrechts negative Außenwirkung finanzielle Auswirkungen	Endkundendaten unterliegen dem Datenschutz, es können rechtliche Schritte folgen, wenn die Integrität oder Vertraulichkeit verletzt würden.
Schlüssel	hoch	Verstoß gegen Gesetze/Vorschriften/Verträge Beeinträchtigung der Aufgabenerfüllung	Die Schlüssel schützen wichtige Daten. Werden sie verfälscht so kann der Zugriff auf Daten verwehrt bleiben. Kaufansprüche des Kunden bleiben offen.

Verbindungs-daten	mittel	Beeinträchtigung der Aufgabenerfüllung	Verbindungsdaten sind für die Funktion des Systems nötig. Da sie aber nicht in direkter Verbindung mit beispielsweise dem Urheberrecht oder Datenschutz stehen ordne ich sie als mittel schützenswert ein. Zwar könnte das System im worst case außer Kraft gesetzt werden, dadurch würden aber keine Gesetze berührt.
Steuerdaten	mittel	Beeinträchtigung der Aufgabenerfüllung	Ebenso verhält es sich mit den Steuerdaten.
XML-Daten (Suchanfragen & Ergebnisse)	niedrig	Beeinträchtigung der Aufgabenerfüllung	Wenn XML Daten nicht oder falsch übermittelt werden, kann ein Kunde zwar keine Daten kaufen, er kann aber auch keine angeforderten verlieren.
Geschäfts-beziehungen	sehr hoch	Verstoß gegen Gesetze/Vorschriften/Verträge Beeinträchtigung des informationellen Selbstbestimmungsrechts negative Außenwirkung finanzielle Auswirkungen	Mit den Geschäftsbeziehungen verhält es sich wie mit den Reseller- und Endkundendaten. Werden Endkundendaten offen gelegt, so ist es ein Gesetzesverstoß.

6.3.2 Schnittstellen

Alle vorhandenen Schnittstellen sind im Black-Box-Diagramm eingezeichnet. Zu unterscheiden sind Schnittstellen, welche im direkten Kontakt zum Nutzer oder Administrator sind, hier Benutzerschnittstellen genannt, und Schnittstellen, welche zum Datenaustausch der Systeme untereinander dienen, diese wurden als Systemschnittstellen bezeichnet.

Die Benutzerschnittstellen sind die Schnittstellen Sa, Sb, Sc und Sd, die Systemschnittstellen S1-S10. Sa, Sc und Sd arbeiten mit Benutzeroberflächen. Auf die Benutzeroberfläche der Schnittstelle Sd können alle Menschen relativ einfach zugreifen. Somit muss diese Schnittstelle bzw. Benutzeroberfläche besonders abgesichert werden. Auf Sa und Sc haben nur Mitarbeiter des Unternehmens Zugriff, doch auch diese müssen, auf Grund der Daten auf welche sie dort Zugriff haben könnten, speziell abgesichert werden. Über Sb haben die Plattenlabel Zugriff auf das System. Ein Zugriffsschutz muss hier auf Seiten des Audio-Servers und der Plattenlabel erfolgen.

S1- S10 sind Schnittstellen, die ähnlich wie die der Plattenlabel ohne Benutzeroberfläche arbeiten. Bei allen Schnittstellen muss geklärt werden, welche Ports offen sein dürfen und ob es eine Zugriffskontrolle gibt, wenn man über sie auf das System zugreift.

Die Gefährdungsklassen der Schnittstellen werden im Black-Box Diagramms farbig dargestellt:

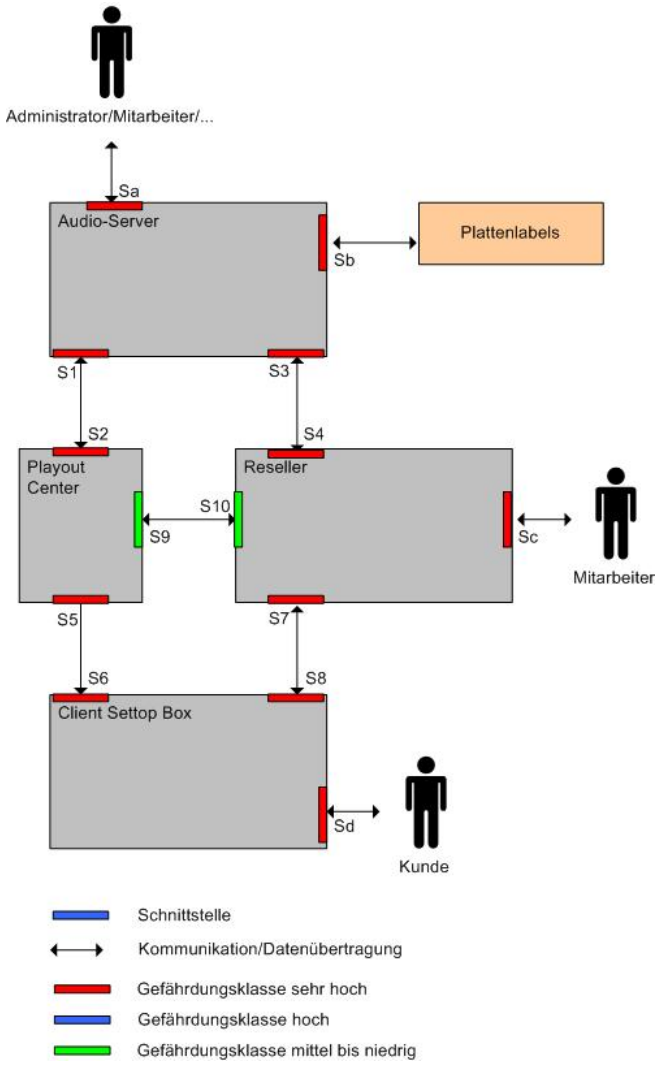


Abbildung 24: Systemanalyse, Analyse der vorhandenen Schnittstellen

6.3.3 Kommunikationsverbindungen

Es werden unterschiedliche Technologien für die Datenübertragung eingesetzt. Bei der Übertragung müssen die Daten abgesichert werden. Um festzustellen, wie hoch der Schutzbedarf ist, werden die Daten, welche über die Kommunikationsverbindungen gehen, betrachtet und deren Gefährdungsklasse auf die Kommunikationsverbindung übertragen. Dieses wird farblich im Black-Box Diagramm gekennzeichnet.

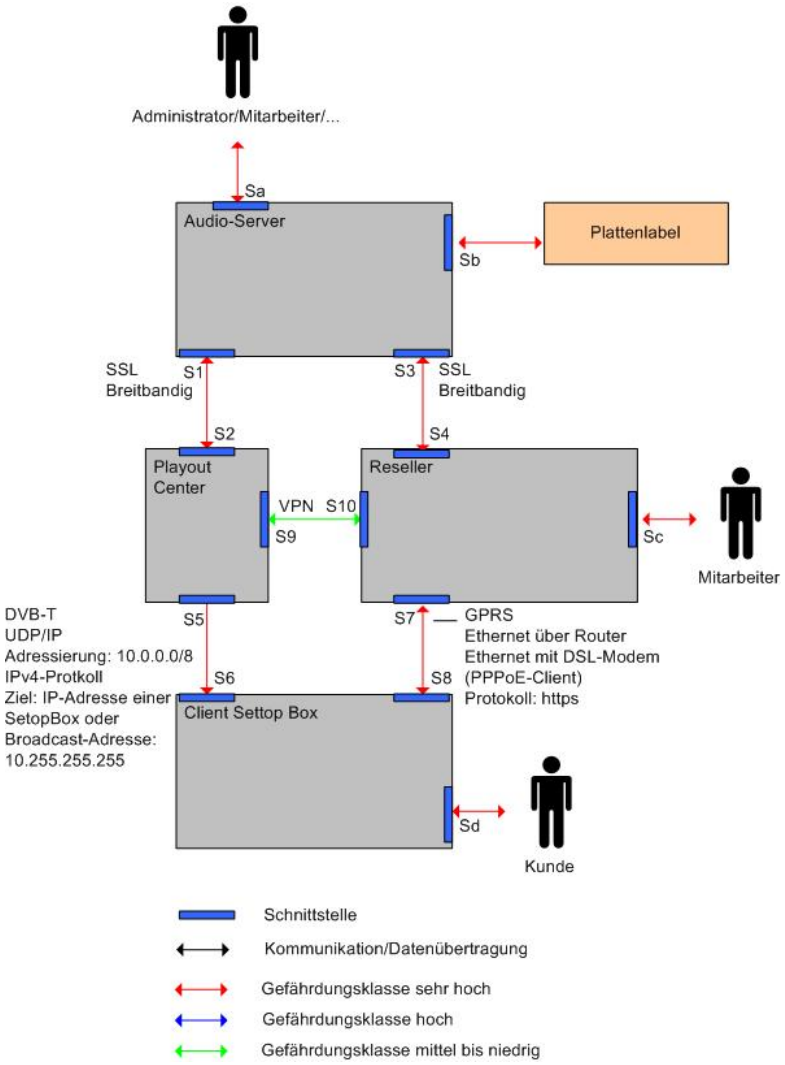


Abbildung 25: Systemanalyse, Analyse der vorhandenen Kommunikationsverbindungen

Eingesetzte Technologien:
DVB-T (Digital Video Broadcasting – Terrestrial)
GPRS
Ethernet über Router
Ethernet mit DSL Modem
VPN

Protokolle:
UDP
TCP
IPv4
SSL (https)

6.4 Schwachstellen und Bedrohungen

6.4.1 Daten

Daten sind durch die drei Grundbedrohungen Verfügbarkeit (a), Integrität (b) und Vertraulichkeit (c) gefährdet.

a) Die Verfügbarkeit der Daten wird durch höhere Gewalt gefährdet. Zur höheren Gewalt zählen Personalausfall, Naturgewalten, Feuer, Verdreckung oder andere technische Katastrophen im Umfeld des Systems. Aber auch der Einfluss von Personen ist von großer Bedeutung. Einbruch, Anschläge oder Diebstahl beeinträchtigen die Hardware des Systems in ihrer Funktion. Dieses kann durch fehlende Zugangskontrolle und/oder Rechtekontrolle, also Schutzmechanismen, begünstigt werden. Verrat oder Zugriff durch Mitarbeiter aus Interesselosigkeit, Angst, Enttäuschung, Routine im Ablauf, Gedankenlosigkeit, Habgier sind weitere Angriffsfelder, welche nicht zu unterschätzen sind.

