Universität Potsdam
Institut für Informatik
Wintersemester 2004/2005
Prof. Dr. K. Rebensburg
Dipl. Inf. T. J. Wilke

Seminar

Umfassende Absicherung komplexer IT-Infrastrukturen

Autoren: Alexander Altmann, Stefan Bartel, Dietmar Bremser, Dennis Brockhoff, Bettina Buchholz, Christian Förster, Rene Freitag, Martin Fürstenau, Jörn Hartwig, Henrik Hinrichs, Hendrik Horn, Jörgen Kosche, Ronny Müller-Kuhle, Johannes Orgis, Hai Anh Pham, Alexander Renneberg, Eldar Sultanow, Sven Tabbert, Michael Werlitz, Francis Zinke

Datum: Potsdam, 12. Februar 2005

Inhaltsverzeichnis

1 Trusted Computer System Evaluation Criteria (TCSEC)

René Freitag, Ronny Müller-Kuhle

Abstract

This document shall give an overview over the Department of Defense standard DOD 5200.28-STD. This standard classifies computer systems in generally four security categories. These categories reach from „Low Security“(Class D) to „Highest Security“. René Freitag and Ronny Müller-Kuhle chose to at first examine the criteria for secure computer systems in 1.2. Those six criteria lead to 6 categories plus the class D, which implements none of these criteria. In 1.3 the classes for secure systems are described in detail. Next, the evaluation process is described (1.4) and example products are introduced in 1.4.1. After the final summary follows an addendum with glossary and bibliography.

1.1 Einleitung

Die „Trusted computer system evaluation criteria“definiert grob vier hierarchische Schichten zur Evaluierung und Entwicklung vertrauenswürdiger Computersysteme. Durch die Evaluation soll ein Anwender jederzeit die Vertrauenswürdigkeit eines Systems erkennen können. Entwickler sollen dadurch eine Hilfe zur Entwicklung solcher Systeme erhalten. Das Dokument beschreibt detailliert die Anforderungen an die verschiedenen Sicherheitsstufen von D, keinerlei Sicherheit, bis A, maximale Sicherheit.

1.1.1 Motivation

Ende der 1960er Jahre wurde auf sensible Daten immer häufiger per Fernzugriff (Rechnernetze) Zugegriffen. Auch die Arbeit verschiedener Personen an einem Computer nahm zu. Daher war es zunehmend wichtig, Systeme zu entwickeln, die Sicherheit garantierten. Es wäre fatal gewesen, wenn jemand ohne Autorisation Zugriff auf die Computer der Abschussrampen für Atomraketen bekommen hätte. Aber nicht nur militärische, sondern auch wirtschaftliche Erwägungen waren von Bedeutung. Auch die Wirtschaft setzte immer mehr Computer ein. TCSEC ist ein Werkzeug, um den verschiedensten Interessengruppen vertrauenswürdige Computersysteme zugänlich zu machen. Ursprünglich zur Evaluierung militärischer und behördlicher Systeme entwickelt, blieb der Einsatz der TCSEC auch hauptsächlich auf diese zwei Gebiete begrenzt.

1.1.2 Entwicklungsgeschichte

Bereits 1967 begann die Arbeit zum Thema vertrauenswürdige Computersysteme. 1970 erschien SSecurity Controls for Computer Systems"mit Politiken und technischen Vorschlägen für Computer mit Fernzugriff.
1972/73 veröffentlichte das Department of Defense die Direktive 5200.28 (M) mit uniformen DoD Politiken und Sicherheitsgrundlagen. In den 1970er Jahren fanden weitere Entwicklungen auf diesem Gebiet statt. 1977/78 begann man in verschieden Workshops damit, Kriterien für sichere Computersysteme zu finden. Dies führte 1981 zur Gründung des DoD Computer Security Centers, dass die Verbreitung von vertrauenswürdigen Computersystemen vorantreiben sollte. 1985 erschien schließlich TCSEC. Durch den recht starren Aufbau wurde TCSEC nach Kritik 1992 durch den Standart Federal Criteria abgelöst.

1.2 Die Sicherheitskriterien nach TCSEC

Die TCSEC spezifiziert grob 6 Hauptkriterien zur Bewertung der Sicherheit von Computersystemen. Anhand dieser Kriterien werden dann die Systeme in eine Sicherheitsklasse eingeordnet. Diese Kriterien kann man grob ordnen von „Schwächstes"bis „Stärkstes".

1.2.1 Discretionary Access Control (DAC)

Das System muss nach Benutzern und Ressourcen unterscheiden können. Dazu ist es notwendig, dass sich jeder Benutzer authentifiziert. Bevor er irgendeine Aktion am System durchführen kann. Über so genannte Access Control Lists (ACL) wird der Zugriff von Benutzern auf Objekte (z.B. Dateien) geregelt. Eigentümer eines Objektes können festlegen, wer auf dieses Objekt zugreifen kann.

1.2.2 Identifikation und Aufzeichnung

Hier muss ein System nicht nur einen Benutzer identifizieren, sondern durch einen geeigneten Mechanismus (z.B. Passwörter) sicherstellen, dass ein Nutzer auch der ist, der er vorgibt zu sein. Weiterhin müssen sicherheitsrelevante Aktionen am System in Log-Dateien gespeichert werden. Unter sicherheitsrelevanten Aktionen versteht man Benutzerlogins aber auch Zugriffe auf sensible Daten des Systems. Diese Log-Dateien müssen durch das System vor unberechtigtem Zugriff geschützt werden.

1.2.3 Mandatory Access Control (MAC)

Bei MAC werden Objekte (Dateien, Peripherie etc.) in Sicherheitsklassen eingeordnet. Jedem Benutzer oder jeder Benutzergruppe werden Klassenrechte vergeben, die den Zugriff auf die einzelnen Sicherheitsklassen regeln. MAC ist dabei als hierarchische Erweiterung zu DAC zu sehen. Ein Benutzer behält weiterhin die Möglichkeit, Zugriffsrechte zu vergeben, sofern der Regelsatz des MAC dies erlaubt.

1.2.4 Strukturierte Sicherheit

Unter Strukturierter Sicherheit verstehen die TCSEC das Vorhandensein einer klar definierten Sicherheitspolitik als Grundlage für das vertrauenswürdige Computersystem.

Weiterhin müssen alle an das System angeschlossene Geräte (Drucker, Monitore, Tastaturen etc.) mit Sicherheitsattributen versehen werden. Dadurch wird sichergestellt, dass Informationen nur dort angezeigt oder eingegeben werden, wo dies auch gewünscht ist. Auch die Authentifikationsmechanismen sollen verbessert werden (z.B. Retinascan, Fingerprint). Für die Wartung des Systems müssen Rollen für den Systemadministrator und für Operatoren definiert sein.

1.2.5 Sicherheitsdomäne

Das System muss vor böswilligen Eingriffen von außen geschützt sein. Alle Sicherheitsmechanismen müssen immer aktiv sein und Zugriffe müssen durch einen Referenzmonitor kontrolliert werden Dieser überwacht sämtliche Zugriffe auf Objekte und entscheidet anhand der Regelsätze, ob ein Zugriff erlaubt oder abgelehnt wird. Als neue Rolle kommt der Sicherheitsbeauftragte hinzu.

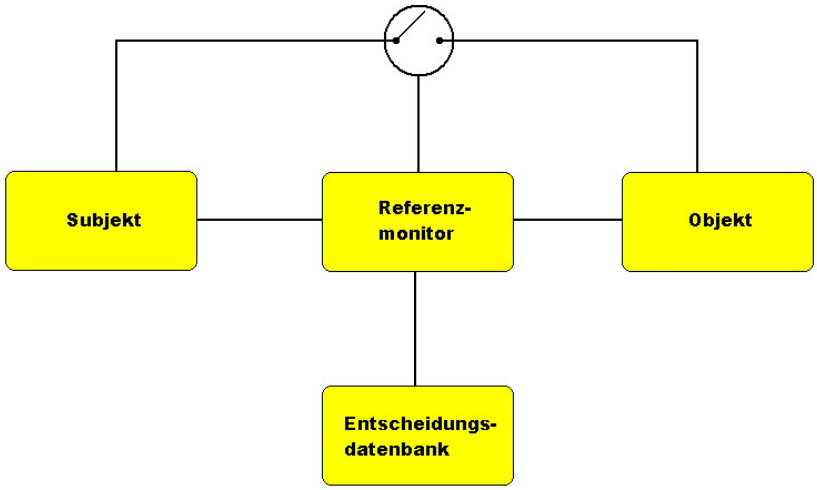

Abbildung 1.1: Der Referenzmonitor (schematisch), (Objekte können auch zu Subjekten werden)

1.2.6 Verifizierung

Um dieses Kriterium zu erfüllen, müssen die Entwickler formal nachweisen können, dass sich ihr System stets so verhält, wie es nach den Kriterien gefordert ist. Dazu ist eine Spezifikation und eine Beweisführung notwendig.

1.3 Die Sicherheitsklassen nach TCSEC

Die Sicherheitsklassen sind hierarchisch geordnet, wobei die Klasse D für die geringste (gar keine) und die Klasse A1 für die höchste Sicherheitsstufe stehen. Jede Klasse, mit Ausnahme von D, enthält Sicherheitskriterien (vergl. 1.2), die sie erfüllen muss. Jede höhere Klasse erfüllt dieselben Kriterien und fügt noch weitere Anforderungen hinzu oder erweitert vorhandene. Die TCSEC geben dabei nicht nur an, welche Kriterien erfüllt werden müssen, sondern in einem gewissen Maße auch wie diese implementiert sind.

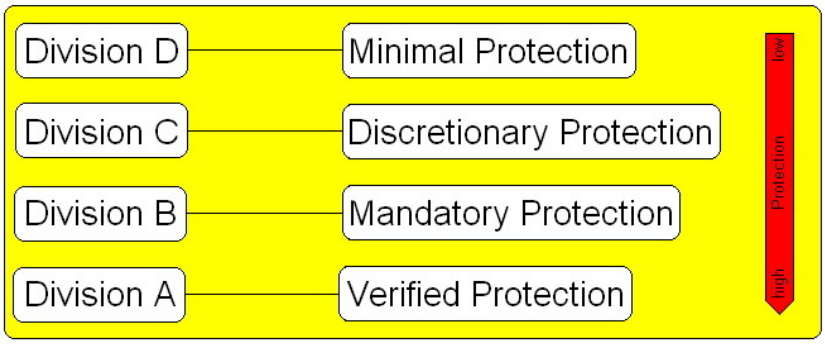

Abbildung 1.2: Die Oberklassen der TCSEC, C und B jeweils nochmals unterteilt

1.3.1 Die Klasse D - Minimal Protection

Diese Klasse beinhaltet alle evaluierten Systeme, die die Anforderungen einer höheren Klasse nicht erfüllen konnten.

1.3.2 Die Klasse C1 - Discretionary Security Protection

Systeme der Klasse C1 erfüllen die Kriterien nach 1.2 und 1.2.1. Solche Systeme schützen Information hauptsächlich vor versehentlichem Lesen und Löschen. C1-Systeme sollten dort zum Einsatz kommen, wo Benutzer sich gegenseitig vertrauen und auch miteinander kooperieren. Die verarbeiteten Informationen sollten die gleiche Sensibilität aufweisen.

1.3.3 Die Klasse C2 - Controlled Access Protection

C2-Systeme erfüllen die die Kriterien 1.2, 1.2.1 und 1.2.2. Die benutzerbestimmte Zugriffskontrolle ist sehr detailliert, dadurch können Aktionen dem jeweiligen Benutzer zugeordnet werden. C2-Systeme erlauben somit die Verfolgung unerlaubter Aktionen und bieten einen Schutz vor gezielten Angriffen durch Unbefugte. Diese Klasse sollte die minimale Sicherheitsstufe auch im zivilen Bereich sein, da sie bereits einen grundlegenden Schutz vor böswilligen Eingriffen bietet.

1.3.4 Die Klasse B1 - Labeld Security Protection

Die Kriterien 1.2, 1.2.1, 1.2.2 und 1.2.3 müssen erfüllt sein. Der Regelsatz des MAC erlaubt es, jedem Benutzer spezielle Rechte auf dem System einzuräumen und so die unterschiedlichen Sicherheitseinstufungen von Personen umzusetzen. Für die Evaluierung ist eine informelle Beschreibung des Sicherheitsmodells und der Regeln notwendig. B1-Systeme kommen dort zum Einsatz, wo Personen mit unterschiedlichen Sicherheitseinstufungen am selben System arbeiten. Dies kann ein militärisches Computersystem sein, bei dem ein General mehr Rechte hat als ein Major. Aber hierarchisch gegliederte Abteilungen eine Wirtschaftsbetriebes könnten solche Systeme einsetzen.

1.3.5 Die Klasse B2 - Structured Pritection

Neben den Kriterien 1.2, 1.2.1, 1.2.2 und 1.2.3muss zusätzlich das Kriterium der Strukturierten Sicherheit 1.2.4 erfüllt sein. Die TCB muss auf einem formalen Sicherheitssystem basieren und zwischen sicherheitsrelevanten und sicherheitsunkritischen Elementen

unterscheiden können. Covert Channels eines Systems müssen identifiziert und nach Möglichkeit eliminiert werden.

1.3.6 Die Klasse B3 - Security Domains

Neben den Anforderungen an die B2 muss diese Klasse auch noch die Forderungen nach einer Sicherheitsdomäne (siehe 1.2.5) erfüllen. Dazu muss eine Referenzmonitor implementiert sein, der gegen jede Beeinflussung und Fälschung von außen geschützt sein muss. Dieser Monitor muss immer aktiv sein, um seine Aufgabe zu erfüllen. Die Implementation muss klein genug sein, um die Testbarkeit mittels formaler Methoden zu gewährleisten. Auch die TCB muss möglichst klein sein, damit die Testbarkeit gewährleistet ist. Die TCB darf daher nur solchen Code enthalten, der zur Durchsetzung der Sicherheitskriterien notwendig ist. Weiterhin muss die Rolle eines Sicherheitsbeauftragten im System definiert sein, die sich ausschließlich mit Fragen der Sicherheit des Systems beschäftigt. In der TCB müssen weiterhin Wiederanlauf-Mechanismen enthalten sein.

1.3.7 Die Klasse A1 - Verified Design

Funktionell sind Systeme der Klassen A1 und B3 genau gleich. Nur durch die Verwendung von formalen Techniken zu Spezifikation und Verifikation unterscheiden die Klasse A1 von B3.

	D	C1	C2	B1[4]	B2	B3	A
Security Policy							
Discretionary Access Control (DAC)	♦	✱	✱	•	•	✱	•
Labels	♦	♦	♦	✱	✱	•	•
Mandatory Access Control	♦	♦	♦	✱	✱	•	•
Accountability							
Identification and authentication	♦	✱	✱	✱	•	•	•
Audit	♦	♦	✱	✱	✱	✱	•
Assurance							
Operation reliability							
System architecture	♦	✱	✱	✱	✱	✱	•
Covert channel analysis	♦	♦	♦	♦	✱	✱	✱
Trusted recovery	♦	♦	♦	♦	♦	♠	•
Development reliability							
System testing	♦	✱	✱	✱	✱	✱	✱
Design specification and verification	♦	♦	♦	✱	✱	✱	✱

♦ : no requirements
• : no additional requirements (All and only the requirements of previous class)
✱ : new or added requirements with respect to those of previous class

Abbildung 1.3: Die Sicherheitsanforderungen im Überblick (Quelle: [5])

1.4 Das Testverfahren nach TCSEC

Die TCSEC gibt genaue Vorgaben, von wem und in welchem Umfang ein zu evaluierendes Produkt getestet werden muss. Jede neue Version (auch Patches) gilt automatisch als nicht-evaluiert. Um aber der Dynamik bei der Weiterentwicklung gerecht zu werden, wird eine Evaluierung von neueren Versionen erleichtert. Im Zuge der Rating Maintenance Phase (RAMP) können speziell geschulte Mitarbeiter des Systementwicklers die Entstehung des neuen Systems überwachen (siehe [2]). Die Evaluierung findet stets in den USA statt. Möchte ein Entwickler sein Produkt evaluieren lassen, so muss er dies bei der NSA anmelden. Die Agentur übergibt dann das Produkt an einen Evaluator. Am Ende der Evaluation wird der Final Evaluation Report (FER) erstellt. Der FER beinhaltet die abschliessenden Ergebnisse nach dem Evaluierungstest. Ein jedes Dokument beschreibt ganz genau die Vorgehensweise beim Test, das eingesetzte System (Hardware und Software) und gibt das Testpersonal an. Diese Berichte geben Aussagen und Analysen über Sicherheitsfunktionen und Funktionsgarantien eines Computersystems. Es ist aber nicht jeder Evaluierungstest öffentlich verfügbar, da einige Systeme natürlich als „Streng geheim“gelten oder eine elektronische Dokumentierung nicht vorliegt.
Alle evaluierten Systeme werden in der EPL (Evaluated Products List) gespeichert. In einer historischen EPL sind alle bisher getesteten System aufgeführt. Aktuellere Systeme erscheinen in einer separaten Liste. In dieser Evaluierungsliste sind die Systeme nach Klasse (class) oder Hersteller (vendor) sortiert, da dies die Suche nach besonderen Anforderung an ein vertrauenswürdigen Computersystem erleichtert. Die folgende Tabelle listet für jede Klasse die benötigten Ressourcen auf. Unter Techniker wird hauptsächlich Informatiker zu verstehen sein, wobei aber auch vergleichbare Ausbildungen denkbar wären.

Klasse	Testpersonen	Testanzahl	Stunden pro Tester	Gesamtdauer
C	2 Techniker (Bachelor)	5 Tests	20	1-3 Monate
B	2 Techniker (Bachelor) 1 Techniker (Master)	15 Tests	30	2-5 Monate
A	3 Techniker (Bachelor) 2 Techniker (Master)	25 Tests	50	3-6 Monate

1.4.1 Beispielsysteme

Hersteller: Wang Government Services, Inc.
Produkt: XTS-200 STOP 3.1.E
Produktart: Betriebssystem
Klasse: B3
Datum: 27.05.1992
Testbericht: CSC-EPL-92/003

Das XTS-200 ist eine Multiprozessorsystem, auf dem das Betriebssystem STOP läuft. Das Mehrbenutzersystem unterstützt maximal 256 Benutzer, DAC, MAC und die umfangreiche Rechtevergabe für Benutzer. Es unterscheidet Regel für den Administrator und den Systembediener. Alle Aktion der Benutzer werden geprüft und protokolliert. Jedem Benutzer sind nur bestimmte beschränkte Privilegien zuweisbar. Die Testergebnisse haben daher ergeben, das alle Sicherheitsfunktionen der Klasse B3 erfüllt werden.

Hersteller: Trusted Information Systems, Inc.
Produkt: Trusted XENIX 4.0
Produktart: Betriebssystem
Klasse: B2
Datum: 17.09.1993
Testbericht: CSC-EPL-92/001.A

XENIX ist ein UNIX-ähnliches Betriebssystem. Es können 4 unterschiedliche Privilegien für Benutzer vergeben werden. Die Aktionen der Benutzer werden geprüft und protokolliert. Über eine Server-/Client-Plattform lässt sich das System von außen kontrollieren. Das Testteam stellte bei der Evaluierung fest, das dieses System alle Kriterien der Klasse C2 erfüllt. Zusätzlich unterstützt es einige Sicherheitsanforderungen wie DAC, Trusted Path, und Trusted Facility Management aus der Klasse B3.

Hersteller: Hewlett Packard Corporation
Produkt: HP-UX BLS release 9.0.9+
Produktart: Betriebssystem
Klasse: B1
Datum: 01.12.1994
Testbericht: CSC-EPL-95/002

Hierbei handelt es sich um eine Hewlett-Packard Version von UNIX. Das Betriebssystem läuft auf Workstations der Serie 700 der HP9000-Maschine. MAC und DoD Password Management wird vom Betriebssystem unterstützt. Alle Kriterien der Klasse B1 werden erfüllt. HP-UX BLS unterstützt ausserdem DAC der Klasse B3 und Trusted Facility Management der Klasse B2. Nach NSA's RAMP erfolgte eine Re-Evaluierung dieser Version des Produktes. Die Netzwerk- und grafische Fensterunterstützung wurde nicht evaluiert.

Hersteller: Microsoft Corporation
Produkt: Windows NT Workstation and Windows NT Server, Version 4.0 , Service Pack 6a
Produktart: Betriebssystem
Klasse: C2
Datum: 11.1999
Testbericht: TTAP-CSC-FER-99/001

Windows NT ist ein 32-bit Betriebssystem mit Multiprozessorunterstützung. Es können verschiedene Benutzer wie Administrator oder Anwender angelegt werden. Es sind grafische Administrierungstools für Benutzerverwaltung, Backup, Druckervergabe usw. vorhanden. Ein Administrator hat die volle Kontrolle über das System. NTFS ermöglicht die volle Zugangskontrolle für alle Objekte des Systems. Dieses Produkt wurde getestet durch die SAIC (Science Applications International Corporation). Die Klasse C2 wird nur mit dem Service Pack 6a erfüllt.

1.5 Zusammenfassung

Die Trusted Computer Evaluation Criteria war die erste Möglichkeit zur Einstufung von Computersystemen in Sicherheitsstufen. Unter Sicherheit wird bei TCSEC allerdings der

Hauptaugenmerk auf die Vertraulichkeit von gespeicherten Informationen gelegt. Auch bleibt der Standart auf jeweils einzelne Computersysteme beschränkt. Das heißt, bis zum Verlassen eines evaluierten Systems kann die Sicherheit anhand der Evualationsstufe garantiert werden. Heutzutage sind aber immer mehr verteilte Rechnersysteme zu finden. Deren Sicherheit zu evaluieren dürfte mit TCSEC schwerfallen. Auch die unflexible Verknüpfung von Funktion und Qualität in den einzelnen Klassen stellte sich schnell als zu unflexibel für die praktische Anwendung heraus. In der Wirtschaft fand TCSEC daher nur wenig Anklang und wurde auch aus Kreisen der Behörden und des Militärs mit Kritik und Ablehnung bedacht. Weiterhin werden Produkte nur von öffentlichen Stellen und unter erheblichen finanziellen und zeitlichen Kosten evaluiert. Selbst die Erleichterung der Re-Evaluierung (RAMP, siehe [2]) von neuen Version schafft hier nur wenig Abhilfe. Trotzdem bleibt der Standart ein Meilenstein. Vorher gab es nur Ansätze, die Sicherheit von Computersystemen zu klassifizieren. So verwundert es kaum, dass Ideen der TCSEC auch in neue Standarts wie der Common Criteria wieder zu finden sind.

Glossar

DoD	Department of Defense, Verteidigungsministerium der Vereinigten Staaten von Amerika
EPL	Evaluated Products List, Listet die evaluierten Produkte auf (siehe [3])
FER	Final Evaluation Report, enthält das detailierte Testergebniss und die Einstufung. Kann als „Streng geheim“eingestuft werden
NSA	National Security Agency, national und international operirende Bundesagentur für Sicherheit der USA
TCB	Trusted Computer Base, Dies ist der Teil eines Computersystems, der die Sicherheitsfunktionen implementiert. Sollte immer nur den Code für diese Sicherheitsfunktionen enthalten
TCSEC	Trusted computer system evaluation criteria, „Orange Book“, Sicherheitskriterium für Computersysteme vom DoD

Literaturverzeichnis

[1] Department of Defense Trusted Computer System Evaluation Criteria . http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html, Dezember 1985.

[2] Historische Evaluated Product List. http://www.radium.ncsc.mil/tpep/process/ourprogram.html, Januar 1997.

[3] Aktuelle Evaluated Product List. http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html, September 2000.

[4] Historische Evaluated Product List. http://www.radium.ncsc.mil/tpep/epl/historical.html, August 2000.

[5] Ronald Rumm Lana Hendrowarsito. Sichere Datenbanksysteme, Sichere Betriebssysteme. http://wwwbayer.in.tum.de/lehre/SS2002/HSEM-bayer/Ausarbeitung9.pdf, Januar 1997.

2 ISO 17799

Bettina Buchholz, Michael Werlitz

Abstract

Im Rahmen des Seminars *Umfassende Absicherung komplexer IT-Infrastrukturen* wurde von Bettina Buchholz und Michael Werlitz das Thema *ISO 17799* gewählt. Es wurde der Inhalt des Standards analysiert und allgemein betrachtet durch wen, unter welchen Bedingungen und mit welchen Einschränkungen eine Umsetzung des Standards in der Realität stattfindet
Zu Beginn wird kurz darauf eingegangen, was die Einführung von Standards zur Informationssicherheit notwendig macht. Danach wird die Entwicklung und Einordnung es Standards betrachtet.
Nachfolgend werden die Themen des Standards kurz erläutert und besprochen, wie es mit einer realen Verwendung des Standards unter Berücksichtigung möglicher Nutzer, gesetzlicher Vorgaben und dem Vorgehen bei einer Umsetzung aussieht.
In der abschliessenden Zusammenfassung werden die Kernaussagen der Ausarbeitung noch einmal in komprimierter Form dargestellt.
Der Anhang der Ausarbeitung enthält ein Glossar, das einige Begriffe und Abkürzungen kurz erklärend darstellt.

2.1 Einleitung

Die Gewinnung, Aufbewahrung und Verarbeitung von Informationen ist für viele Organisationen unserer heutigen Gesellschaft ein elementarer und überlebenswichtiger Bestandteil einer erfolgreichen Geschäftstätigkeit. Informationen werden somit von vielen Unternehmen, Behörden und Non-profit Organisationen gleichermaßen als wertvolles „Gut“ betrachtet, dass es zu schützen gilt. Die Gefahrensituationen für die Informationssysteme und Netzwerke dieser Organisationen sind real und vielfältig. Neben denkbaren Gefahren, wie computergestützter Betrug, Spionage, Sabotage, Vandalismus, Einwirkung durch Elemente, wie Feuer oder Wasser, nimmt insbesondere die Gefährdung für die informationstechnische Infrastruktur, durch Denial of Service-Attacken, Virenbefall und massenhaften SPAM-Eingang deutlich zu. Die Ausweitung der technischen Infrastruktur und deren Verbindung mit fremden Netzwerken, wie zum Beispiel dem Internet, sowie die zunehmende Abhängigkeit von Informationssystemen und (externen) Diensten, hat dabei zu einer Verschärfung, besonders der letztgenannten Gefahren, geführt.
Um die Fortführung der Geschäftstätigkeit solch Informations-abhängiger Organisationen auch im schlimmsten Falle zu gewährleisten, bzw. um einen Schaden zu minimieren, bedient man sich der *Informationssicherheit*. Die Informationssicherheit dient laut [3] der Bewahrung der *Vertraulichkeit*, der *Integrität* und der *Verfügbarkeit* von Informationen. Sie versucht präventiv ein wirksames Set von Kontrollen, d.h. Policies, Prozeduren,

Organisationsstrukturen und Softwarefunktionen, einzuführen, um das spezifische Sicherheitsbedürfnis einer Organisation zu gewährleisten.

Im Jahr 2000 wurde durch die ISO (International Organization for Standardization) und IEC (International Electrotechnical Commission) der Standard ISO 17799 *Information technology — Code of practice for information security management* verabschiedet. Mit diesem Standard wird den Organisationen Empfehlungen und Richtlinien (2.3) zum Management der Informationssicherheit in die Hände gegeben. Diese bilden die Sicherheit im Großen ab und betreffen die an der Informationsverarbeitung beteiligten Menschen, Prozesse und IT-Systeme. Weiterhin werden übergreifende Aspekte der Informationssicherheit berücksichtigt.

Die hier vorliegende Ausarbeitung wurde im Rahmen des Seminars *Umfassende Absicherung komplexer IT-Infrastrukturen* im Wintersemester 2004/2005 an der Universität Potsdam erstellt. Sie vollzieht die Entstehung des Standards nach, ordnet den Standard gegenüber anderen IT-Sicherheitskriterien ein, umreißt die im Standard behandelten Themen, sucht nach den Nutzern des Standards, hinterfragt die Wirkung von gesetzlichen Vorgaben und fasst die wichtigsten Aussagen zu ISO 17799 nochmals zusammen.

2.2 Entwicklung und Einordnung von ISO 17799

2.2.1 Zeitliche Entwicklung

Zeit	Ereignis
September 2002	Updated version of BS 7799-2 (revised and corrected)
2001	Review of BS 7799-2
December 2000	ISO/IEC 17799:2000
1999	Updated version of BS 7799 Parts 1 and 2
1998	BS 7799 Part 2
1995	BS 7799 Part 1

Tabelle 2.1: Entwicklung von ISO 17799; Callio Technologies [5]

Auch wenn der Standard ISO 17799 erst im Jahr 2000 verabschiedet wurde, wie man aus der Tabelle 2.1 erkennen kann, sind dessen Anfänge in den frühen 90er Jahren zu suchen.
1995 veröffentlichte die BSI (British Standard Institution) eine Standardisierung mit der Bezeichnung *BS7799 A Code of Practice for Information Security Management*. Dieser Standard lehnte sich wiederum an eine zwei Jahre ältere Publikation namens *PD0005 Code of Practice* an. BS7799 kam zustande, weil die britische Industrie, der Handel und die Regierung gleichermaßen nach einem einheitlichen Rahmen zur Entwicklung, Umsetzung und Messung von Sicherheitsmanagementfunktionen verlangt hatten. Der Standard war auf den damaligen Erkenntnissen zum Thema Sicherheit in und zwischen Unternehmen aufgebaut.
Ab 1996 kam es zu einer zunehmenden Nachfrage nach Zertifizierungen zu diesem Standard, was von einigen Zertifizierungs-Unternehmen sofort aufgenommen wurde.
Im Jahr 1997 fand der erste Versuch statt den BS7799 international über die ISO zu veröffentlichen, was jedoch aufgrund der vielen technischen Details und der Herkunft des

Standards (er stammte eben nicht von der ISO selbst) abgelehnt wurde.
1998 wurde der BS7799 Part 2 publiziert, wodurch die vorher erstellte Version des Standards in BS7799 Part 1 umbenannt wurde.
Während die beiden Teile des BS7799-Standards von der BSI im Laufe der Zeit immer mal wieder an die veränderten Sicherheitsbedürfnisse angepasst wurden, hatten sich ISO und IEC bis zum Dezember 2000 endlich dazu durchgerungen ihrerseits einen solchen Standard, mit der Bezeichnung ISO 17799, zu veröffentlichen. Die Bezeichnung des Standards wurde gewählt, da man nun doch den BS7799 Part 1 übernommen hatte. Zur Übernahme des zweiten Teils des britischen Standards kam es nicht, da man ISO 17799 nicht technisch und nicht zu spezifisch gestalten wollte.

Seit dem Jahr 2000 sind keine Veränderungen am ISO 17799 vorgenommen worden. Laut einem Papier der NIST (National Institute of Standards and Technology) vom November 2002 [4] sind erst einmal auch keine weiteren Veröffentlichungen zu diesem Standard vorgesehen:

> At this time, ISO/IEC JTC 1 has no plans to generate a part 2 of ISO/IEC 17799 as a future work item.

Die Begründung für dieses Vorgehen scheint zu sein, dass die Richtlinen des Standards recht allgemein und wenig technisch gehalten sind und somit weniger Bedarf nach andauernden Erneuerungen besteht.
Im Gegensatz dazu wurde der BS7799 Part 2 im September 2002 erneut verändert. Dies geschah hauptsächlich, um ihn mit den ISO-Standards 9000 (Standard(s) rund um das Thema Qualitätsmanagement-Modelle) und ISO 14000 (Standards zu den Themen Unweltmanagement, Umweltmanagementsysteme und Umweltschutz) zu harmonisieren.

2.2.2 Einordnung gegenüber anderen Standards

Die Ziele [3] der ISO für den Standard ISO 17799 waren unter anderem:

- der Standard sollte einfach zu verstehen sein,
- er sollte keine Abhängigkeiten zu spezifischen Technologien aufweisen,
- er sollte nicht nur die IT umfassen,
- und er sollte betriebswirtschaftliche Aspekte berücksichtigen.

Die Abbildung 2.1 bewertet die Einordnung verschiedener Standards anhand zweier Kriterien.
Erstens, sind diese technisch oder eher nicht-technisch ausgelegt. Das bedeutet (für technisch) es sind in den jeweiligen Standards Maßnahmen festgelegt, die eine konkrete Umsetzung vorschreiben, bzw. ermöglichen. Im anderen Fall (nicht-technisch) sind die Ausführungen des Standards so allgemein gehalten, dass eine konkrete Umsetzung indivduell und damit außerhalb des Fokus des Standards erfolgen muss.
Zweitens, ist eine Standardisierung eher auf ein System (Organisationen, Teilbereiche einer Istitution) oder einzelne Produkte (konkrete Sicherheitsmechanismen, wie z.B. die Kryptographie (FIPS 140)) anwendbar.
Im Fall von ISO 17799 stellt man, unter Zuhilfenahme dieser Betrachtungsweise, fest, dass der Standard systembezogen und nicht-technisch ist.
Diese Betrachtung wird damit auch den oben genannten Zielen der ISO gerecht.