   Sabotage und Manipulation sind die Mittel der Angreifer. Durch Zerstören, Löschen oder Veränderung von Daten können diese unbrauchbar werden und das System im ungünstigsten Fall komplett ausfallen. Ein Ausfall kann aber auch durch Virenbefall, Programmierfehler, Sicherheitslücken in Betriebssystem oder anderweitiger Software entstehen.

   Sind die Schutzmechanismen, also die Autorisierung und Authentizität, nur unzureichend oder gar nicht im System implementiert, so haben viele der Angreifenden ein leichtes Spiel. Zu nennen wäre hier eine nachlässige Passwort- und Zugriffshandhabung. Dies gilt sowohl für das System als für alle daran beteiligten Benutzer und Mitarbeiter.

b) Sabotage und Manipulation sind auch hier gefährliche Bedrohungen, allerdings auf eine andere Art und Weise als bei der Verfügbarkeit. Unkontrolliertes Duplizieren, wodurch Rechte geändert werden könnten, oder Veränderung von Daten durch Angreifer sind hier die Bedrohungen.

   Der Verrat oder der Zugriff durch Mitarbeiter aus Interesselosigkeit, Angst, oder Enttäuschung auf das System sind hier die Hauptgefährdungen. Aber auch Viren und Trojaner können Schäden anrichten. Wie auch bei der Verfügbarkeit sind fehlende und unzureichende Sicherheitsmechanismen der Grund dafür, dass die Angreifer eine Chance haben. Wieder sind es die Passworthandhabung, die Rechtekontrolle, Sicherheitslücken des

Betriebssystems oder der Software, Programmierfehler oder die Zugriffsrechte, welche Schwachstellen bieten.

c) Bei der Vertraulichkeit sieht es nicht anders aus, wieder sind es Mensches, welche das System in seiner Funktion durch Sabotage beeinträchtigen. Interesselosigkeit, Angst, Enttäuschung sind die Antriebsgründe.

Alle die hier angeführten Bedrohungen können durch betriebsinterne oder betriebsfremde Personen und sowohl beabsichtigt als auch unabsichtlich geschehen, dies hängt davon ab durch welchen Fehler und welche Schwachstelle es geschieht.

Nachdem die Bedrohungen zusammengetragen sind, können die gewonnenen Erkenntnisse zusammengefasst und Gruppen gebildet werden. Fehlende Ergebnisse können nachgetragen werden.

- Organisatorische Mängel
    - Fehlende oder unzureichende Schutzmechanismen (Autorisierung und Authentizität), also Zugangskontrolle und/oder Rechtekontrolle
    - ...
- Menschliche Fehlhandlungen
    - Fehlende oder unzureichende Schutzmechanismen
    - Fehlende oder unzureichende Protokollierung des Ablaufs
    - Programmierfehler
    - Fahrlässigkeit des Benutzers, zum Beispiel fehlendes Logout
    - ...
- Höhere Gewalt
    - Naturgewalten
    - ...
- Vorsätzliches Handeln
    - Einbruch, Anschläge, Diebstahl
    - Verrat oder Zugriff durch Mitarbeiter
    - Ausspähen, Zerstören, Löschen, unkontrolliertes Duplizieren oder Veränderung von Daten, Hacker, Datenveränderungen, Viren
    - Manipulation der Software
    - ...

- Technisches Versagen
    - Sicherheitslücken in der Betriebssystemsoftware
    - Hardwaredefekt
    - ...

6.4.2 Schnittstellen

Daten, welche von einem System zum anderen gelangen, müssen den Weg über die Schnittstellen gehen. Bei den Schnittstellen spielen offene Ports und Zugriffsrechte eine große Rolle. Mit Hilfe von TCP- oder UDP-Portscans kann systematisch ermittelt werden, auf welchem Port ein Verbindungsaufbau möglich ist, welche Dienste ein Server anbietet und welche Betriebssysteme verwendet werden.

Angriffe, welche über Ports laufen, sind immer vorsätzliche, welche durch organisatorische Mängel und menschliche Fehlhandlungen des Programmierers oder Administrators begünstigt werden. Offene Ports durch technisches Versagen stellen eine Seltenheit dar.

Da der Zugriff auf das System über offene Ports erfolgt, müssen die Zugriffsrechte überprüft werden. Es muss geklärt werden, ob der Benutzer wirklich der Benutzer ist, der er vorgibt zu sein und ob dieser Benutzer auf das System zugreifen darf, also eine Prüfung der Authentizität und Autorität ist notwendig. Im Audio-Server ist eine Rechteverwaltung vorgesehen. Bislang werden hier aber nur die Schnittstellen S1 und S3 überprüft. Alle anderen Systeme haben keinerlei derartige Absicherung, auch eine Firewall für eine Portkontrolle ist auf keinem der Systeme installiert.

6.4.3 Kommunikationsverbindungen

Anders als bei den Schnittstellen sind einige der Übertragungstechnologien und Protokolle bekannt. Somit können jetzt schon die bekannten Schwachstellen eingetragen werden.
Die Kommunikationsverbindungen sind unterschiedlichen Angriffen ausgesetzt, diese können sowohl die Soft- als auch die Hardware betreffen.

- Verkehrsanalyse ist eine Technik, welche auf die Analyse der Kommunikationsbeziehungen abzielt. Die Angreifer können wertvolle Informationen abgreifen und eventuell weiterverarbeiten. Es kommt zu einem Verlust der Vertraulichkeit.
- Durch Vortäuschung der Identität kann versucht werden an diverse Daten heran zu kommen. Die Integrität wird angegriffen.

- Sind die Daten nicht gesichert oder verschlüsselt, so kann man durch unbefugtes Abhören Informationen abgreifen. Der Verlust der Vertraulichkeit der Daten ist die Folge.
- Durch Aufzeichnung einer Nachricht und wiedereinspielen kann versucht werden illegal ins System einzudringen. Die Integrität und ein Verlust der Originalität sind die Folge.
- Weitere Bedrohungen, welche ein Ausfall der Kommunikationsverbindung zur Folge haben kann, ist die Verhinderung oder Unterbrechung einer Kommunikation, also der Verlust der Verfügbarkeit.
- Durch Netzüberlastung kann der Verlust der Verfügbarkeit die Folge sein.
- Ein Ausfall der Kommunikationseinrichtungen kann durch einen Anschlag auf die Hardware vollzogen werden, wodurch es zum Verlust der Verfügbarkeit kommt.
- ...

eingesetzte Technologien

	Schwachstellen	Bedrohungen
Übertragungsart:		
DVB-T max. Übertragungskapazität: 39Mbps	• Keinerlei Sicherheitsmechanismen • Jeder kann mithören. • Der Absender ist für eine eventuelle Verschlüsselung der Daten zuständig	Die Schwachstellen und somit auch die Art der Bedrohung der Kommunikationsübertragungs-technologien sind abhängig von den jeweils verwendeten Protokollen, welche verwendet werden. Sicherlich besteht eine Gefahr in der Überlastung der Hardware, wenn die Übertragungskapazität nicht ausreicht.
GPRS max. Übertragungskapazität: 21,4 kBit/s pro Kanal	• Hochgradig unzuverlässig, was den Datentransport angeht	
Ethernet über Router	• Keinerlei Sicherheitsmechanismen	
Ethernet mit DSL Modem	• Keinerlei Sicherheitsmechanismen	
VPN		

Protokolle:		
UDP	• Unzuverlässig • verbindungslos • Differenzierte Filterung durch Firewall nicht möglich	Verlust, Vervielfachung und Reihenfolgeveränderung von Nachrichten UDP Spoofing, Flooding
TCP		Sequenznummern-Angriff, TCP-Syn-Flooding, Hijacking, Land-Attacke, Out-of-Band, TCP-Sequenznumber-Attack, TCP-Man-in-the-middle, Reset-Attacke

IPV4	• Keine Sicherheitsmechanismen für Nutzdaten • Keine Verschlüsselung • Keine Signierung • Angriffe zum Beispiel über RIP Protokoll • IP Datagramme sind unsicher und leicht fälschbar.	Daten-Spoofing, IP-Spoofing, Denial-of-Service Angriff, Sniffing, Verbindungs-Hijacking, ICMP Angriff, IP-Fragmentierung, Fragmentationsangriff, Tunneln, Soure-Routing Attacke, Ping-of-Death Attacke, Tiny-Fragment Attacke, Overlapping-Fragment Attacke, Ping-Flooding, Smurf, ICMP-Destination-Unreachable, ICMP-Fragmentation-Needed-And, DF-Set, ICMP-Redirect
SSL (https)	• „Das SSL-Protokoll wurde ursprünglich von der Firma Netscape entwickelt. In der Version 2 fanden sich noch kleinere Sicherheitslücken, die in der Folgeversion 3.0 beseitigt wurden.“ [dahe]	Cipher-Suite-Rollback Angriff, Bleichenbacher Angriff, Key-Exchange-Algorithm-Rollback, Version-Rollback Angriff

[OKya] [CEck] [cotec]

6.4.4 Zusammenfassung

In der Bedrohungsmatrix werden die Ergebnisse zusammengefasst und die organisatorischen Mängel, menschliche Fehlhandlungen, Höhere Gewalt, vorsätzliches Handeln und technisches Versagen eingetragen. Je nach Auslöser und Gefährdungsbereiche kann diese Matrix erweitert werden. Da es sich in dieser Analyse um ein Beispiel handelt, ist die Auswahl auf die wichtigsten Aspekte eingeschränkt.

Das SecHazop Verfahren, Bedrohungs- oder Fehlerbäume, das Ishikawa-Daiagramm und das PHA und FHA Verfahren wurden in dieser Analyse nicht angewendet, da beim Beispielsystem zu wenig Systemdetails bekannt sind. Wann diese anzuwenden sind, ist im vorangegangenen Kapitel nachzulesen.

	Programmierer	Administrator	Unternehmens-führung	User	Externe Angreifer	Interne Angreifer	Betriebs-systeme	Software	Sonstiges
Audio Server	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel		Vorsätzliches Handeln	Vorsätzliches Handeln	Technisches Versagen	Technisches Versagen	Technisches Versagen, Höhere Gewalt
Playout Center	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel		Vorsätzliches Handeln	Vorsätzliches Handeln	Technisches Versagen	Technisches Versagen	Technisches Versagen, Höhere Gewalt
Reseller	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel		Vorsätzliches Handeln	Vorsätzliches Handeln	Technisches Versagen	Technisches Versagen	Technisches Versagen, Höhere Gewalt
Settop Box	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt		Organisatorische Mängel, Menschliche Fehlhandlungen, Vorsätzliches Handeln	Vorsätzliches Handeln	Vorsätzliches Handeln	Technisches Versagen	Technisches Versagen	Technisches Versagen, Höhere Gewalt
Kommunika-tionsverbin-dungen	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt		Menschliche Fehlhandlungen	Vorsätzliches Handeln	Vorsätzliches Handeln	Technisches Versagen	Technisches Versagen	Technisches Versagen, Höhere Gewalt
Schnittstellen	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt	Organisatorische Mängel, Menschliche Fehlhandlungen, Höhere Gewalt		Menschliche Fehlhandlungen	Vorsätzliches Handeln	Vorsätzliches Handeln	Technisches Versagen	Technisches Versagen	

Im Anschluss wird mit Hilfe des Black-Box Diagramms darstellt, an welchen Stellen Schwachstellen sind.

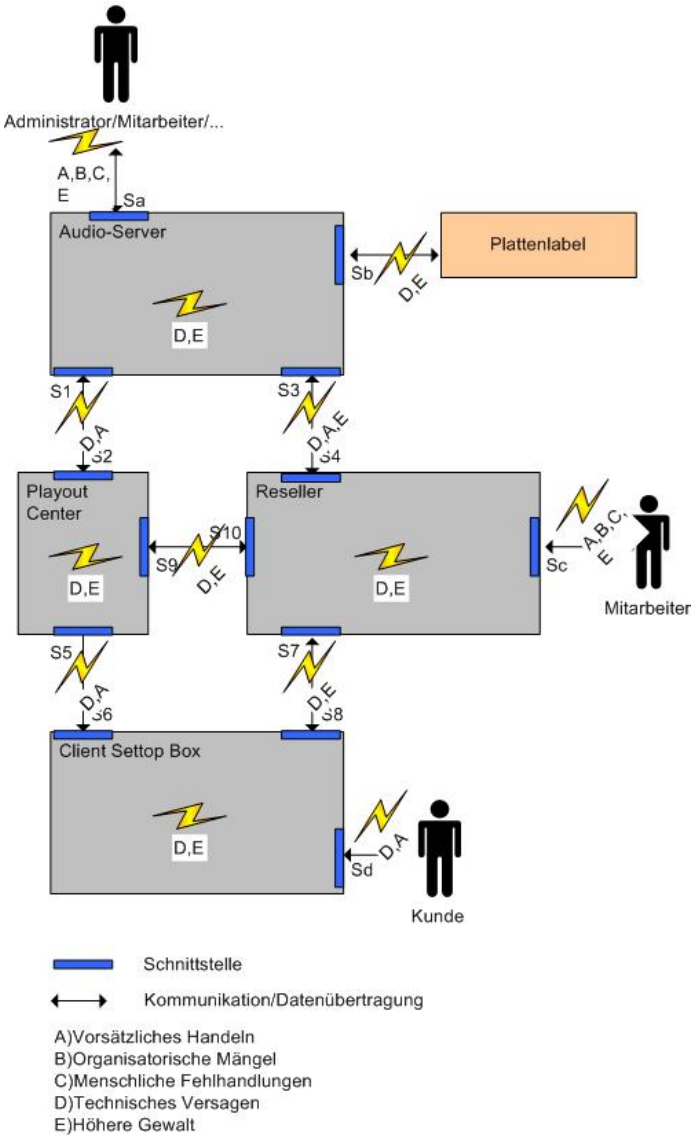


Abbildung 26: Schwachstellen des Systems

6.5 Ermittlung des Soll-Zustandes

Die Ermittlung des Soll-Zustandes befasst sich in diesem Fall hauptsächlich mit dem informations-technischen Bereich und ist eine Zusammenfassung der notwendigen Informationen. Die Bereiche des baulichen, organisatorischen und personellen, wurden nur kurz angerissen. Der Grund hierfür ist, dass zu dem derzeitigen Stand der Entwicklung zu wenig Systemdetails und keinerlei infrastrukturellen Gegebenheiten bekannt sind.

6.5.1 Daten

Da alle Daten mit anderen Daten im Zusammenhang stehen, wurde festgelegt, dass allen Daten ein gleiches Maß an Sicherheit zukommen muss.

Soll-Zustand	Audio-Server
Resellerkundendaten Mediadaten DRM Daten Endkundendaten Schlüssel Schlüsseldatenbank Verbindungsdaten Steuerdaten XML-Daten (Suchanfragen und Ergebnisse) Geschäftsbeziehungen	• Bei Übertragung der Daten muss eine Autorisierung und Authentifikation durch das System stattfinden. Der Zugriff auf das System soll durch Passwortabfrage oder ähnlicher Maßnahmen gesichert werden. • Die Daten sollten zur Übertragung asynchron verschlüsselt werden und die Übertragung sollte synchron verschlüsselt erfolgten, also ein hybrides Verfahren. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb der Systeme nicht verschlüsselt sein, da ihre Gefährdungsklassen nur als niedrig, bzw. mittel ermittelt wurden. • Sollten Fehler auftreten sind sie unbedingt zu behandeln und zu protokollieren. • Eine ausführliche Dokumentation ist unbedingt notwendig • Auf dem Audio-Server sollten die Daten mit hoher Gefährdungsklasse geschützt gelagert werden. Dieser Schutz kann durch eine entsprechend konfigurierte Datenbank oder einem asynchronen Verschlüsselungsalgorithmus erfolgen.

Soll-Zustand	Playout Center
Resellerkundendaten Mediadaten DRM Daten Endkundendaten Schlüssel Schlüsseldatenbank Verbindungsdaten Steuerdaten XML-Daten (Suchanfragen und Ergebnisse) Geschäftsbeziehungen	• Bei Übertragung der Daten muss eine Autorisierung und Authentifikation durch das System stattfinden. Der Zugriff auf das System soll durch Passwortabfrage oder ähnlicher Maßnahmen gesichert werden. • Die Daten sollten zur Übertragung asynchron verschlüsselt werden und die Übertragung sollte synchron verschlüsselt erfolgten, also ein hybrides Verfahren. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb der Systeme nicht verschlüsselt sein, da ihre Gefährdungsklassen nur als niedrig, bzw. mittel ermittelt wurden. • Sollten Fehler auftreten sind sie unbedingt zu behandeln und zu protokollieren. • Eine ausführliche Dokumentation ist unbedingt notwendig • Wenn die Daten beim Playout Center oder dem Reseller durchgeschleust werden sind die asynchron verschlüsselt. • Die synchrone Verschlüsselung sollte durch das jeweilige System erfolgen.

Soll-Zustand	Reseller
Resellerkundendaten Mediadaten DRM Daten Endkundendaten Schlüssel Schlüsseldatenbank Verbindungsdaten Steuerdaten XML-Daten (Suchanfragen und Ergebnisse) Geschäftsbeziehungen	• Bei Übertragung der Daten muss eine Autorisierung und Authentifikation durch das System stattfinden. Der Zugriff auf das System soll durch Passwortabfrage oder ähnlicher Maßnahmen gesichert werden. • Die Daten sollten zur Übertragung asynchron verschlüsselt werden und die Übertragung sollte synchron verschlüsselt erfolgten, also ein hybrides Verfahren. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb der Systeme nicht verschlüsselt sein, da ihre Gefährdungsklassen nur als niedrig, bzw. mittel ermittelt wurden. • Sollten Fehler auftreten sind sie unbedingt zu behandeln und zu protokollieren. • Eine ausführliche Dokumentation ist unbedingt notwendig • Wenn die Daten beim Playout Center oder dem Reseller durchgeschleust werden sind die asynchron verschlüsselt. • Die synchrone Verschlüsselung sollte durch das jeweilige System erfolgen.

Soll-Zustand	Settop Box
Resellerkundendaten Mediadaten DRM Daten Endkundendaten Schlüssel Schlüsseldatenbank Verbindungsdaten Steuerdaten XML-Daten (Suchanfragen und Ergebnisse) Geschäftsbeziehungen	• Bei Übertragung der Daten muss eine Autorisierung und Authentifikation durch das System stattfinden. Der Zugriff auf das System soll durch Passwortabfrage oder ähnlicher Maßnahmen gesichert werden. • Die Daten sollten zur Übertragung asynchron verschlüsselt werden und die Übertragung sollte synchron verschlüsselt erfolgten, also ein hybrides Verfahren. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb der Systeme nicht verschlüsselt sein, da ihre Gefährdungsklassen nur als niedrig, bzw. mittel ermittelt wurden. • Sollten Fehler auftreten sind sie unbedingt zu behandeln und zu protokollieren. • Eine ausführliche Dokumentation ist unbedingt notwendig • Auf der Client Settop Box kommen die Daten hybride verschlüsselt an. Die Archivierung der Daten sollte entweder in einer Datenbank geschehen welche entsprechend geschützt ist oder die Daten sollten asynchron verschlüsselt archiviert werden

[bsigshb]

6.5.2 Schnittstellen

Soll				
	Audio-Server	Playout Center	Reseller	Client Settop Box
Ports	• Durch die Konfiguration des Systems oder durch eine Firewall dürfen nur die minimal nötigen Ports offen sein. Sinnvoll ist es nicht standardmäßige Ports auszuwählen.			
Sonstiges	• Der Zugriff auf das System muss durch eine Zugriffskontrolle gesichert werden. Passwörter müssen den Vorgaben des BSI entsprechen.			