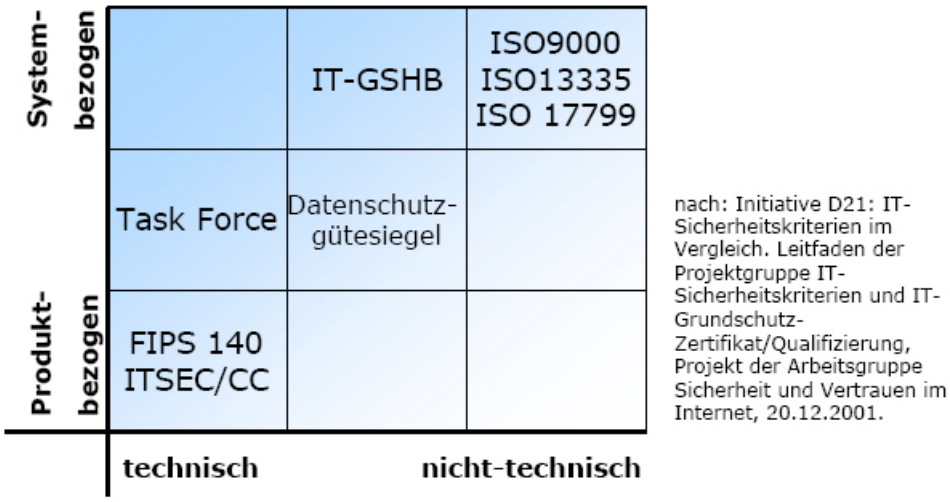

Abbildung 2.1: Einordnung des Standards; *Prof. Federrath* [1]

2.3 Inhalt des Standards ISO 17799

ISO 17799 ist in seiner aktuellen Form eine Sammlung von Empfehlungen für IT-Sicherheitsverfahren und -methoden, die sich in der Praxis bewährt haben. Der Standard umfasst 10 so genannte Überwachungsbereiche, die im folgenden einzeln vorgestellt werden sollen.

Die Abbildung 2.2 vermittelt einen Überblick über die Anordnung dieser Überwachungsbereiche im Spannungsfeld der Organisation. Bereiche die, in der Pyramide weit oben angesiedelt sind, werden meist von der Führung festgelegt und gelten global für die gesamte Organisation. Ganz unten befinden sich die Bereiche der Informationssicherheit, die im operativen Geschäft und dort jeweils angepasst an die vorherrschende Situation, durchgesetzt werden müssen.

Die im folgenden verwendeten deutschen Bezeichnungen der Überwachungsbereiche entsprechen keiner offiziellen deutschen Übersetzung des Standards, da eine solche von der ISO bisher nicht herausgegeben wurde. Sie sind an einen Vortrag von Prof. Federrath [1] angelehnt.

2.3.1 Security policy

Für eine Organisation ist es wichtig grundsätzliche Richtlinien im Umgang mit dem Thema Sicherheit festzulegen. Eine solche Grundlage kann später auch immer als Hilfestellung für anstehende Entscheidungen des Managements genutzt werden.
Die *Sicherheitspolitik* (security policy) soll deshalb die *grundsätzliche Position der Organisation bezüglich der Informationssicherheit* darstellen. Dazu ist es notwendig ein *Policy-Dokument* anzufertigen, welches auch regelmässig begutachtet und ggf. erneuert werden muss.
Das Dokument umfasst folgende Punkte:

Abbildung 2.2: Anordnung der Überwachungsbereiche; Callio Technologies [6]

- Die Definition von Informationssicherheit aus Unternehmenssicht.
- Die Definition des Managementziels bezüglich der Informationssicherheit.
- Die Definition der Zuständigkeiten für die Informationssicherheit.
- Eine Kurzbeschreibung von:
  - Der Übereinstimmung der Maßnahmen mit geltendem Recht und bestehenden vertraglichen Vereinbarungen.
  - Die Anforderung an Schulungsmaßnahmen.
  - Die Abwehr von Viren und anderen schädlichen Softwarecodes.
  - Das business continuity management, welches alle Maßnahmen und Planungen umfasst, die den Geschäftsbetrieb bei Ausfall der IT oder einzelnen Komponenten aufrechterhalten.
  - Die Verfahrensweise bei Verstößen gegen die Policy.
- Die Verweise auf Dokumente, welche zur Umsetzung des Policy-Dokumentes dienen.

2.3.2 Organizational security

Unter dem Begriff der *organisatorischen Sicherheit* (organizational security) wird die Schaffung einer *Verwaltungsstruktur* für die Sicherheit innerhalb des Unternehmens oder der Organisation empfohlen. Diese legt fest, wer für welche Sicherheitsbereiche zuständig ist und wie Vorfälle behandelt werden sollen.

Infrastrukturmaßnahmen

Mit *Infrastrukturmaßnahmen* soll ein organisatorisch-technischer Rahmen für das Management der Informationssicherheit innerhalb der Organisation geschaffen werden.
Hierzu muss unter anderem ein Security Manager ernannt werden, der die Überwachung und Beurteilung von Sicherheitsverstößen, sowie die Änderung der Sicherheitslage überwacht.
Auch die Billigung von Maßnahmen zur Verbesserung des Sicherheitsniveaus gehört dazu.
Des weiteren soll eine Koordinationsgruppe für Informationssicherheit zusammengestellt werden, sowie das Festlegen der jeweiligen Zuständigkeiten.

Zugriff auf das Unternehmen durch Dritte

Es muss ein organisatorisch-technischer Rahmen geschaffen werden, *so dass Dritte Zugriff auf etwaige Unternehmensdaten erhalten können*. Hierbei müssen die Zugriffsarten festgelegt werden und eine Beschreibung, für welche Aufgaben der Zugriff von Nöten ist.

Outsourcing (Verlagerung von Geschäftsprozessen nach Außen)

Trotz *Outsourcing* muss das festgelegte Sicherheitsniveau erhalten bleiben. Es muss dabei eine vertragliche Festlegung der Sicherheitsanforderungen existieren, welche die Einhaltung der gesetzlichen Vorschriften (z.B. Datenschutz) garantiert.

2.3.3 Asset classification and control

Mit der *Einstufung und Kontrolle der Werte* (asset classification and control) fordert man das Führen einer *„Inventarliste“*, die alle Aktiva der Organisation, seien es physikalische Anlagegüter, Software, aber auch Informationen und Dienste, beinhaltet. Diese müssen nach ihrer Notwendigkeit und Wichtigkeit klassifiziert werden, so dass der Grad ihres Schutzes festgelegt werden kann.

2.3.4 Personnel security

In der *personellen Sicherheit* (personnel security) wird auf die Notwendigkeit hingewiesen, dass sämtliche *Mitarbeiter* darüber *informiert werden sollen*, was von ihnen in Bezug auf Sicherheits- und Vertraulichkeitsfragen erwartet wird und welche Rolle sie im Sicherheitsgefüge spielen, bzw. wie etwaige Vorfälle behandelt werden. Hierzu gehört nicht nur die Formulierung der Sicherheitsanforderungen an die Stelleninhaber, sondern auch eine Geheimhaltungserklärung, eine Sicherheitsprüfung der Mitarbeiter und eine Klausel im Vertrag der Mitarbeiter, die auf die Einhaltung der Sicherheitsmaßnahmen hinweist.
Zur Personellen Sicherheit gehört außerdem die Schulung und Training in der korrekten Verwendung von Software und Geräten, sowie die Schulung und Sensibilisierung um Umgang mit Information.

2.3.5 Physical and environmental security

Die *physische und umgebungsbezogene Sicherheit* (physical and environmental security) befasst sich mit der Notwendigkeit die *sensiblen Bereiche einer Organisation zu schützen*, sowie die *Gerätesicherheit* durchzusetzen.

Zu allererst werden dafür in einer Organisation so genannte Sicherheitsbereiche festgelegt, sowie folgende Maßnahmen eingeleitet:

- Der Aufbau physischer Barrieren, z.B. Sicherheitsmodule, die über Brandschutz, Zugangsschutz, Klimatisierung und unabhängige Stromversorgung verfügen.
- Die Festlegung von Besucherbereichen.
- Die Errichtung von Zugangskontrollen an Gebäuden, Räumen und Systemen.
- Die Absicherung von Büros und Einrichtungen.
- Gewährleistung der Arbeitsplatzsicherheit.
- Die Sicherung von Ein-, Aus- und Verladebereichen.

Ebenso muss die Gerätesicherheit festgelegt werden. Dazu gehört neben dem Verhalten der Mitarbeiter im Umgang mit den Geräten, auch der Zustand der Ausrüstung, d.h. verfügen diese über eine geeignete Energieversorgung, ist die Sicherheit der Verkabelung gewährleistet, erfolgt eine sichere Entsorgung von Datenträgern usw.
Letztendlich müssen auch noch allgemeine Regeln am Arbeitsplatz festgeschrieben werden, wie z.B. das Dokumente verschließbar aufzubewahren, vertraulichen Dokumenten zu sichern, sensible Ausdrucke sofort aus den Druckern zu nehmen sind, etc.

2.3.6 Communications and operations management

Das *Management der Kommunikation und des Geschäftsbetriebs* (communications and operations management) lässt sich in sieben Bereiche unterteilen.

1. *Zuständigkeit für den sicheren Betrieb der Informationsverarbeitungseinrichtung*, z.B. Dokumentation von Betriebsabläufen, Nutzung externer Dienste und Dienstleistungen, Regeln zur Aufrechterhaltung des Sicherheitsniveaus bei Änderungen im Ablauf von Prozessen.
2. *Systemplanung*, z.B. Planung von Kapazitäten, Tests neuer Software, Bereitstellung von Dokumentationen der Geräte.
3. *Schutz vor fehlerhafter und böswilliger Software*, z.B. Installation von Virenscannern, Erstellung von Update.
4. *Housekeeping*, z.B. Protokollierung von Fehlern, Erstellung von Backups.
5. *Netzmanagement*, z.B. Sicherheitsmaßnahmen zur Gewährleistung von Vertraulichkeit, Verschlüsselung auf Übertragungsstrecken.
6. *Sicherer Umgang mit Medien*, z.B. Löschung nicht mehr genutzter Daten, Sichere Datenaufbewahrung.
7. *Informationsaustausch zwischen Unternehmen*, z.B. E-Commerce-Sicherheit, Datenträgertransport

2.3.7 Access control

Mit der *Zugriffskontrolle* (access control) wird auf die Bedeutung von *Kontroll- und Überwachungsmaßnahmen* für den Zugriff auf Netzwerke und Anwendungsressourcen zum Schutz von internem Missbrauch und externen Systemeindringlingen verwiesen. Hierzu gehören Mechanismen der Zugriffskontrolle (z.B. Nutzerregistrierung, Passwort-Management), entfernter Zugriff über Rechnernetze (z.B. Einschränkung und Überwachung der Zugriffe), Zugriffskontrollen auf Anwendungs- und Betriebssystemebene, Protokollierung der Zugriffe, Verantwortlichkeiten der Nutzer (Passwortsicherheit) und so weiter.

2.3.8 Systems development and maintenance

Mit der *Systementwicklung und Wartung* (systems development and maintenance) wird darauf hingewiesen, dass auch im Entwicklungsprozess und bei Betreuung von Systemen alle IT-Maßnahmen unter dem Gesichtspunkt der *Sicherheit* ausgeführt werden müssen. Demnach sollen die Sicherheitsanforderungen bereits bei der Entwicklung eines Systemdesigns definiert werden und auch während des Entwicklungsprozesses selbst sind Sicherheitsmaßnahmen einzuhalten. Die Sicherheit muss in Anwendungssystemen und für Systemdateien gleichermassen gewährleistet werden und kryptografische Verfahren sind stets einzusetzen.

2.3.9 Business continuity management

Im *Management des kontinuierlichen Geschäftsbetriebs* (business continuity management) geht es um die *Entwicklung von Gegenmaßnahmen bei möglichen Unterbrechungen der Geschäftstätigkeit* und die Schutzmaßnahmen für geschäftskritische Verfahren bei Systemausfällen.
Für das Verhindern von Unterbrechungen werden folgende Maßnahmen empfohlen:

- Die Entwicklung eines Prozesses zur Erstellung von business continuity plans innerhalb der Organisation.
- Die Analyse von möglichen Ursachen zur Unterbrechung des Geschäftsbetriebs verbunden mit einer jeweiligen Risikobewertung.
- Das Aufstellen von business continuity plans zu den einzelnen Risiken.
- Das Testen der business continuity plans auf die zu erzielende Wirkung, auftretende Nebeneffekte, usw.

2.3.10 Compliance

Unter der *Einhaltung der Richtlinien* (compliance) werden alle Organisationen darauf hingewiesen, dass sie zu prüfen haben, ob ihre ergriffenen Sicherheitsmaßnahmen mit anderen gesetzlichen Vorgaben in Einklang zu bringen sind, bzw. mit ihnen in Konflikt stehen. Dazu gehören u.a., je nach nationalem Wirkungsbereich der Organisation, das Copyright, Softwarerechte, Datenschutz und Strafverfolgung bei etwaigen Missbrauch.
Auch wird ein Abgleich bzw. gegebenenfalls eine Anpassung der ergriffenen Maßnahmen zur Informationssicherheit mit der ganz oben erwähnten *security policy* empfohlen.

2.4 ISO 17799 in der Realität

Wie schon in der Einordnung 2.2.2 und in der Vorstellung des Inhalts 2.3 des Standards deutlich gemacht, handelt es sich bei ISO 17799 um einen Standard der Empfehlungen für die Umsetzung von Informationssicherheit in Organisationen gibt. Ein besonderes Augenmerk wird dabei auf die an der Informationsverarbeitung beteiligten Menschen, Prozesse und IT-Systeme gerichtet.
Wer jedoch nutzt solche Richtlinien? Welchen Einfluss haben gesetzliche Vorgaben und Bestimmungen auf die Verwendung? Wie setzt man ihn um? Diese Fragen sollen hier geklärt werden.

2.4.1 Nutzer

Sehr allgemein kann man festhalten, dass sich für ISO 17799 theoretisch jedes Unternehmen und jede Behörde interessieren könnte. Sie alle besitzen Strukturen, Informationswege und zu verarbeitende Informationen, die es zu schützen gilt.
In der Praxis werden von dieses Richtlinen jedoch eher große Organisationen angesprochen, die ein dringendes Bedürfnis haben, Sicherheit transparent und strukturiert, auf verschiedenen hierarchischen Ebenen (siehe Abbildung 2.2) abzubilden. Der Aufwand für kleinere Unternehmen wäre überproportional hoch, besonders da dieser Standard keine konkreten sicherheitstechnischen Umsetzungen beinhaltet. Diese müssen zusätzlich eigenständig erarbeitet werden.
Das ISO 17799 für die Umsetzung durch Privatanwender ungeeignet ist, kann man aus den gleichen Gründen ebenfalls schließen.

Neben der Betrachtung, welche Organisationen eher für eine Verwendung des Standards in Frage kommen, kann man sich auch noch ansehen, wer innerhalb der Organisation eher von einer Umsetzung des Standards profitieren würde. Laut [1] würde sich eine Verwendung eher für Personen im Management, also das Unternehmensmanagement, Mitarbeiter im Projektmanagement, die IT-Leitung und IT-Sicherheitsbeauftragte, empfehlen.
Für Mitarbeiter, die innerhalb der für die Informationssicherheit relevanten Bereiche arbeiten, wie zum Beispiel Administratoren oder Revisoren[1], scheint eine Umsetzung weniger sinnvoll zu sein. Sie haben oftmals konkretere Richtlinien für die Durchsetzung der Informationssicherheit - wie zum Beispiel das Grundschutz-Handbuch für den Administrator. Diese sind ihrem Tätigkeitsbereich eher angemessen. Zudem betreuen diese Mitarbeiter meist keine untergeordneten organisatorischen Strukturen, für die sie weisungsbefugt wären. Viele Elemente von ISO 17799 (zum Beispiel der Aspekt der personellen Sicherheit) würden also damit von diesen Mitarbeitern gar nicht umgesetzt werden können.

2.4.2 Gesetze und Vorgaben

Warum sollte eine Organisation, die denkt ihr Sicherheitsmanagement auch ohne ISO 17799 im Griff zu haben, auf den doch scheinbar recht unkonkreten Standard ISO 17799 setzen? Zum Teil weil sie durch gesetzliche Maßgaben dazu bewogen werden.
Allgemein ist zu sagen, dass das Thema Informationssicherheit je nach Herkunftsland der Organisation ganz unterschiedlich gehandhabt wird. Um jedoch einige Beispiele für

[1] Rechnungsprüfer, bzw. Wirtschaftsprüfer

Gesetze und Richtlinien zu erbringen, werden an dieser Stelle einige Gesetze aus Deutschland und den USA aufgeführt. Diese können einerseits dazu führen, dass man auf einen Standard wie ISO 17799 zurückgreift, aber auch das bestimmte Maßnahmen in der Anwendung des Standards eingeschränkt werden (siehe dazu, das im Standard behandelte Thema zur *Einhaltung der Richtlinien* 2.3.10).

Deutschland

Am 1. Mai 1998 ist ein *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* in Kraft getreten. Diese, im Aktien- und GmbH-Gesetz verankerte, Vorschrift fordert die aktive Überwachung und damit Überprüfung von Risiken. Ein Risikomanagement ist somit erforderlich. Genauer besagt *§91 II AktG*, das:

> ...der Vorstand geeignete Massnahmen zu treffen (hat), insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Laut Tele-Consulting GmbH [2] ist mittlerweile anerkannt, dass diese Richtlinie auch für Gesellschaften anderer Rechtsformen maßgebend ist. Weiterhin heisst es dort [2]:

> Damit gehört Risk-Management zu den Sorgfaltspflichten des Vorstandes bzw. Geschäftsführers, über deren Erfüllung er auch Rechenschaft ablegen muss. Diese Rechenschaft ist ohne zuverlässiges Risk-Management nicht zuverlässig erstellbar. Diesbezügliche Versäumnisse können bei prüfungspflichtigen Unternehmen zu einem Versagen des Bestätigungsvermerks führen und der Vorstand/Geschäftsführer ist im Schadensfalle den Anteilseignern persönlich haftbar.

Da das Risikomanagement ein wichtiger Bestandteil von ISO 17799 ist, und hier auch auf andere Standards zur Risikobewertung/-analyse (z.B. ISO 13335) zurückgegriffen werden kann, bietet sich eine Verwendung durchaus an.

In Deutschland haben unter anderem auch der *Datenschutz*, der *Arbeitnehmerschutz*, die *Verpflichtungen der Banken und Finanzdientsleister* und die damit verbundenen Gesetze, einen deutlichen Einfluss auf die Möglichkeiten aber auch Begrenzung der Informationssicherheit. So dürfen zum Beispiel Arbeitnehmer in Deutschland nicht ohne weiteres per Video am Arbeitsplatz überwacht werden, selbst wenn es augenscheinlich der Informationssicherheit einer Organisation dienen könnte.

USA

Die Tabelle 2.2 listet einige gesetzliche Regelungen auf, welche die Informationssicherheit von Organisationen in den USA betreffen.

Einige dieser Gesetze, wie der Gramm-Leach-Biley Act oder der Health Insure Portability and Accountability Act, legen fest, dass konkrete Maßnahmen zu treffen sind um den Missbrauch im Umgang mit Informationen zu verhindern. Diese Gesetze sollen vor allem den neuen technischen Möglichkeiten der Aufbewahrung und der Verarbeitung von Informationen gerecht werden.
Andere Gesetze, wie der Sarbanes-Oxley Act und der Computer Security Act, legen vor

Gesetz	Betroffene	Thema
Computer Security Act of 1987	Firmen	Legt die Verantwortungspflicht der Firmen bei computergestütztem Betrug oder Missbrauch fest.
Gramm-Leach-Biley Act of 1999	Finanzinstitute	Sicherung der Kundendaten.
Health Insure Portability and Accountability Act (HIPAA)	Institutionen im Gesundheitswesen	Sicherung der in elektronischer Form vorliegenden Daten der Patienten.
Sarbanes-Oxley Act of 2002	Firmen	Erweiterung der Verantwortlichkeiten des Managements. Höhere Anforderungen an die Genauigkeit und Vollständigkeit von veröffentlichten finanzwirtschaftlichen Informationen. Verschärft Offenlegungs- und Prüfungspflichten.

Tabelle 2.2: Beispiele für relevante US-amerikanische Gesetze

allen Dingen wert darauf Verantwortlichkeiten festzulegen oder Konsequenzen bei Missachtung zu erhöhen, um somit einen korrekten Umgang mit Informationen innerhalb von Organisationen durchzusetzen. Auch diese Gesetze sind in dieser Ausarbeitung zu berücksichtigen, da sie eine Motivation zur Verwendung eines Standards wie ISO 17799 darstellen können.

2.4.3 Umsetzung von ISO 17799

Ein Teil des ISO 17799 Dokuments [3] beschäftigt sich damit, wie der Standard in der Realität am besten umzusetzen sei.
Zuerst sollte eine Organisation ihre Sicherheitsbedürfnisse ermitteln. Dafür gibt es verschiedene Quellen:

- das Abschätzen der Risiken für die Organisation in einer Risikobewertung/-analyse,
- einzuhaltende Gesetze und Richtlinien (siehe 2.4.2),
- bestehende oder geplante Verbindungen mit Vertragspartner,
- und ein Set von Prinzipen, Zielen und Vorraussetzungen der Informationsverarbeitung, welche für den Erhalt der Geschäftstätigkeit notwendig sind.

Wenn die Bedürfnisse ermittelt wurden, sollten Kontrollen gewählt und umgesetzt werden, welche die ermittelten Risiken auf ein akzeptables Maß mindern. Viele Möglichkeiten zur Kontrolle finden sich in ISO 17799 innerhalb der Beschreibung der Überwachungsbereiche. Die Kontrollen müssen jedoch auf die spezifischen Bedürfnisse der Organisation angepasst bzw. für diese erweitert werden. ISO 17799 kann hier nur eine Grundlage bilden.
Bei jeder Einführung und Implementation eines Überwachungsbereichs sollten die „Kosten“ (auch diejenigen ohne konkreten monetären Gegenwert, wie zum Beispiel der Verlust der Reputation durch für Kunden unliebsame Maßnahmen) berücksichtigt werden.

Man muss bei diesem Vorgang stets im Auge behalten, dass es sich bei dem Standard nur um Empfehlungen und Richtlinien handelt. Es kommt auf die Wünsche, Bedürfnisse und Möglichkeiten der betroffenen Organisation an, diesen Standard mehr oder weniger genau umzusetzen. Nichts spricht dagegen aus ISO 17799 Organisations-eigene Richtlinien zur Informationssicherheit zu schaffen.

Abbildung 2.3: Tool zur Evaluierung; Callio Technologies [5]

Viele Beratungsfirmen, welche auch Zertifizierungen anbieten, versuchen den Organisationen die oben genannten Prozesse abzunehmen, und damit ihr Geld zu verdienen. Oftmals wird dabei die Umsetzung von ISO 17799 zusammen mit anderen Standards, wie BS7799 Part 2, angeboten. Damit soll das Beste aus einer Verbindung der „groben“ Richtlinien für die Organisation und den „konkreten“ Vorgaben für die verwendeten Techniken gewonnen werden.
Manche dieser Beratungs- und Zertifizierungsunternehmen, wie Callio Technologies, vertreiben zusätzlich Software 2.3 zur Evaluierung der in den Standards geforderten Kriterien.

2.5 Zusammenfassung

ISO 17799 ist ein Standard zur Durchsetzung und Gewährleistung der Informationssicherheit in vorzugsweise großen Organisationen.
Die im Standard vorgestellten Richtlinien und Empfehlungen betreffen vorallen Dingen die Struktur und Verwaltung und weniger die technischen Aspekte der Organisation. Werden Anmerkungen zu technischen Sicherheitsmaßnahmen gemacht, so sind diese sehr

allgemein gehalten, ohne auf eine konkrete Technologie Bezug zu nehmen.
Die Verwendung dieses Standards erfolgt hauptsächlich durch Organisationen, wie Unternehmen und Behörden, welche das Bedürfnis haben ihre Sicherheitsmaßnahmen transparent, in einem Top-Down-Ansatz, in der gesamten Organisationsstruktur durchzusetzen. Die Ursachen für dieses Bedürfnis können rein wirtschaftlicher Natur sein, wie eine durchgeführte Risikoanalyse oder aber Vorgaben von potentiellen Auftraggebern. Es ist jedoch ebenso denkbar, dass eine Organisation durch gesetzliche Vorschriften zu dieser Maßnahme gezwungen wird.
Die Umsetzung von Sicherheit im Kleinen kann der Standard nicht leisten. Hier muss man von dem was in ISO 17799 allgemein gefordert wird, selbst auf konkrete Umsetzungen (in Hardware, Software, bauliche Maßnahmen, etc.) schließen oder gegebenenfalls entsprechend speziell darauf ausgerichtete Standards hinzuziehen.
Da es neben der Möglichkeit zur selbständigen Umsetzung des Standards auch viele Beratungs- und Zertifizierungsfirmen gibt, die ihre Dienstleistung in diesem Bereich anbieten, kann man davon ausgehen, dass dieser Standard allgemein anerkannt ist. Durch Zusatzangebote, wie softwaregestützte Risikoanalysen, Maßnahmenkataloge und einer Kombination von Sicherheitsstandards, versuchen diese Firmen die oben genannten Schwächen des Standards zu kompensieren.
Man kann festhalten, dass mit ISO 17799 vorallen Dingen den obersten Ebenen einer Organisation ein wirksames und für sie auch nachzuvollziehendes Werkzeug zur vollständigen Durchsetzung der Informationssicherheit mitgegeben wird. Es werden ihnen bekannte betriebswirtschaftliche Kenngrößen genannt mit denen sie rechnen können, auch werden für sie wahrscheinlich verwirrende, technische Details ausgelassen. Informationssicherheit kann mit diesem Standard endlich auch im Bewusstsein des Managements umgesetzt werden und ist damit nicht mehr nur das Anliegen einzelner, kleiner IT-Abteilungen oder Service-Firmen.

Glossar

Availability	siehe Verfügbarkeit
BSI	British Standard Institution. Britische Organisation zur Standardisierung.
Confidentiality	siehe Vertraulichkeit
IEC	International Electrotechnical Commission. Internationale Organisation zur Standardisierung.
Informationssicherheit	Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (engl. information security).
Information security	siehe Informationssicherheit
Integrität	Informationen müssen fehler- und verlustfrei behandelt werden (engl. integrity).
Integrity	siehe Integrität
ISO	International Organization for Standardization. Internationale Organisation zur Standardisierung.
ISO 9000	Quality management systems - Fundamentals and vocabulary. Ein umfangreiches Werk bestehend aus Leitfäden, Normen, Begriffen, und Qualitätsmanagement-Modellen. Zuletzt aktualisiert im Jahr 2000. Neben dem konkreten Standard wird oft als die Kurzform der Werke ISO 9000 - ISO 9004 incl. der Normen DIN 9000 ff., sowie der europäischen Norm DIN EN 9000 ff. verwendet.
ISO 13335	Umfassende Sammlung von fünf Normdokumenten zum Management von Informationssicherheit.
ISO 14000	Environment management systems and standards. Dieser Begriff wird häufig für den Standard ISO 14001 benutzt, steht aber oft auch für eine ganze Familie an Standards (ISO 14001 bis 14050). Die Standards stehen für Unweltmanagement, Umweltmanagementsysteme und Umweltschutz.

ISO 17799	Information technology - Code of practice for information security management. Der Standard umfasst eine Sammlung von Empfehlungen für Informationssicherheitsverfahren und -methoden , die sich in der Praxis bewährt haben (Best Practices). Dieser Standard wird in diesem Artikel betrachtet.
NIST	National Institute of Standards and Technology. US-Amerikanische Organisation zur Standardisierung.
Risikobewertung	Umfasst die Bewertung, bzw. Berechnung, von Gefahren für die Informationen oder Informationsprozesse, sowie die Wahrscheinlichkeit des Gefahreneintritts (engl. risk assessment).
Risikomanagement	Beschreibt den Prozess der Identifikation, Kontrolle und Minimierung, bzw. Eliminierung, von Sicherheitsrisiken, die Informationssysteme betreffen könnten (engl. risk management).
Risk assessment	siehe Risikobewertung
Risk management	siehe Risikomanagement
Verfügbarkeit	Der Zugriff auf Informationen und damit verbundene Optionen ist für autorisierte Personen im vollen Umfang gewährleistet (engl. availability).
Vertraulichkeit	Auf Informationen dürfen nur autorisierte Personen und Prozesse zugreifen (engl. confidentiality).

Literaturverzeichnis

[1] Prof. Dr. Hannes Federrath. *Management der Informationssicherheit Nach ISO 17799*. Lehrstuhl Management der Informationssicherheit , Universität Regensburg, 2003-08-27. http://www-sec.uni-regensburg.de/publ/2003/2003-08-27ISO17799.pdf.

[2] Tele-Consulting GmbH. *Services im Bereich Risk-Management*, 2004-12-13. http://www.tele-consulting.com/download/unternehmen/services-risk_management.pdf.

[3] ISO/IEC. *International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management*. ISO/IEC, 2000-12-01.

[4] National Institute of Standards and Technology (NIST). *ISO/IEC 17799:2000 FAQ*, November 2002.

[5] Callio Technologies. *Präsentation BS7799 / ISO 17799*, 2003-08-11. http://www.callio.com/files/17799_and_secura_en.ppt.

[6] Callio Technologies. *BS7799 / ISO 17799 Solution*, 2004-06-10. http://www.callio.com/files/wp_iso_en.pdf.

3 ITSEC & Common Criteria

H. A. Pham, S. Tabbert

Abstract

In diesem Paper soll ein Überblick über die Entstehung, die Grundlagen und den Aufbau sowie die Funktionsweise von ITSEC und Common Criteria gegeben werden. Des weiteren wird erläutert, wie eine Zertifizierung abläuft.

3.1 Einleitung

Vertraulichkeit, Verfügbarkeit und Integrität von Hard- und Software spielen schon immer in sensiblen Einsatzbereichen wie im staatlichen und militärischen Sektor, bei Banken und Versicherungen eine große und wichtige Rolle. Daher ist es verständlich, dass Evaluierungsorganisationen typischerweise auf amtliche Stellen zurückgehen, die zum Teil ursprünglich für eine Bewertung militärischer oder staatlicher Rechnersysteme zuständig waren. Dazu zählt speziell in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI). Seit 1997 gibt es aber auch private Zertifizierungsstellen. Die Voraussetzung für die Anerkennung von Zertifikaten privater Zertifizierungsstellen ist, dass deren Zertifikate eine dem Sicherheitszertifikat des BSI gleichwertige Sicherheit nachweisen. Vom BSI anerkannte Zertifikate lassen sich anhand des gemeinsamen Logos 'Deutsches IT-Sicherheitszertifikat' erkennen.

Neben der Funktionalität eines IT-Produkts bzw. -Systems ist deren vertrauenswürdige Realisierung ein wesentliches Auswahlkriterium für den Anwender. Um die vertrauenswürdige Realisierung nachzuweisen, werden die IT-Produkte und -Systeme durch eine neutrale Stelle nach objektiven Kriterien evaluiert (Prüfung und Bewertung) und zertifiziert. Das Ziel solch einer Zertifizierung ist es, IT-Produkte / -Systeme hinsichtlich ihrer Sicherheitseigenschaften transparent und vergleichbar zu bewerten. Das schafft: [6]

- einerseits Anwendern Detailinformationen und Orientierungshilfen bei der Auswahl von Produkten zu bieten,
- andererseits den betreffenden Herstellern eine Bestätigung über die Qualität der Sicherheitseigenschaften ihrer Produkte zu geben.

3.1.1 Begriffsdefinition

Im Text werden die Begriffe IT-Produkt bzw. -systeme des Öfteren benutzt, die hier zunächst definiert werden. Ein IT-System ist eine spezielle IT-Installation mit einem definierten Zweck und einer bekannten Einsatzumgebung. Bei einem IT-Produkt handelt

es sich um ein Hardware- und/oder Softwarepaket, das "von der Stange"gekauft und in eine Vielzahl von Systemen eingebaut werden kann. Ein IT-System setzt sich im allgemeinen aus mehreren Hardware- und Software-Komponenten zusammen.

3.1.2 Sicherheitskriterien als (internationaler) Standard

Die Grundlage der Evaluierung und Zertifizierung von IT-Produkten/-Systemen bilden die Sicherheitskriterien. In Deutschland angewandte Kriterienwerke sind die internationalen Common Criteria (CC) und die europäischen ITSEC, wobei die Common Criteria aus den ITSEC, den US-amerikanischen TCSEC/FC (Trusted Computer System Evaluation Criteria ('Orange Book') / Federal Criteria for IT Security) und den kanadischen CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) entstanden sind. Die CC wurden 1996 entwickelt und im Dezember 1999 von der Internationalen Standardisierungsorganisation (ISO) als den Standard ISO/IEC 15408 veröffentlicht. Die CC liegen derzeit in der Version 2.1 vor, die ITSEC seit 1991 in der Version 1.2.

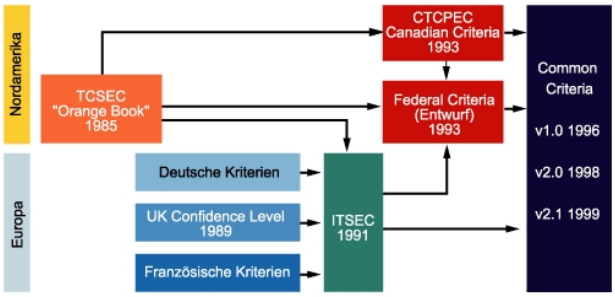

Abbildung 3.1: Entstehungshistorie der CC Quelle: [5]

Da die CC viele Ähnlichkeiten mit den ITSEC haben, ist es deshalb möglich, alle ITSEC-Zertifikate in CC-Zertifikate umzuwandeln. Re-Zertifizierung von ITSEC-Zertifikate in CC-Zertifikate wurden bereits erfolgreich durchgeführt.