[bsigshb]

6.5.3 Kommunikationsverbindungen

Für die Sicherheit der Netze ist ein Netzkonzept aufzustellen. Die hier genannten Fakten sind nur Ansätze eines solchen Konzeptes. Ein komplettes Konzept muss noch ausgearbeitet werden. Unterstützend kann hierbei das IT-Grundschutzhandbuch eingesetzt werden [bsigshb].

Eine Verschlüsselung der Daten muss bei jeder Datenübertragung geschehen. Diese Verschlüsselung geschieht auf Applikationsebene, so dass die Technologien und Protokolle davon nicht betroffen sind. Bei Kommunikationsverbindungen, bei denen SSL vorsehen ist, sollte trotzdem die Verschlüsselung auf Applikationsebene stattfinden. Dies wurde als sinnvoll erachtet, da somit keine erneute Ver- oder Entschlüsselung im Playout Center oder beim Reseller geschehen muss und somit die Daten ohne Bearbeitung weitergeleitet werden können. Nur bei der VPN Verbindung ist es nicht unbedingt notwendig, eine zusätzliche Verschlüsselung vorzunehmen, da es sich ausschließlich um Steuer- und Verbindungsdaten handelt, welche übertragen werden.

Eingesetzte Technologien:	Schutzmaßnahme
DVB-T	• Übertragung der hybrid verschlüsselten Daten. • Zugriffssteuerung durch die jeweiligen Systeme
GPRS	
Ethernet über Router	
Ethernet mit DSL Modem	
VPN	• Sicherheit durch Tunnel-Technik

Protokolle	
UDP	• Übertragung der hybrid verschlüsselten Daten. • Zugriffssteuerung durch die jeweiligen Systeme
TCP	
IPv4	
SSL (https)	• Nur ab Version 3 einsetzen, da ab dieser Version eine Server Authentifikation eingesetzt wird.

[bsigshb]

6.6 Soll-Ist-Vergleich

Für einen Soll-Ist-Vergleich muss das System soweit entwickelt sein, dass alle Softwarekomponenten und eingesetzten Technologien bekannt sind. In diesem Fall ist ein Soll-Ist-Vergleich nur eingeschränkt möglich, da viele Punkte noch nicht bekannt sind.

Der Soll-Ist-Vergleich steht eng im Zusammenhang mit dem nächsten Kapitel „Realisierung und Schutzmaßnahmen“. Für den Soll-Ist-Vergleich wird die Differenz zwischen Soll und Ist ermittelt und in einer Tabelle dargestellt. So können die fehlenden Maßnahmen ermittelt werden.

6.6.1 Daten

Differenz	Audio-Server
Resellerkundendaten	• Zugriffskontrolle, Autorisierung und Authentifikation • Fehlerprotokollierung • Dokumentation aller Verfahren, Fehler usw. • Auf dem Audio-Server sollten alle Daten mit hoher Gefährdungsklasse geschützt gelagert werden. Dieser Schutz kann durch eine entsprechend konfigurierte Datenbank oder einem asynchronen Verschlüsselungsalgorithmus erfolgen. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb des Systems nicht verschlüsselt sein, nur während der Übertragung
Mediadaten	
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Differenz	Playout Center
Resellerkundendaten	• Zugriffskontrolle, Autorisierung und Authentifikation • Fehlerprotokollierung • Dokumentation aller Verfahren, Fehler usw. • Daten welche durchgeschleust werden sollten asynchron verschlüsselt sein. Die synchrone Verschlüsselung sollte durch das jeweilige System erfolgen. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb des Systems nicht verschlüsselt sein, nur während der Übertragung
Mediadaten	
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Differenz	Reseller
Resellerkundendaten	• Zugriffskontrolle, Autorisierung und Authentifikation • Fehlerprotokollierung • Dokumentation aller Verfahren, Fehler usw. • Daten welche durchgeschleust werden sollten asynchron verschlüsselt sein. Die synchrone Verschlüsselung sollte durch das jeweilige System erfolgen. • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb des Systems nicht verschlüsselt sein, nur während der Übertragung
Mediadaten	
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

Differenz	Settop Box
Resellerkundendaten	• Zugriffskontrolle, Autorisierung und Authentifikation • Fehlerprotokollierung • Dokumentation aller Verfahren, Fehler usw. • ankommende Daten sind hybrid verschlüsselt • Gespeicherte Daten asynchron verschlüsseln oder anderweitig zum Beispiel durch Datenbankfunktion sichern • Steuerdaten, XML-Daten und Verbindungsdaten müssen innerhalb des Systems nicht verschlüsselt sein, nur während der Übertragung
Mediadaten	
DRM Daten	
Endkundendaten	
Schlüssel	
Schlüsseldatenbank	
Verbindungsdaten	
Steuerdaten	
XML-Daten (Suchanfragen und Ergebnisse)	
Geschäftsbeziehungen	

6.6.2 Schnittstellen

Differenz	
Ports	• Durch die Konfiguration des Systems oder durch eine Firewall dürfen nur die minimal nötigen Ports offen sein. Sinnvoll ist es nicht standardmäßige Ports auszuwählen.
Sonstiges	• Der Zugriff auf das System muss durch eine Zugriffskontrolle gesichert werden. Passwörter müssen den Vorgaben des BSI entsprechen.

6.6.3 Kommunikationsverbindungen

Eingesetzte Technologien:	Schutzmaßnahme
DVB-T	• Übertragung der hybrid verschlüsselten Daten. • Zugriffssteuerung durch die jeweiligen Systeme
GPRS	
Ethernet über Router	
Ethernet mit DSL Modem	
VPN	• Sicherheit durch Tunnel-Technik

Protokolle	
UDP	• Übertragung der hybrid verschlüsselten Daten. • Zugriffssteuerung durch die jeweiligen Systeme
TCP	
IPv4	
SSL (https)	• Nur ab Version 3 einsetzen, da ab dieser Version eine Server Authentifikation eingesetzt wird.[ESte]

6.6.4 Zusammenfassung

Viele der nötigen Maßnahmen sind im Beispielsystem noch gar nicht oder nur unzureichend bedacht worden. Zugriffsrechte wurden bislang nur auf dem Audio-Server vorgesehen, wobei es eine der wichtigsten Schutzmaßnahmen ist.

Die Entwicklung eines Kryptokonzepts existiert nur im Ansatz, wie genau die Verschlüsselung geschehen soll ist noch nicht bekannt, dementsprechend wurde bislang nur ansatzweise über eine Überprüfung und den Abruf von personenbezogenen Daten nachgedacht.

Regelung für Passwörter oder ein Schlüsselmanagement, welche für die Zugriffsrechte und das Kryptokonzept unbedingt notwendig sind, wurden bislang noch gar nicht erwähnt.

Ebenso verhält es sich mit einer sinnvollen Fehlerbehandlung und Protokollierung.

Ein Netzkonzept existiert nur in eingeschränktem Rahmen. Es wurden Vorschläge unterbreitet, diese Überlegungen scheinen aber nicht ausgereift zu sein. Daher ist die Entwicklung eines umfassenden Netzkonzeptes unbedingt notwendig.

Eine Protokollierung unter anderem der Kommunikation und vor allem der Fehlerfälle wurde nur im Bereich des Resellers bedacht.

Die Dokumentation des bislang erreichten Entwicklungsstandes ist nur unzureichend, obwohl sie eines der wichtigsten Punkte bei der Entwicklung darstellt.

Welche Aspekte im weiteren Verlauf der Entwicklung noch berücksichtigt werden müssen, wird in den folgenden Unterkapiteln genauer erläutert.

6.7 Empfehlung von Schutzmaßnahmen und für das weitere Vorgehen

Nicht nur die Entwicklung eines sicheren Systems ist entscheidend für den Erfolg eines Unternehmens, auch der sichere Betrieb des gesamten Unternehmens ist von großer Bedeutung, so das IT-Grundschutzhandbuch des BSI [bsigshb]. Um diesen aufrecht zu halten ist ein IT-Sicherheitsmanagement unbedingt notwendig. Die wesentlichen Schritte für einen IT-Sicherheitsprozess sind die folgenden:

- Entwicklung einer Sicherheitspolitik
- Auswahl und Etablierung einer geeigneten Organisationsstruktur für das IT-Sicherheitsmanagement
- Erstellung eines IT-Sicherheitskonzepts
- Realisierung der IT-Sicherheitsmaßnahmen
- Schulung und Sensibilisierung
- Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb.