3.2 Information Technology Security Evaluation Criteria (ITSEC)

3.2.1 Allgemeines

Im Kritirienwerk ITSEC wird von drei Grundbedrohungen ausgegangen: Verlust der Vertraulichkeit, Verlust der Integrität und Verlust der Verfügbarkeit. Die Bewertung in den ITSEC wird durch eine Zweigliederung realisiert: Auf der einen Seite wird die Sicherheitsfunktionalität bewertet und auf der anderen die Vertrauenswürdigkeit, also die Qualität der Sicherungsmaßnahmen. Dabei wird die Vertrauenswürdigkeit wiederum in Korrektheit und Wirksamkeit aufgeteilt. In den ITSEC findet eine Unterscheidung zwischen IT-Produkten und IT-Systemen statt. Dadurch wird ein neuer Oberbegriff in den ITSEC eingeführt, nämlich der des Evaluationsgegenstand (**EVG**).
Im Zertifikat wird das Ergebnis solch einer Evalution nach ITSEC wiedergegeben. Man erhält:

1. eine Beschreibung der evaluierten *Funktionalität*,

2. eine *Evaluationsstufe* (E0 - E6), welche Aussagen über die Korrektheit, d.h. der Nachweisbarkeit der Qualität, macht und

3. eine Aussage über die *Wirksamkeit* (Widerstandsfähigkeit) der Sicherheitsmechanismen.

3.2.2 Funktionalität

Durch die ITSEC erhält der Antragsteller die Möglichkeit, die zu evaluierende Funktionalität selbst zu bestimmen. Aber es werden auch vordefinierte Funktionalitätsklassen im Anhang A angeboten; doch sind diese widerum mehr als Beispiele zu verstehen. Sowohl im Fall der selbst spezifizierten Funktionen als auch im Fall der vordefinierten Funktionsklassen muss der Antragsteller die Sicherheitsvorgaben für die Evaluation definieren. Die Sicherheitsvorgaben enthalten folgende Aussagen:

- die erwarteten Bedrohungen und Sicherheitsziele,
- die Spezifikation der Sicherheitsfunktion,
- die Definition der erforderlichen Sicherheitsmechanismen und
- der angestrebten Mindeststärke der Mechanismen und der angestrebten Evaluationsstufe.

Die ITSEC bieten dazu Hilfsmittel zur Erstellung dieser Sicherheitsfunktionalitäten an. Die sogenannten "generische Oberbegriffe", [1] diese sind allgemeine anerkannte Begriffe für Sicherheitsfunktionen z.B.: Empfohlene vordefinierte Funktionsklassen, Erläuterungen zur Erbringung der Nachweise zur Korrektheit, etc.

3.2.3 Vertrauenswürdigkeit

Die Vertrauenswürdigkeit eines Evaluationsgegenstandes (EVG) ist das Mass der Qualität der Sicherungsmaßnahmen. Sie wird anhand der Korrektheit (nachweisbare Qualität) und der Wirksamkeit (Widerstandsvermögen) bewertet:

Korrektheit

Korrektheit ist die Eigenschaft eines Evaluationsgegenstands, die aufgeführten Eigenschaften in den Sicherheitsvorgaben des betreffenden Systems oder Produkts korrekt zu implementieren. Bei der Bewertung der Korrektheit werden **Konstruktions**- und **Betriebsaspekte** betrachtet:
Die Bewertung der Korrektheit dieser Aspekte erfolgt in sieben Evaluationsstufen, wobei E0 die niedrigste und E6 die höchste zu erreichende Evaluationsstufe darstellt:

E0: Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.

E1: Die Sicherheitsvorgaben für den EVG und eine informelle Beschreibung des Architekturentwurfs müssen vorhanden sein. Weiterhin sind Funktionale Tests durchzuführen,

[1] Identifikation und Authentisierung, Zugriffskontrolle, Beweissicherung, Protokollauswertung, Wiederaufbereitung, Unverfälschbarkeit, Zuverlässigkeit der Dienstleistung, Übertragungssicherheit

Konstruktionsaspekte	Betriebsaspekte
Entwicklungsprozess:	**Betriebsdokumentation:**
- Anforderungen	- Benutzerdokumentation
- Architekturentwurf	- Systemverwalter-Dokumentation
- Feinentwurf	**Betriebsumgebung:**
- Implementierung	- Auslieferung und Konfiguration
Entwicklungsumgebung:	- Anlauf und Betrieb
- Konfigurationskontrolle	
- Sicherheit beim Entwickler	
- Implementierung	

Tabelle 3.1: Aspekte zur Bewertung der Korrektheit

um die Anforderungen in den Sicherheitsvorgaben nachzuweisen.

E2: E1 + eine informelle Beschreibung des Feinentwurfs. Die Aussagekraft der funktionalen Tests muss bewertet werden und weiterhin muss ein Konfigurationsmodellsystem und ein geeignetes Distributionsverfahren vorhanden sein.

E3: E2 + Die Quellcodes bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen müssen bewertet werden und weiterhin die Aussagekraft dieser Test der Sicherheitsmechanismen.

E4: E3 + ein formales Sicherheitsmodell das Teil der Sicherheitsvorgaben ist. Weiterhin müssen die sicherheitsspezifischen Funktionen, der Architekturentwurf und des Feinentwurf als semiformale Beschreibung vorliegen.

E5: E4 + es muss ein enger Zusammenhang zwischen Feinentwurf und dem Quellcodes bzw. den Hardware- Konstruktionszeichnungen aufgezeigt werden.

E6: E5 + die sicherheitsspezifischen Funktionen und die Beschreibung des Architekturentwurfs müssen in einer formalen Notation vorliegen, die konsistent mit dem zugrundeliegende formalen Sicherheitsmodell ist.

Wirksamkeit

Die Wirksamkeit ist die Eigenschaft eines Evaluationsgegenstands, welche angibt, wieviel Sicherheitsfunktionalität der Evaluationsgegenstand mit seiner tatsächlichen oder vorgesehenen Umgebung bietet. Folgende Kriterien werden untersucht:

Konstruktionsaspekte	Betriebsaspekte
- Eignung der Funktionalität	- Benutzerfreundlichkeit
- Zusammenwirken der Funktionalität	- Bewertung der operationalen
- Stärke des Mechanismus	Schwachstellen
- Bewertung der Konstruktionsschwachstellen	

Tabelle 3.2: Aspekte zur Bewertung der Wirksamkeit

Basierend auf der Schwachstellenanalyse wird ermittelt, wie stark die Mechanismen des Evaluationsgegenstands bzw. der Sicherheitsfunktionen sind. Diese Widerstandsfähigkeit wird als Stärke der Mechanismen in drei Stufen (niedrig, mittel, hoch) angegeben:

Niedrig: Mechanismen bieten Schutz gegen zufälliges unbeabsichtigtes eindringen. Während sie aber von einen sachkundigen Angreifer überwunden werden.

Mittel: Mechanismen bieten Schutz gegen Angreifer mit beschränkten Gelegenheiten und Betriebsmitteln.

Hoch: Mechanismen können nur von Angreifern überwunden werden, die sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher Angriff als normalerweise nicht durchführbar beurteilt wird.

Die Bewertung der Qualität eines evaluierten Evaluationsgegenstandes wird immer als Paar (aus Evaluationsstufe, also Bewertung der Korrektheit der Sicherheitsfunktionalität und der Einstufung der Wirksamkeit der verwendeten Sicherheitsmechanismen) angegeben.

Im Folgenden soll ein Beispiel betrachtet werden: "Das Unix-Derivat AIX4.2 von IBM wurde nach (E3, hoch) evaluiert. Das Bedeutet, dass eine informelle Beschreibung des Architektur-Feinentwurfs vorliegt, dass durch funktionale Tests die Erfüllung der Sicherheitsanforderungen nachgewiesen, und dass die Testergebnisse sowie die sicherheitsrelevanten Teile des Quellcodes und der Hardware bewertet wurden" [3].

3.3 Common Criteria for Information Technology Security Evaluation (CC)

3.3.1 Anwendungsbereich und Zielgruppen

Die CC befassen sich mit dem Schutz von Informationen vor nicht autorisierter Preisgabe, Modifizierung sowie Verlust oder aber auch mit Sicherheitsaspekte, die nicht in diese drei Kategorien passen. Die CC gelten für Sicherheitsmaßnahmen, welche in Hardware, Firmware oder Software enthalten sind. Es gibt insgesamt drei große Zielgruppen der CC. Die erste Gruppe sind die *Anwender*, die ihre Sicherheitsbedürfnisse ausdrücken und prüfen können, ob ein Produkt die geforderten Merkmale erfüllt. Dadurch können unterschiedliche Produkte und Systeme miteinander verglichen werden. Die zweite Gruppe sind die *Entwickler*, denen durch die CC die Möglichkeit geschaffen wird, bei ihrer Vorbereitung und Mitwirkung in der Prüfung ihres Produktes oder Systems sowie bei der Spezifikation der zu erfüllenden Sicherheitsanforderungen zu unterstützen. Die letzte große Gruppe sind die *Evaluatoren*. Für diese Gruppe enthält die CC neben den Kriterien zur Beurteilung der Produkte und Systeme, auch allgemeine Aktionen, die der Evaluator innerhalb einer Prüfung auszuführen hat. Neben diesen drei großen Gruppen sind die CC auch für all jene gedacht, die ein Interesse an IT-Sicherheit haben.

3.3.2 Aufbau der CC

Die CC bestehen aus drei getrennten, aber zusammengehörigen Teilen.

Teil 1 der CC: Einführung und allgemeines Modell

Im ersten Teil wird eine Einführung in die CC gegeben, die allgemeine Konzepte und Prinzipien der IT-Sicherheitsevaluation, Modelle der Prüfung und Bewertung sowie Konstrukte zum Ausdrücken bzw. Auswählen von Sicherheitszielen und Sicherheitsanforderungen beinhalten. Des weiteren werden in den Anhängen dieses Teils die Evaluation von Schutzprofilen (Protection Profile - PP), die Sicherheitsvorgaben (Security Target - ST) und der Evaluationsgegenstand (EVG) definiert.

Eine wesentliche Neuerung bei den Common Criteria ist das Konzept der **Schutzprofile** (PP - Protection Profiles). Die Common Criteria bieten Anwendergruppen und Herstellern die Möglichkeit, die Anforderungen für Produkt-/Systemklassen (z.B. Firewalls, Geldkarten, Betriebssysteme) in Schutzprofilen festzulegen. Das Konzept der Schutzprofile stellt wesentlich mehr Flexibilität zur Verfügung als die vorgegebenen Funktionalitätsklassen der ITSEC. Ein Schutzprofil enthält eine Menge von Sicherheitsanforderungen sowie eine zugehörige Vertrauenswürdigkeitsstufe. Ein Schutzprofil sollte wiederverwendbar sein und die Anforderungen an Produkte oder Systeme zur Erfüllung der funktionalen Schutzziele und der Vertrauenswürdigkeit beinhalten. Ein Schutzprofil bezieht sich auf eine Menge von Produkten und Systemen. Sicherheitsvorgaben erlauben die Darstellung von Sicherheitsanforderungen an einen konkreten Evaluierungsgegenstand und verweisen auf ein Schutzprofil oder direkt auf funktionale oder Vertrauenswürdigkeitkomponenten der CC. Bei Beginn der Evaluation werden die Schutzprofile in Sicherheitsvorgaben integriert. Die Sicherheitsvorgaben selber werden separat vor der eigentlichen Evaluation geprüft. Es soll damit verhindert werden, dass in den Sicherheitsvorgaben Sicherheitsanforderungen an den EVG angeführt werden, die keine Erhöhung der Sicherheit bringen.

Teil 2 der CC: Funktionale Sicherheitsanforderungen

Dieser Teil beschäftigt sich mit den funktionalen Komponenten, Familien und Klassen der CC. Die Sicherheitsanforderungen (Teil zwei) sind hierarchisch aufgebaut und lassen sich wie bereits erwähnt in Klassen, Familien und Komponenten gliedern.
Klassen stellen die allgemeinste Gruppierung von Sicherheitsanforderungen dar. Alle Mitglieder einer Klasse haben dieselbe Zielrichtung, jedoch unterscheiden sie sich in der Abdeckung der Sicherheitsziele. Eine Klasse wird durch einen Kurznamen (drei Zeichen lang) gekennzeichnet, z.B. XXX.
Die Mitglieder einer Klasse werden als Familien bezeichnet. Eine Familie ist dabei eine Gruppe von Sicherheitsanforderungen, die gemeinsame Sicherheitsziele aufweisen. Sie unterscheiden sich aber in ihrer Betonung und Schärfe. Die Kennzeichnung der Familie erfolgt durch den Kurznamen der Klassen, gefolgt von einem Unterstrich und dem drei Zeichen langen Kurznamen der Familie (XXX_YYY).
Die Mitglieder einer Familie werden als Komponenten bezeichnet. Eine Komponente beschreibt dabei eine spezielle Menge von Sicherheitsanforderungen. Zudem stellt eine Komponente die kleinste auswählbare Menge von Sicherheitsanforderungen dar, welche in Strukturen (Schutzprofil, Sicherheitsvorgaben) der CC aufgenommen werden können. Die Komponenten sind aus Elementen aufgebaut, wobei ein Element einer Sicherheitsanforderung entspricht. Die Darstellung der Komponenten erfolgt durch das Familienkürzel, gefolgt von einem Punkt und der jeweiligen Zahl der Komponente. Bei Elementen wird an die Komponentenbezeichnung noch ein Punkt und die Zahl des Elements

drangehängt (XXX_YYY.1). Zwischen Komponenten kann es natürlich Abhängigkeiten geben, falls zum Beispiel eine Komponente alleine nicht ausreicht. Eine vorläufige Zusammenstellung von Komponenten wird Paket genannt. Pakete sollen vor allem den Nutzen der Wiederverwendbarkeit bringen.
Sicherheitsvorgaben sind ein zentrales Dokument, das die Darstellung von Sicherheitsanforderungen an einen konkreten Evaluierungsgegenstand darstellt und die Basis für die Evaluierung / Zertifizierung bildet. Dabei können diese nicht nur auf ein Schutzprofil verweisen, sondern auch direkt auf die Sicherheitsfunktionen oder Vertrauenswürdigkeitskomponenten der CC. Im Teil 2 der CC wird eine umfangreiche Auswahl von beschriebenen Funktionskomponenten für die Beschreibung der Sicherheitsfunktionalitäten detailliert beschrieben. Diese vorgegebenen Funktionskomponenten ermöglichen eine transparente und vergleichbare Definition der Sicherheitsfunktionalität in den Sicherheitsvorgaben. Falls es zu einer geforderten Funktionalität keine vordefinierte Komponente gibt, kann diese auch frei definiert werden.

Abk. Klasse	**Name**	**Anzahl Familien**
FAU	Sicherheitsprotokollierung	6
FCO	Kommunikation	2
FCS	Kryptografische Unterstützung	2
FDP	Schutz der Benutzerdaten	13
FIA	Identifikation und Authentisierung	6
FMT	Sicherheitsmanagement	6
FPR	Privatheit	4
FPT	Schutz der TSF	16
FRU	Betriebsmittelnutzung	3
FTA	EVG-Zugriff	6
FTP	Vertrauenswürdiger Kanal/Pfad	2

Tabelle 3.3: Funktionalitätsklassen

Teil 3 der CC: Sicherheitsanforderungen an die Vertrauenswürdigkeit

Der letzte Teil behandelt die Vertrauenswürdigkeitskomponenten, -familien und -klassen. Hier werden auch die Evaluationskriterien für das Schutzprofil und die Sicherheitsvorgaben sowie die Stufen der Vertrauenswürdigkeit beschrieben. Neben dem Funktionsumfang ist die Bewertung der Vertrauenswürdigkeit eines IT-Produkts/-Systems von entscheidender Bedeutung. Die CC legen im Teil 3 Anforderungen an die Vertrauenswürdigkeit gemäß bestimmter Vertrauenswürdigkeitsstufen (Evaluation Assurance Level EAL1 bis EAL7) fest. Dabei wird die Vertrauenswürdigkeit durch die Prüfung und Bewertung des Evaluationsgegenstandes einschließlich der zugehörigen Entwicklungsdokumentation nachgewiesen. Mit zunehmender Vertrauenswürdigkeitsstufe nehmen dabei die Anforderungen an Umfang und Tiefe der Beschreibung und des Testens zu.
Die Vertrauenswürdigkeitsstufen sind hierarchisch angeordnet, wobei EAL1 unterhalb der Evaluierungsstufe E1 der ITSEC einzuordnen ist und die niedrigste Stufe bildet. Diese Stufe ist entwickelt worden, um den Zugang für Hersteller von Produkten/Systemen zur Evaluierung zu erleichtern. Im Folgenden werden die Vertrauenswürdigkeitsstufen,

wie im CC Kriterienwerk angegeben, kurz charakterisiert:

Stufen	Anforderungen
EAL-1	funktionell getestet
EAL-2	strukturell getestet
EAL-3	methodisch getestet und überprüft
EAL-4	methodisch entwickelt, getestet und durchgesehen
EAL-5	semiformal entworfen und getestet
EAL-6	semiformal verifizierter Entwurf, getestet
EAL-7	formal verifizierter Entwurf, getestet

Tabelle 3.4: Evalualtionsstufen EAL1 - EAL7 (CC)

EAL1 prüft und bewertet das Evaluationsgegenstand (EVG), wie er an Kunden ausgeliefert wird. Unabhängiges Testen auf der Grundlage einer Spezifikation der Sicherheitsfunktionen und überprüfter Handbücher sind in dieser Prüfung enthalten. Eine erfolgreiche EAL1-Evaluation ohne Hilfestellung durch den Entwickler (mit minimalen Ausgaben) soll dadurch beabsichtigt werden. Es bietet einen Zuwachs an Vertrauenswürdigkeit gegenüber einem nicht-evaluierten IT-Produkt /-System.

EAL2 wird von Benutzern angewendet, die eine niedrige bis mittlere Stufe an unabhängig geprüfter Sicherheit fordern. Eine vollständige Entwicklungsdokumentation fehlt und ist in solchen Situationen denkbar, wenn die Sicherheit an Altanwednungen geprüft werden oder der Entwickler beschränkt verfügbar ist. Es bietet einen bedeutenden Zuwachs an Vertrauenswürdigkeit gegenüber EAL1, weil u.a. Schwachstellen analysiert werden und Entwicklertests erforderlich sind.

EAL3 wird von Benutzern angewendet, die eine mittlere Stufe an unabhängig geprüfter Sicherheit sowie eine gründliche Untersuchung des EVG und dessen Entwicklung benötigen. Diese EAL ist "vertrauenswürdiger" als EAL2, weil eine Testabdeckung er Sicherheitsfunktionen vollständiger ist und zusätzliche Verfahrensweisen zur Entwicklung erforderlich sind. Somit entsteht das Vertrauen, dass während der Entwicklung der EVG nicht manipuliert wird.

EAL4 wird von Benutzer angewendet, die eine mittlere oder hohe Stufe unabhängig geprüfter Sicherheit für konventionelle, marktübliche EVG verlangen. Zusätzliche Entwicklungskosten, die die Sicherheit betreffen, übernimmt der Benutzer. Gegenüber EAL3 wächst die Vertrauenswürdigkeit, weil weitergehende und detailliertere Entwurfsbeschreibung, Teilbeschreibungen der Implementierung und verbesserte Verfahren erforderlich sind. Somit entsteht das Vertaruen, dass während der Entwicklung und Auslieferung der EVG nicht manipuliert wird.

EAL5 wird von Benutzern angewendet, die eine hohe Stufe unabhängig geprüfter Sicherheit und eine strenge Entwicklungsmethodik für eine geplante Entwicklung benötigen, mit dem Ziel, dass übermäßige Zusatzkosten durch die Verwendung von Spezialtechniken zur Entwicklung von Sicherheitsfunktionalität nicht entstehen. Diese EAL ist "vertrauenswürdiger" als EAL4, weil semiformale Entwurfsbeschreibungen, eine stärker struktu-

rierte Architektur und eine Analyse der verdeckten Kanäle erforderlich sind. Des weiteren werden weitere Anforderungen an das Entwicklungsverfahren gestellt.

EAL6 ist für die Entwicklung von EVGs dann anwendbar, die unter erhöhten Sicherheitsbedingungen eingesetzt werden sollen. Zudem sollen die Zusatzkosten bei deren Gebrauch die Bedeutung der geschützten Werte rechtfertigen. Die Vertrauenswürdigkeit wächst gegenüber EAL5, weil Analysen umfassender und die Entwicklungsdokumentation deutlicher strukturiert sind. Zudem wird eine systematische Identifikation der verdeckten Kanäle und stärkere Kontrolle der Entwicklungsumgebung sowie ein umfassendes, automatisiertes Konfigurationsmanagement gefordert.

EAL7 ist für die Entwicklung von EVGs dann anwendbar, die unter Hochsicherheitsbedingungen eingesetzt werden sollen. Zudem sollen die geschützten Werte die Zusatzkosten rechtfertigten. Diese EAL ist "vertrauenswürdiger" als EAL6, da die Analysen unter Verwendung formaler Darstellungen noch umfassender sind. Eine formale Übereinstimmung sowie ein umfassendes Testen wird erfordert.

„Die Vertrauenswürdigkeit basiert dabei sowohl auf der Korrektheit der Implementierung der Sicherheitsfunktionen als auch auf deren Wirksamkeit. Auch bei Nachweis der Korrektheit bleibt im Regelfall ein Restrisiko bestehen, da die Abwesenheit unerwünschter Funktionalität nicht unbedingt abschließend nachweisbar ist. Mit zunehmender Vertrauenswürdigkeitsstufe nimmt dieses Restrisiko zwar ab, ein minimales Restrisiko wird jedoch auch bei hohen Evaluationsstufen vorhanden sein. Mit anderen Worten, eine hundertprozentige Sicherheit kann durch ein Zertifikat nicht bestätigt werden, das Risiko wird mit steigender Evaluationsstufe jedoch erheblich reduziert.“ [6]
Nachfolgend werden zwei Zertifizierungsbeispiele betrachtet.
SuSE und IBM haben das Common Criteria Sicherheits-Zertifikat EAL-2 für den SuSE Linux Enterprise Server 8 auf IBM eServer xSeries erhalten. Windows 2000 erhielt Ende Oktober 2002 die Vertrauenswürdigkeitsstufe EAL4, das höchstmögliche Sicherheitsniveau im internationel Vergleich.

3.4 Zertifizierung

3.4.1 Zertifizierungsverfahren

Realisierte IT-Produkte unterschiedlichster Art (z.B. Chipkarten, PC-Sicherheitsprodukte, Betriebssysteme) und IT-Systeme (z. B. Betriebssystem mit Anwendungen) in Software uns/oder Hardware können / werden zertifiziert, sofern Sicherheitsfunktionalität im Zusammenhang mit

- Verfügbarkeit von Daten und Dienstleistungen,
- Vertraulichkeit von Informationen und
- Unversehrtheit / Integrität von Daten

vorhanden ist.
Derzeit liegt international das Interesse der Zertifizierung auf dem Gebiet der Smartcards und Firewalls. Um geeignete Anforderungen an die Sicherheitsfunktionalität und Vertrauenswürdigkeit festzulegen, werden entsprechende Schutzprofile entwickelt und von

den nationalen Behörden registriert. Die Zertifizierung eines IT-Produkts/ -Systems kann vom Hersteller oder Vertreiber eines Produkts oder von einer Bundesbehörde als Anwender bei der Zertifizierungsstelle des BSI beantragt werden. Die Evaluierung der Produkte wird beim BSI selbst oder von akkreditierten und lizenzierten Prüfstellen durchgeführt. Es sind verschiedene Arten des Zertifizierungsverfahrens möglich:

- Zertifizierung eines fertigen Produkts
- entwicklungsbegleitende Zertifizierung
- Re-Zertifizierung eines bereits zertifizierten Produkts
- Maintenance-Verfahren

Entwicklungsbegleitende Zertifizierung

Bei der entwicklungsbegleitenden Zertifizierung wird paralell evaluiert und zertifiziert. Dieses Verfahren bringt den Vorteil, dass das Zertifikat mit dem fast zeitgeleichen Erscheinen einer neuen Produktversion erstellt wird. Zudem können hier noch in der Entwicklungsphase Fehler und Schwachstellen korrigiert und beseitigt werden. Ein Zertifikat kann nicht für eine bestimmte Produktreihe vergeben werden, sondern immer nur für eine bestimmte Version oder ein Release eines Produkts.

Re-Zertifizierung

Heutzutage erscheinen immer neue Versionen innerhalb kürzester Zeit auf dem Markt. Da das Zertifikat keine Gültigkeit auf die neue Version des Produkt mehr besitzt, müssen Re-Zertifizierung durchgeführt werden. Dabei entsteht für den Hersteller den Vorteil, dass nur die sicherheitsrelevanten Änderungen des Produkts geprüft werden und das alte Zertifikat auf die neue Version übertragen wird. Dadurch verkürzt sich das Verfahren erheblich.

Maintenance-Verfahren

Insbesondere im Smartcard-Bereich treten sehr kurze Produktzyklen auf. Um diesen schnellen Veränderungen entgegenzuwirken, finden derzeit international Diskusionen und Abstimmungen über möglichst effiziente Verfahrensweisen zur Aufrechterhaltung eines Zertifikats statt. Das sogenannte Maintenance-Verfahren soll einen kontinuierlichen Sicherheits- und Qualitätsnachweis für ein IT-Produkt (auch nach kleinen Nachbesserungen oder Änderungen) sicherstellen. Es wird den Herstellern bei solch einem Verfahren unter bestimmten Voraussetzungen erlaubt, Teile einer Re-Evaluierung selber durchzuführen. Das Maintenance-Verfahren ermöglicht dem Hersteller, ein zertifiziertes Produkt im Anschluß an die Erstzertifizierung kontinuierlich weiter zu entwickeln und das Zertifikat für Folgeversionen aufrecht zu erhalten.

3.4.2 Ablauf des Zertifizierungsverfahrens

Der Ablauf eines Zertifizierungsverfahrens lässt sich in drei Phasen gliedern:

1. Vorbereitung der Zertifizierung
2. Evaluierung

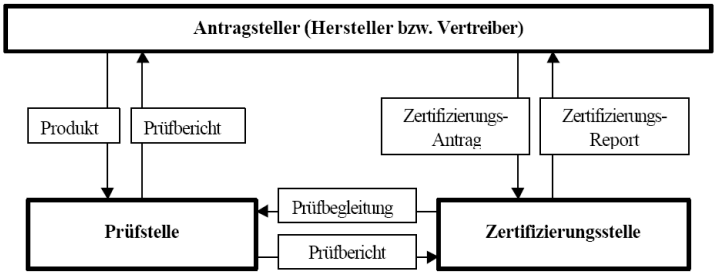

Abbildung 3.2: Ablauf des Zertifizierungsverfahrens [6]

3. Zertifizierung

1. Hier findet i.d.R. ein Beratungsgespräch zwischen dem Hersteller und
In der Vorbereitungsphase findet ein Beratungsgespräch i. d. R. zwischen der Zertifizierungsstelle und dem Hersteller statt. Es wird über das Verfahren und das zu zertifizierende Produkt geeinigt. Dieses Gesprächs beinhaltet neben verfahrenstechnische Details den zeitlichen Ablauf. Ggf. sind Herstellerdokumente etc noch erforderlich. Ziel dieses Gesprächs ist es, die Sicherheitfunktionen des Produkts herauszuarbeiten. Falls ein ähnliches Schutzprofil schon registriert wurde, können diese Sicherheitsfunktionen auch auf dieses abgebildet werden. Danach sucht sich der Hersteller eine Prüfstelle aus und schließt mit dieser Prüfstelle einen Vertrag für die Evaluierung ab. Das erste gemeinsame Evaluierungsgespräch, in dem ein Projekt- und Meilensteinplan aufgestellt wird, beendet die Vorbereitungsphase. Der Hersteller stellt danach einen Antrag auf Zertifizierung.
2. Die Evaluierung erfordert eine enge Zusammenarbeit aller Parteien und wird durch ein Evaluationsteam der Prüfstelle durchgeführt. Es werden Prüfberichte erstellt, die die einzelnen Prüfschritte und die Ergebnisse der Evaluierung beinhalten. Um die Gleichwertigkeit aller Prüfungen durch die Zertifizierungsstelle über das gesamte Verfahren hin zu gewährleisten, werden wesentliche Maßnahmen ergriffen, die hier zu nennen sind: [6]

- Festlegung der Rahmenbedingungen (Vorgehensweise bei der Prüfung, Dokumentationsmuster, Zusammenspiel Prüfstelle / Zertifizierungsstelle)
- Einheitliche und verbindliche Interpretationen der zugrundeliegenden Sicherheitskriterien (CC oder ITSEC)
- Anwendung der zugehörigen Evaluationsmethodologie (CEM[2] oder ITSEM[3])
- Prüfbegleitung: Jede Evaluierung wird mit dem Ziel, eine einheitliche Vorgehensweise und Methodik sicherzustellen, durch Mitarbeiter der Zertifizierungsstelle begleitet. Die Prüfberichte der Prüfstellen werden von diesen Mitarbeitern der Zertifizierungsstelle abgenommen. Es erfolgt hierbei ein Abgleich der Bewertungen mit denen aus anderen Zertifizierungsverfahren.
- Überwachung der Prüfstellen auf Einhaltung aller Rahmenbedingungen (z.B. Wahrung der Vertraulichkeit).

Die CEM als Evaluationsmethodologie für die CC liegt für die Stufen EAL1 bis EAL4 in der referenzierten Version vor. Diese wird in den laufenden Verfahren bereits angewandt.

[2] Common Methodology for Information Technology Security Evaluation
[3] Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik

Für höhere Stufen befindet sich die CEM noch in der Entwicklung. Die Evaluierung endet mit dem Evaluationsendbericht, der von der Prüfstelle verfasst wird. Darin sind die Ergebnisse der Evaluierung dokumentiert. Die Evaluierungsphase endet mit der Abnahme des Endberichtes durch die Zertifizierungsstelle. Auf Grundlage der Empfehlung der Prüfstelle erfolgt von der Zertifizierungsstelle die Bewertung des Produkts/Systems.

3. Auf Grundlage der Empfehlung der Prüfstelle wird das Zertifikat und der Zertifizierungreport bei positivem Ergebnis erstellt. Der Zertifizierungsreport beinhaltet neben Vorbemerkungen und Erläuterungen die Beschreibung der evaluierten Sicherheitseigenschaften des Produkts sowie Hinweise für den Anwender. „Die Aussagen im Zertifizierungsreport und Zertifikat gelten nur unter der Voraussetzung, dass diese Hinweise beachtet werden.“[6] Das Ergebnis des Zertifizierungsverfahrens wird dem Hersteller zugeschickt. Sofern der Hersteller mit der Veröffentlichung keine Einwände hat, wird das zertifizierte Produkt in die BSI-Liste der zertifizierten Produkte aufgenommen. Diese Liste wird regelmäßig aktualisiert und veröffentlicht. Zertifizierungsreporte können i.d.R. beim Hersteller oder über die Webseite des BSI eingesehen werden.

3.4.3 Zeitverhalten und Kosten

„Die Länge des Verfahrens der Evaluierung und Zertifizierung kann - in Abhängigkeit von der Komplexität des Produkts und der angestrebten Evaluationsstufe - stark differieren. Bei einem PC-Sicherheitsprodukt sind i. d. R. 3 Monate, bei einem mittleren Betriebssystem 9 - 12 Monate für eine Erstevaluierung anzusetzen.“[6] Die Kosten für eine Evaluation liegt zwischen 50.000 und mehreren Millionen US-Dollar [8]. Bei guter Entwicklungsmethodik und -dokumentation des Herstellers lässt sich viel Zeit sparen.

3.5 ITSEC vs. CC

Wie die ITSEC erlauben die CC eine getrennte Prüfung und Bewertung der Funktionalität und der Vertrauenswürdigkeit. Die CC bieten mit etwa 150 detaillierten Funktionalitätskomponenten sehr viel konkretere Funktionalitätskriterien als die ITSEC. Dennoch können wie bei den ITSEC auch weitere sicherheitsspezifische Funktionen evaluiert werden, die nicht explizit in den Kriterien aufgelistet sind. Basis für die Vertrauenswürdigkeitsbewertung sind sieben (ITSEC: sechs) Vertrauenswürdigkeitsstufen, die inhaltlich etwa den E-Stufen der ITSEC entsprechen:

ITSEC	E0	---	E1	E2	E3	E4	E5	E6
Common Criteria	---	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7

Abbildung 3.3: Vergleich der Vertrauenswürdigkeitsstufen von ITSEC und CC

Grundlagen der Evaluation sind wie bisher die Sicherheitsvorgaben entsprechend den ITSEC. Die CC enthalten Prüfkriterien für die Sicherheitsvorgaben, mit denen evaluiert wird, ob das Sicherheitskonzept dem Sicherheitsproblem angemessen ist. Das Konzept der ITSEC-Funktionalitätsklassen wird in den CC durch die Schutzprofile abgelöst.