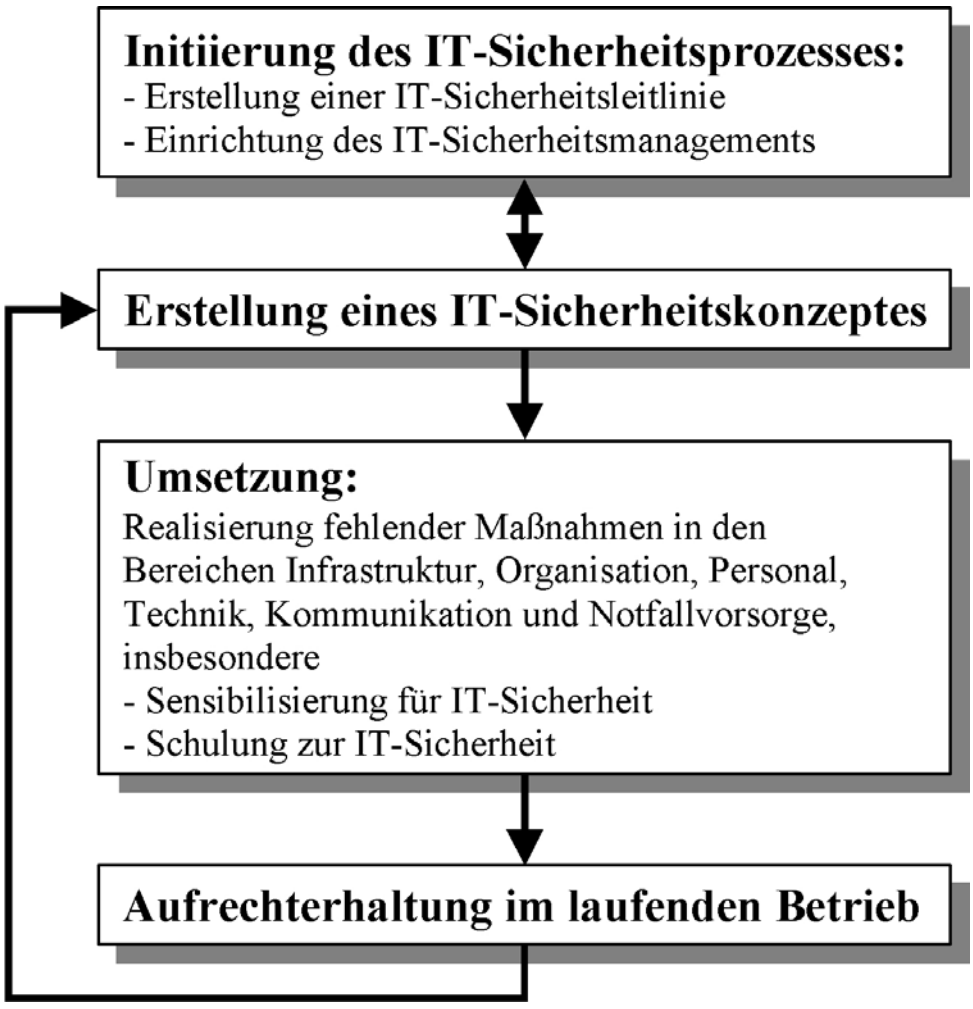


Abbildung 27: Ablauf eines IT-Sicherheitsmanagements [bsigshb]

Nach Abschluss der Entwicklungsphase sollte daher unbedingt auch ein IT-Sicherheitsprozess erstellt werden, um auch die Umgebung des Systems sicher zu gestalten.

Für die Umsetzung der IT-Sicherheitsmaßnahmen ist es notwendig alle Mitarbeiter eines Unternehmens einzubinden. Die Verantwortlichen für Informationen, Anwendungen und IT-Komponenten sollten daher festgelegt werden und allen Mitarbeitern bekannt sein.

Um die Sicherheit zu garantieren sollte auf Funktionstrennung geachtet werden. So sollten zum Beispiel Aufgaben der Rechteverwaltung und Revision, Netzadministration und Revision, Programmierung und Test, der selbst entwickelten Software, Datenerfassung und Zahlungsanordnungsbefugnis und Revision und Zahlungsanordnungsbefugnis in unterschiedlichen Händen sein, um Sicherheitsvorkommnisse oder Sicherheitslücken von vornherein auszuschließen oder zumindest einzudämmen.

Wichtige Aspekte für die Sicherheit eines Unternehmens sind unter anderem auch Vertretungsregelungen, Schulungsmaßnahmen und geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern [bsigshb].

6.7.1 Kryptokonzept

Fast jedes Unternehmen ist von seiner informationstechnischen Infrastruktur abhängig. Daher sind Sicherheitskonzepte erforderlich, die über die bloße Verschlüsselung hinausgehen, man nennt dieses Kryptokonzept. Das genaue Vorgehen wird im IT-Grundschutzhandbuch [bsigshb] erläutert. Auf die Grundlagen, welche hierfür erforderlich sind, wird in dem Buch „Kryptographie und Public-Key-Infrastrukturen im Internet“ von Klaus Schmeh
[KSch], sowie im Buch „IT-Sicherheit“ von Claudia Eckert [CEck] genaustens eingegangen.

Die Verschlüsselung der Daten, welche übertragen werden, kann auf mehreren Ebenen geschehen:

- Auf Applikationsebene: Die kommunizierenden Anwendungen müssen dabei jeweils über die entsprechenden Ver- und Entschlüsselungsmechanismen verfügen.
- Auf Betriebssystemebene: Die Verschlüsselung wird vom lokalen Betriebssystem durchgeführt. Jede Kommunikation über das Netz wird automatisch oder auf Anforderung verschlüsselt.
- Auf Netzkoppelelementebene: Die Verschlüsselung findet zwischen den Routern.

Für das Beispielsystem ist eine Verschlüsselung auf Applikationsebene vorgesehen, da man unabhängig von den Übertragungstechnologien und Protokollen die Daten sichern kann.

Bei der Auswahl von kryptografischen Algorithmen ist zunächst zu klären, welche Arten von kryptografischen Verfahren benötigt werden. Hierfür stehen symmetrische, asymmetrische oder hybride Verfahren zur Verfügung, welche mit einem geeigneten Algorithmus mit entsprechender Mechanismenstärke, also Schlüssellänge, arbeiten. Zu diskutieren sind folgende Punkte: Das Verschlüsselungsverfahren, die Authentisierungsverfahren und schließlich die Hashverfahren. Wo welche Daten verschlüsselt werden müssen und mit welchen Verfahren genau, muss noch genauer spezifiziert werden. Die Aufstellung eines Kryptokonzepts ist also unumgänglich!
Die Datenübertragung sollte auf jeden Fall hybrid verschlüsselt werden, innerhalb der Systeme asymmetrisch. Das asymmetrische Verfahren sichert mit einem geheimen Schlüssel die Kommunikation ab. Das symmetrische Verfahren die Daten. Sind Daten sowohl symmetrisch als auch asymmetrisch verschlüsselt spricht man von hybrider Verschlüsselung.

Einfache Verschlüsselungsalgorithmen oder polyalphabetische kommen für das Beispielsystem nicht in Frage. Für den symmetrischen Bereich würde ich daher mindestens den Triple DES oder gar den AES vorsehen. Wichtig hierbei ist, dass die Schlüssellänge mindestens 128 Bit betragen sollte. Für das asymmetrische Verfahren kommen beispielsweise RSA mit einer Schlüssellänge von mindestens 1024 Bit oder ECC (Elliptic Curve Cryptography) mit mindestens 135 Bit in Frage.
Je größer die verwendete Schlüssellänge bei einem kryptografischen Verfahren ist, desto länger dauert es, ihn z. B. durch eine Bruce-Force Attacke zu berechnen.

Die Wahrscheinlichkeit, dass Implementierungsfehler auftreten, sollte durch ausführliche Qualitätssicherung und durch eine regelmäßige Überprüfung des Systems reduziert werden.

Bei Langzeitangriffen, zum Beispiel nach einem Diebstahl des Systems, muss die Vertraulichkeit der gespeicherten Daten gewährleisten bleiben. Eine Möglichkeit wäre, dies durch einen Boot-Schutz und Festplattenverschlüsselung zu realisieren.

Alle Kryptografische Verfahren müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen, da die verwendeten Algorithmen jederzeit durch neue technische Entwicklungen zu schwach werden könnten. Gegebenenfalls müssen sie durch neue aktuelle und sicherere ersetzt werden.

Abbildung 28: Inhalte eines Kryptokonzepts [bsigshb]

6.7.2 Zugriffsrechte

Der Zugriff auf alle IT-Systeme oder Dienste muss durch Identifikation und Authentifikation des zugreifenden Benutzers oder IT-Systems abgesichert werden. Zugriffsrechte sind Lesen, Schreiben, Ändern, Ausführen und Bestellen von IT-Anwendungen, Teilanwendungen oder Daten. Je nach Funktion der Person sind die Zugriffsrechte mehr oder weniger zu beschränken. Wie genau diese Zugriffsrechte aussehen, muss innerhalb des Kryptokonzepts genau spezifiziert, festgelegt und umgesetzt werden. Es sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist, so das BSI [bsigshb] ("Need-to-know-Prinzip"). Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Beim Zugriff aus externen Netzen, wie es bei dem Beispielsystem der Fall ist, sollten starke Authentisierungsverfahren eingesetzt werden. Beim Anmeldevorgang sollten keine Informationen über das IT-System oder den Fortschritt der Anmeldeprozedur angezeigt werden, bis dieser erfolgreich abgeschlossen ist. Die Authentifikationsdaten dürfen erst dann überprüft werden, wenn sie vollständig eingegeben wurden.

Es gibt mehrere Möglichkeiten eine Authentifizierung durchzuführen. Dies könnte mit Hilfe

- einer Passworteingabe
- einer Chipkarte
- biometrische Verfahren, also Fingerabdruck, Irisscan usw.
- eines Kerberos-Authentifikationssystem

geschehen.

6.7.3 Passwörter

Das BSI [bsigshb] empfiehlt für Passwörter folgendes:

- Ein Passwort darf nicht leicht zu erraten sein, also kein Trivialpasswort. Mindestens ein Zeichen sollte verwendet werden, das kein Buchstabe ist. Wenn für das Passwort nur alphanumerische Zeichen gewählt werden, sollte es mindestens 8 Zeichen lang sein und wenn für das Passwort nur Ziffern zur Verfügung stehen, sollte es mindestens 6 Zeichen lang sein. Sinnvoll bei diesem System ist es Passwörter zu verwenden, welche Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen enthalten. Voreingestellte Passwörter müssen unbedingt durch individuelle Passwörter ersetzt werden.

- Für die Erstanmeldung sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Ein Passwort muss außerdem regelmäßig gewechselt werden, z. B. immer nach 90 Tagen, dann wenn es der Benutzer möchte und auf jeden Fall, wenn es unautorisierten Personen bekannt geworden ist. Alte Passwörter sollten nach einem Passwortwechsel nicht erneut benutzt werden dürfen, dies könnte durch eine Passworthistorie ausgeschlossen werden.

- Die Übertragung von Passwörtern sollte immer in verschlüsselter Form passieren.

- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden, sie müssen geheim gehalten werden und sollten nur dem Benutzer persönlich bekannt sein. Somit dürfen sie bei der Eingabe auch nicht auf dem Bildschirm angezeigt werden.

- Nach wenigen Fehlversuchen ist das Authentisierungssystem für eine bestimmte Zeitspanne oder dauerhaft zu sperren.

[bsigshb]

6.7.4 Schlüsselmanagement

Das Schlüsselmanagement umfasst im IT-Grundschutzhandbuch [bsigshb] mehrere Punkte. Die Schlüsselerzeugung, die Schlüsseltrennung, die Schlüsselverteilung und der Austausch, die Schlüsselinstallation und -speicherung, die Schlüsselarchivierung, Zugriffs- und Vertreterregelungen, der Schlüsselwechsel und schließlich die Schlüsselvernichtung. Ein solches Schlüsselmanagement ist innerhalb des Kryptokonzepts vorgesehen und für die Sicherheit des Systems von großer Bedeutung. Kryptografische Sicherheitsmechanismen setzen Schlüssel voraus welche vertraulich, integer und authentisch erzeugt wurden, des Weiteren betrifft dies auch die Verteilung und Installation.

Moderne Systeme bedienen sich heute asymmetrischer kryptografischer Verfahren zur Schlüsselverteilung und zum Schlüsselaustausch. Zum Nachweis der Authentizität der öffentlichen Schlüssel kann eine vertrauenswürdige Zertifizierungsstelle eingerichtet werden. Die Kommunikationsteilnehmer müssen sich gegenüber der Zertifizierungsstelle ausweisen und dort ihren öffentlichen Schlüssel durch eine digitale Signatur der Zertifizierungsstelle beglaubigen lassen. Das so erzeugte digitale Zertifikat sollte mindestens den öffentlichen Schlüssel und ein Identifikationsmerkmal des Kommunikationsteilnehmers, die Gültigkeitsdauer des Zertifikats und die digitale Signatur der Zertifizierungsstelle enthalten. Mit Kenntnis des öffentlichen Signaturschlüssels der Zertifizierungsstelle ist jeder Kommunikationsteilnehmer in der Lage, die Authentizität des öffentlichen Schlüssels des Kommunikationspartners zu verifizieren.

Grundlagen zum Schlüsselmanagement sind auch in dem Buch „IT-Sicherheit“ vom Claudia Eckert [CEck], sowie dem Buch „IT-Sicherheit“ von Rolf Opplinger [ROpp] nachzulesen. Mit öffentlichen Schlüsselverfahren und Sicherheitsinfrastrukuren befasst sich außerdem Volker Hammer [VHam] in seinem Buch „Die 2. Dimension der IT-Sicherheit“.

6.7.5 Netzkonzept

Um die Verfügbarkeit, Vertraulichkeit und Integrität eines Netzes zu erhalten muss ein Netzkonzept erarbeitet werden. Drei wesentliche Schritte sind hierfür notwendig.

- Konzeption der Netztopographie und Netztopologie
- Konzeption der Netzprotokolle
- Konzeption der Kommunikationsübergänge im LAN und WAN

Nachdem dieses Netzkonzept erarbeitet wurde, können die Maßnahmen zur Erstellung eines Netzmanagementkonzeptes durchgeführt werden. Für die Umsetzung sind wiederum drei Schritte notwendig.

- Entwicklung eines Netz-Realisierungsplans
- Entwicklung eines Netzmanagement-Konzeptes
- Geeignete Auswahl eines Netzmanagement-Protokolls

Das genaue Vorgehen zur Erstellung eines Netzkonzeptes und eines Netzmanagement-Konzeptes wird im IT-Grundschutzhandbuch [bsigshb] erläutert.

Die vorgesehenen Übertragungstechnologien sind DVB-T, GPRS, Ethernet und VPN und als Protokolle UDP, TCI, Ipv4 und SSL. Außer VPN sind alle Übertragungsarten ungeschützt. Da aber eine hybride Verschlüsselung vorgesehen ist, sind die Daten trotzdem abgesichert.

Bei den Protokollen muss die Verwendung von UDP überprüft werden. Es ist zu überdenken, ob es sinnvoll ist das UDP-Protokoll gegen das TCP-Protokoll einzutauschen. UDP ist unzuverlässig und verbindungslos. Eine Filterung durch Firewall ist nicht möglich. Ob dieser Tausch praktikabel ist, ist aber noch zu überprüfen.

Bei SSL ist darauf zu achten, dass es ab der Version 3 eingesetzt wird, da ab dieser Version eine Server-Authentifikation eingesetzt wird. Es können verschiedene kryptografische Algorithmen mit verschiedenen Schlüssellängen eingesetzt werden, es ist eine Schlüssellänge zu wählen welche dem Sicherheitsstandard angepasst ist. Genaueres steht hierzu im Kapitel Schlüsselmanagement.

Nach Möglichkeit sollte IPV6 statt IPV4 eingesetzt werden. Die Vorteile dieses neuen Internet-Protokolls sind die größere Sicherheit, eine bessere Unterstützung von Echtzeitanwendungen sowie eine höhere Routerleistung. IPV6 soll bis 2005 nach und nach eingeführt werden. Die Abwärtskompatibilität mit Software und Netzwerkkomponenten, die den IPv4-Standard verwenden, soll laut dem IETF gewährleistet bleiben.

Unterstützend können bei der Erstellung des Netzkonzeptes die Bücher „Der IT-Sicherheitsleitfaden“ von Norbert Pohlmann [NPoh], „Kryptographie“ von Klaus Schmeh [KSch] und „IT-Sicherheit“ von Claudia Eckert [CEck] sein.

6.7.6 Übertragung und Abruf personenbezogener Daten

Daten dürfen nur durch Autorisierte abgerufen, übertragen oder verarbeitet werden. Laut dem IT-Grundschutzhandbuch [bsigshb] kann dies durch folgende Maßnahmen erfolgen:

- Jeder Benutzer muss sich gegenüber den IT-Systemen, von denen die personenbezogenen Daten abgerufen werden, eindeutig identifizieren und authentisieren.
- Die im Kapitel „Passwörter“ aufgeführten Maßnahmen sind bei der Übertragung und dem Abruf personenbezogener Daten von größter Bedeutung.
- Der Abruf von personenbezogenen Daten und die Gründe hierfür müssen unbedingt protokolliert werden, außerdem über welchen Anschluss und welche Endgeräte die Übertragung stattfindet.
- Alle Mitarbeiter sind zum Datenschutz zu verpflichten. Eine Weitergabe von Daten an Dritte ist vertraglich zu untersagen.

6.7.7 Schnittstellen

Die einzelnen Komponenten müssen klar definiert werden, so dass es nicht zu Missverständnissen oder Sicherheitslücken kommt. Durch eine entsprechende Konfiguration des Systems oder durch eine Firewall sollten nur die notwendigen Ports offen sein. Eventuell sind nicht standardmäßige Ports sinnvoll. Alle Änderungen an Schnittstellendefinitionen müssen dokumentiert und in Bezug auf die Auswirkungen auf die Sicherheit des Systems geprüft werden.

Im Maßnahmenkatalog des IT-Grundschutzhandbuches [bsigshb], „M 4.85 Geeignetes Schnittstellendesign bei Kryptomodulen“ ist genau erläutert, wie Schnittstellen beschaffen sein müssen, wenn sie in einem Kryptomodul integriert sind.

6.7.8 Fehlerbehandlung

Alle Fehler, die IT-Systeme oder Kommunikationsverbindungen betreffen, müssen gemeldet und protokolliert werden. Die Protokolle über gemeldete Fehler sollten, laut IT-Grundschutzhandbuch [bsigshb], folgende Angaben enthalten:

- Bezeichnung und Versionsnummer der betroffenen IT-Systeme und Software
- den Zeitpunkt der Meldung
- eine Beschreibung, ob bzw. inwiefern die Nutzung der betroffenen IT-Systeme eingeschränkt ist
- den Namen des für die Behebung Verantwortlichen sowie
- den Zeitpunkt der Fehlerbehebung

6.7.9 Sicherheitslücken, Updates und Patches

Wenn es weder einen zuverlässigen Patch gibt noch ein Ersatzteil beschafft werden kann, ist es sinnvoll den Fehler erst einmal im System zu lassen, so das IT-Grundschutzhandbuch [bsigshb]. Dieses ist im Protokoll zu vermerkt, ebenso inwieweit es dadurch zu Funktionseinschränkungen kommt. Die Protokolle sollten regelmäßig daraufhin überprüft werden, ob sie aktuell sind und ob alle gemeldeten Fehler behoben wurden.

Bevor eine Software, ein Update, ein Patch oder eine Hardware eingesetzt wird muss sie auf Fehler und Sicherheitslücken überprüft werden, um unerwünschte Nebeneffekte auszuschließen.
Was genau alles hierbei zu beachten ist, ist im IT-Grundschutzhandbuch nachzulesen.

Größere Korrekturmaßnahmen müssen durch den Verantwortlichen zunächst auf vom Wirknetz getrennten Systemen getestet werden, da diese unerwünschte Nebeneffekte haben können. Nach der Fehlerbeseitigung müssen die geänderten IT-Systeme bzw. Komponenten erneut abgenommen und freigegeben werden.

6.7.10 Virenschutz

Ein Computer-Virenschutzkonzept ist zu entwickeln. Wie ein solches Computer-Virenschutzkonzeptes konzipiert und umgesetzt wird, ist im IT-Grundschutzhandbuch [bsigshb] nachzulesen. Für die Auswahl eines geeigneten Viren-Suchprogramms sollte die ITSEC zur Hilfe gezogen werden, in ihr ist eine Funktionalitätsklasse für Anti-Virus-Produkte (F-AVIR) enthalten, welche hilfreich sein kann.