3.6 Zusammenfassung

Die ITSEC und die CC sind Kriterienwerke, um IT-Produkte/-Systeme zu zertifizieren. Zertifizierungen können sowohl von staatlichen als auch von privaten Zertifizierungsstellen durchgeführt werden. Da die ITSEC als ein europäisches Werk gelten, sind diese Kriterien - im Gegensatz zu den CC - weltweit nicht anerkannt. Evaluierte und zertifizierte Produkte und System nach den vorgängig beschriebenen Kriterien können dem Anwender eine Hilfe auf dem grossen Markt der Informationstechnik sein, dasjenige Produkt zu wählen, welches seinen Sicherheitsanforderungen genügen soll. Durch die ITSEC und insbesondere die CC sind die Kriterien komplexer und umfrangreicher geworden. Daher bietet die CC beispielsweise nur in der Hinsicht eine Hilfe, wenn der Anwender die Materie versteht. Es ist somit schwieriger geworden die Funktionalität des jeweiligen Produkts/Systems zu beurteilen: Man ist bei den Common Criteria gezwungen das jeweilige Schutzprofil mit den eigenen Sicherheitsanforderungen zu vergleichen. Ein Kaufentscheidung nur anhand des Zertifikationslevels zu fällen, ist unter diesen Umständen nur wenig sinnvoll, beschreibt die Einstufung doch nur die bestandene Prüfung, nicht aber das Mass an Funktionalität, welches das Produkt bzw. System bietet. Immerhin ist mit den Common Criteria ein weltweit anerkannter Standard gesetzt worden, der gerade wegen seiner Offenheit, die die Sicherheitsprofile bieten, wahrscheinlich länger Bestand haben wird.
Bei zertifizierte Produkten/Systemen muss man sich immer im klaren sein, dass eine Zertifikat nie 100%-ige Sicherheit garantiert. Es wird immer ein Restrisiko bleiben. Zwar hat man mit einem Zertifikat, die Gewissheit über die verifizierter Korrektheit eines Produkts/Systems, aber leider garantiert es nicht, dass es beispielsweise gegen unbekannte Attacken geschützt ist. Auch sollte man speziell erwähnen, dass Produkte/Systeme in der Regel in einem größeren Gesamtsystem (Organisation, Umfeld, technische (Teil-) Systeme) stehen und das Prinzip "Jedes System ist so schwach, wie sein schwächster Bestandteil"gilt.

Literaturverzeichnis

[1] BSI. *Common Criteria*. http://www.bsi.de/cc.

[2] BSI. *ITSEC*. http://www.bsi.de/zertifiz/itkrit/itsec.htm.

[3] BSI. *ITSEC*. Oldenbourg Verlag GmbH, München, 2001.

[4] Common Criteria - Official Website. http://www.commoncriteriaportal.org.

[5] Computerwoche. *Common Criteria: TÜV für IT-Sicherheit, 10.05.2004*. http://www.computerwoche.de .

[6] Dipl.-Math. Irmela Ruhrmann, Dr. Thomas Schöller. *IT-Sicherheitszertifikate auf der Grundlage der Common Criteria*. http://www.it-security-area.de/handout/2004/BL_FR_15_00_Schoeller.pdf.

[7] Dr. Vesna Hassler. IT-Sicherheit: Common Criteria. http://www.a-sit.at/informationen/praesentationen/on_010920vh.pdf.

[8] Kai Rannenberg. *Kriterien und Zertifizierung mehrseitiger IT-Sicherheit*. Teubner Verlag, 1998.

4 IT-Grundschutzhandbuch – Baseline Protection Manual

Eldar Sultanow, Joern Hartwig

Abstract

Im folgenden Papier wird auf den grundschutzhandbuchgetreuen Modellierungs- und Umsetzungsprozess von sicherheitsrelevanten Maßnahmen eingegangen werden. Im Vordergrund stehen dabei Richtlinien und Vorschläge, die durch das Grundschutzhandbuch vorgegeben werden. Die korrekte Umsetzung der hier gemachten Anweisungen erfordert die Zuhilfenahme der im Grundschutzhandbuch aufgezeigten Regeln und Maßnahmen.

4.1 Einleitung

Die zunehmende "Verautomatisierung" unserer Gesellschaft bringt zwangsläufig einen stark erhöhten Einsatz von IT-Systemen mit sich. Die Informationstechnologie deckt alle Bereiche des öffentlichen aber auch des privaten Lebens ab. In der Industrie aber auch in der öffentlichen Verwaltung nimmt die Komplexität dieser Systeme ständig zu. Äquivalent entwickelt sich auch das Schutzbedürfnis dieser Systeme. Die systemgesteuerte Verarbeitung und Haltung von Daten verlangt nach angemessenen Schutzmechanismen, da viele, um nicht zu sagen alle Nutzungsarten dieser Systeme auf den reibungslosen und vor allem sicheren Betrieb dieser angewiesen, wenn nicht sogar abhängig von diesem sind. Es lässt sich demnach die Behauptung: „Ein Erreichen der Behörden- und Unternehmensziele ist nur bei ordnungsgemäßem und sicheren IT-Einsatz möglich." [Grundschutzhandbuch] problemlos aufstellen und nachvollziehen. Die Schäden durch Fehlfunktionen in IT-Systemen können unterschiedlichsten Grundfehlerarten zugeordnet werden. Am häufigsten und auch am auffälligsten ist in der Regel der Verlust der Verfügbarkeit. Weitere Grundtypen sind der Verlust der Vertraulichkeit von Daten, der Verlust der Integrität und seit kurzem auch der Verlust der Authentizität als ein Teilbereich der Integrität. Da große, aber auch kleine und mittelgroße Systeme meist nicht 100-prozentig frei von Schwachstellen sind, besteht ein allgemeines Interesse, die verarbeiteten Daten und Informationen zu schützen. Ein angemessener und ausreichender Schutz von enormen Datenmengen ist meist nicht ohne sorgfältig geplante Vorgehensweisen zu realisieren und zu kontrollieren. Begünstigt durch viele Faktoren steigt das Gefährdungspotenzial eines IT-Systems in absehbarer Zukunft, im Verhältnis zur Größe beziehungsweise dem Vernetzungsgrad des jeweiligen Systems, überproportional an. Gründe für dieses überproportionale Wachstum sind unter anderem die wachsende Abhängigkeit mehrerer Systeme voneinander, die Verantwortungsverteilung innerhalb eines Projekts auf meist mehrere Personen (Tendenz steigend), das auf Grund der steigenden sicherheitsrelevanten Informationen unzureichende Wissen der verantwortlichen,

die steigende geforderte Funktionalität und damit auch die Komplexität der Systeme und die weitgehende Öffnung der Systeme für Dritte. (Onlineangebot der Arbeitsagentur mit online-Zugriff auf "systeminterne" Daten.)

4.2 Grundschutz

Das Gefährdungspotenzial lässt sich in vorsätzlich herbeigeführte und durch "zufällige Ereignisse" verursachte Schäden unterscheiden. Zu den "zufälligen Ereignissen" zählen Störungen durch höhere Gewalt, technisches Versagen, Nachlässigkeit und Fahrlässigkeit. Längerfristig betrachtet verursachen diese "zufälligen Ereignisse" den weitaus größten Teil der Schäden. Schäden die auf vorsätzliche Handlungen zurückzuführen sind, sind zwar seltener, aber bei Eintritt häufig sicherheitskritischer als "zufällig" verursachte. Bei beiden Störungsarten kann jeweils dahingehend unterschieden werden, ob die Ursache des Schadens innerhalb oder außerhalb des Systems liegt. Angesichts der vorgestellten Gefährdungspotenziale und der steigenden Abhängigkeit stellen sich für öffentliche oder private Institutionen die entscheidenden Fragen:

- Sicherheitsgrad meines Systems?
- Mögliche IT-Sicherheitsmaßnahmen?
- Konkrete Umsetzung dieser Maßnahmen?
- Wahrung oder Verbesserung des erreichten Sicherheitsniveaus?
- Sicherheitsgrad von vernetzten Kooperationssystemen?

Wichtig für die Beantwortung der Fragen im Einzelfall ist, daß diese nicht ausschließlich unter dem technischen Gesichtspunkt zu beantworten sind. Neben den technischen Aspekten ist auch den organisatorischen, personellen und baulich-infrastrukturellen Aspekten besondere Aufmerksamkeit zuzuwenden. Die Komplexität des resultierenden Szenarios macht die Einführung eines IT-Sicherheits- managements unerlässlich. Dieses Sicherheitsmanagement muss im Stande sein, die Aufgaben zur IT-Sicherheit zu konzipieren, zu koordinieren und deren Umsetzung beziehungsweise Einhaltung zu überwachen. Betrachtet man nun die gebräuchlichen IT-Systeme von Institutionen, so hebt sich eine spezielle Gruppe von IT-Systemen hervor. Systeme dieser Gruppe lassen sich relativ einfach umschreiben:

- Es sind repräsentative IT-Systeme, also keine Individuallösungen.
- Der Schutzbedarf der IT-Systeme bezüglich Vertraulichkeit, Integrität und Verfügbarkeit ist normal.
- Zum sicheren Betrieb der IT-Systeme werden Standard- Sicherheitsmaßnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge benötigt.

Findet man einen konkreten "gemeinsamen Nenner", der die Sicherheitsmaßnahmen für die Systeme der beschriebenen Gruppe beschreibt, so erleichtert das die Beantwortung obiger Fragen für die Gruppe der "typischen" IT-Systeme erheblich. Individualsysteme oder IT-Systeme mit sehr hohem Schutzbedarf die außerhalb dieser Gruppe liegen, können sich dann zwar an den Standard-Sicherheitsmaßnahmen orientieren, bedürfen

letztlich aber einer individuellen Betrachtung. Das vom Bundesministerium für Sicherheit in der Informationstechnologie herausgegebene IT-Grundschutzhandbuch, im Verlauf dieses Textes auch Grundschutzhandbuch genannt, beschäftigt sich umfangreich mit diesen Standard-Sicherheitsmaßnahmen, die ähnlich für jedes IT-System zu beachten sind. Konkret umfasst das IT-Grundschutzhandbuch die folgenden "Haupt"-Kapitel.

- Standardsicherheitsmaßnahmen für typische IT-Systeme mit normalem Schutzbedarf,
- eine Darstellung der pauschal angenommenen Gefährdungslage,
- ausführliche Maßnahmen-beschreibungen als Umsetzungshilfe,
- eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus und
- eine einfache Verfahrensweise zur Ermittlung des erreichten IT- Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs.

Das IT-Grundschutzhandbuch enthält und beschreibt Standardsicherheitsmaßnahmen für typischerweise im alltäglichen IT-Einsatz befindliche Systeme. Neben Standardsicherheitsmaßnahmen finden sich Umsetzungshinweise und Hilfsmittel die der zügigen Lösung von verbreiteten und bekannten Sicherheitsproblemen dienen. Das haupsächliche Ziel ist es, das allgemeine Sicherheitsniveau von IT-Systemen zu erhöhen und die dafür notwendige Erstellung von IT-Sicherheitskonzepten zu vereinfachen. Die im Grundschutzhandbuch genannten Sicherheitsmaßnahmen und Regeln, orientieren sich stark an den zeitgemässen Schutzbedürfnissen der meissten, sich im Einsatz befindlichen, IT-Systeme. Die sonst aufwendig durchgeführten und meist sehr komplexen Analysen der Bedrohungen inklusive ihrer jeweiligen Eintrittswahrscheinlichkeiten entfallen mit der sachgerechten Anwendung des Grunschutzhandbuchs, da lediglich ein Abgleich des vorgeschriebenen "Maßnahmen-Solls" mit dem tatsächlichen "Maßnahmen-Ist" erfolgen muss. Werden auf Grund der durchgeführten Analyse Sicherheitsschwachpunkte identifiziert, können diese mit den jeweilig entsprechenden Sicherheitsmaßnahmen behoben beziehungsweise verhindert werden. Werden die im Grundschutzhandbuch genannten Regeln und Hilfestellungen für die Erstellung und Planung von IT-Systemen befolgt, resultiert in der Regel eine erhebliche Arbeitszeiteinsparung, welche im Allgemeinen eine enorme Kostenersparnis bewirkt. Das Grundschutzhandbuch ist als "weiterentwicklungsfähiges Werk" konzipiert und wird in einem halbjährlichen Rhythmus erweitert. Dadurch kann sicher gestellt werden, daß der Inhalt dem sich ständig aktualisierenden Wissenstand zu aktuellen Sicherheitsproblemen regelmäßig angepasst wird. Bei dieser halbjährlichen Aktualisierung werden Ratschläge von Anwendern des Grundschutzhandbuchs ebenso beachtet und integriert, wie die Forschungsergebnisse vieler spezialisierter Mitarbeiter des Bundesamtes für Informationssicherheit.

4.3 Anwendung des Grundschutzhandbuchs

Die Anwendung des Grundschutzhandbuchs der IT-Sicherheit soll in erster Linie die Durchsetzung und Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus sicherstellen. Dieses wird durch ein geplantes und organisiertes Vorgehen aller Beteiligten

gewährleistet. Grundlage für erfolgreiche Umsetzung von Schutz- und Sicherheitsmaßnahmen ist ein wohlgeplanter Sicherheitsprozess. Der grobe Ablauf eines solchen Prozesses sei an dieser Stelle graphisch veranschaulicht.

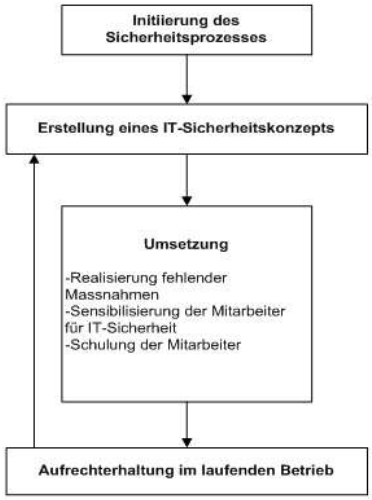

Abbildung 4.1: Sicherheitsprozess

Der durch das Grundschutzhandbuch definierte Sicherheitsprozess erfordert die anfängliche Definition der allgemeinen Sicherheitsziele und der gleichzeitigen Einrichtung eines Sicherheitsmanagement, welches durch erfahrene Personen zu besetzen ist. Die wesentlichen Aufgaben des Sicherheitsmanagements sind die Erstellung eines Sicherheitskonzepts und dessen Realisierung.

4.3.1 IT-Sicherheitsmanagement

Das IT-Sicherheitsmanagement muss ist in die Managementstrukturen einer jeden Organisation eingebettet sein. Im Kapitel 3.0 (IT-Sicherheitsmanagement) des Grundschutzhandbuchs wird systematisch ein Weg aufgezeigt, wie ein funktionierendes IT-Sicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Auf Grund der benötigen Integration in vorhandene Strukturen hat die beschriebene Vorgehensweise lediglich Mustercharakter. Spezifische Ausprägungen sind den jeweilig vorhandenen Gegebenheiten anzuzpassen. Mit der, unter anderem gesetzlich, geforderten Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb kehrt der IT-Sicherheitsprozess regelmäßig zur Erstellung des Sicherheitskonzepts zurück.

4.3.2 IT-Sicherheitskonzept

Im folgenden wird beschrieben, wie ein IT-Sicherheitskonzept im Detail unter Verwendung des IT-Grundschutzhandbuchs erstellt werden kann beziehungsweise dem Grundschutzhandbuch folgend erstellt werden muß. Im Anschluss an die vollständige Erfassung der vorhandenen Informationstechnik, inklusive aller integrierten und vernetzten Komponenten, wird eine Schutzbedarfsfeststellung durchgeführt. Diese soll den tatsächlichen Bedarf eines Schutzes für entsprechende Komponenten beziehungsweise des Gesamtsystem klären. In der folgenden IT-Grundschutzanalyse wird das betrachtete System durch Bausteine des Grundschutzhandbuchs soweit wie möglich nachgebildet. Anschließend

findet ein Soll-Ist-Vergleich zwischen den durch das Grundschutzhandbuch empfohlenen Standardsicherheitsmaßnahmen und den bereits, durch das System, realisierten Maßnahmen statt. Sollten bei der Schutzbedarfsfeststellung Komponenten mit einem hohen oder sehr hohen Schutzbedarf identifiziert worden sein, empfiehlt das Grundschutzhandbuch, nach der IT-Grundschutzanalyse eine ergänzende IT-Sicherheitsanalyse. Ebenso

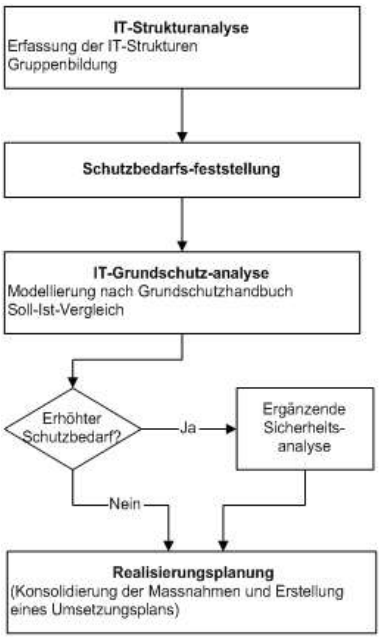

Abbildung 4.2: Sicherheitskonzept

wird diese zusätzliche Sicherheitsanalyse für den Fall, dass im Grundschutzhandbuch keine passenden "Bausteine" identifizierbar sind, dringlichst empfohlen. Den Abschluss der Erstellung eines IT-Sicherheitskonzepts repräsentiert die Erstellung eines Realisierungsplans für die jeweils identifizierten und konsolidierten Sicherheitsmaßnahmen. Im folgenden wird nun auf die einzelnen, in der obigen Abbildung, nochmals verdeutlichten Schritte, kurz eingegangen werden.

4.3.3 Strukturanalyse

Die IT-Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines IT-Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Sie gliedert sich in folgende Teilaufgaben:

- Netzplanerhebung
- Komplexitätsreduktion durch Gruppenbildung
- Erhebung der IT- Systeme
- Erfassung der IT- Anwendungen und der zugehörigen Informationen

Die Strukturanalyse dient als grundlegende Vorbereitung für die eigentliche Erstellung des Sicherheitskonzepts. Es werden, wie bereits erwähnt, alle involvierten Systeme und

Komponenten erfasst und dargestellt. Das grobe Aussehen einer Strukturanalyse kann wie folgt umrissen werden. Um eine graphische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung zu erlangen empfiehlt es sich einen detaillierten Netzplan zu erstellen, welcher die wichtigsten Objekte des Systems beinhaltet.

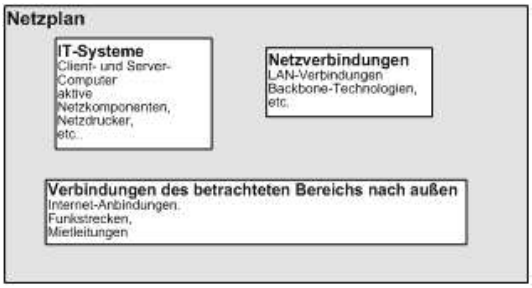

Abbildung 4.3: Bestandteile des Netzplans

Bei der Erstellung des Netzplans ist darauf zu achten, dass für alle Komponenten die jeweiligen Eigenschaften wie z.B. Typ, Funktion, Plattform, Standort, der zuständige Administrator, die Art der Netzanbindung und die zugehörige Netzwerkadresse angegeben sind. Ausserdem sind für die Verbindungen zwischen den Systemen Informationen zur Art der Verbindung, zur Übertragungsrate, zu den verwendeten Protokollen und sonstige relevante Informationen zu ergänzen. Der Netzplan sollte bei jedem Durchlauf des Sicherheitsprozesses auf Aktualität überprüft und gegebenenfalls angepasst werden. Als nächster grosser Arbeitsschritt wird die Optimierung des Netzplanens empfohlen, beziehungsweise vorgeschrieben. Um die Übersichtlichkeit des Plans zu erhöhen, werden bei dieser Optimierung jeweils gleichartige Komponenten zu einer Gruppe zusammengefasst die im Netzplan durch ein einziges Objekt repräsentiert wird. In einer "Komponentengruppe" lassen sich Objekte dann anordnen, wenn sie:

- vom gleichen Typ sind,
- annähernd gleich konfiguriert sind,
- nahezu gleich im Netz eingebunden sind
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen und
- die gleichen Anwendungen bedienen.

Als ein veranschaulichendes Beispiel sei an dieser Stelle die Zusammenfassung von mehreren hundert gleichartigen Workstations zu einem Workstationobjekt, welches als zusätzliche Eigenschaft die Anzahl der includierten Workstations besitzt, genannt. Im nächsten Arbeitsschritt wird eine Liste der vorhandenen und geplanten IT-Systeme in tabellarischer Form aufgestellt. Der Begriff IT-System umfasst dabei nicht nur Computer im engeren Sinn, sondern auch aktive Netzkomponenten, Netzdrucker, TK-Anlagen, etc. Sämtliche Komponenten sind erneut mit ihren Eigenschaften zu representieren. Ein weiterer und auch der letzte Schritt der Strukturanalyse ist die Erfassung der IT-Anwendungen und

der zugehörigen Informationen. Zur Reduzierung des Aufwands werden die jeweils wichtigsten laufenden oder geplanten IT-Anwendungen erfasst. Es ist darauf zu achten, dass zumindest die sicherheitssensiblen IT-Anwendungen des jeweiligen IT-Systems erfasst werden. Um die Erfassung aller sicherheitssensiblen Anwendungen sicherzustellen, sollten bei der Erfassung die Benutzer bzw. die für die IT-Anwendung Verantwortlichen nach ihrer Einschätzung befragt werden. Zur Dokumentation der Ergebnisse wird die Darstellung in tabellarischer Form empfohlen.

4.3.4 Schutzbedarfsfeststellung

Nach der Definition der Schutzbedarfskategorien wird mit Hilfe von typischen Schadensszenarien der Schutzbedarf der jeweiligen Anwendungen bestimmt, um daraus den Schutzbedarf der einzelnen IT-Systeme abzuleiten. Abschließend wird der Schutzbedarf der Übertragungsstrecken und der Räume, welche mit den IT-Systemen im Zusammenhang stehen abgeleitet.

Schutzbedarfsfeststellung für IT- Anwendungen

Die Schutzbedarfsfeststellung definiert für jede im Netzplan erfasste IT-Anwendung inklusive der verwalteten und bearbeiteten Daten den jeweiligen Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit. Entscheidend bei der Festlegung des jeweiligen Schutzbedarfs ist der entsprechende schlimmste eintretbare Schadensfall. Das Grundschutzhandbuch beschränkt sich bei der Festlegung von Schutzbedarf auf die drei Gefährdungsklassen "niedrig bis mittel", "hoch" und "sehr hoch". Die genaue Definition der Schutzbedarfskategorien lässt sich in zwei "Arbeitsschritten" durchführen. Der erste Schritt ist hierbei die Definition von Schutzbedarfskategorien mit anschliessender Zuordnung der jeweiligen Objekte.

- Verstoß gegen Gesetze/ Vorschriften/ Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Außenwirkung und
- finanzielle Auswirkungen.

Im zweiten Schritt werden ausgehend von der Möglichkeit, dass Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-Anwendung oder der zugehörigen Informationen verloren gehen, die maximalen Schäden und Folgeschäden betrachtet.

Schutzbedarfsfeststellung für IT- Systeme

Um den Schutzbedarf eines IT-Systems zu ermitteln, müssen alle Anwendungen genauer betrachtet werden, welche in direktem Zusammenhang mit diesem stehen. Eine Übersicht, welche IT-Anwendungen relevant sind, wurde bereits durch die Erfassung der IT-Anwendungen und der zugehörigen Informationen erstellt und sollte nun für die Schutzbedarfsfestellung des Systems verwendet werden. Alle möglichen Schäden der relevanten IT-Anwendungen in ihrer Gesamtheit müssen betrachtet werden um anhand des

schwerwiegendsten möglichen Schadens einer Anwendung den Schutzbedarf eines gesamten IT-Systems festzustellen. Diese Festlegung orientiert sich also am Maximum-Prinzip beziehungsweise an der worst-case-Regel.

Schutzbedarfsfeststellung für Kommunikationsverbindungen

Nach einer Schutzbedarfsfestellung für die Systeme folgt nun die Festellung des Schutzbedarfs der Vernetzungsstruktur. Grundlage hierfür ist erneut der bereits erarbeitete Netzplan.

Schutzbedarfsfeststellung für IT- Räume

Es muss zunächst eine Übersicht erstellt werden, welche Räumlichkeiten von welchen Systemkomponenten genutzt werden, dabei kommt erneut der bereits erzeugte Netzplan, insbesondere die Eigenschaften der Komponenten bezüglich ihres Standorts, zum Einsatz. Es sollte nun aus den Ergebnissen der Schutzbedarfsfeststellung der jeweiligen IT-Systeme abgeleitet werden, welcher Schutzbedarf für die entsprechenden Räume veranschlagt werden muss. Diese Festlegung des Schutzbedarfs orientiert sich wieder an dem bereits erwähnten maximum-Prinzip. Die tabellarische Erfassung der notwendigen Informationen ist auch hier, der Übersicht wegen, sehr empfehlenswert.

4.3.5 Grundschutzmodellierung

Nachdem alle notwendigen Informationen aus der IT-Strukturanalyse und der Schutzbedarfsfeststellung erfasst und dokumentiert wurden, wird der betrachtete IT-Verbund mit Hilfe der vorhandenen Bausteine des IT-Grundschutzhandbuchs nachgebildet. Das Ergebnis dieser Nachbildung ist ein IT-Grundschutzmodell des entsprechenden Verbunds, welches aus verschiedenen Bausteinen des Handbuchs besteht. Dieses Grundschutzmodell ermöglicht es nun Zusammenhänge zwischen den jeweiligen Bausteinen und den sicherheitsrelevanten Aspekten des IT-Verbunds zu erkennen. Die Abbildung eines IT-Verbundes wird mit Hilfe eines fünf- schichten-Modells realisiert. Die einzelnen Schichten repräsentieren hierbei die unterschiedlichen Sicherheitsaspekte. Diese Schichtenmodell wird im Grundschutzhandbuch wie folgt definiert.

Schicht 1

"...umfasst sämtliche übergreifenden IT Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept."

Schicht 2

"...befasst sich mit den baulich-technischen Gegebenheiten, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. Dies betrifft insbesondere die Bausteine Gebäude, Räume, Schutzschränke und häuslicher Arbeitsplatz."

Schicht 3

"...betrifft die einzelnen IT-Systeme des IT-Verbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die IT-Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Stand-alone-Systemen behandelt. In die Schicht 3 fallen damit beispielsweise die Bausteine Unix-System, Tragbarer PC, Windows NT Netz und TK-Anlage."

Schicht 4

"...betrachtet die Vernetzungsaspekte der IT-Systeme, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Heterogene Netze, Netz- und Systemmanagement und Firewall."

Schicht 5

"...schließlich beschäftigt sich mit den eigentlichen IT-Anwendungen, die im IT-Verbund genutzt werden. In dieser Schicht können unter anderem die Bausteine E-Mail, WWW-Server, Faxserver und Datenbanken zur Modellierung verwendet werden." Die durch den IT-Grundschutz definierte Modellierung besteht nun darin, für alle Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des IT-Verbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein. Beispiele sind einzelne Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten, usw. Das IT-Grundschutzmodell, also die Zuordnung von Bausteinen zu Zielobjekten sollte in Form einer Tabelle mit folgenden Spalten dokumentiert werden:

- Titel des Bausteins
- Gruppenzugehörigkeit
- Hinweise und Begründungen für die Modellierung.

4.3.6 Realisierungsplanung

Voraussetzung für die Erstellung eines Realisierungsplans ist die vorherige Durchführung der Strukturanalyse, der Schutzbedarfsaufstellung und die Modellierung. Neben diesen Voraussetzungen müssen ausserdem die Ergebnisse des Basis-Sicherheitschecks verfügbar sein. Sollte durch die Feststellung eines höheren Schutzbedarfs eine ergänzende Sicherheitsanalyse durchgeführt worden sein, müssen die erarbeiteten Maßnahmenvorschläge ebenfalls vorliegen und in den weiteren Prozess integriert werden. Sollten sich auf Grund der Komplexität des betrachteten Systems eine Vielzahl von nötigen Maßnahmen ergeben, empfiehlt es sich die in sechs Stufen beschriebenen Realisierungshinweise des Grundschutzbuchs zu nutzen. Sind die identifizieren Maßnahmen jedoch beschränkt, kann auf die im folgenden beschriebenen Stufen Eins, Drei und Vier verzichtet werden.

Stufe Eins: Sichtung der Untersuchungsergebnisse

Es werden zu Beginn die fehlenden oder nur teilweise umgesetzten IT-Grundschutzmaßnahmen ausgewertet. Eventuell zusätzliche Maßnahmen werden den vorher betrachteten Zielob-

jekten der Modellierung und den entsprechenden IT-Grundschutz-Bausteinen thematisch zugeordnet.

Stufe Zwei: Validierung der Maßnahmen

Es werden alle noch umzusetzenden IT-Sicherheitsmaßnahmen konsolidiert. Hierbei wird geprüft, welche IT-Grundschutzmaßnahmen möglicherweise entfallen können, da zu realisierende höherwertige IT-Sicherheitsmaßnahmen sie überdecken. Die lediglichen Empfehlungen des Grundschutzhandbuchs müssen für die ausgewählten Maßnahmen in einigen Fällen konkretisiert bzw. an die organisatorischen und technischen Gegebenheiten angepasst werden. Alle identifizierten Sicherheitsmaßnahmen müssen im Anschluss auf Wirksamkeit und tatsächliche Machbarkeit hin überprüft werden. Dabei ist besonders zu beachten, dass keine Maßnahme eine andere einschränkt beziehungsweise behindert. Um im späteren Verlauf die Entwicklung der zu implementierenden Sicherheitsmaßnahmen rückverfolgen zu können, müssen alle Entwicklungs- und Konsolidierungsschritte ausreichend dokumentiert werden.

Stufe Drei: Kosten- und Aufwandsschätzung

Wie allgemein bekannt sein sollte, sind Budgets zur Umsetzung von Sicherheitsmaßnahmen in der Regel begrenzt. Diese Begrenztheit macht eine Einschätzung der auftretenden Kosten nötig. Wichtig dabei ist, dass einmalige Kosten von wiederkehrenden unterschieden werden. Für jede einzelne Maßnahme sollte hierzu aufgelistet werden, welche Investitionskosten und welcher Personalaufwand benötigt wird. Auf jeden Fall ist zu ermitteln, inwieweit die identifizierten Maßnahmen tatsächlich, unter einem vertretbaren finanziellen Aufwand, realisierbar sind. Sollte sich ein unzumutbarer Kostenaufwand herausstellen, muss überlegt werden, durch welche "kostengünstigeren" Ersatzmaßnahmen diese Maßnahmen ersetzt werden können. Wichtig bei der Entscheidung zu Alternativmaßnahmen ist die nachvollziehbare Dokumentation. Geordnet nach ihrem jeweiligen Schutzbedarf sollten die festgestellten Schwachstellen zur Sensibilisierung aller Beteiligten vorgestellt werden. Während Kostenaufstellung sollte eine Entscheidung über das Budget erfolgen. Kann kein ausreichendes Budget für die Realisierung bereitgestellt werden, muss aufgezeigt werden können, welches Restrisiko dadurch entsteht, daß einige Maßnahmen nicht oder nur teilweise umgesetzt werden. Alle weiteren Stufen können erst nach Entscheidung der Leitungsebene über die Tragbarkeit des Restrisikos erfolgen. Hierbei ist entscheidend, daß die Leitungsebene die alleinige Verantwortung für alle Konsequenzen trägt.

Stufe Vier: Festlegung der Umsetzungsreihenfolge der Maßnahmen

Sollte es vorkommen, daß alle aufgezeigten Maßnahmen nicht umgehend durchführbar sind, muss ein entsprechender Zeitplan erstellt werden. Dieser muss sich an den Prioritäten der einzelnen Maßnahmen orientieren. Es ist selbstverständlich daß Maßnahmen mit einer hohen Priorität vor Maßnahmen mit geringerer Priorität abgearbeitet werden. Maßnahmen mit großer Breitenwirkung oder größerem Einfluss auf die Systemsicherheit sind vor anderen gleichrangigen Maßnahmen zu behandeln. Bausteine mit auffallend vielen fehlenden Maßnahmen repräsentieren Bereiche mit vielen Schwachstellen. Sie werden ebenfalls bevorzugt behandelt.

Stufe Fünf: Festlegung der Verantwortlichkeiten

Um eine fristgerechte Umsetzung der Maßnahmen zu garantieren sind die Verantwortungen für die einzelnen Maßnahmen an geeignete, also in jedem Fall qualifizierte Personen zu übertragen. Es ist festzulegen an wen der Abschluss der Realisierung der einzelnen Maßnahmen zu melden ist. Im Normalfall muss diese Meldung an den IT-Sicherheitsbeauftragten erfolgen. Der Fortschritt der Realisierung sollte in regelmäßigen Abschnitten überprüft werden, damit sich die Realisierung nicht verzögert, beziehungsweise, damit mögliche Probleme bei der Umsetzung frühzeitig identifiziert werden können. Der mit diesem Arbeitsschritt fertige Realisierungsplan sollte nach dem Grundschutzhandbuch die folgenden Informationen umfassen:

- Beschreibung des Zielobjektes als Einsatzumfeld,
- Nummer des betrachteten Bausteins,
- Maßnahmentitel bzw. Maßnahmenbeschreibung,
- Terminplanung für die Umsetzung,
- Budgetrahmen,
- Verantwortliche für die Umsetzung und
- Verantwortliche für die Überwachung der Realisierung.