6.7.11 Firewall

Für die Sicherheit des zu schützenden Netzes sollte eine geeignete Firewall eingesetzt werden. Damit diese Firewall einen effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein. Die Firewall muss

- auf einer umfassenden Sicherheitspolitik aufsetzen,
- im IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Wie genau ein solches Firewallkonzept auszusehen hat, sollte man an der entsprechenden Stelle des IT-Grundschutzhandbuches [bsigshb] nachlesen.

6.7.12 Protokollierung

Unter Protokollierung ist im datenschutzrechtlichen Sinn, laut dem BSI [bsigshb], die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

Folgende Vorkommnisse sind von gesteigertem Interesse und sollten unbedingt protokolliert werden:

- falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze
- Versuche von unberechtigten Zugriffen
- Stromausfall
- Daten zur Netzauslastung und -überlastung

Das Thema Protokollierung wird im IT-Grundschutzhandbuch ausführlich für unterschiedliche Systeme erläutert. Es sollte daher, wenn die Infrastruktur des Systems bekannt ist, noch einmal ein Blick in das IT-Grundschutzhandbuch geworfen und die Protokollierung überprüft werden. Die Ausarbeitung eines Konzeptes für die Protokollierung ist unbedingt notwendig. Hilfreich kann es hierbei sein, sich mit dem Buch „Datensicherheit und Datenschutz“ von Gerd W. Wähner [GWäh] zu befassen. In diesem Buch wird ausführlich auf Protokollierung eingegangen.

6.7.13 Archivierung

Die Archivierung ist ein Teil eines Dokumentenmanagement-Prozesses. Neben der Erzeugung, Bearbeitung und Verwaltung der Dokumente und Mediadaten spielt die Archivierung eine große Bedeutung. Die Dokumente und Mediadaten müssen bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sein und die Vertraulichkeit und Integrität müssen gewahrt bleibt. Die Mediadaten sollten aber auf jeden Fall auch darüber hinaus erhalten bleiben.

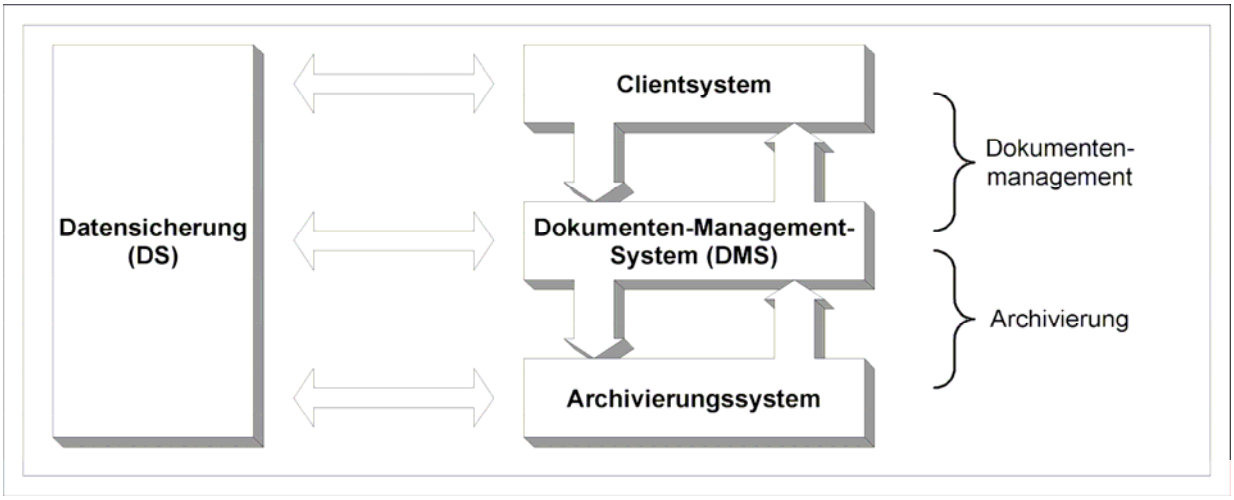


Abbildung 29: Dokumentenmanagement- und Archivierungsprozess [bsigshb]

6.7.14 Dokumentation

Das System muss in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden, um einen ordnungsgemäßen IT-Betrieb gewährleisten zu können. Alle wichtigen Entscheidungen, diverse Rechtevergaben, zugelassene Benutzer usw. müssen ausführlich dokumentiert werden. Dies ist notwendig, da die Planung, Steuerung, Kontrolle und Notfallvorsorge auf einer aktuellen Dokumentation des vorhandenen IT-Systems basieren. Aus diesem Grund müssen alle Änderungen am System dokumentiert werden.

Der Ablauf des IT-Sicherheitsprozesses und alle Arbeitsergebnisse sollten während aller Entwicklungsphasen dokumentiert werden. Die Dokumentation hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist dabei, dass nicht nur die jeweils aktuelle Version der betreffenden Unterlagen griffbereit gehalten wird, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird.

Die Dokumentation des IT-Sicherheitsprozesses sollte sich mindestens auf die folgenden Dokumente erstrecken:

- IT-Sicherheitsleitlinie
- IT-Systemübersichten
- IT-Sicherheitskonzepte
- Umsetzungspläne für IT-Sicherheitsmaßnahmen
- Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz
- Dokumentationen von Überprüfungen, Protokollen usw.
- Sitzungsprotokolle und Beschlüsse des IT-Sicherheitsmanagementteams

- Managementreports zur IT-Sicherheit
- IT-Sicherheits-Schulungspläne und
- Meldungen über sicherheitsrelevante Vorfälle

7 Zusammenfassung und Ausblick

7.1 Zusammenfassung

Ziel der Arbeit war es, eine Methodik zur Sicherheitsanalyse von Datenkommunikationssystemen zu entwickeln. Oberste Priorität hatte hierbei die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten.

Als Einführung in die Thematik einer Sicherheitsanalyse wurde ein kurzer Einblick in Standards und Normen, sowie in Methoden der Sicherheits- und Bedrohungsanalyse gewählt. Die Entwicklung der Methode zur Sicherheitsanalyse von Datenkommunikationssystemen basierte auf den Kenntnissen, welche während dieser Einführung gewonnen wurden. Die Schritte der Sicherheitsanalyse sind die folgenden:

- Anforderungsanalyse
- Vereinfachung des Systems
- Systemanalyse
- Schwachstellen- und Bedrohungsanalyse
- Ermittlung des Soll-Zustandes
- Soll-Ist Vergleich
- Realisierung und Schutzmaßnahmen

Um die entwickelte Methodik nachvollziehbar und anschaulich zu machen, wurde ein praxisnahes Beispiel gewählt. Mit Hilfe dieses wurde die Analyse anhand der entwickelten Methodik durchgeführt.
Folgende Ergebnisse wurden heraus gearbeitet:

- Die Wirksamkeit des Sicherheitskonzeptes ist immer abhängig von der Vollständigkeit.
- Die Durchsetzung und Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus kann nur durch ein geplantes und organisiertes Vorgehen aller Beteiligten gewährleistet werden.
- Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von IT-Sicherheitsmaßnahmen ist ein durchdachter und gesteuerter IT-Sicherheitsprozess. Zu diesem IT-Sicherheitsprozess gehören Maßnahmen in den Bereichen Infrastruktur, Organisation, Personal, Technik, Kommunikation und Notfallvorsorge. Nur wenn diese zusammen arbeiten und keine Sicherheitslücken auftreten, kann ein sicherer Betrieb gewährleistet werden.

- Die Aktualisierung der Soft- und Hardwarekomponenten bei Auftreten von neuen Sicherheitslücken oder Erkenntnissen spielt für die Sicherheit des Systems eine große Rolle. Bei der Behebung dieser ist darauf zu achten, dass es erst an einem Probesystem getestet wird um Nebeneffekten im System auszuschließen.
- Eine Kontrolle des bestehenden Systems, durch Protokollierung der Abläufe, stellt bei der Fehlerbehebung und Nachvollziehung dieser einen wichtigen Aspekt dar.

Anwendung findet diese Methode für Sicherheitsanalyse bei Systemen, welche neu entwickelt werden, aber auch bei bestehenden Systemen. Empfehlenswert ist es diese Analyse während der Entwicklungsphase durchzuführen, da somit Sicherheitslücken von vornherein ausgeschlossen werden können. Wird die Analyse erst nach Abschluss der Entwicklung vorgenommen, kann es schwieriger sein die gewonnenen Erkenntnisse im System umzusetzen und zu integrieren, ohne dass es zu unerwünschten Nebeneffekten kommt.

7.2 Ausblick

Das Ziel heißt: „Kein Papier mehr, keine Kabel unter den Schreibtischen. Drucker, Faxgerät: wozu? Korrespondiert wird elektronisch und drahtlos. Lediglich ein schlanker Monitor mit Tastatur wird auf unserem Schreibtisch stehen. So sehen Experten aus der Informations- und Telekommunikationsbranche die nahe Zukunft der digitalen Prozesse.“, so die Initiative für mehr IT-Sicherheit in NRW. Die Abhängigkeit von den IT-Infrastrukturen wächst. Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen - das wirtschaftliche und gesellschaftliche Leben ist zunehmend digitalisiert. Daher zählt heute die Sicherheit von IT-Infrastrukturen zu den elementaren Herausforderungen für Unternehmen jeder Größe. Es müssen die betriebsinternen Datenbestände oder die betriebsexterne Kommunikation gegen Datenverlust oder Datenmissbrauch geschützt, die Stabilität der Systeme gesichert werden. Die Zukunft, also die Existenz und der wirtschaftliche Erfolg vieler Unternehmen, hängt daher unter anderem von drei Faktoren ab: Den IT-Sicherheitsstrukturen, von internationalen gesetzlichen Regelungen, sowie von spezialisierten Mitarbeitern, die diese umsetzen.