Stufe Sechs: Realisierungsbegleitende Maßnahmen

Zu den realisierungsbegleitenden Maßnahmen zählt unter anderem die Sensibilisierung der von der Maßnahme betroffenen Mitarbeiter. Ein ständiger Abgleich mit den fest definierten Zielen ist unabdinglich

4.4 Zertifizierungen

Das Bundesministerium für Sicherheit in der Informationstechnologie (BSI) zertifiziert nach der europäischen Sicherheitsnorm ITSEC. Da das Grundschutzhandbuch ursprünglich als Anleitung angedacht war, wie ein entsprechender Sicherheitsstandard gewahrt oder erreicht werden kann, wurde ursprünglich auch keine Zertifizierung nach dem Grundschutzhandbuch vorgesehen. Da sich allerdings mehrere Anfragen mit der Frage nach einem "Grundschutzhandbuch-Zertifikat" an das BSI richteten, erarbeitete man in Zusammenarbeit mit der Wirtschaft einen entsprechenden Zertifizierungsprozess. An dieser Stelle erscheint es sinnvoll das Bundesministerium zu zitieren.

> "Aufgrund häufiger Anfragen ... hat das BSI dieses Thema aufgegriffen..." und "...gemeinsam mit Interessenten aus der Wirtschaft ein Zertifizierungsschma für den IT-Grundschutz erarbeitet"

Die Überprüfung wird nach diesen festgelegten "Regeln" von einem durch das Bundesministerium für Sicherheit in der Informationstechnik lizenziertem IT-Grundschutz-Auditor durchgeführt.

4.5 Zusammenfassung

Die hier beschriebene Anwendung des IT-Grundschutzhandbuchs soll nur einen kleinen Überblick verschaffen, um den Einstieg in die Arbeit mit diesem "Regelwerk" zu erleichtern. Ziel war es die Vorteile eines generalisierten und standartisierten Sicherheitsregelwerks zu zeigen. Das das Grundschutzhandbuch in nationalen und internationalen Unternehmen zum Einsatz kommt , zeigt die allgemeine Akzeptanz dieses Regelwerks.

4.6 Ausblick

Das Grundschutzhandbuch wird durch die herausgebende Behörde ständig erweitert und aktualisiert. Aktualisierungen in der Printausgabe, welche über die Bundesdruckerei als "loses Blattwerk" zu beziehen ist, erfolgen in einem halbjährlichen Rhythmus. Rund 400 Mitarbeiter beschäftigen sich mit der Sicherheit von IT-Systemen. Die Aktualität und Relevanz der einfließenden Informationen wird durch eine enge Kooperation mit der Wirtschaft gestärkt. Dieses Zusammenspiel einer Behörde mit der Wirtschaft lässt weiterhin auf die zukünftige Qualität und Aktualität des Grundschutzhandbuchs schließen. Das Grundschutzhandbuch erscheint in den Sprachen Deutsch und Englisch und findet im internationalen, insbesondere im europäischen, Raum großen Zuspruch. Die englische Version ist unter der Bezeichnung "BPM ", wie die deutsche Ausgabe auch , auf den Internetseiten des BSI zu finden.

4.7 Quellenangabe

Als Quelle wurde nur das IT-Grundschutzhandbuch in der Version 2004 verwendet. Diese Ausgabe ist auf Anfrage beim BSI auf CD-ROM erhältlich und wird gegen Unkostenerstattung vom BSI per Post versendet.

5 FIPS 199

Dennis Brockhoff, Alexander Renneberg

Abstract

FIPS publication 199 (Standards for Security Categorization of Federal Information and Information Systems) stellt einen verpflichtenden föderalen Kategorisierungsstandard dar, welcher von der U.S. Regierung ins Leben gerufen wurde. Dieser Standard ist der erste Schritt einer Systematisierung des Schutzes große verteilte Informationssysteme. Es geht um IT-Systeme, die den Betrieb von föderalen Regierungsinstitutionen, sicherstellen. FIPS 199 basiert auf einem einfachen und etablierten Konzept, passende Sicherheitsprioritäten (e.g. Verwundbarkeit) für IT-Systeme zu bestimmen, um anschließend passende Maßnahmen zur Absicherung dieser Systeme anzuwenden.

5.1 Einleitung

Der E-Government Act von 2002 berücksichtigt die stets wachsende Bedeutung von Informationssicherheit für die nationale und ökonomische Sicherheit der Vereinigten Staaten. Die NIST (National Institute of Security Standards) wurde im Rahmen des FISMA (Federal Information Security Management Act) beauftragt, Standards und Richtlinien für das Management von Sicherheitsrisiken zu entwickeln. Dazu zählen die unten aufgeführten Punkte.

- Standards müssen von allen föderalen Institutionen genutzt werden, um alle Informationen und Informationssysteme, die von diesen Institutionen gewartet oder betrieben werden, zu kategorisieren.
- Die Kategorisierung basiert auf Faktoren, die sich auf eine angemessene Stufe für Informationssicherheit berufen. Die NIST schlägt konkrete Richtlinien zur Empfehlung der Kategorisierung der Informationen und Informations-Systeme vor.
- Minimale Informations-Sicherheits-Anforderungen (Management, betriebliche und technische Steuerung und Kontrolle) werden von der NIST ausgearbeitet und überwacht.

Das FIPS 199 Dokument (Federal Information Processing Standards Publication) widmet sich nur dem ersten Punkt, der Entwicklung von Standards für die Kategorisierung von Informationen und Informationssystemen. Der Zweck dieser Kategorisierung liegt darin, einen einheitlichen Rahmen zu schaffen, um Sicherheitsaspekte für die Regierung zu verstehen und zu adressieren. Dazu zählt die Übersicht und das effektive Management von allen föderalen IT Systemen und die Koordinierung von IT-Sicherheitsstandards bei

zivilen und polizeilichen Institutionen, hierzu zählt auch national security, Notfallkräfte sowie Heimatschutzorganisationen.
Außerdem fordert FIPS 199 eine übergreifende Überwachung und konsistente Berichterstattung an den Kongress der Vereinigten Staaten. Dazu zählen das Office of Management and Budget (OMB) und das Senate Comittee on Commerce, wo Senator John McCain aus Arizona den Vorsitz hat. Die Adäquatheit und Effektivität der Informationssicherheits-Richtlinien und praktische Anwendung wird von diesen Institutionen überwacht.
FISMA trägt dem Fakt Rechnung, dass kommerziell entwickelte IT-Sicherheits-Produkte zum Teil schon fortgeschrittene, dynamische, robuste und effektive IT-Sicherheits-Lösungen beinhalten. Diese verfügbaren Marktlösungen sollen bei Regierungsorganisationen eingesetzt werden. Dabei muss überwacht werden, dass falls die Sicherheitslösungen vom privaten Wirtschaftssektor bereitgestellt oder betrieben werden, diese bestimmten Anforderungen genügen müssen. Zudem soll die Auswahl der speziellen Hardware und Software den einzelnen Regierungs-Institutionen überlassen werden. Dazu benötigt es aber einen gesetzlichen Rahmen (dem FISMA), welcher definiert, welche kommerziellen Lösungen eine adäquate Sicherheit bieten.
Einen besonderen Wert wird auf die Absicherung von Systemen gelegt, welche die nationale Sicherheit der Vereinigten Staaten betreffen. Der Begriff "national security system" beschreibt alle Informationssysteme, dazu zählen auch Telekommunikationssysteme, welche von einer Regierungsinstitution oder einem kommerziellen Vertragspartner betrieben oder genutzt werden. Um ein Informationssystem als "national security system" zu bezeichnen, muss es mit geheimdienstlichen Aktivitäten, kryptographischen Vorgängen, Steuerung und Befehlsvorgängen von militärischen Kräften oder hoch-kritischen Waffensystemen in Verbindung gebracht werden.

5.2 National Institute of Standards and Technology (NIST)

Dieser Abschnitt stellt die Instrumente und Institutionen der U.S. Regierung vor, welche hinter dem FIPS 199 Kategorisierungs-Standard stehen. Dazu werden die Aufgaben des National Institute of Standards and Technology (NIST), dessen eingegliedertes Information Technology Laboratory (ITL) und den Federal Information Processing Standards (FIPS) Veröffentlichungen vorgestellt.
Das Hauptarbeitsfeld des ITL, welches ein Teilbereich des NIST darstellt, beschränkt sich auf Aktivitäten im Bereich des IT-Systems Engineering. Dazu zählt die Entwicklung von Verfahren für Tests, Messungen, für Konzeptevaluierungen und anderen technikbezogenen Bereichen, um die Forschung von zukunftsweisenden Technologien zu fördern.
Mit dem Information Technology Management Reform Act, welcher der U.S. Kongress verabschiedete, darf der amerikanische Wirtschaftsminister Standards und Richtlinien für föderale IT-Systeme einführen, welche vom NIST entwickelt wurden. Diese Standards und Richtlinien werden vom NIST als Federal Information Processing Standards veröffentlicht, die regierungs-weit eingehalten werden müssen. NIST entwickelt FIPS, wenn für signifikante und entscheidende Anforderungen der Regierung wie für Security und Interoperabilität keine akzeptablen Industrie- Standards oder Lösungen existieren. Freiwillige Industriestandards werden vom American National Standards Institute (ANSI) verwaltet und mit entwickelt. Sollte kein zufrieden stellender industrieweiter Konsens bzgl. Standards rechtzeitig gefunden werden, wird ggf. ein neuer FIPS entwickelt.
Viele Ausnahmen, die gestatteten, dass Regierungsorganisationen bestimmte FIPS Richtlinien nicht anwenden mussten, wurden im Rahmen des FISMA abgeschafft.

Eine Auswahl von FIPS werden an dieser Stelle vorgestellt. Die FIPS stehen auf den Webseiten des ITL online zur Verfügung.

FIPS_120(27.09.1983) Guideline for Computer Security Certification and Accreditation Standard beschreibt den Prozess der Zertifizierung und Akkreditierung von Computerprogrammen in Bezug auf die technische Evaluierung über die Einhaltung von Sicherheitsanforderungen.

FIPS_9-1(30.11.1990) Congressional Districts of the U.S.FIPS 9-1 spezifiziert eine numerische Struktur zur Abbildung von föderalen Wahlbezirken.

FIPS_188(06.09.1994) Standard Security Label for Information TransferFIPS 197 definiert eine Security Label Syntax für Informationen, welche über Datennetze auf der Anwendungs- und Netzwerk-Schicht übertragen werden.

FIPS_186-2(27.01.2000) Digital Signature Standard (DSS)Standard spezifiziert passenden Algorithmen für Anwendungen, welche digitale, anstatt von hand-schriftlichen, Unterschriften erfordern.

FIPS_197(26.11.2001) Advanced Encryption Standard (AES)FIPS 197 beschreibt kryptographischen symmetrischen Algorithmus, um elektronische Daten zu schützen (cipher und decipher).

5.3 Kategorisierung von Informationen und Informationssystemen

FIPS 199 schreibt eine Sicherheitskategorisierung für Informationen und Informationssysteme vor. Informationen werden nach ihrem Informationstyp eingeordnet. Ein Informationstyp ist einer speziellen Informationskategorie (private, medizinische, finanzielle, untersuchungsrelevante, vertragssensible) zugeordnet, die wiederum von Direktiven oder Gesetzen vorgeschrieben wurden. Die Aufstellungen der Sicherheitskategorien basieren auf der potentiellen Wirkung (Schaden), die eine Institution erfährt, wenn die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Informationssysteme verletzt wird. Dieses bedeutet, es wird die Frage beantwortet, inwieweit die primäre Funktion einer Regierungsorganisation, deren Besitz, deren juristische Verantwortlichkeiten, deren tagesgeschäftlichen Funktionen und deren Mitarbeiter zu beschützen bzw. sicherzustellen, gefährdet wird. Die Sicherheitskategorisierung wird im Zusammenhang mit der Verletzbarkeit und dem Bedrohungspotential, um das Risiko für eine Organisation zu bewerten, aufgestellt.

5.4 Definitionen

Das FISMA definiert den Begriff der Informationssicherheit (information security). "information security" bedeutet Informationen und Informationssysteme vor nicht-autorisierten Zugriffen, der Nutzung, der Herausgabe, der Störung, der Modifizierung und der Vernichtung zu schützen. Die FISMA schreibt drei zu berücksichtigende Sicherheitsfaktoren für Informations-systeme vor.

- Vertraulichkeit (Confidentiality) Vertraulichkeit bedeutet die Sicherstellung von Autorisierungseinschränkungen auf Informationszugriff und Veröffentlichung, um

die persönliche Privatsphäre und institutionsgeheime Informationen zu schützen. Eine Verletzung der Vertraulichkeit resultiert in einer nicht-autorisierten Herausgabe von Informationen.

- Integrität Integrität beschreibt die Absicherung eines IT-Systems gegen unsachgemäße Modifizierung und Vernichtung von Daten, dazu zählt die Sicherstellung von Non Repudiation und Authentifizierung. Eine Verletzung der Integrität resultiert in einer nichtautorisierten Modifizierung oder Vernichtung von Informationen.

- Verfügbarkeit (Availability) Verfügbarkeit bezeichnet die Zusicherung von rechtzeitigen und zuverlässigen Zugriff und Nutzung von Informationen. Eine Verletzung der Integrität resultiert in der Störung auf Zugriff und Nutzung von Informationen und Informationssystemen. Das Prinzip der Verfügbarkeit ist eng mit dem Themenbereich "Safety" verbunden. FIPS 199 adressiert die vorsätzliche Korrumpierung der Verfügbarkeit und nicht softwaretechnische Fehler, die auch ohne fremde Einwirkung zu einer Beeinträchtigung der Verfügbarkeit führen können.

5.5 Potentielle Wirkung auf Institutionen und Individuelle

Drei unterschiedliche "potential impact" Stufen wurden für eine Verletzung der Sicherheit (Verlust von Vertraulichkeit, Integrität und Verfügbarkeit) definiert. Die Anwendung dieser Definitionen muss im Gesamtkontext jeder einzelnen Institution und im Gesamtkontext der nationalen Sicherheit (national security) getroffen werden.

- Potentielle Wirkung - NIEDRIG Der unautorisierte Zugriff und die Veröffentlichung von Informationen hat beschränkt nachteilige Auswirkungen auf OAI (Betrieb der Anlagen von Institutionen oder Individuen). Eine beschränkt nachteilige Auswirkung bedeutet, dass eine Absinkung der übergeordneten Fähigkeit einer Institution eingetreten ist. Allerdings können die primären Aufgaben einer Institution noch ausgeführt werden, doch die Effektivität ist in Teilen eingeschränkt. Der Besitz einer Institution ist nur unerheblich gefährdet. Die finanziellen Schäden halten sich in Grenzen.

- Potentielle Wirkung MODERAT Der unautorisierte Zugriff und die Veröffentlichung von Informationen hat ernsthaft nachteilige Auswirkungen auf OAI (Betrieb der Anlagen von Institutionen oder Individuen). Eine ernsthaft nachteilige Auswirkung bedeutet, dass eine spürbare Absinkung der übergeordneten Fähigkeit einer Institution eingetreten ist. Allerdings können die primären Aufgaben einer Institution noch ausgeführt werden, doch die Effektivität ist im erheblichen Maße eingeschränkt. Der Besitz einer Institution ist erheblich gefährdet. Finanzielle Schäden treten in jedem Fall auf. Das Leben von Menschen ist allerdings nicht in Gefahr.

- Potentielle Wirkung - HOCH Der unautorisierte Zugriff und die Veröffentlichung von Informationen hat katastrophal nachteilige Auswirkungen auf OAI (Betrieb der Anlagen von Institutionen oder Individuen). Eine katastrophal nachteilige Auswirkung bedeutet, dass nicht nur eine Absinkung der übergeordneten Fähigkeit einer Institution eingetreten ist, sondern auch dessen primären Aufgaben nicht mehr ausgeführt werden können. Als Resultat ist eine katastrophale oder signifikante negative Auswirkung auf Menschenleben und den Besitz der staatlichen Institution zu erwarten.

5.6 Anwendung der Kategorisierung auf Informationstypen

Die Sicherheitskategorie eines Informationstypen können mit Nutzer und System-Informationen assoziiert werden. Zu Systeminformationen gehören z.B. Network Routing Tables, Passwortdateien, Kryptographie-Schlüssel-Informationen. Diese müssen auf im Besonderen auf der Stufe geschützt werden, wo die hoch-kritischen Informationen bearbeitet, gespeichert oder diese vom Informationssystem übertragen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen abzusichern. Die Kategorisierung der Informationstypen kann als Eingabe für die Kategorisierung von Informationssystemen genutzt werden. Um die korrekte Sicherheitskategorie einem Informationstypen zuzuordnen, muss die potentielle Wirkung für jeden Sicherheitsfaktor (Vertraulichkeit, Integrität, Verfügbarkeit) ermittelt werden. An dieser Stelle wird das generelle Format für die Benennung der Sicherheitskategorie SC vorgestellt.

SC Informations Typ = {(Vertraulichkeit, Wirkung), (Integrität, Wirkung), (Verfügbarkeit, Wirkung)} Dabei können an der Stelle "Wirkung" die Werte NIEDRIG, MODERAT oder HOCH eingesetzt werden. Darüber hinaus ist auch bei dem Sicherheitsfaktor Vertraulichkeit der Wert NICHT ANWENDBAR gültig.
Als erstes Beispiel fungiert eine Institution, welche öffentliche Informationen auf deren Web Server bereitstellt. Für den Faktor Vertraulichkeit existiert für diese Institution keine negative Auswirkung. NICHT ANWENDBAR wird daher ausgewählt. Die Institution folgert, dass die potentielle Wirkung bei einem Verlust der Integrität und der Verfügbarkeit als MODERAT einzustufen ist.

SC Öffentliche Informationen = {(Vertraulichkeit, NICHT ANWENDBAR), (Integrität, MODERAT), (Verfügbarkeit, MODERAT)} Als zweites Beispiel wird eine polizeiliche Institution betrachtet, welche sensible Untersuchungs-Informationen verwaltet. Die Institution stuft die Wirkung bei einem Verlust der Vertraulichkeit wegen der Geheimhaltungsabsicht als HOCH ein, den Verlust der Integrität als MODERAT und den Verlust der Verfügbarkeit auch als MODERAT.

SC Untersuchung-Informationen = {(Vertraulichkeit, HOCH), (Integrität, MODERAT), (Verfügbarkeit, MODERAT)}

5.7 Anwendung der Kategorisierung auf Informationssysteme

Um die korrekte Sicherheitskategorie für ein Informationssystem zu beurteilen, müssen im Besonderen die auf dem System genutzten Informationstypen und deren Sicherheitskategorien berücksichtigt werden. Es wird durch FIPS 199 gefordert, dass jeweils der höchste Wirkungswert (NIEDRIG, MODERAT, HOCH) aus allen Informationstypen, allerdings für jeden Sicherheitsfaktor einzeln, für die Kategorisierung des Informationssystem verwendet werden müssen. Das Format für die Sicherheitskategorie richtet sich wiederum nach dem Format, welches bei den Informationstypen verwendet wurde.
Als Beispiel soll ein Energiewerk dienen, welches eine SCADA System (supervisory control and data acquisition) benutzt. SCADA steuert die Verteilung des elektrischen Stroms für große militärische Installationen. Das System besteht aus Echtzeit-Sensor Daten und routinemäßigen administrativen Informationen. Das Management in dem Energiewerk bestimmt, dass die potentielle Wirkung bei einem Verlust der Vertraulichkeit bei den

Sensor Daten NICHT ANWENDBAR ist. Dagegen stuft sie die Wirkung bei Integrität und Verfügbarkeit beiderseits auf HOCH ein. Für die administrativen Daten, die vom System verarbeitet werden, wird für alle drei Faktoren die Stufe NIEDRIG ausgewählt. Die sich daraus ergebenen Sicherheits-Kategorien werden an dieser Stelle aufgelistet.

SC Sensor-Daten = {(Vertraulichkeit, NICHT ANWENDBAR), (Integrität, HOCH), (Verfügbarkeit, HOCH)}

SC Administrative Daten = {(Vertraulichkeit, NIEDRIG), (Integrität, NIEDRIG), (Verfügbarkeit, NIEDRIG)} Aus den Sicherheitskategorien der Informationstypen kann folgende Sicherheits-kategorie für das Informationssystem abgeleitet werden.

SC SCADA System = {(Vertraulichkeit, NIEDRIG), (Integrität, HOCH), (Verfügbarkeit, HOCH)} Die maximalen Werte für die potentielle Wirkung der Informationstypen wurden für das SCADA Systeme jeweils angewendet. Die Leitung des Energiewerkes entscheidet sich nach Aufstellung dieser Sicherheitskategorien, die Wirkung bei Verlust der Vertraulichkeit von NIEDRIG auf MODERAT zu erhöhen, da von einer realistischen Sichtweise eine nicht-autorisierte Herausgabe von System-Level-Informations (administrative Informationen) eine höhere negative Wirkung haben könnte, falls ein Angriff auf das System erfolgt.
Die endgültige Sicherheitskategorie wird an dieser Stelle vorgestellt.

SC SCADA System = {(Vertraulichkeit, MODERAT), (Integrität, HOCH), (Verfügbarkeit, HOCH)}

5.8 FIPS 199 Konformität - Kommerzielle Umsetzung der FIPS 199 Standards

Die in FIPS 199 vorgestellte Kategorisierung trägt nicht dem Fakt Rechnung, welche Art der technischen Umsetzung ein FIPS 199 Sicherheitskriterium erfordert. Zumeist bieten kommerzielle Anbieter Produkte und Tools an, welche die passende Implementierung zur Absicherung von IT Systemen nach den FIPS 199 Kategorien bereitstellen. Dieser Abschnitt stellt kurz vor, welche Lösungen die IT Industrie zum Thema FIPS 199 Konformität entwickelt, und ob diese Lösungen auch wirklich die Vorstellungen und die Vorgaben von NIST/ITL erfüllen.
Das Tool DeviceAuthority Suite von AlterPoint Inc. schreibt in dem diesbezüglichen White Paper sich auf die Fahnen, FIPS 199 Konformität für Netzwerk-Infrastrukturen herzustellen. Die Applikation implementiert Methoden, um Netzwerke zu analysieren und um diese zu steuern. DeviceAuthority Suites Compliance Reports erlaubt es Netzwerk-Administratoren und Security Officers detailierte Log-Dokumente zu erstellen, um die Konformität zu internen Sicherheitsrichtlinien, aber auch zu Industrieanforderungen zu prüfen und herzustellen.
Damit sich das Produkt selbst FIPS 199 compliant nennen darf, listet der Produzent zu jedem Sicherheitsfaktor bestimmte konkrete Umsetzungen auf.

Vertraulichkeit

- Sicheres Data Repository

- Rollen-basierte Authentifizierung und Autorisierung
- Sichere Applikationsschicht-Protokolle (SSH, SCP, HTTPS)

Integrität

- Nachvollziehen wer, was, wo, wann, warum und wie Aspekte in der Netzwerk-Infrastruktur geändert wurden.
- Echtzeit Auffinden und Meldung von Änderungsereignissen
- Regulatory Policy Trackingo: Sofortige Meldung, wenn Komponenten aus dem System herausgenommen werden

Verfügbarkeit

- Standardisierung von Richtlinien, um das Risiko von Netzausfällen, welche aus Konfigurationsfehlern hervorgehen, zu reduzieren
- Versionierung der Konfiguration, um die mean-time-to-repair zu reduzieren
- Automatisierung von kritischen Software Konfigurations-Änderungen bzgl. der Netzwerk Infrastruktur, um Netzwerk-Performanz, Verfügbarkeit und Security zu erhöhen

Das Marketing des Produkts DeviceAuthority Suite zielt darauf ab, das Erreichen von FIPS 199 Konformität als große Anforderung an IT-Systemen zu verkaufen. Allerdings hat ITL sich zum Thema FIPS 199 Konformität in Bezug auf die Auswahl von kommerziellen Anbietern geäußert.
Ein offizieller Newsletter des ITL mit dem Titel Selecting Information Security Products weist Regierungs-Institutionen an, auf welchen technischen Grundlagen IT Sicherheitsprodukte von kommerziellen Anbietern ausgewählt werden sollten. Dabei wird darauf hingedeutet, dass die FIPS 199 Sicherheits-Kategorisierung nur als Startpunkt fungieren kann. Das Draft-Dokument NIST SP 800-36 mit dem Titel Recommended Security Controls for Federal Information Systems enthält Empfehlungen für ein Minimum von Sicherheitskonzepten, die mit den in FIPS 199 definierten Sicherheitskriterien (SC) assoziiert werden können.
Das Dokument NIST SP 800-36 beschreibt die folgenden IT Security Produkt-Kategorien, mit den Typen von Produkten in jeder Kategorie, die Produkt-Charakteristika und die Umgebungsaspekte für jede Kategorie. Bestimmte Produkt-Kategorien könnten auch mehr als einem Sicherheitsfaktor zugeordnet werden. Dabei wurde im Rahmen dieser Ausarbeitung eine eigene Zuteilung zu den Faktoren vorgenommen.

NIST SP 800-36 Auflistung (Produktkategorien zur FIPS 199 Umsetzung)

Vertraulichkeit

- Public Key Infrastructure Systeme, welche kryptographische Schlüsselpaare bereit halten und den Haltern von Schlüsseln mit den öffentlichen Schlüssels assoziieren können.
- Produkte für Identifizierung und Authentifizierung mit Security Tokens, Authentifizierungs Protokolle und biometrische Steuerungssysteme

Integrität

- Produkte für das Aufdecken von Eindringlingen mit Netzwerk-, host und anwendungsbasierten Systemen
- Produkte zur Umsetzung von Firewalls für die Steuerung des Netzwerkverkehrs zwischen Netzen oder zwischen einem Host und einem Netz
- Forensische Systeme, welche rechnerbasierte Nachweise identifiziert, schützt, extrahiert und dokumentiert
- Produkte für das nichtrekonstruierbare Löschen und Modifizieren von Daten

Verfügbarkeit

- Produkte zum Schutz vor manipulierten und gefährlichen Quellcode mit Code-Scannern, Integritätsprüfern, Verwundbarkeitsanalysen und Blockern von gefährlichem Verhalten.
- Produkte zum Scannen von Verwundbarkeit, welche Server, Workstations, Firewalls und Router für bekannte Schwachstellen untersucht.

Dabei implementiert das Produkt DeviceAuthority Suite hauptsächlich den letzten Punkt (Scannen von Verwundbarkeit) der NIST SP 800-36 Auflistung. Das gesamte Spektrum der relativ abstrakten FIPS 199 Kategorien wird mit dem Tool von AlterPoint Inc. nicht erfasst. Eine vollständige FIPS 199 Konformität erfolgt mit DeviceAuthority Suite nicht.

5.9 Zusammenfassung

FIPS 199 wurde im Gesamtkontext der FISMA Gesetzesvorlage entwickelt, um eine konsistente und übergreifende Kategorisierung von Sicherheitsrisiken herzustellen. Als Grundlage für diese Kategorisierung dient dazu der potentielle Schaden, welcher mit einem Verlust der IT Sicherheit einhergehen kann. Dabei werden nur die Faktoren Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationssystemen betrachtet. Dabei enthält FIPS 199 keinerlei spezielle Anforderungen an IT-Systeme, da FIPS 199 für einen großen Zeitraum angelegt wurde. Im Gegensatz dazu ändern sich die IT Sicherheitskonzepte ständig. Anhand der FIPS 199 Richtlinien können staatliche Institutionen ihre Ausschreibungen an die kommerzielle Industrie kategorisieren. Die kommerzielle Industrie kann damit abschätzen, mit welchem Einsatz und Technologien sie diese IT Systeme absichern müssen.

5.10 Literatur

- DeviceAuthority Suite, Solution Note: Federal Information Processing Standards (FIPS) compliance, AlterPoint Inc.
- Shirley Radack, ITL Bulletin: Selecting Information Security Products, NIST, April 2004
- FIPS Listed by Number, FIPS PUBS
- General Information, FIPS PUBS

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- US E-Government Act, Title III Information Security
- Bert, FIPS 199 A Generell Overview, 2003

6 Towards Security of Integrated Enterprise Systems Management

Dietmar Bremser

Abstract

Dieses Dokument befasst sich mit Wechselwirkungen zwischen den Geschäftsprozessen und der informationstechnische Infrastruktur von Unternehmen, im Jahre 1999 aus betriebswirtschaftlicher Sicht im Papier gleichen Titels beschrieben von Alexander D. Korzyk. Sr., Virginia Commonwealth University[3]. Ziel ist dabei ein ganzheitlicher Ansatz bei der Realisierung eines Software-Systemes zur Verwaltung, Überwachung und Sicherung der heterogenen IT-Systeme in Unternehmen sowie die Durchsetzung von Unternehmenspolitik vermittels eines derart homogenen informatischen Werkzeuges.
Im letzten Kapitel wird der hier vorgestellte Ansatz bezüglich gegenwärtiger Anforderungen diskutiert.

6.1 Die Gegenwart

Die Befragung von gängigen Suchmaschinen der heutigen Zeit bezüglich des im Titel genannten Begriffes ergab etwa 300.000 Treffer[1] und beweist eine Vielfalt vom Software-Lösungen bezüglich des Einsatzes von Werkzeugen zur Unterstützung von Unternehmsprozessen. Allerdings sind diese Lösungen häufig fragmentiert, also nur auf Teilprobleme bedacht und erzeugen damit bei der Umsetzung von Unternehmenspolitik hohen Aufwand und unnötige Hindernisse[15, S. 123]:

> if a company's system is fragmented, its business is fragmented

So kann man den Ergebnissen der Suchmaschine entnehmen, was verschiedene Software-Unternehmen und Berater unter Sicherheit von "Enterprise Systems" verstehen. Das Unternehmen "Bull Evidian" referenziert mit seinem Produkt "AccessMaster NG" Sicherheit ausschließlich als Benutzerverwaltung in verteilten Umgebungen[6], ebenso wie das Unternehmen "BEA Systems Inc."[5] und IBM[12].
Microsoft hingegen zielt auf die Software-Lösungen ihrer Betriebssystem-Familie ab, weshalb eine Sicherheitsarchitektur nach ihrer Auffassung nur die technischen Aspekte der IT-Infrastruktur wie Datenintegrität, -sicherheit und -verfügbarkeit umfasst[11].
C|Net: C|Level Asia[8], symantec sowie Ernest and Young fokussieren nur auf traditionelle Mechanismen wie Firewalls, Intrusion Detection, Virus Protection etc.
Die Folge ist ein Konflikt zwischen dem Software-Engineering und dem Business-Engineering, welcher sich in einer Fülle/Überlast an informatischen Werkzeugen zur Umsetzung

[1] Google, Stand: 12.Oktober 2004

von Unternehmenspolitik, die jeweils aber kaum miteinander kooperieren und/oder nur Teilbereiche eines Problems lösen[9], ausdrückt.
Die Aufzählung verdeutlicht aber auch die Ursachen dieses Konfliktes, nämlich die verschiedenen technischen Abstraktionen der zu lösenden Probleme mit teilweise zu fokussierten Betrachtungswinkeln sowie divergente Sichten auf die Systeme.

Und so nimmt es nicht wunder, dass der "Leidensdruck" von Unternehmen immer stärker wird, wie der "Etre Technology Conference" in Canne zu entnehmen war[14]

> "Enterprises are more exposed than a year ago. The hackers have won!" (Eli Barkat, Managing Director von BRM Capital)
> "You have four or five different point solutions and they don't all work together." (Phillip Dunkelberger, Präsident und CEO von PGP)

Eine andere, unterschätzte Folge ist die Unmöglichkeit der Implementierung einer einheitlichen Unternehmenspolitik.
Die Generierung einer Politik ist häufig ein algebraischer Vorgang, indem sie Elemente einer Menge und deren Eigenschaften bestimmt. Diese Mengenelemente bzw. Objekte werden dann klassifiziert, so dass verbindliche Regeln bezüglich der Interaktion von und den zulässigen Aktivitäten auf den Objekten festgelegt werden. Auf diese Weise werden die lokalisierten Objekte und ihre Eigenschaften in einen Kontext gestellt, also ein Wirkungsbereich bzw. Domäne dieser Regeln festgelegt.
Unternehmen differenzieren bei der Festlegung einer Politik aber nicht zwischen der IT-Infrastruktur und den Geschäftsprozessen[2], sondern sie beziehen sich ausschließlich auf letzere. Folglich hat die IT-Infrastruktur eines Unternehmens sich der Politik unterzuordnen und Realisierung dieser zu unterstützen, wofür die gegenwärtigen Lösungen ungeeignet sind.
Dieser Konflikt ist Thema dieser Ausarbeitung.

Eine Anmerkung: der Begriff des "Enterprise System" findet im Deutschen nur eine sehr umständliche Übersetzung[3]. Deshalb wird hier der originale englische Begriff annotiert.

6.2 Konzept eines integrierten IT-Systemes für Unternehmen

6.2.1 Motivation

In einem historischen Abriss stellt der Autor Korzyk folgenden Beitrag der Informatik für die Steuerung und Verwaltung der Geschäftsprozesse fest, der einerseits in der stetig steigenden Leistung der Hardware und andererseits in der Dezentralisierung der Daten zu verorten ist. Dabei wird der Einsatz informatischer Technologien in Unternehmen vornehmlich von der Optimierung der Kostenkalkulationen und einem steigenden Wettbewerbsdruck getrieben.
Allerdings blieb beim zunehmenden Einsatz dieser Technologie, beginnend bei singularisierten und physisch geschützten mainframes, über Intranetze bis hin zur Utilisierung

[2] Ein Geschäftsprozess ist eine Menge von verbundenen Prozeduren oder Aktivitäten, die gemeinsam ein Geschäftsziel realisieren oder eine Strategie verfolgen, und liefert zu einem gegebenen Input einen Output. Dies geschieht im Kontext einer Organisationsstruktur, die funktionale Rollen und deren Beziehungen festlegt.

[3] wie etwa "Soft- und Hardware-Systeme zur Verwaltung unternehmensinterner Daten sowie Durchsetzung und Überwachung von Unternehmenspolitik"

des Internet vermittels des World Wide Web, die Steuerungssysteme lokal, wohingegen die gesteuerten Prozesse globaler wurden.
Auf diese Weise etablierten sich in den 90'er Jahren des 20. Jahrhunderts sogenannte Systeme des "Enterprise Ressource Planning" (ERP) zur Verknüpfung von IT-Infrastruktur und Geschäftsprozessen. Dieses System stellt der Autor Korzyk dem "Enterprise System Management" (ESM) gegenüber:

ESM ermöglicht die Integration von Daten ausschließlich auf der Ebene des Netzwerkes, indem sie die Verbindung zwischen der IT-Infrastruktur des Unternehmens und des Lieferanten sowie die Konversion der Daten zwischen beiden ermöglicht. Die unternehmensinternen Prozesse bleiben von diesem System unberührt.

ERP bedeutet die direkte Integration der Informationstechnologie in die Geschäftsprozesse, also die Automatisierung und übergreifende Verkettung von Geschäftsprozessen wie etwa dem Einkauf und der Buchhaltung. Dieser strukturierte Ansatz stellt für die meisten Unternehmen ein Problem dar, da sie nicht nur eine tiefgreifende Umstrukturierung ihrer internen Strukturen betreiben, sondern diese nach dem Vorbild des Architekturmodells des Softwaresystems gestaltet müssen und nicht umgekehrt, trotzdem ERP-Systeme häufig modular aufgebaut sind. Die sehr hohen Installations- und Unterhaltskosten sprechen ebenfalls gegen ERP.[15, S. 125].

Die historischen Betrachtungen der Synergien zwischen den informatischen Technologien und den Geschäftsprozessen münden für Korzyk in den folgenden vier Erkenntnissen:

1. die ernüchternden bis katastrophalen Erfahrungen der Unternehmen bei der Implementierung von Enterprise-Resource-Planning-Systemen (ERP)[15, S. 122]
2. die eingangs beschriebene Heterogenität der Software- Lösungen[3, S. 7]
3. das Extranet, also die IT-Systeme der Unternehmensexternen wie Kunden oder Lieferanten, welche über das Internet in das Intranet des Unternehmens eingebunden werden, im weiteren Sinne also eine Utilisierung des Internet als Distributionskanal der Unternehmen[3, S. 4]

   > the extranet creates instant electronic supply chain among suppliers and customers

4. die "theory of power" aus der Managementlehre:

   > control the access on information ... sharing of knowledge requires an integrated Enterprise System Security Management

Das "Extranet" ist dabei für Korzyk der Schlüssel zu einer zeitgemäßen Architektur eines "Enterprise System", die zwangsläufig eine Sicherheitsarchitektur integrieren muss und nicht wie traditionell üblich addiert.
Diese Architektur soll dabei den zwei Paradigmen folgen:

business-process-view: die "Rotation" der Sichtweise auf ein "Enterprise System" (Abb. 6.1) von der traditionellen, auf Ressourcen fokussierten hin zur prozessorientierten, d.h. dass für die Analyse unternehmensrelevanter Information nicht jede einzelne horizontal liegende Ebene des Systems herangezogen wird, sondern dass ein Geschäftsprozess die "tradionellen" Grenzen der technischen Schichten überschreitet und die Applikation die Komplexität des Systems verbirgt

Service-Level-Agreement: die Festlegung von verbindlichen Regelungen innerhalb des Unternehmens für die Benutzung, Verwaltung und Wartung des "Enterprise System", aber auch die Festlegung verbindlicher Vereinbarungen und Garantien für Unternehmensexterne, vor allem beim Zugriff auf unternehmensinterne Informationen, die Behandlung ihrer Daten sowie die Ausführung der durch sie angestoßenen Prozesse bspw. in Form von Liefergarantien

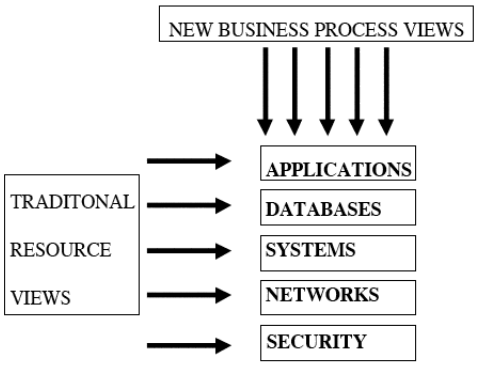

Abbildung 6.1: Wandel der Sichtweise auf IT im Unternehmen: "Business Process View"

6.2.2 Enterprise Systems

Wissenschaftlicher Ansatz bzw. Architektur

Auf der Basis der oben erläuterten Erkenntnisse leitet Korzyk Anforderungen für eine integrierte IT-Infrastruktur ab, die im Gegensatz zu ERP-Systemen eine zu enge Verzahnung der IT-Infrastruktur mit den unternehmensinternen Prozessen vermeiden will. Dabei lokalisiert er drei Aufgabengebiete eines "Enterprise System"(Abb. 6.2), welche die Schnittstellen zwischen den Geschäftsprozessen und einer IT-Infrastruktur darstellen und nennt diese Abstraktion "Enterprise System Architecture" (ESA).

	Enterprise	System	Architecture
Layers	**Database Stack**	**Application Stack**	**Security Stack**
Output Layer	Administration	Job	User
Process Layer	Backup & Recovery	Performance	System
Action Layer	Scheduling	Sizing	Monitoring

Abbildung 6.2: Die drei Aufgabengebiete eines "Enterprise System"

1. Database Stack: erfasst die Daten über die Performanz der Datenbank, aber nicht der Applikationen

2. Security Stack: erfasst die Daten der Sicherheitskomponenten der Datenbank und des Netzwerks, aber nicht der Applikation

3. Application Stack: erfasst und visualisiert die Daten der anderen Stacks, erfasst auch die Daten über die Performanz der Applikationen, welche die Geschäftsprozesse unterstützen; realisiert also die System-Verwaltung der IT-Infrastruktur

Jedes der Aufgabengebiete ist in drei Schichten unterteilt, weshalb Korzyk sie als "Stacks" bezeichnet. Diese drei Schichten sind, von der höchsten zur tiefstliegenden Schicht:

- "output": in welcher Form werden von dem Aufgabengebiet verwertbare Informationen ausgegeben,
- "process": welche funktionalen Aspekte herrschen bei diesem Aufgabengebiet vor,
- "action": welche technischen Aspekte bzw. Operationen soll die jeweilige Funktion des Aufgabengebietes ermöglichen.

Auf diese Weise soll nach Korzyks Willen ein modularer Aufbau von Werkzeugen zur Verwaltung der IT-Infrastruktur möglich sein. Allerdings lässt der Autor den Leser mit Erklärungen der verwandten Termini allein, so dass die oben stehenden Erläuterungen der Stacks teilweise ein Vorgriff auf Korzyks Vorschlag einer "Enterprise System Management Architecture" sind. Im Dokument wird zudem in keiner Weise deutlich, ob Korzyk mit seinem ESA-Modell nun die funktionale Logik der Schichten einer Three-Tier-Architecture meint, wie etwa die Zuständigkeit der Datenbank-Schicht für den Datenzugriff, oder nur die administrativen Sichten auf das System.
Ferner bleibt die Zuordnung zwischen den Aufgabengebiet und dem konkreten Stack undurchschaubar bspw. der Zusammenhang von "Architecture" und "Security Stack".
Deshalb ist seine implizite Forderung an die Informatik, auf Basis dieser Abstraktionen eine "framework" zu entwickeln, schwer zu realisieren.

Verwaltung, Steuerung und Durchsetzung von Unternehmenspolitik

Korzyk folgert aus seinen vier Erkenntnissen (Kap. 6.2.1) und seinem ESA-Konzept (Abb. 6.2), dass eine Metaschicht notwendig ist. Eine Metaschicht, welche die genannten Aufgabengebiete eines "Enterprise System" beherrschbar und anpassbar macht und als "Enterprise System Management" bezeichnet wird:

> a set of tools and processes designed to help control and operate complex technology in applications it supports

Diese Schicht soll gerade wegen der Anforderung der Konnektierung des Extranet mit dem Intranet vermittels eines "Network-Stack" realisiert werden. Dieser umfasst als Netzwerk- und Internet-Management die folgenden Eigenschaften:

1. intelligente Agenten, die auf dem einzelnen System in der Hardware oder Software resident sind, Daten über die Ereignisse sammeln und darauf basierend Meldungen oder Aktionen auslösen
2. ein allgemeines Protokoll zum Austausch von Informationen innerhalb des Netzwerkes und zwischen den einzelnen Systemen
3. die Metapher eines "Cockpits", um die verschiedenen Verwaltungsinformationen über das Netzwerk und die einzelnen Systeme aggregiert auszugeben

Auf Basis dieser Überlegungen konstruiert Korzyk dann eine "Enterprise System Management Architecture" (ESMA), welche zwar alle vormals genannten Aufgabenbereiche bzw. Stacks enthält, aber aus informatischer Sicht seinem eigenen ESA-Modell widerspricht. Denn es fällt im Vergleich der ESA mit der ESMA eine Verkreuzung und

	Enterprise	System	Management	Architecture
Layer	**Network Stack**	**Database Stack**	**Application Stack**	**Security Stack**
Output Layer	Configuration	Administration	Job	User
Process Layer	Distribution	Backup & Recovery	Performance	System
Action Layer	Addressing	Scheduling/Replication	Sizing	Monitoring

Abbildung 6.3: Das "Enterprise System": ergänzt um die Management-Ebene

Verschiebung der Aufgabengebiete und der zugehörigen Stacks auf, bspw. dass der "Application-Stack" im ESA der "System"-Sichtweise zugeordnet ist, aber im ESMA der "Management"-Sichtweise. Problematisch sind diese beiden Modelle deshalb, weil beide die gleiche Architektur repräsentieren, denn das - laut Korzyk modulare - ESA-Modell soll durch Addition einer vereinheitlichten und zentralisierten Administration ein ESMA-Modell ergeben. Es findet also effektiv keine Veränderung der Schichten der Architektur statt, so dass ein Systemtechniker Korzyk zwangsläufig Inkonsistenzen in seiner Modellierung und Begriffsbildung vorhalten muss.
Korzyk will auf diese Weise nicht nur die Administration von IT-Infrastrukturen in Unternehmen vereinheitlichen, sondern auch gleichzeitig ihre Absicherung einschließen:

> the management of an enterprise system necessarily involves the management of the enterprise system as one application out of many applications[3, S. 6]. ... ESMA should insulate management applications from the distributed environment by providing a common GUI, object repository, and event services required to create multiple, unified views of the enterprise infrastructure[3, S. 7].

Auf diese Weise soll erreicht werden, dass die Daten der Ressourcen besser mit den Geschäftsprozessen korreliert werden können und[9]:

> instead of the information technology controlling business, the business process controls business

Allerdings sei jetzt schon bemerkt, dass Korzyks Konzept die Integration von Sicherheitsmechanismen in die IT-Infrastruktur nur tangiert, weil er die Verzahnung von Geschäftsprozess und Informationstechnologie vermeidet.

Implikationen für die Sicherheit

Die vorherigen Kapitel haben ergeben, dass Sicherheit in einem "Enterprise System" sich

1. einerseits in einem Prozessschutz bzw. ein Vertrauen der Unternehmensbeteiligten in das System äußert, indem das System die Geschäftsprozesse stützt sowie die Beherrschung und Konfiguration der heterogenen IT-Infrastrukturen ermöglicht,

2. andererseits in einem Objektschutz bzw. Datensicherheit äußert, welche wegen der beschriebenen Anforderungen im System integriert und nicht beigegeben ist.

Die Anforderungen an den Objektschutz bzw. eines "Enterprise System Security Management" leitet Korzyk direkt aus den Kapabilitäten der ERP-Systeme ab[3, S. 3]:

> 1) Cross-platform capabilities to manage the business environment in multiple instances from a central console require authorizations;
> 2) Auto-discovery of ERP resources requires monitoring;
> 3) Event and resource management requires monitoring audit logs to alert management systems of a perilous condition;
> 4) ERP systems are mission critical and must rely on database backup and recovery procedures; and
> 5) ERP systems have a business process orientation which relies on role based security.

Wegen Korzyks Extranet-Metapher, die entgegen den traditionellen Sicherheitsmechanismen den Zugriff von Externen erlaubt, ist es erforderlich, dass die Sicherheitsmechanismen bzw. ihre realisierenden Dienste miteinander Kontrolldaten über die Benutzer sowie den Zugriff auf Unternehmensdaten und Ressourcen austauschen[3, S. 7]. Deshalb müssen diese auf den Einzelsystemen vorhanden sowie interoperabel sein und im Netzwerk die Ereignisse überwachen, um ferner eine zentral definierte Sicherheitspolitik eines Unternehmens effektiv durchzusetzen[3, S. 8].
Deshalb sind die Sicherheitsmechanismen den Mechanismen zur Administration der IT-Infrastruktur untergeordnet und deshalb in selbige integriert.
Korzyk spezifiziert diese Mechanismen dann wie folgt[3, S. 8]:

Single Sign On: die Anmeldung des Benutzers an seinem lokalen System mit einer Nutzeridentität und -passwort, das System hält aber auf Basis der Sicherheitspolitik Kennzeichnungen der Gruppenzugehörigkeit und Berechtigungen des Nutzer für den Zugriff auf entfernte Dateien, Datenbanken und Verzeichnissen vor;
Kostenersparnis (lt. Korzyk): 50$ pro Benutzer und Jahr

Zentrales Antivirus-Management: um Datenkorruption und -verlust zu vermeiden, werden alle Speicherelemente eines "Enterprise System" kontinuierlich auf Viren überprüft, diese beseitigt und der Weg ihrer Ausbreitung im Unternehmen verfolgt, außerdem ist ein "update-management" sowie eine "virus firewall" vonnöten;
Kostenersparnis (lt. Korzyk): 203$ pro Benutzer und Jahr

unitary logon: Benutzer können sich an jedem entfernten Rechner eines Unternehmens anmelden und jede dort befindliche Applikation ausführen, für die sie autorisiert sind, ist effektiv eine Erweiterung des "Single Sign On" unter dem Aspekt des Prozessschutzes,
Kostenersparnis (lt. Korzyk): nicht angegeben

Kontrolle und Ereignisauslösung: alle sicherheitsrelevanten Ereignisse werden von "intelligenten Agenten" des "Enterprise Systems" global überwacht und Verletzungen der Sicherheitspolitik werden von ihnen behandelt und nötigenfalls an den Sicherheits-Administrator gemeldet;
Kostenersparnis (lt. Korzyk): 87$ pro Benutzer und Jahr

Auf diese Weise soll dann Sicherheit in die gesamte IT-Infrastruktur integriert werden, also auf den einzelnen Systemen, den Applikationen, Datenbanken, etc. sowie die Extranet-Metapher in die IT-Infrastruktur hineingetragen werden, so dass den Unternehmen die Transformation von der industriellen Logik der Automatisierung zur informationellen Logik der Wissensteilung möglich wird.

6.3 Kritik des Papieres von Korzyk

Das Konzept von Korzyk ist wegen seinem Fokus auf das Extranet ausschliesslich informationszentriert und orientiert sich an dem von "Computer Associates" ins Leben gerufenen Projekt "MERIT: Maximizing Efficiency of Resources in Information Technology", das vor allem auf die Beschleunigung des Datendurchsatzes in der IT-Infrastruktur von Unternehmen[15, S. 121,125], der Beseitigung von Kommunikationsbarrieren und die Optimierung der Medien hinsichtlich einer möglichen Äquivokation abzielt.
Außerdem wird aus den vorhergehenden Kapiteln ersichtlich, dass Korzyk mit seiner "management toolbox" nur eine zusätzliche technische Schicht aufsetzt, wobei sein erklärtes Ziel, nämlich die Integration von Sicherheitsmechanismen in die IT-Infrastruktur und damit auch ihre umfassende Absicherung, auf der Strecke bleibt, weil er nur auf die (Kosten-) Optimierung des administrativen Aufwands abstellt.
Die folgende Tabelle soll die Ziele (Kap. 6.2.2, [3, S. 3, Absatz 2]) und Lösungsvorschläge Korzyks (Kap. 6.2.2) sowie die aktuell notwendigen Sicherheitsmechanismen gegenüber stellen, um die Inkonsistenzen von Korzyks Papier zu verdeutlichen:

Ziele Korzyks	**Vorschlag Korzyks**	**aktuelle Erfordernisse**
zentrale, autorisierte Steuerung der heterogenen Ressourcen	Sammlung aller administrativen Aktivitäten in einem Werkzeugkasten mittels einer homogenisierten Benutzerschnittstelle(Kap. 6.2.2)	"divide et impera": Zerlegung und Dezentralisierung der administrativen Autorität über alle Schichten einer IT-Infrastruktur
Überwachung der physischen Existenz von Ressourcen	ausschließlich logische Lösung mittels sogenannter, noch zu erforschender intelligenter Agenten	physische Absicherung der Ressourcen, Schutz vor administrativen bzw. horizontalen Angriffen
Ereignis- und Ressourcenverwaltung inklusive Melde- bzw. Warnsystem	intelligente Agenten im Netzwerk, interferiert mit vorgenanntem Punkt	Kapselung der einzelnen Systeme mittels Integration von interoperablen Sicherheitskomponenten
Sicherungskopie und Wiederherstellung der Datenbank	keine Vorschläge, stellt auf den Mechanismen der heterogenen Ressourcen ab	obsolet: in der Gegenwart in den Datenbanksystemen realisiert
Orientierung am Geschäftsprozess mittels rollenbasierten Sicherheitsmodells	Single Sign On, Unitary Logon: kollidiert mit Zentralisierung der administrativen Aktivitäten	"divide et impera"

Absicherung des Netzwerkes	Zentrales Anti-Virus-Management(?), "Internet-Management"(?) bspw. VPN[3, S.4, Kap. 3.1]	Markierung der Datenpakete mit Kontextinformationen, um sicherheitsrelevante Ereignisse verorten zu können

Das Problem von Korzyks Konzept lässt sich wie folgt subsumieren:
Korzyk stellt die gesamte Sicherheitspolitik auf der Benutzeridentität ab und verlässt sich auf die - möglicherweise inexistenten oder leicht zu kompromittierenden - lokalen Sicherheits- und Verwaltungsmechanismen der heterogenen Ressourcen. Dies verlangt geradezu nach einer Kapselung der einzelnen Systeme, so dass überhaupt effektive Mechanismen zur Behandlung von Ereignissen auch bei Missachtung der Warnmeldungen durch die administrative Autorität vorhanden sind, z.B. in der Form dass ein System sich durch Einstellung der Aktivität physisch schützt.
Korzyk widerspricht mit seinen Vorschlägen zur Benutzerautentifizierung seinem Ziel der rollenbasierten Sicherheitsmechanismen, weil ein "Single Sign On" auf dem gegenseitigen Vertrauen von Applikationen und nicht einer Benutzeridentität mit abgestuften Rechten basiert. Seine Interpretation des "Single Sign On" entspricht zudem den traditionellen einstufigen Sicherheitsmechanismen von Betriebssystemen.
Außerdem bleibt die Komplexität heterogenen Ressourcen der administrativen Autorität mittels seiner "management tools" verborgen, aber nicht dem Benutzer, was wiederum Angriffsmöglichkeiten bspw. durch eine unbemerkte Installation einer schädlichen Applikation eröffnet.
Weiterhin überlasst Korzyk dem Netzwerk mittels nicht näher beschriebener bzw. als Forschungsempfehlung verklausulierter intelligenter Agenten alias "neugents"[3, S. 9],[2] die Durchsetzung einer Sicherheitspolitik und ignoriert dabei, dass dem Netzwerk der Kontext der transportierten Daten fehlt. Das Netzwerk kann ebenso wie die intelligenten Agenten nicht zwischen schädlichen und unschädlichen Daten unterscheiden. Denn einerseits steht beiden das Wissen um die Pakete nur in begrenztem Maße zur Verfügung, also ein Anti-Viren-Agent kann Hacker-Angriffe wegen der fehlenden typischen Signatur nicht erkennen, und andererseits müsste der Agent oder "das Netzwerk" die Nutzdaten der Pakete einsehen, was bei verschlüsselten Nutzdaten unmöglich ist.
Einen fundamentalen Fehler begeht Korzyk, indem er lediglich die technische Sicht mit der administrativen Aktivität in Form eines Werkzeugkasten zusammenfasst. Damit widerspricht er seinem Konzept des "Business Process View", weil die IT-Infrastruktur die Kompetenzen eines Akteurs im Geschäftsprozess auf die Rechte an den Schichten der IT-Infrastruktur abbilden muss, so dass bspw. ein Abteilungsleiter die Rechte seiner Mitarbeiter an einer Datenbank selbst deligieren kann und nicht der Administrator. Dieses Konzept des "divide et impera" schützt zudem vor administrativen Angriffen bzw. horizontalen Angriffen auf die einzelnen Schichten der IT-Infrastruktur, die von Korzyks Konzept ebenfalls nicht erfasst sind.
Zusammenfassend lässt sich Korzyks Konzept deshalb wie folgt bewerten:

1. es löst das Problem der umfassenden Absicherung von IT-Infrastrukturen nicht, vor allem weil er wegen der Erfahrungen mit ERP-Systemen die Probleme nur auf technischer Ebene lösen will und die Verzahnung von Geschäftsprozess und IT-Infrastruktur scheut, die aber bei einem rollenbasierten Sicherheitsmodell zwangsläufig notwendig wird;

2. es ist überdimensioniert bzw. nur für große Unternehmen geeignet, weil es sich an Unternehmen mit einer "just-in-time"-Bindung an Lieferanten und Kunden wendet; Unternehmen, die nicht darauf angewiesen sind, finden in Korzyks Papier kaum Lösungen zur Durchsetzung von Unternehmens- und Sicherheitspolitik;

3. es erzeugt Probleme bei einem Fokuswechsel der Unternehmenspolitik, denn Korzyks Fixierung auf die Utilisierung des Extranets, das den Schutz der Unternehmensdaten vor Externen in den Mittelpunkt stellt, kollidiert mit dem aktuellen Trend des Out-Sourcing, bei dem bspw. administrative Aktivitäten von Unternehmensexternen erbracht werden und damit die Frage des Schutzes vor horizontalen Angriffen immanent wird;
   ein anderer Aspekt ist die Modularisierung von Geschäftsprozessen, also die Vergabe Teilen der Geschäftsprozesse an Unternehmensexterne, die umsomehr eine Delegation von Autorität bzw. rollenbasierte Mechanismen erfordert

Schlussendlich bleibt zu bemerken, dass vor dem Einsatz eines jeden "Enterprise System" stets eine Analyse des Automatisierungsbedarfes und der Wechselbeziehungen zwischen den Geschäftsprozessen und der IT-Infrastruktur vorausgehen muss, um nötigenfalls ein "Reengineering"-Prozess beider anzustoßen, den selbst Korzyk unterbewertet. Sonst machen Unternehmen ähnlich unangenehme Erfahrungen wie bei den ERP-Systemen, wie die "Harvard Business Review" anmahnt[15, S. 131]:

> Many chief executives ... continue to view the installation of an ES as primarily a technological challenge. They push responsibility for it down to their information technology department. ... If the development of an enterprise system is not carefully controlled by management, management may soon find itself under the control of system.

6.4 Vorschlag einer zeitgemässen Architektur eines "Enterprise System"

6.4.1 Die Architektur

Im vorangehenden Kapitel wurde angedeutet, dass Korzyks Konzept nicht vor horizontalen Angriffen, also auf das Netzwerk oder die Datenbank, von administrativen Autoritäten schützt, was besonders bei dem Out-Sourcing bzw. der Erbringung administrativer Leistungen an der IT-Infrastruktur durch Externe zum Tragen kommt. Eine weitere Schwachstelle ist zu bei genauerer Betrachtung der Geschäftsprozessen zu erkennen. Denn häufig werden in einem Geschäftsprozess nicht ausschließlich Daten oder Leistungen aufbereitet oder/und verarbeitet, sondern auch Entscheidungen auf Basis erteilter Kompetenzen getroffen. Diese Delegation von Kompetenzen im Geschäftsprozess sollte sich in der IT-Infrastruktur widerspiegeln, dass ein Abteilungsleiter die fachbedingten Zugriffsrechte wie die Sichtbarkeit oder die Manipulation von Daten für einen Mitarbeiter individuell setzen kann und die Personalabteilung nicht nur die Daten des Mitarbeiter in die Personalverwaltung einpflegt, sondern auch seine Rechte in der gesamten IT-Infrastruktur festlegen kann und weitere Aktionen, wie die Einrichtung eines Terminkalenders mit Einspielung aller wichtigen Daten oder die Eirichtung eines Ordners auf dem File-Server, anstösst. Allerdings legt Korzyk in seinem Konzept die zentrale Verfügungsgewalt über das System die Hände weniger Administratoren, was nicht nur ein erhebliches Sicherheitsrisiko darstellt, sondern auch bei einer lokalen Verteilung der

Ressourcen sowie einer gestuften Verteilung von Rechten als kritisch zu betrachten ist. Die Notwendigkeit einer Kapselung der Ressourcen sowie der Implementierung des Konzepts der Delegation von Rechten an der IT-Infrastruktur, besser bekannt als Prinzip des "divide et impera" oder "multilateral/mulitlevel authority", ist Inhalt der hier entwickelten Architektur.
Angemerkt sie, dass der Begriff der SLA hier weiter gefasst ist. Eine SLA ist sowohl die Formalisierung von technischen Parametern und Leistungsanforderungen der IT-Infrastrukur als auch ihre Wechselbeziehung zu den Geschäftsprozessen. Denn nur auf diese Weise kann die notwendige Verzahnung von Geschäftsprozessen und der IT erkannt werden, Optimierungsbedarf formuliert, Restrukturierungsprozesse angestoßen und der Erfolg gemessen werden.
Damit ergeben sich folgende Anforderungen:

1. Schutz des einzelnen Objektes: jedes einzelne System muss
   a) gekapselt sein bzw. nicht autorisierte Zugriffe verhindern
   b) mit anderen Systemen kommunizieren können und Zugriffe autorisieren können
   c) aus der Ferne konfigurierbar sein
2. Schutz des Datenstromes: das Netzwerk muss geschützt sein z.B. durch Tunneling und Autorisierung unterstützen
3. die Datenbank muss sowohl physisch als auch logisch geschützt sein
4. Unternehmenspolitik muss global setzbar sein, wobei diejenigen Ziele und Prozesse zu lokalisieren sind, welche durch informatische Technologien unterstützt oder automatisiert werden können, dabei insbesondere unterschieden nach
   a) Sicherheitspolitik in der IT-Infrastruktur wie eben Zugriffsrechte auf andere Rechner
   b) Geschäftsprozesse ("business process view") bspw. Vorwarnsysteme

Der letztgenannte Hauptpunkt, also die Speicherung einer global formulierten Unternehmenspolitik[4], wird ermöglicht durch den "Global Policy Store".
Dieser kann mittels des "Lightweight Directory Access Protocol" (LDAP) realisiert werden, da er einerseits die Hierarchisierung bzw. Baumstrukturierung von Datenobjekten erlaubt, andererseits in Anlehnung das X.509-Protokoll die Speicherung von PKI-Zertifikaten also von digitalen Daten über die Identität und Rechten von Personen unterstützt. LDAP ermöglicht wegen der Baumstruktur der Objekte auch die Delegation von manipulativen Zugriffsrechten an Personen bezüglich des (Teil-)Baums bzw. "autoritativen Subdomänen", womit dem Konzept der "multilateral authority" Rechnung getragen wird.
Die Baumstruktur dieses Speichers ist zudem eine Aggregation aller Teilbäume bzw. Politik-Speicher, d.h. dass der Speicher lokal verteilt werden kann und vor Ort mittels der delegierten Autorität verfeinert werden kann. Folglich ist ein sogenannter "Local Policy Store" je Niederlassung vonnöten.
Ferner erlaubt LDAP die Definition von individuellen Objektattributen, so dass auch die elementaren Regeln (SLA) für die Beziehungen des Unternehmens zu seinen Kunden sowie zwischen der IT-Abteilung und den internen Nutzern des Systemes formuliert

[4] Hinweise zur Formulierung: siehe[13] sowie BS 15000

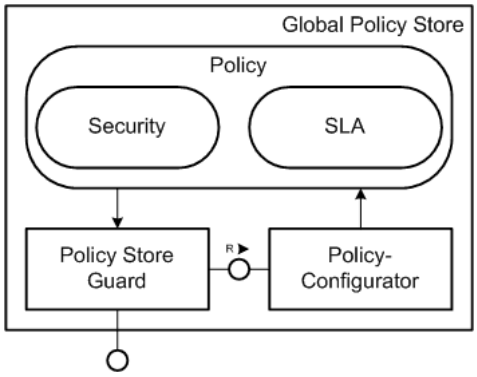

Abbildung 6.4: Vorschlag für ein "Enterprise System": Der unternehmensweite "Politik-Speicher"

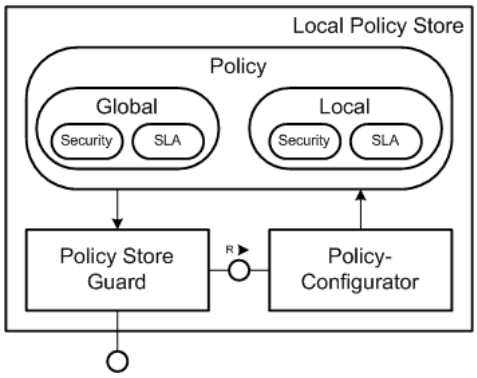

Abbildung 6.5: Vorschlag für ein "Enterprise System": Der "Politik-Speicher" einer Unternehmens-Filiale

werden können. Die Daten der SLA und der Sicherheitspolitik liegen disjunkt in diesem Speicher, um die Konzentration von sowie die Überlastung der administrativen Autorität zu verhindern.
Der "Policy Guard" dieses Speicher realisiert die Kapselung des Systemes, stellt als für lesende und schreibende Zugriffe die Berechtigungen der anfragenden Person fest. Allerdings wird der schreibende Zugriff nicht vom "Policy Guard" selbst, sondern nach erfolgreicher Authentifizierung vom "Policy Configurator" realsiert, da dieser über Mechanismen verfügt, Kollisionen innerhalb der Sicherheitspolitik, der SLA sowie zwischen einander zu erkennen.
Der "Local Policy Store" erweitert - wie bemerkt - die globalen Regeln um die lokalen Gepflogenheiten der Niederlassung wie etwa die regionale Kultur bei der Geschäftsabwicklung sowie die Identitäten und individuellen Rechte der Mitarbeiter. Diese Subdomäne kann wiederum als global aufgefasst und in Subdomänen zerlegt werden, der Einfachheit halber sei hier nur eine bezeichnet.