Begriffserklärung

BSI

Das BSI wurde 1991 gegründet. Es war bei der Entwicklung der ITSEC und der CC beteiligt. [OKya]

Common Criteria

"Common Criteria for Information Technology Security Evaluation" bzw. "Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik". [demo]

DRM-Daten

Digital-Rights-Management

ISO (International Standardization Organisation)

Wurde 1946 als Untereinrichtung der UNESCO gegründet und ist die Dachorganisation der nationalen Normungsgremien. Sie ist für die globale Normung in vielen Gebieten zuständig. In Deutschland wird sie durch die DIN vertreten. [ESte]

GPRS (General Packet Radio Service)

Weiterentwicklung von GSM mit einer maximalen Datenrate bis zu 160kbit/s. [ESte]

GSM (Global System für Mobile Communications)

GSM ist das derzeit aktuelle, weit verbreitete Mobilfunksystem. [ESte]

SSL (Secure Sockets Layer)

SSL ist ein Schichtenmodell zwischen der Anwendungsschicht und der Transportschicht eingefügt. Für Anwendungen wie http, FTP, SMTP ... verhält sich SSL wie TCP/IP. [Este]

Anhang

Auf der beiliegenden CD befinden sich die im Literaturverzeichnis angegeben Internet-Quellen.

Literaturverzeichnis

[CEck] IT-Sicherheit
Dr. habil. Claudia Eckert
Oldenburg Wirtschaftsverlag GmbH, 2001
ISBN 3-486-25298-4

[ESte] Taschenbuch Rechnernetze und Internet
Prof. Dipl. Ing. Erich Stein
2. Auflage, 2004, Fachbuchverlag Leipzig
ISBN 3-446-22573-0

[GG] Grundgesetz für die Bundesrepublik Deutschland
Herausgeber: Deutscher Bundestag – Verwaltung –
Referat Öffentlichkeitsarbeit, Bonn 1993
Druckhaus Coburg

[GWäh] Datensicherheit und Datenschutz
Dr. sc. Gerd W. Wähner
VDI Verlag GmbH, 1993
ISBN 3-18-401297-2

[KSch] Kryptographie und Public Key Infrastrukturen im Internet
Klaus Schmeh
Dpunkt Verlag GmbH
2. Auflage 2001
ISBN 3-93258-90-8

[NPoh] Der IT-Sicherheitsleitfaden
Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards in Unternehmen
Prof. Dr. Norbert Pohlmann, Hartmut F. Blumberg
1. Auflage 2004-08-31 mitp-Verlag/Bonn
ISBN 3-8266-0940-9

[OKya] Sicherheit im Internet
Othmar Kyas
2. Auflage – Bonn: Internat. Thomson Publ., 1998
ISBN 3-8266-4024-1

[ROpp] IT-Sicherheit – Grundlagen und Umsetzung in der Praxis
Rolf Opplinger
Vieweg Verlag, 1997
ISBN 3-528-05566-9

[VHam] Die 2. Dimension der IT-Sicherheit
Volker Hammer
Friedr. Viewg & Sohn Verlagsgesellschaft mbH, 1999
ISBN 3-528-05703-3

[beko] Sicherheit braucht Methode
http://www.bekonet.at/downloads/security.pdf
Bekonet, 16.09.2004

[bfd] Bundesdatenschutzgesetz
http://www.bfd.bund.de/information/pdf/info_1.pdf
Bundesbeauftragte für den Datenschutz
Druckerei Moeker Merkur GmbH, 15.11.2004

[bhit] Wieviel IT-Sicherheit braucht ihr Unternehmen?
http://www.bhit.ch/bilder/IT_Sicherheit/it_sicherheit_info.pdf
Basler & Hofmann, 24.08.2004

[bsicc] IT-Sicherheit auf Basis der Common Criteria
http://www.bsi.de/cc/cc_leitf.pdf
Bundesamt für Sicherheit in der Informationstechnik, 16.09.2004

[bsigshb] IT-Grundschutzhandbuch
http://www.bsi.de/gshb/deutsch/download/GSHB2003.pdf
Bundesamt für Sicherheit in der Informationstechnik, 16.09.2004

[bsiiso] Studie zu ISO-Normungsaktivitäten ISO/BPM
Anforderungen an Information Security Management Systeme
http://www.bsi.de/literat/studien/gshb/ISO-BPM-ISMS_040305.pdf
Bundesamt für Sicherheit in der Informationstechnik, 16.09.2004

[bund] Bundesdatenschutzgesetz
http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf
Bundesministerium des Inneren, 16.11.04

[cotec] Diplomarbeit, Klaus Bauer: Konzeption und Realisierung eines Firewallsystems zur Internet-Intranet Kopplung
http://www.computec.ch/dokumente/allgemein/
konzeption_und_realisierung/node1.html; DiplomarbeitKlausBauer.zip
Fachhochschule München, Klaus Bauer, 22.11.2004

[comp] Historische Entwicklung der Normen
http://www.computerwoche.de; SHOWpdf.pdf
IDG BUSINESS VERLAG GMBH, 26.10.2004

[dahe] Einunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten
Professor Dr. Friedrich von Zezschwitz
http://www.datenschutz.hessen.de/Tb31/K12P03.htm; dahe.zip
Professor Dr. Friedrich von Zezschwitz, 22.11.2004

[dakr] Diplomarbeit, Tobias Krause : Sicherheitsmechanismen beim Einsatz
von Web Services in der BMW Group
http://home.in.tum.de/~krause/DA_Ausarbeitung_Krau03.html; ToKr.zip
Technische Universität München, Tobias Krause, 16.11.2004

[darm] Diplomarbeit Anne-Kathrin Walter: Klassikation und Entwicklung von Verfahren zur Bedrohungs- und Risikoanalyse für IT-Systeme
http://www.sec.informatik.tu-darmstadt.de/lang_neutral/
diplomarbeiten/docs/walter_diplom.pdf
Universität Bremen, Anne-Kathrin Walter, 27.11.2004

[decu] "IT-Sicherheitskriterien im Vergleich"
http://www.decus.de/slides/sy2002/17_04/2F05.pdf
Dr. Harald Niggemann, 16.9.2004-11-19

[demo] Lexikon der Informationssicherheit
http://www.demonium.de/th/home/sicherheit/lexikon/buchstabe_c.phtml; buchc.pdf
Diplom-Informatiker Thomas Hungenberg, 16.11.2004

[dfn] Von der Qualität zur Informations-Sicherheit
http://www.dfn-cert.de/dfn/berichte/db092/bsi7799.PDF
Produktmanager ISMS, Reinhard Witzke, 16.11.2004

[eday] Professional Business Security
http://www.eday.at/vortraege/huelber-indust.pdf
Siemens Business Services, 16.08.2004

[fhbb] Technisches Risikomanagement
http://www.fhbb.ch/01/03/1/manuskripte/pdf/technisches_risikomanagement.pdf
Fachhochschule beider Basel, 20.09.2004

[fhzheta] Risiko und Sicherheit von Netzwerken, Methoden der System-Analyse
http://pubwww.fhzh.ch/~rmock/public/ Vorlesung/pdf/rm_eta_prec_RSN04.pdf
Zürcher Fachhochschule, Dr. –Ing. Ralf Mock, 16.09.2004

[ifida] Sicherheitsmanagement für neue Organisationsformen
http://www.ifi.unizh.ch/events/SIS/SIS2000/slides/damm.pdf
Institut für Informatik der Universität Zürich,
D.Damm, S. Röhrig, D.Hafner, 25.10.2004

[iid] Gesetz zur Regelung der Rahmenbedingungen
für Informations- und Kommunikationsdienste
http://www.iid.de/rahmen/iukdgbt.pdf
Bundesministerium für Bildung und Forschung, 16.11.2004

[influe] Diplomarbeit Andrè Lübke, Entwurf einer Sicherheitsarchitektur
für den Einsatz mobiler Endgeräte
http://users.informatik.haw-hamburg.de/ ~ubicomp/arbeiten/diplom/luepke.pdf
Hochschule für angewandte Wissenschaften Hamburg,
Andrè Lübke,16.09.2004

[ini] IT-Sicherheitskriterien im Vergleich
http://www.initiatived21.de/druck/news/publikationen2002/doc/22_1053502380.pdf
Initiative D21 e.V., 16.09.2004

[isc] Internetnutzerzahlen
http://www.isc.org/index.pl?/ops/ds/ ; InternetSystemsConsortium.pdf
Internet Systems Consortium, 18.09.2004

[magd] Fehlerbäume
http://isgwww.cs.uni-magdeburg.de/sim/vilab/2003/presentations/sylvia4on1.pdf
Institut für Simulation und Grafik, Sylvia Glaßer, 20.09.2004

[netz] IT-Sicherheitsmanagement basierend auf internationalen Standards
Workshop „Einführung eines IT-Sicherheitsmanagements an Hochschulen“
http://www.netzagentur.nrw.de/netzagentur/ extern/
Workshop2004/Downloads/Final-Handout-Moll.pdf
Institut für Informatik IV der Universität Bonn, Dipl. -Inform. W. Moll, 16.09.2004

[pete] Fischgrät-Diagramm
http://www.peters-helbig.de/Download/Ishikawa.pdf
Henning Peters & Peter Helbig Unternehmensberatung, 3.12.2004

[seco] BS 7799
http://www.secorvo.de/whitepapers/secorvo-wp10.pdf
Secorvo Security Consulting GmbH, Jörg Völker, 16.11.2004

[soko] Sicherheitsanalyse-Verfahren
http://www.software-kompetenz.de
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V., 1.11.2004

[suco] Rechtliche Pflichten im Bereich der IT-Sicherheit
http://www.surfcontrol.com/general/guides/SurfControl_RechtlicherLeitfaden.pdf
Heussen Rechtsanwaltsgesellschaft mbH, R. Niedermeier, Dr. M. Junker, 16.09.2004

[wiki] Urheberrechtsgesetz
http://de.wikipedia.org/wiki/Urheberrechtsgesetz ; Urheberrechtsgesetz.pdf
Wikimedia Foundation Inc., 16.11.2004

Hiermit versichere ich, dass ich die vorliegende Arbeit im Sinne der Prüfungsordnung nach §22(4) ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den 10.12.2004

_____

Katrin Scholz