Dieses Konzept kann aber nur funktionieren, wenn die lokalen Ressourcen nicht nur über das Wissen der Konfiguration der Politik verfügen, sondern auch Mechanismen zur Verarbeitung dieser vorhalten. Auf jedem lokalen System ist ebenfalls "Policy Guard" vorgeschaltet, der auf Basis der formulierten Politik, die wahlweise entweder direkt von

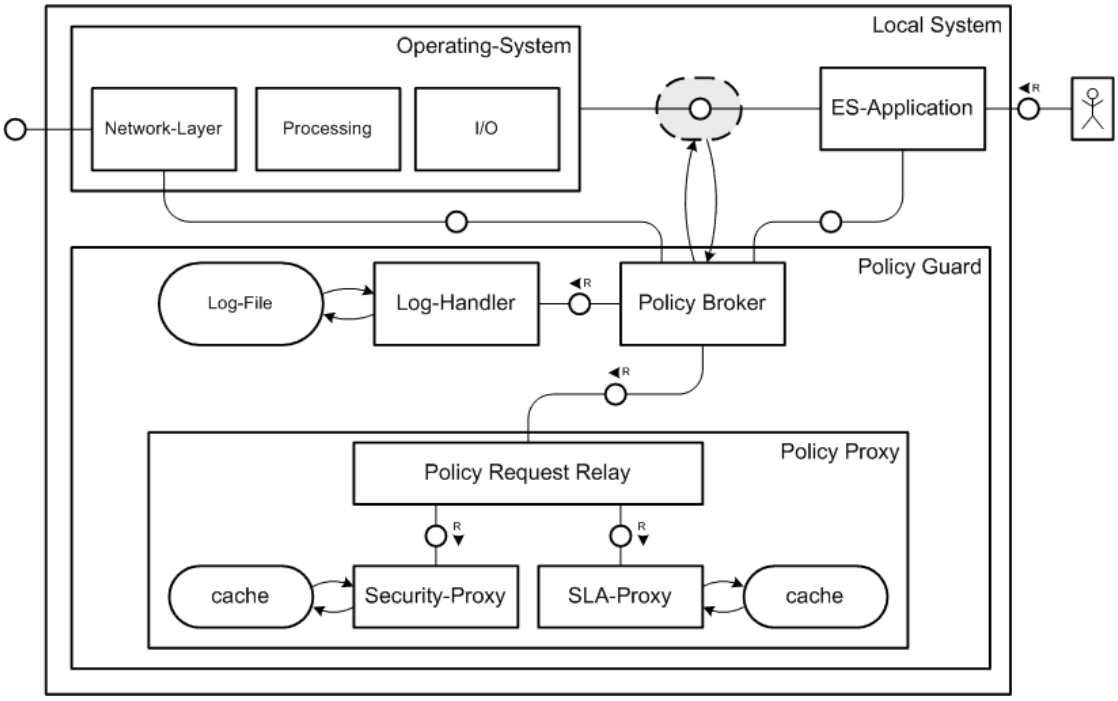

Abbildung 6.6: Vorschlag für ein "Enterprise System": Das lokale System

dem "Local Policy Store" ausgelesen wird oder lokal auf dem "Policy Proxy" des Systems gespeichert wird. Seine wichtigste Komponente ist der "Policy Broker", welcher jeder Interaktion mit dem ES vorgeschaltet ist, um das System zu kapseln. Einerseits realisiert er bidirektional das "single sign on", also sowohl für den lokalen wie auch für entfernte Benutzer und nach erfolgreicher Autorisierung die Herstellung einer Verbindung zu den benötigen Ressourcen.
Andererseits die Ereignisse im System zu protokollieren sowie Verstöße gegen die Sicherheitspolitik zu behandeln oder an einen "Domain Security Alerter" weiterzuleiten. Dabei kann es sich um ein physisches Ereignis wie die Entfernung einer Festplatte oder ein logisches wie ein Angriff handeln.
Eine weitere Fähigkeit dieser Komponente ist die Verarbeitung von Regeln der SLA bspw. der Anstoß von Warnmeldungen an den Benutzer bei Überschreitungen von Fristen aus dem Terminkalender.
Bemerkt sei, dass auch das Datenbanksystem und der Web-Server über einen "Policy Guard" verfügen, diese häufig nur über sehr eingeschränkte Protokollfunktionen verfügen, die auf der Feststellung einer Systemfunktionalität fokussiert ist, aber selten die Quelle eines Angriffes lokalisieren lässt. Es ist streitbar, ob für moderne Datenbanksystemen ein separater Sicherheits-Agent notwendig ist, da sie die Granularisierung von Zugriffsrechten ermöglichen, allerdings schließen sie die Literatur reichlich zitierten[4, S. 34-36] physischen und horizontalen Angriffe von Autoritäten nicht aus.

Das Zusammenspiel der Komponenten eines "Enterprise System" ist nun besser zu verstehen.
Der "Domain Security Alerter" dient wie bemerkt der Sammlung von relevanten Ereignissen auf den lokalen Systemen und leitet sie entsprechend ihrer Art entweder an den

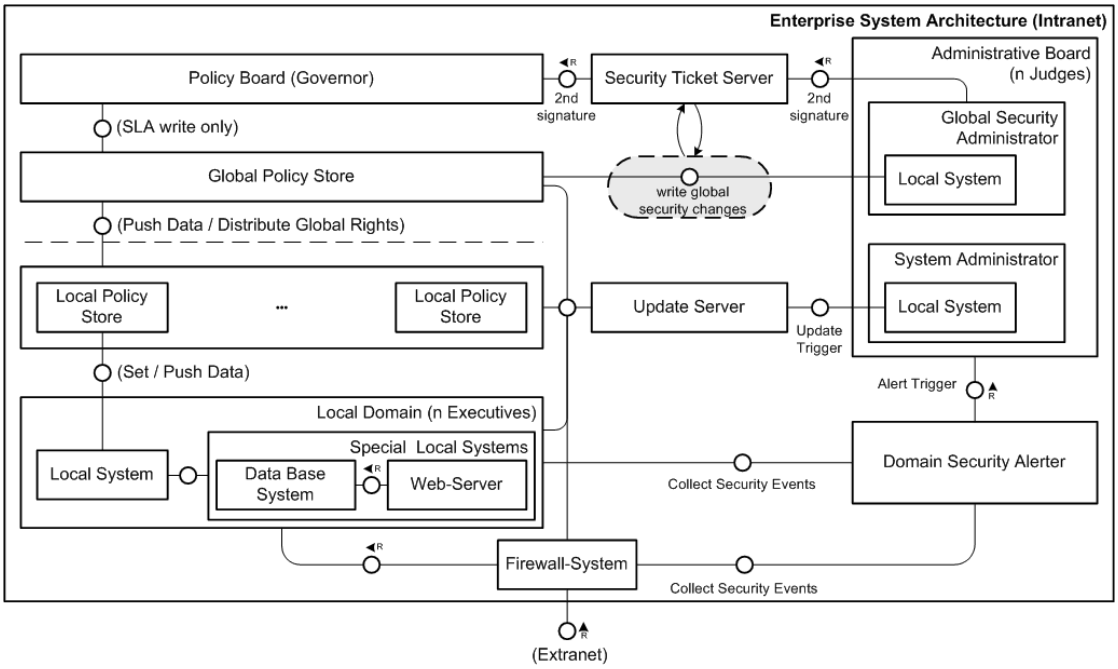

Abbildung 6.7: Vorschlag für ein “Enterprise System”: Die Architektur

System-Administrator oder den Sicherheits-Administrator weiter, wobei er diese Botschaften an eine Rückmeldung des zuständigen Administrators knüpft, ohne die eine Meldung in zyklischen Zeitabständen mit evtl. steigender Priorität wiederholt wird.
Der System-Administrator ist nicht nur für die Verwaltung und Wartung der physischen Ressourcen sowie die Performanz des Software-System zuständig, sondern auch für den “Update-Server”, welcher die Fernwartung von Software-Systemen, wie etwa Anti-Virus-Software, Treiber oder das Patch-Management übernimmt. Die dafür benötigte Software wird entweder lokal vom Administrator eingespielt und dann zur Verteilung auf die lokalen Systeme angestoßen oder von einem entfernten Server des Software-Produzenten. Letztere Variante stellt allerdings weitere Sicherheitsanforderungen, die hier nicht betrachtet werden.

Interessant ist dagegen die Frage nach der Selbstkontrolle der Autoritäten. Denn diesen kommt selbst durch die Definitionen grober Schemen für die SLA und weiterer Autoritären auf den darunter liegenden Ebenen eine gewisse Macht zu, die höher zu bewerten ist, als die eines einzelnen Mitarbeiters.
Also sollten am Prozess der Definition von Sicherheits-Regeln mindestens zwei Autoritäten beteiligt sein, nämlich eine des “Policy Board” bzw. den “Gesetzgebern” und ein Sicherheits-Administrator. Beide zusammen sind Inhaber von Signatur, die sie beide zusammen für einen Schreibvorgang auf die Sicherheitsrichtlinien beim “Security Ticket Server” vorhalten müssen. Dieser erzeugt auf Basis dieser Signaturen temporär für jede Transaktion Ticket, dass die Art, den Umfang und das Datum der Transaktion beschreibt.

Die SLA werden von den “Gesetzgebern” bzw. Unternehmenseignern definiert, da diese die Unternehmenspolitik festlegen.

Zu guter letzt sollte noch deutlich unterstrichen werden, dass die Partitionierung von Autorität über die Mitarbeiter sowie die Kapselung der lokalen Systeme auch nur dann hinreichend ist, wenn das Netzwerk den Schutz des Datenstromes unterstützt.
Dieser Schutz kann heutzutage aber schon durch IPv6-Technologien oder in IPv4-Netzen durch IPSec unterstützt werden.
Dabei kann je nach Vertraulichkeit der Daten entweder kein Schutz, ein schwacher Schutz mittels authentifizierter Datenpakete[5] oder ein starker Schutz mittels Kapslung in kryptographisch verschlüsselten Paketen [6] gewählt werden.

6.4.2 Begründung

Die Begründung dieses Systementwurfes findet sich nicht nur in den oben zitierten Sichten und den Paradigmen von Korsky, sondern auch in den folgenden drei Überlegungen.

"company of citizenship"[1, S. 48]: diese Überlegung stellt auf der Organisation von Arbeit ab und orientiert sich dabei an der Bürgerschaft der Antike:

> People with expertise came forward whenever their skills were needed without becoming part of any standing bureaucracy

Diese Idee repräsentiert nicht nur die als "Out-sourcing" bekannte Arbeitsform, sondern auch die Gestaltung der Geschäftsprozesse in Projektform, für welche die jeweils benötigten Kräfte bei Bedarf akquiriert werden,
das für ein ES konkret, dass die Menge der "Unternehmensexternen" um freie Mitarbeiter bzw. "knowledge worker" erweitert wird, womit nicht nur die Datenbasis eines Unternehmens sondern auch die Geschäftsprozesse in Modulform aus dem Extranet zugänglich sein müssen;
dies bedeutet effektiv die allmähliche Auflösung der tradierten Organisationsformen mündet dann in folgende Anforderungen eines ES

- der Grad der Heterogenität der beteiligten Systeme wird steigen bspw. bedingt durch die Ressourcen der "Tele-Worker"
- das Konzept der ERP-Systeme, die Geschäftsprozesse vollständig funktional auf die Informationstechnologie abzubilden wird zunehmend wegen der Modularisierung der Geschäftsprozesse obsolet werden
- die Rechte der wechselnden Akteure am System je Projekt bedeuten einen steigenden Verwaltungsaufwand, der am ehesten mittels der Delegation von Rechten und damit autoritativer Arbeitsteilung zu bewältigen ist
- Sicherheitsfragen müssen von der Datenbasis eines Unternehmens auf die informatischen Technologien ausgeweitet werden, welche die Prozesse unterstützen

"Responsible Business Enterprise"[10]: diese Idee fundiert die Ideen der "multilateral security" aus Sicht des Geschäftsprozesses insofern, dass

- die Unternehmenseigner eine Politik bzw. SLA definieren[10, S. 2,7]:

[5] besser bekannt als "Authentication-Header" := AH
[6] besser bekannt als "Encapsulated Security Payload" := ES

> When standards, procedures, and expectations are not well established, owners and managers may not safely delegate their authority or expect stakeholders to be well served. ...
> When the board (of owners) is setting management limitations ... they set "basic executive constraints".

- Autorität delegiert von den Unternehmenseignern auf den Manager und von diesem auf andere Mitarbeiter im Unternehmen delegiert wird[10, S. 5]:
- regionale bzw. kulturelle Unterschiede bei der Abwicklung von Geschäftsprozessen nicht ignoriert werden können[10, S. 5]:

> However, an increasing number of studies suggest that ethical decision-making processes differ, if not in the result, by country, nationality, and culture.

"Corporate Social Responsibility"[7, S. 64-70]: Unternehmen sehen sich vermehrt mit sozialen Fragen konfrontiert, welche häufig mit dem technikzentrierten Ansatz der Optimierung von Geschäftsprozessen kollidieren,
diese Anforderung äußert sich dann in der Unternehmenspolitik in zweierlei Weise

1. im Gegensatz zu Korzyks Konzept steht nunmehr der Unternehmensexterne im Mittelpunkt der Geschäftspolitik, welchem die Ressourcen des Unternehmens mittels Dienstleistungen angeboten werden, was eben auch die Delegation von Autorität zum Zwecke der Kundenbindung sowie der Einbindung externer Projektmitarbeiter bedeutet (vergl. auch Kritik von Foster-Melliar)
2. die sozialen Fragen haben auch Auswirkungen auf die interne Struktur eines Unternehmens, in der Form, dass die Authentizität des Unternehmens als "lebendiger Organismus" vermittels menschliche Arbeitskraft und nicht als "just-in-time Automat mit elektronischer Kommunikationsschnittstelle" gegenüber Aussenstehenden zu vertreten wird

Diese Grundsätze, erweitert durch gemeinnützige Tätigkeit der Unternehmen, kann man unter dem eben genannten Begriff zusammenfassen oder wie es das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung im Aktionsprogramm 2005 ausdrückt:

> Die Unternehmen verpflichten sich zur Beachtung sozialer, menschenrechts- und umweltrelevanter Grundsätze bei der Geschäftstätigkeit und ihren Beziehungen zu Arbeitnehmern, Anteilseignern und Konsumenten ...

Literaturverzeichnis

[1] . Building a Company of Citizenship. *Harvard Business Review*, January 2003.

[2] AberdeenGroup, Inc. Computer Associates' Unicenter TNG Enters the Next Dimension. *Analysis, Rating*, 1997. http://www.ca.com/analyst/111/.

[3] Alexander D. Korzyk. Sr. Towards Security of Integrated Enterprise Systems Management. *Research Paper*, 1999. http://csrc.nist.gov/nissc/1999/proceeding/papers/p32.pdf.

[4] Andrew Nash, William Duane, Celia Joseph, Derek Brink. *PKI e-security implementieren.* mitp-Verlag, 2002. ISBN 3-8266-0781-3.

[5] BEA Systems Inc. BEA Weblogic Enterprise Security. *Public Relations*, 2004. http://de.bea.com/produkte/weblogic_enterprise_security.jsp.

[6] Bull. Bull Evidian announces AccessMaster NG, a new-generation software suite to secure the extended enterprise. *Public Relations*, 2003. http://www.wcm.bull.com/internet/pr/rend.jsp?DocId=34039&lang=en.

[7] Christian Sywottek. Schwerpunkt: Verantwortung übernehmen _Corporate Social Responsibility. *brand eins*, Dezember 2004.

[8] C|Level Asia, Symantec, Ernst & Young. A Strategic Guide To Enterprise Security. *Security Insights*, 2004. http://www.ey.com/global/download.nsf/Singapore/A_Strategic_Guide_to_Enterprise_Security/$file/CLevel%20Asia%20Security%20Supplement.pdf.

[9] Computer Associates. Unicenter TNG: Enterprise Management Strategy. *Public Relations*, 1997. http://www.ca.com/products/unicent/whitepap.htm.

[10] ITA. Standards, Procedures, and Expectations for the Responsible Business Enterprise. *Tutorial*, 2003. http://www.ita.doc.gov/goodgovernance/adobe%20files/bem_section_3/chapter_5.pdf.

[11] Microsoft. Best Practices for Enterprise Security. *Microsoft Solutions Framework: Best Practices for Enterprise Security*, 2004. http://www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.mspx.

[12] P.Kovari, D.Karpenter, P.Creswick, P.Kisielewicz, F.Langley, D.Leigh, R.Maheshwar, S.Pipes. IBM WebSphere V5.0 Security WebSphere Handbook Series. *IBM Redbooks*, 2004. http://publibb.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/SG246573.html?Open.

[13] Rick Leopoldi. IT Service Management A Description of Service Level Agreements. *Offer for Service*, 2002. http://www.itsm.info/SLA%20description.pdf.

[14] Scarlet Pruitt. Enterprise security is worst ever, experts say. *Etre Technology Conference, Cannes*, 12.10.2004. http://www.infoworld.com/article/04/10/12/HNsecurityworst_1.html.

[15] Thomas H. Davenport. Putting the Enterprise into the Enterprise System. *Harvard Business Review*, July - August 1998.

7 Plattformübergreifende Sicherheitsmanagement-Systeme

Alexander Altmann

Abstract

Diese Ausarbeitung beleuchtet Datensicherheit in Unternehmen und die Möglichkeiten, diese durch den Einsatz von Software zu verbessern. Dabei wird die Softwaregattung „Sicherheits-Managementsysteme“ untersucht und es werden existierende Lösungen kommerzieller Anbieter und Produkte aus dem Open-Source-Bereich vorgestellt.

7.1 Einleitung - Was ist Sicherheitsmanagement?

Sicherheit ist das Vorhandensein von Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit in einem geplanten Ausmaß. Wenn es um die computertechnische Sicherheit eines Unternehmens geht, so geht es um die Sicherheit der Daten dieses Unternehmens - welche inhaltlich und formal unverändert bleiben, ständig bereitgehalten, als auch vor unberechtigtem Zugriff geschützt werden müssen.

Zu den Bedrohungsquellen zählen dabei Unzuverlässigkeiten der Infrastruktur beziehungsweise ihrer Komponenten, Handlungen durch Mitarbeiter oder Dritte und ganz allgemein Umgebungseinflüsse (wie Naturkatastrophen).

Wie man sich leicht vorstellen kann, sind die Bedrohungen im Speziellen vielfältig. Gegenmaßnahmen müssen deshalb gezielt, aber ebenso umfassend sein - der beste Schutz gegen böswillige Dritte, die von außen elektronisch in das Firmennetzwerk eindringen könnten, nützt nichts, wenn keine physische Alarmanlage das Firmengebäude gegen den Diebstahl einiger Festplatten sichert.

Die hier besprochenen Sicherheitsmanagement-Systeme sind nur in einem Bereich tätig - Schäden zu vermeiden, die aus den Handlungen von Mitarbeitern oder Dritten entstehen können. Gegen Unzuverlässigkeiten der Infrastruktur wird anderweitig mit Redundanz von Komponenten (Netzteile, Festplatten, komplette Server, ...) vorgegangen, gegen Umgebungseinflüsse wie Naturkatastrophen oft ebenso (z.B. geographisch verteilte Server).

Existierende Sicherheitsmanagement-Systeme wirkten aber auch weiterhin unvollständig, wenn man nicht noch den Bereich des Hardware-Schutzes ausklammerte. Hier sollten Diebstahlschutz, herkömmliche Alarmanlagen, hohe Zäune und all die anderen bewährten

Mittel im Kampf gegen physisches Verschwinden von Sachen oder Personen eingesetzt werden.

Wofür sind Sicherheitsmanagement-Systeme also zuständig? Grob gesagt sollen sie Daten mit Hilfe von Software sichern - was weit über das Anlegen von Backups hinausgeht.

7.2 Die verschiedenen Ansätze

Das Sicherheitsmanagement soll Schäden verhindern und damit wirtschaftliche Verluste für das Unternehmen abwenden. Eine komplexe Aufgabe, die kein Programm allein bewältigen kann, die existierenden Lösungen setzen deshalb unterschiedliche Schwerpunkte.

7.2.1 Management-Systeme

Bei diesem vielleicht ältesten Ansatz der besprochenen Systeme geht es nicht vornehmlich um Sicherheit. Mit der steigenden Zahl von Computern pro Unternehmen und der Verbreitung unterschiedlicher Betriebssysteme wuchs auch der Wunsch, alle Computer unter einer einheitlichen Oberfläche zu verwalten. Zu weit sind die Wege in großen Gebäuden, zu umständlich und zu langwierig ist es für die kleine Schar oder den einzelnen Administrator, jedem Computer einzeln genau die Behandlung angedeihen zu lassen, die er benötigt.

Die Lösung liegt im zentralen Management dieser Computer - auf jedem Rechner wird ein Client (angepaßt an das Betriebssystem oder die Umgebung) installiert, welcher die Fernsteuerung des Rechners erlaubt. Von einem zentralen Platz aus können nun alle Computer überwacht und gesteuert, in Gruppen zusammengefaßt und mit neuen Aufgaben betreut werden.

Die Sicherheit der Einzelrechner kann natürlich ebenfalls überwacht werden (zentrales Auslesen der Logdateien, Überprüfung von Paßwörtern, ...). Hier eignet sich ein Management-System vor allem, um Handlungen oder fehlende Sorgfalt der eigenen Mitarbeiter aufzudecken oder zu verhindern.

7.2.2 Anti-Viren-Systeme

In den letzten Jahren ist die Zahl der netzwerkfähigen Viren ständig gestiegen und einige Exemplare haben in hoher Verbreitung schon erhebliche Schäden in Unternehmen verursacht. Dabei werden weniger die Server oder die Infrastruktur an sich angegriffen, sondern die PCs, welche hauptsächlich unter Microsoft Windows laufen. Da diese aber für viele (z.B. Büro-) Tätigkeiten benötigt werden, kann deren Ausfall ein Unternehmen für mehrere Stunden (in Einzelfällen mehrere Tage) lahmlegen. Dazu kommt eine erhöhte Netzlast, die allein schon für den Ausfall von Firmennetzen gesorgt hat.

Das Filtern von Viren kann zum Beispiel am Mailserver stattfinden - mit Virendatenbanken für mehrere Betriebssysteme kann dieser plattformübergreifend gegen die Schädlinge

vorgehen.

7.2.3 Anti-Cracker-Systeme/NIDS

Ging es bei den Viren noch um automatisierte kleine Schadprogramme, die es meist nicht speziell auf Unternehmen abgesehen haben, sind die Systeme dieser Gruppe gegen menschliche Eindringlinge von außen gerichtet, die sich gezielt an ein Unternehmen wenden.

Dafür müssen diese Systeme das gesamte Netzwerk überwachen und bekamen so auch ihren Namen - „Network Intrusion Detection Systems“ (NIDS). Um dieser Rolle gerecht zu werden, muß es alle Daten, die im Netz ausgetauscht werden, mitlesen können und wird dazu meist an einen speziellen Port eines zentralen Netzwerk-Switches angeschlossen.

NIDS können „Denial-of-Service“-Angriffe filtern, Einbruchsversuche bei Einzelrechnern gleich im Netzwerk stoppen und auch Viren auf diese Art an ihrer Verbreitung hindern.

7.2.4 Hostbasierte IDS (HIDS)

Ein NIDS kann alle Verbindungen zwischen, von und zu Computern im überwachten Netzwerk kontrollieren, allerdings keine Ereignisse, die sich lokal auf einem Rechner abspielen. Ist es einem Cracker gelungen, in einen Rechner einzudringen (und zum Beispiel eine SSH-Verbindung aufzubauen, um nicht abgehört zu werden), bekommt ein NIDS nicht mit, wenn er dort Dateien verändert, Log-Dateien löscht, ein Rootkit installiert, etc. - für diese Aufgabe ist ein Host Intrusion Detection System (HIDS) zuständig.

Das HIDS überwacht den Zustand von Dateien eines System mittels Checksummen, Zeitstempeln, Größenvergleichen und ähnlichem und schlägt Alarm, sollten sich überwachte Dateien ändern.

7.3 Die Ansätze am Beispiel

7.3.1 Management-System: IBM Tivoli (Security Compliance Manager)

IMBs Tivoli ist für eine Vielzahl von Plattformen verfügbar und in heterogenen Firmennetzwerken einsetzbar. IBM verkauft und unterstützt seit langer Zeit mehrere Hardwareplattformen und Betriebssysteme für große Unternehmen und war dadurch angehalten, die Administrationsoberfläche zu vereinheitlichen.

Obwohl im Laufe der Zeit bis heute UNIX-basierte Betriebssysteme in Unternehmen vorherrschten, gibt es doch verschiedene Ausprägungen von Unix mit teilweise unterschiedlicher Bedienung. Hinzu kamen vor einigen Jahren auch einige Microsoft Windows-Varianten.

IBMs Tivoli nutzt eine Client-/Server-Architektur, bei der die Clients auf den verwalteten Rechnern laufen und über gesicherte Verbindungen mit einem Server kommunizieren, welcher auf eine Datenbank (IBMs DB2) zugreift. Der Administrator benutzt einen speziellen Client (die „Administration console“), mit der er das so entstandene Netzwerk überwachen und kontrollieren kann.

Die Palette reicht hier von der zentralen User- und Paßwort-Verwaltung bis zum Verteilen von Anwendungen, dem automatischen Ein- und Ausschalten von Computern über das Netz bis zum Versenden von Nachrichten an alle Anwender.

Der Server ist eine Java-Anwendung mit einer DB2-Datenbank im Hintergrund, in der sämtliche Daten über das Netz gespeichert werden. Clients registrieren sich beim Server, können von ihm in Gruppen zusammengefaßt, aktualisiert und gelöscht werden.

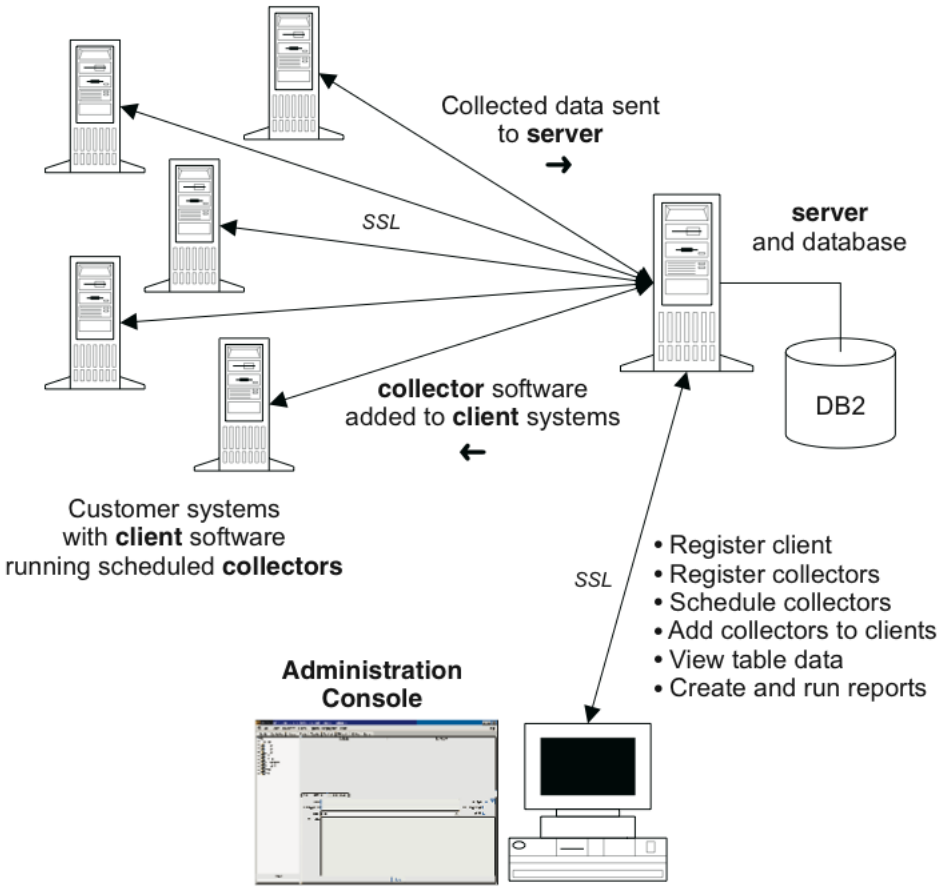

Figure 1. Tivoli Security Compliance Manager components

Auf dem Server wird die Benutzerstruktur des Netzes festgelegt und verwaltet - die Administratoraccounts, Paßwörter und Anwendergruppen können über Betriebssystemgrenzen hinweg konsistent gehalten werden. Er speichert Schlüssel, Logdateien, zu verteilende Software und selbst deren Ausgaben.

Ein Client ist ein ebenfalls in Java geschriebenes Programm, welches auf fast allen Plattformen seine eigene Java Virtual Machine gleich mitbringt, um die Installation zu erleichtern. Der Client läuft genauso wie der Server mit root-Rechten und stellt die Verbindung zu diesem her, zusätzlich stellt er den auszuführenden Programmen eine Laufzeitumgebung zur Verfügung.

Diese Laufzeitumgebung wird von den Collectors genutzt, kleinen Programmen, welche ihrem Namen getreu Daten auf dem Clientsystem sammeln. Sie werden bei IBM in Form von JAR-Dateien verteilt und können Dateien lesen, Programme starten und deren Ausgaben aufzeichnen und unter Windows die Registry lesen.

Die Collectors werden über verschlüsselte Verbindungen (SSL) vom Server zum Client übertragen, welcher sie dann ausführt. Ein Zeitplan und Parameter sind Teil des JAR-Paketes, in welchem ein Collector transportiert wird.

Während seiner Laufzeit sammelt der Collector Daten, die vom Client gespeichert und in regelmäßigen Abständen (gewöhnlich jede Minute) zum Server geschickt werden, welcher sie in der Datenbank ablegt.

Um die Kontrolle des Netzwerkes einfacher zu realisieren, können Collectors in sogenannten Policies organisiert werden, um bestimmte Bedingungen zu überprüfen. So kann eine Policy zum Beispiel festlegen, daß alle Anwenderpaßwörter länger als 6 Zeichen sein sollen - die Collectors werden mit Hilfe der auf allen Computern installierten Clients dem Server melden, welche Accounts auf welchen Computern diese Regel nicht erfüllen.

Die Administrationskonsole läuft nur unter MS Windows, unter allen Betriebssystemen gibt es jedoch Kommandozeilenwerkzeuge zur Administration. Wie bereits erwähnt, laufen Server und Clients mit Hilfe einer Java Virtual Machine (JVM) auf fast allen Systemen.

Zusammenfassend kann gesagt werden, daß IBMs Tivoli sich durch die plattformunabhängige Implementation in Java, die Client-/Server-Architektur mit Datenbank und seine flexiblen Collectors sehr gut für große Unternehmen mit einer heterogenen Rechnerlandschaft eignet. IBM ist in diesen Märkten zu Hause, insofern mag das nicht überraschen.

Tivoli ist aber ein Managementsystem und nicht primär ein Sicherheits-Managementsystem. Es kann helfen, die einzelnen Computer sicherer zu machen, kann aber auch das Gegenteil bewirken. Gelingt es einem Angreifer, sich Zugang zur Administratorkonsole zu verschaffen, kann er nach Belieben Paßwörter ändern, Computer umkonfigurieren, Programme auf ihnen starten, jede Art von gesammelten Daten auslesen, etc. . Dies ist die „Achillesferse“ des Systems, allerdings könnte er auch versuchen, manipulierte Clients auf die Computer zu bringen oder einfach die zentrale Datenbank angreifen. Man sieht, daß Sicherheit kein Designziel des Systems war.

Es handelt sich letztlich um ein Beobachtungs- und Verteilsystem, welches geschaffen wurde, um die Arbeit von Administratoren in großen Unternehmen zu erleichtern. Erst in letzter Zeit versuchen die Hersteller, im Sicherheitsbereich entsprechende Lücken zu

schließen.

Selbst wenn das System in der Lage ist, sich selbst zu verteidigen, realisiert es ansonsten nicht Sicherheit für die Unternehmensdaten. Im Gegenteil - statt sie zu schützen, werden sie womöglich noch zentralisiert und damit leichter angreifbar.

7.3.2 Anti-Viren-/NIDS-Systeme: McAfee IntruShield & Snort

Einen anderen Ansatz als IBM verfolgt McAfee mit ihren IntruShield-Systemen. Die Firma ist Heimanwendern vor allem durch ihre Virenscanner und „Personal-Firewalls“ bekannt, einigen vielleicht durch den Aufkauf von PGP vor einigen Jahren.

Das IntruShield-System ist hardwarebasiert und wird als zusätzlicher Bestandteil in ein bestehendes Netzwerk eingebaut. Seine Hauptaufgabe besteht darin, Viren und Würmer zu erkennen und unschädlich zu machen. Darüber hinaus beherrscht es auch die Abwehr von Denial-of-Service (DoS)-Attacken, welche entweder bestimmte Schwachstellen in Betriebssystemen ausnutzen („Teardrop“, ...) oder Unzulänglichkeiten in Protokollen (Syn-Flood). Eine Besonderheit ist hier, dass IntruShield bei Installation der entsprechenden Schlüssel auch SSL-Verbindungen in Hardware decodiert und dabei sehr hohe Geschwindigkeiten erreicht.

Der Administrator kann über SNMP (Simple Network Management Protocol), EMail, Pager oder SysLog alarmiert werden, es gibt eine Managementkonsole und Berichte können automatisch erstellt werden. Das System funktioniert als Firewall und IDS, es kann in einer „Phase des Lernens“ das Netzwerk kennenlernen und danach bei Abweichungen vom erlernten Verhalten des Netzwerks reagieren. Die Reaktion kann eine bloße Warnmeldung sein, aber auch ein Blockieren der IP-Adresse.

IntruShield verläßt sich außerdem beim Erkennen von Viren und DoS-Attacken auf Signaturen, diese werden regelmäßig von McAfee aktualisiert, der Anwender kann jedoch eigene hinzufügen.

Snort ist ein „Network Intrusion Detection System“ aus der Open-Source-Welt. Es läuft auf vielen Plattformen, darunter den BSD-Unices, Linux, Solaris und sogar Windows. Die Geschwindigkeit ist natürlich von der eingesetzten Hardware abhängig, aber auch von der Betriebsart und der Menge der Regeln. Snort kann als einfacher Packet Logger jedes Paket aufzeichnen, kann aber auch als IDS sehr spezifische Regeln verwenden, die Pakete nach diversen Kriterien (Protokoll, Größe, Herkunft, Ziel, ...) filtern. Snort kann im Gegensatz zu IntruShield keine Viren erkennen.

Snort selbst ist nur ein „Detection System“, fuer die Abwehr von Angriffen kann es aber z.B. mit der linuxinternen Firewall kombiniert werden und somit zum „Intrusion Prevention System“ (IPS) werden.

In das für Open-Source und UNIX typische Baukastensystem reiht sich die nächste Anwendung ein: ACID. Ausgeschrieben „Analysis Tool for Intrusion Databases“, kennt man auch schon fast seinen Anwendungszweck: Es ist eine graphische Konsole zur Auswertung der mit Snort oder ähnlichen IDS gesammelten Daten. ACID ist Webserver- und

PHP-basiert und stellt dem Administrator graphisch Paketstrukturen und statistische Auswertungen des Netzwerkverkehrs dar.

Snort & ACID sind recht populär, es gibt sogar ein „...for Dummies“-Buch darüber.

Wie man sieht, verstehen McAfee und die Snort-Entwickler etwas anderes unter „Sicherheits-Managementsystem“ als IBM - das IntruShield-System und Snort müssen nicht auf allen Rechnern installiert werden und haben daher auch wenig mit dem Management dieser Rechner zu tun. Was auf den Client-Rechnern geschieht, können IntruShield und Snort nicht wissen. Sie schützen daher nicht vor schwachen Paßwörtern, schlechter Konfiguration, nicht genutzten Accounts und ähnlichem, sondern ausschließlich vor Attacken, die mit dem Netz zu tun haben - und hier hat es den Anschein - vor allem vor Attacken von außen.

Interessant ist, daß Symantec (eine wie McAfee ebenfalls aus dem Anti-Viren-Umfeld stammende Firma) unter dem Namen SESA (Symantec Enterprise Security Architecture) ein System entwickelt, welches ganz ähnlich aufgebaut sein soll wie IBMs Tivoli (und teilweise sogar dieselben Komponenten benutzt: IBM DB2). Symantec plant Java-Agenten für die Clients, eine relationale Datenbank, einen Webserver, LDAP-Server und eine Administrationskonsole in einem Webbrowser mit Java-Applets.

Allerdings hat IBM einen gehörigen Vorsprung, Symantec plant die Fertigstellung des Systems erst in zwei Jahren ein. Schritt für Schritt sollen nach der Grundversion dann verschiedene Datenbanken (Oracle, MS SQL Server) und Administrations-Plattformen (Solaris, Linux) hinzukommen. Nach diesen folgt ein Policy-Management und erst die letzte Version wird die schon von IBM bekannten Collectors hinzufügen.

7.3.3 Hostbasierte IDS: Tripwire & Co.

Sind die Rechner zentral gemanaget, vor Viren und Angriffen aus dem Netz geschützt, hindert einen Mitarbeiter oder Dritten noch immer nichts daran, sich vor die Tastatur des Rechners zu setzen und eine wichtige Systemdatei gegen eine manipulierte auszutauschen. Das gleiche könnte auch ein Virus tun, den der Virenscanner übersehen hat - sobald sich der Virus danach löscht, wird man Schwierigkeiten haben, die Veränderung zu bemerken.

Es sei denn...man benutzt eine Datei-Integritäts-Überprüfung. Da gerade unter UNIX-Systemen so ziemlich alles eine Datei ist, kann diese Form eines „Host Intrusion Detection Systems“ sehr effektiv im Aufdecken von Eindringlingen sein.

Das Prinzip von Tripwire oder AIDE („Advanced Intrusion Detection Environment“) ist eine Datenbank mit Einträgen für wichtige Dateien eines Systems. Diese Datenbank wird von einem sauberen, virenfreien, Dateisystem angelegt und dient fortan als Maßstab. Tripwire, AIDE & Co. können nun Veränderungen am Dateisystem anhand verschiedener Kriterien feststellen - Dateiattributen, Rechten, Zeitstempeln, Größe und, vielleicht am wichtigsten, Checksummen.

Eine Checksumme kann mit verschiedenen Algorithmen erstellt werden (MD5, SHA1,

...) und wird über den Inhalt der Datei gebildet. Ein Virus, der eigenen Code in ein Programm einschleusen will, kann den Inhalt des Originals komprimieren und seinen Code vor diesem einbauen. So könnte er die Dateigröße beibehalten und IDS ohne Checksummen leicht täuschen. Systeme mit Tripwire, AIDE, etc. würden auch hier Alarm schlagen.

7.4 Zusammenfassung

Keines der Programmsysteme, ob kommerzieller Natur oder nicht, kann das diffuse Ziel „Sicherheit“ in einem Unternehmen allein ermöglichen. Um diesem Ziel näher zu kommen, muß es erstmal klarer definiert werden - was soll gesichert werden, wovor, mit welchem Aufwand, etc.? Sind die grundlegenden Vorstellungen vorhanden, kann man sich (nach dem Kauf von redundanten Netzteilen und hohen Zäunen) Gedanken um die einzusetzende Software machen.

Es ist erfreulich, daß die meisten Programmsysteme für Unternehmen (wenn sie nicht aus dem Hause Microsoft kommen) heutzutage plattformübergreifend einsetzbar sind. In vielen Unternehmen kommt das der Realität doch sehr entgegen, in der verschiedene Systeme für verschiedene Aufgaben im Einsatz sind. Man muß sich als potentieller Käufer hier also auch nicht auf ein Betriebssystem oder eine Hardwareplattform festlegen.

Da (zum Beispiel) die Systeme von IBM und McAfee so unterschiedlich sind, stellt sich die Frage, ob man sie nicht zusammen nutzen sollte, als gegenseitige Ergänzung. Meiner Meinung nach wäre dies keine schlechte Idee, wenn man auf ein paar Besonderheiten achtgibt (und zum Beispiel die SSL-Verbindungen von Tivoli nicht mit IntruShield entschlüsseln läßt, da sonst der IntruShield-Administrator wieder Zugriff auf möglicherweise geheime Daten des Tivoli-Systems und der Client-Rechner hätte).

Auch Tripwire könnte als drittes Mitglied im Bunde noch Sicherheitslücken schließen. IntruShield sorgt für die Abwehr von Viren und netzwerkbasierten Angriffen von außen, Tripwire stellt die Integrität der Dateien auf jedem System sicher und die Logdateien beider Programme von allen Rechnern werden über Tivoli an einen zentralen Server übertragen, wo der Administrator sie bequem auswerten kann.

Wie man aber am möglichen Zusammenspiel von Tivoli und IntruShield beispielhaft sieht, ist die Kombination von Sicherheitsmanagement-Systemen nicht ganz einfach, kann neue Probleme schaffen und neue Sicherheitslücken öffnen. Der Ansatz der Zentralisierung aller Daten sollte auch kritisch überdacht werden - macht er doch den Angriff der zentralen Datenbank wesentlich lukrativer.

„Sicherheits-Management“ ist dabei keine Softwaregattung, sondern eine Aufgabe. Das gleiche kann für „Sicherheit“ gesagt werden. Es ist eine Aufgabe für jedes einzelne Unternehmen, welche durch den Einsatz vorgefertigter Software erleichtert, aber nicht aus der Welt geschafft werden kann.

Die fortwährende Bewältigung dieser Aufgabe erfordert nicht nur Software, nicht nur

zusätzliche Hardware, sondern Menschen mit einem Konzept, Zeit und Wissen über das zu schützende Unternehmen und seine Bedürfnisse.

Eine einfache Wahrheit - die „umfassende Absicherung komplexer IT-Infrastrukturen“ ist komplex, wenn sie umfassend sein soll.

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutzhandbuch 2004*. Bundesamt für Sicherheit in der Informationstechnik, 2004. http://www.bsi.bund.de.

[2] Edwin E. Mier and David C. Mier. In Search Of The Smartest Sentry. *BUSINESS COMMUNICATIONS REVIEW*, 2004. http://www.mcafeesecurity.com/us/audience/enterprise_home.asp.

[3] IBM Corp. IBM Tivoli Security Compliance Manager Administration Guide. 2004. http://www.ibm.com/software/tivoli/library.

[4] Institut für Informatik der Universität Zürich. Sicherheitsmanagement. http://www.mnf.unizh.ch.

[5] Symantec Corp. Symantec Enterprise Security Architecture. 2002. http://enterprisesecurity.symantec.com.

[6] The Snort Project. Snort Users Manual. 2004. http://www.snort.org.

8 Common Information Model (CIM)

Martin Fürstenau, Francis Zinke

Abstract

Gegenstand dieses Paper ist das Common Information Model, ein Datenmodell zur Beschreibung großer Systemumgebungen. Ziel von CIM ist es, als Standard das Management verteilter heterogener Systeme zu vereinfachen. Desweiteren wird das dazugehörende Framework Webbased Enterprise Management vorgestellt, sowie eine Implementierung, das Windows Management Interface. Hauptquelle für das Paper war die DMTF [3].

8.1 Einleitung

Das Common Information Model (CIM) ist ein Standard der Distributed Management Task Force (DTMF) [3]. Die DTMF ist eine nicht-profitorientierte und firmen-unabhängige Organisation. Ihre Hauptziele sind die Entwicklung, Adaption und Vereinheitlichung von Management-Standards und -Initiativen für Desktop, Enterprise und Internet-Umgebungen [2].
Der CIM-Standard ist ein konzeptionelles Informationsmodell zur Beschreibung von Entitäten[1] in den vorher genannten Umgebungen. Es umfasst eine Spezifikation und ein Schema. Die Spezifikation definiert die Details zur Integration mit anderen Management-Modellen, während das Schema zur Modellbeschreibung genutzt wird.
Diese Ausarbeitung stellt das Common Information Model allgemein, die Motivation und einige ausgewählte Bereiche des CIM vor.

8.2 Das Managementproblem

Heutige grosse heterogene Systeme stehen mit anderen Systemen in Verbindung. Damit Konnektivität, Interaktion und Dienstebereitstellung über Systemgrenzen hinaus gewährleistet werden können, müssen verschiedenste Informationen verwaltet werden. In einer heterogenen und verteilten Umgebung ist es völlig unzureichend, wenn Personal-Computer, Subnetze, der Netzwerkkern und verschiedene individuelle Systeme isoliert verwaltet werden. Die Einführung eines umfassendes System-Management-Standards wird somit zu einer Notwendigkeit. Dazu sollte der Einsatz anderer Standards nicht nötig sein und das Systems-Management sollte unabhängig von der Implementierung des zu verwaltenden System sein.

[1] Eine Entität beschreibt ganz allgemein etwas Vorhandenes, dessen spezielle Ausprägung nicht relevant ist

8.3 Das Common Information Model

Das Common Information Model (CIM) ist ein hierarchisches, objektorientiertes Modell zur Beschreibung von Management-Information in einer Netzwerk- und/oder Firmenumgebung [3]. Es definiert und strukturiert ein einheitliches, umfassendes und mächtiges Datenmodell, das unabhängig von Implementierungen und Architekturen ist. Implementierungsunabhängig bedeutet, dass es mittels CIM möglich ist, von Details der Implementierung mehrerer Applikationen zu abstrahieren und ein Datenmodell vorzufinden, das für alle gleich ist. Dazu zählt auch das Verwenden von offenen Kommunikationsstandards. Architekturunabhängigkeit bezieht sich auf die Rechnerarchitektur, als auch auf das zugrundeliegende Betriebssystem.
Zur Darstellung der CIM-Architektur wird die UML[2] genutzt. Zusätzlich konnten ältere Standards, wie SNMP[3] und der Vorgänger DMI[4] integriert werden.
Das CIM-Datenmodell besteht aus einer Spezifikation und einem Schema. Die Spezifikation beschreibt ein objekt-orientiertes Meta-Modell, welches auch als Meta-Schema bezeichnet wird. Es legt die Meta-Schema-Elemente und die für sie geltenden Regeln fest. Das CIM-Schema beschreibt Managementdaten in einem Standardformat, mittels dessen die Daten zwischen verschiedenen Management-Applikationen ausgetauscht werden können.
Die folgenden Kapitel beschreiben die Spezifikation (respektive das Meta-Schema) und das Schema.

8.4 Meta-Schema

Das Meta-Schema ist eine formale Definition von Syntax und Regeln zur Beschreibung von Modellen, es beschreibt also, wie Dinge in CIM abgebildet werden. In dieser Spezifikation werden keine Implementationen oder Protokolle beschrieben. Das geschieht mittels des CIM-Schema. Die Syntax-Sprache, welche auf der Interface Definition Language (IDL) basiert, wird Managed Object Format (MOF) genannt. MOF dienen der automatisierten Verarbeitung und dem Austausch von Klasseninformationen.
Die Abbildung 8.1 zeigt das Meta-Schema als UML-Klassendiagramm. [3]
Das oberste Element des Meta-Schemas ist das `Named-Element`. Es enthält nur den Namen eines zu verwaltenden Elements.
Ein `Schema` ist eine Gruppe von Klassen mit einem einzelnen Besitzer. Klassennamen müssen innerhalb des Schemas einzigartig sein und den Schemanamen enthalten. Zusätzlich muß der Schemaname einzigartig sein, bspw. kann dies für Firmen durch Nutzung ihres DNS-Eintrages gewährleistet werden.
Jede `Klasse` ist ein Prototyp für ein Element, das betreut werden muss. Sie enthält `Eigenschaften` und `Methoden` für ihre Nutzung.`Eigenschaften` haben einen Namen, einen Datentypen und Werte und optional einen Standardwert. `Methoden` haben einen Namen, einen Rückgabewert (CIM-Datentyp) und optionale Ein- und Ausgabeparameter. Die Vererbungsbeziehung zwischen zwei Klassen wird über die Subtype-Supertype-Assoziation dargestellt. Dabei ist es möglich, Attribute und Methoden der Oberklasse zu überschreiben, was die Property-/Method Override-Assoziation zeigt.
Jedes `Named-Element` verfügt über eine beliebige Menge an `Qualifiern`. Diese bezeich-

[2] Unified Modeling Language
[3] Simple Network Management Protocol
[4] Desktop Management Interface

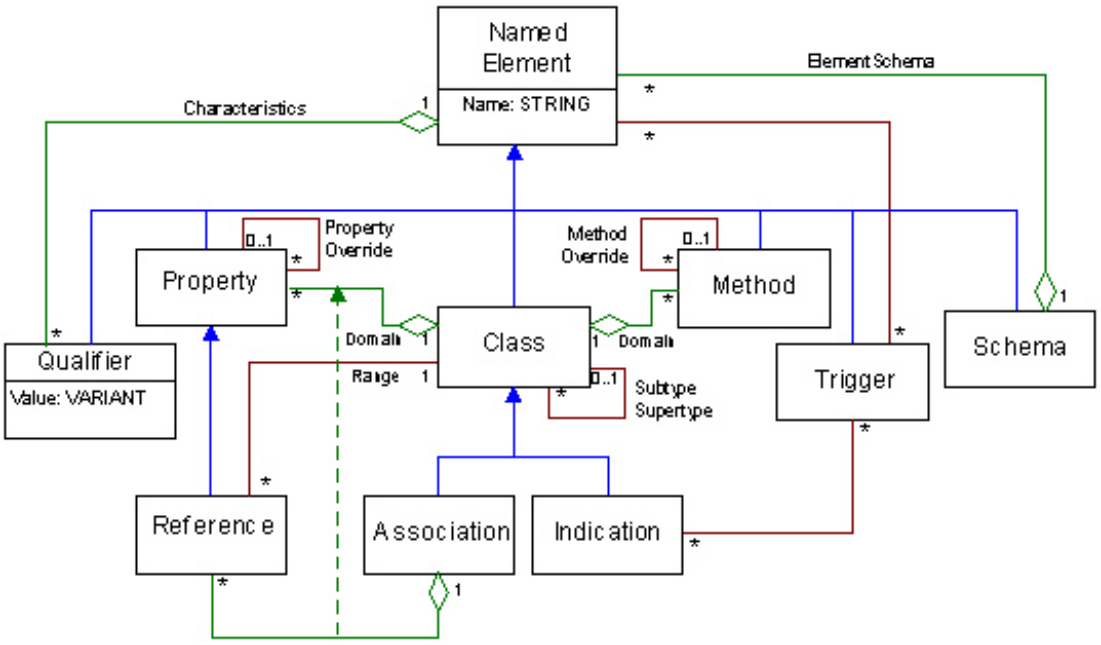

Abbildung 8.1: Klassen und Beziehungen des CIM-Meta-Schema in UML

nen bei Attributen und Methoden insbesondere ihren Datentyp bzw. Rückgabewert, können aber auch weitere Angaben zu einem beliebigen Named Element machen.
`Referenzen` definieren die Rollen, die Objekte in einer `Assoziation` spielen. Eine `Assoziation` repräsentiert Beziehungen zwischen mindestens zwei `Klassen`
Eine `Indication` repräsentiert das Auftreten eines Events. Damit ein Element ein Event empfangen kann, muß sich das Element beim Event registrieren. Eine `Indication` ist nicht persistent, d.h. ein Event tritt auf und verschwindet dann wieder.
Management-Informationen werden im MOF-Format ausgetauscht. Dabei werden Objekte textuell repräsentiert. Die Notation wird in erweiterter Backus-Naur-Form dargestellt.

8.5 CIM-Schema

Das CIM-Schema ist eine Sammlung von Bausteinen für Management-Plattformen und -Applikationen. Definiert werden einige grundlegende Klassen. Diese sind soweit generalisiert, dass sie für alle Aspekte des Systems Management verwendet werden können. Das CIM-Schema besteht aus einem Core-,einem Common-Model und einem Extension-Model.

8.5.1 Core-Model

Das Core-Model ist eine Menge von Klassen, Assoziationen und Eigenschaften, die ein Basisvokabular für das Beschreiben von Management-Systemen anbieten. Es ist die Grundlage für das Common-Model und wird deshalb mit ihm gemeinsam von der DMTF weiterentwickelt.
Das Core-Model besitzt ein einziges Wurzelelement namens `ManagedElement` 8.2.

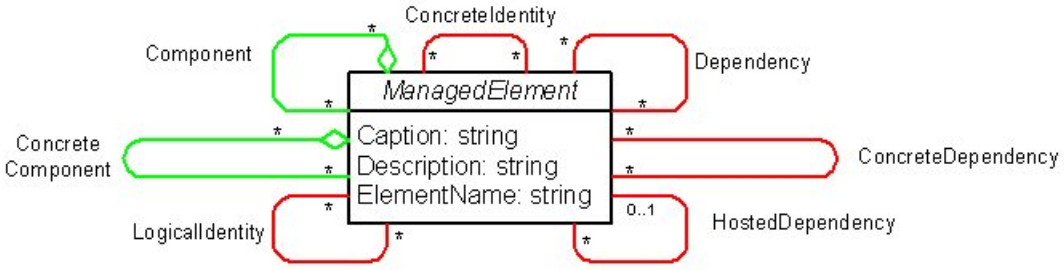

Abbildung 8.2: Wurzelklasse ManagedElement

Dieses Element ist eine Referenz für Assoziationen, die sämtliche Entitäten der Hierarchie betrifft. Es wird von einer Vielzahl weiterer Klassen direkt oder indirekt spezialisiert. Das Modell expandiert von hier aus in eine Vielzahl verschiedener Richtungen, um die vorhandenen Managementprobleme zu lösen[5].
Wie schon weiter oben erwähnt, werden sämtliche Objekte mittels MOF beschrieben. Das folgende Beispiel zeigt das `ManagedElement` in seiner textuellen Form. Sie ist in der Datei `Core28_CoreElements.mof` zu finden [1].

```
// ==================================================================
// ManagedElement
// ==================================================================
   [Abstract, Version ( "2.7.0" ), Description (
       "ManagedElement is an abstract class that provides a common "
       "superclass (or top of the inheritance tree) for the "
       "non-association classes in the CIM Schema.")]
class CIM_ManagedElement {

      [Description (
          "The Caption property is a short textual description (one- "
          "line string) of the object."),
       MaxLen ( 64 )]
   string Caption;

      [Description (
          "The Description property provides a textual description of "
          "the object.")]
   string Description;

      [Description (
          "A user-friendly name for the object. This property allows "
          "each instance to define a user-friendly name IN ADDITION TO "
          "its key properties/identity data, and description "
          "information. \n"
          "Note that ManagedSystemElement's Name property is also "
          "defined as a user-friendly name. But, it is often "
          "subclassed to be a Key. It is not reasonable that the same "
          "property can convey both identity and a user friendly name, "
          "without inconsistencies. Where Name exists and is not a Key "
          "(such as for instances of LogicalDevice), the same "
          "information MAY be present in both the Name and ElementName "
          "properties.")]
   string ElementName;
};
```

Aus dieser Beschreibung lässt sich herauslesen, dass das `ManagedElement` eine abstrakte Klasse ist. Sie enthält drei Attribute:

[5] Aufgrund der hohen Komplexität und Anzahl an Ableitungen ist eine vollständige textuelle als auch visuelle Beschreibung hier nicht zweckmäßig

- `Caption` - eine Kurzbeschreibung des Objekts
- `Description` - ermöglicht eine ausführliche Beschreibung des Objekts
- `ElementName` - ein menschenlesbarer Name des Objekts.

8.5.2 Common-Model

Das Common-Model beschränkt sich auf Teilgebiete der Betreuung von Systemen und nutzt dafür die Basisobjekte des Core-Model. Es bleibt trotzdem unabhängig von der Technologie und Implementation. Die Teilgebiete sind detailliert genug, um sie als Basis für das Programmdesign oder gar die Implementation zu nutzen.

Application: Die Klassen des Applicationmodel erlauben es insbesondere, Softwareprodukte in ihrer Ausführung und ihrem Lebenszyklus zu betreuen. Unter dem Lebenszyklus von Software versteht man die Entwicklung, danach die Installation und Konfiguration, die Ausführung und den laufenden Betrieb, inklusive Monitoring. Auch können Abhängigkeiten von Softwarepaketen untereinander und zu Betriebssystemen modelliert werden.

Database: Das Database-Model dient der Modellierung von Datenbanken. Dargestellt werden können Datenbanksoftware, -instanzen und -dienste. Normalerweise werden drei Entitäten modelliert: das Datenbanksystem (repräsentiert die Softwareaspekte der Datenbankumgebung); die Datenbank (repräsentiert die strukturierten Daten) und die Datenbankservices (führen Aufgabe für die Datenbank aus, z.B. Anwendern die Arbeit auf der Datenbank zu gewähren)

Device: Mittels des Device-Model werden Klassen zur Darstellung von Hardwarekonfigurationen vorgegeben. Dazu gehören zum Beispiel die Spannungsversorgung, Prozessoren, Controller, Bussysteme, Netzwerkkarten, FibreChannel, Medien, PC-Peripheriegeräte und Drucker. Auch Konzepte wie Redundanz und Load Balancing wurden hier berücksichtigt.

Event: Das Event-Model dient der Beschreibung von Ereignissen, die in einer CIM-Umgebung ausgelöst werden können und als Indications bezeichnet werden. Es definiert deren Behandlung, die bei der Modifikation von Klassen ausgelöst werden können. Wenn ein Webserver beispielsweise nicht mehr genügend Speicher hat, muss darauf entsprechend reagiert werden.

Interoperability: Das Interoperability-Model definiert die Management-Komponenten, die die WBEM[6]-Infrastruktur beschreiben und wie andere WBEM-Komponenten, wie Provider und Protokoll-Adapter mit der Infrastruktur interagieren. Dies ermöglicht das Verwalten von Software, die für eine Implementierung clientseitig eingesetzt wird und die Beschreibung von CIM-Infrastrukturen. Auf WBEM wird später noch ausführlicher eingegangen.

Physical: Das Physical-Model definiert Klassen für die Beschreibung von Hardware, wie Gehäuse, Schränke, Stecker, Kabel, Karten, Chips, Medien und Aufstellungsorte.

[6] WebBased Enterprise Management

System: Das System Schema behandelt alle Klassen, die von einem Computersystem abgeleitet werden, aus logischer Sicht. Dazu gehören Prozesse, Dienste, Zeitzonen, Hard- und Softwareressourcen, Protokolle, Diagnoseroutinen und Spezialisierungen für UNIX-Betriebssysteme.

User: Das User-Model definiert alle Klassen, die in Bezug zur Security- und Benutzerverwaltung stehen. Zudem gibt es organisatorische Klassen, welche Kontaktinformationen der Firmen und deren Beziehungen darstellen.

Policy: Mittels des Policy-Model können Regeln, bestehend aus Bedingungen und Aktionen, definiert werden. Dies ermöglicht die Repräsentation von Service Level Agreements.

Metrics: Das Metrics Schema definiert Klassen zur Repräsentation von Einheiten, insbesondere von Arbeitseinheiten für die Abrechnung von Geleistetem (sowohl von Personen als auch von EDV), was für das Performance Management von Bedeutung ist.

Network: Das Network Schema beinhaltet Klassen für die Repräsentation von Netzwerkgeräten und -strukturen. Es bietet Klassen wie RangeOfIPAddresses (IP-Adressbereich), FilterList (Netzwerkfilterung), Routingbeschreibungen, SNMP-Integration und die Darstellung von Routingprotokollen wie OSPF, BGP und Spanning Tree.

Support: Dieser Bereich bildet den Solution Exchange Standard (SES) ab. Dabei handelt sich um ein Modell für die Repräsentation von Ticketsystemen und Knowledgebases.

8.5.3 Extension-Model

Ein CIM Extension-Model ist ein erweitertes Modell, das ein spezifisches Hard- oder Softwareprodukt repräsentiert und im Idealfall mit diesem ausgeliefert wird [4]. Da ein Extension-Model nicht mehr generisch ist, wird es auch nicht durch die DMTF normiert. Statt dessen werden in einem Extension-Model Klassen des Common-Model durch Vererbung für ein konkretes Produkt angepasst.
Durch den objektorientierten Ansatz von CIM ist es auf diese Weise jederzeit möglich, auch proprietäre Systeme einheitlich zu verwalten, solange das Common-Model als Modellierungsgrundlage verwendet wird. Klassen, die in einer CIM-Umgebung instanziiert werden, sind immer Klassen des Erweiterungs-Modell, da nur sie Objekten der realen Welt entsprechen. Vorhandene Implementierungen und somit auch Extension-Models werden noch vorgestellt.

8.6 Web Based Enterprise Management

Spezifikation und Datenmodell von CIM wurden vorgestellt. Jetzt wird etwas näher auf das Framework 8.3 eingegangen, das die Kommunikation zwischen Manager und den Ressourcen ermöglicht. Der Manager ist der Client in der CIM-Umgebung, die Ressource ist das verwaltete System und damit der Server.
Der CIM-Server verarbeitet die Anfragen vom Client und beantwortet diese. Die Codierung der Klassen, Instanzen und möglicher Operationen erfolgt in XML[7]. Die Daten

[7] Extensible Markup Language - Beschreibungssprache für Daten, welche eine Untermenge der Standard Generalized Markup Language (SGML) ist

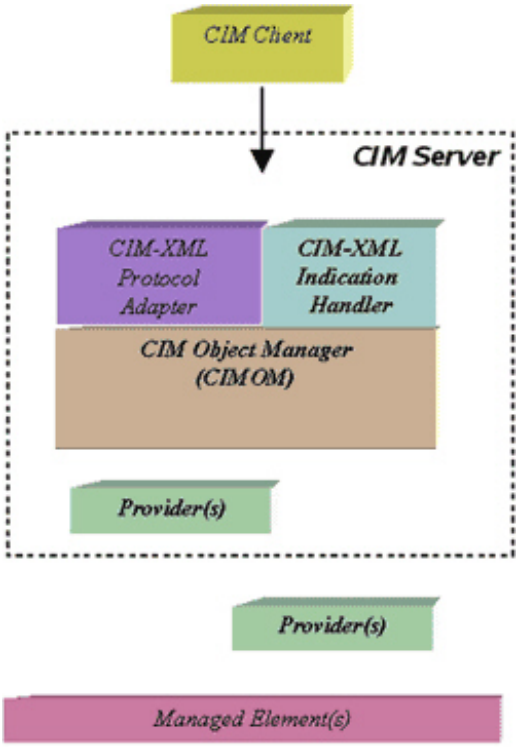

Abbildung 8.3: Infrastruktur des WBEM

werden über das Hypertext Transfer Protocol transportiert. HTTP eignet sich als verbindungsorientiertes Protokoll für den Transport.

- da die Verarbeitung in einer sicherheitsorientierten Umgebung durch Firewalls und Proxys möglich ist,
- im HTTP-Header Informationen über die WBEM-Operation mit übertragen werden können,
- Authentifizierungsmechanismen möglich sind.

Der TCP-Port für die Verbindung auf eine CIM-Ressource ist 5988.
Für die Repräsentation von CIM in XML, genannt xmlCIM, ist eine Document-Type-Definition(DTD) notwendig, welche die inhaltliche Struktur eines XML-Dokuments definiert. Die DTD wird nur für das Metaschema definiert, da eine Abbildung auf das gesamte Modell zu aufwendig wäre und die Verarbeitung performanter wird.
Während für das Management beliebige Applikationen zum Einsatz kommen können, die gegebenenfalls spezielle Verwaltungsaufgaben erfüllen, wie beispielsweise die Überwachung von kritischen Systemzuständen oder die Konfiguration von Anwendungen, bedarf es serverseitig einer verwobeneren Infrastruktur, damit ein System mit WBEM betreubar ist. Der CIM-Object Manager(CIMOM) ist die zentrale Komponente des Servers, welche die Kommunikation über den Protocol-Adapter und den Indication-Handler steuert. Er weiß, welche Klassen, Assoziationen und Qualifier existieren, fungiert als zentrale Schaltstelle für alle WBEM-Anfragen und bearbeitet sie. Ist eine Anfrage auf eine Klasse bezogen, wird sie über den CIMOM behandelt und den Protocol-Adapter beantwortet. Bezieht

sich die Anfrage dagegen auf eine Instanz, wird sie an den entsprechenden Provider weitergeleitet.
Für den umgekehrten Weg in Form einer Indication, ist der Indication-Handler zuständig. Er weiß, welches Ereignis, das von einem Provider gemeldet wird, an welchen Manager zuzustellen ist. Die interne Datenbank des CIMOM ist ein Repository in welchem die Klasseninformationen hinterlegt sind.

8.7 Implementationsbeispiel Windows Management Interface

Integrierte CIM-Lösungen sind Betriebssysteme, bei denen ein CIMOM sowie Provider und Instrumentierung mitgeliefert werden. Als Beispiel wird das Windows Management Interface (WMI), das einen einheitlichen Zugriff auf alle Systemparameter garantiert, näher vorgestellt. Sun bietet auch ein WBEM an, mit dessen Extension Model, große Teile der Betriebssystemumgebung per CIM verwaltet werden können.
CIM ist seit Windows NT4 Fixpack 4 unter dem Namen WMI integriert. Damit wirbt Micrsoft für WBEM-Fähigkeit von Windows, doch in Wirklichkeit kommunizieren CIM-Clients über COM und DCOM. Mit WMI betreubar sind bspw. der Betriebssystemkern, die Registry, die Netzwerkinterfaces, etc.
Mit dem Kommandozeilenprogramm wbemdump.exe können Klassen und Instanzen abgefragt, Methoden aufgerufen, sowie komplexere Anfragen formuliert werden. Der WMI-Browser erlaubt es, die CIM-Klassenhierarchie zu betrachten, mit dem CIM Studio, das auf den WMI-Browser aufbaut, können auch Instanzen bearbeitet werden. Die mitgelieferte VisualBasic-Script-API ermöglicht es scriptbasierend beliebige Managementtätigkeiten durchzuführen. Eine typische Anfrage in WMI an einen Client-Rechner sieht wie in Abb. 1.4 aus [6].

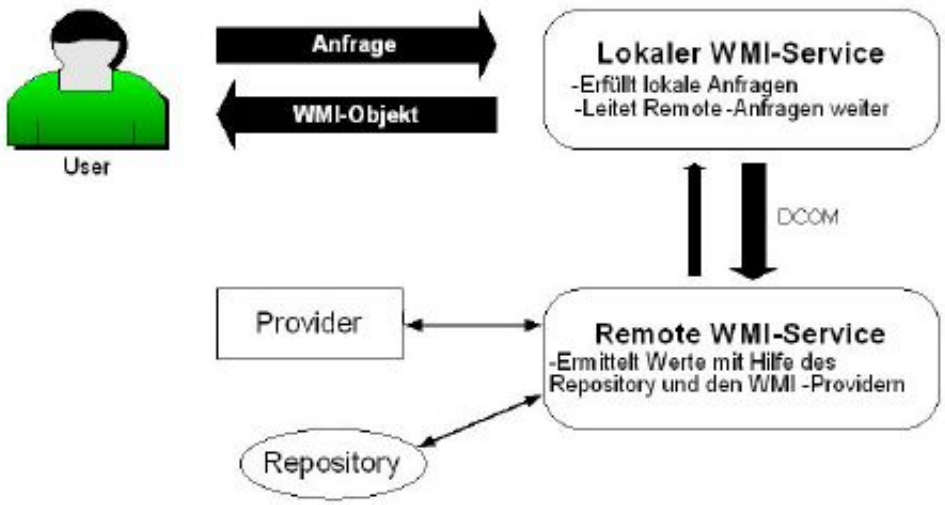

Abbildung 8.4: Weg einer Anfrage

Um Informationen abzufragen muß die WinMgmt.exe, der CIMOM, auf dem Client gestartet sein. Sie entscheidet, ob sich die gewünschte Information im CIM-Repository befindet oder ob die Anfrage an einen Provider weitergeleitet wird. In letzterem Fall ist

außerdem zu entscheiden, welches der geeignete Provider ist und wo er sich befindet. Diese Daten werden mit der Registrierung eines Providers verfügbar.[5]

8.8 Produkte zur Systemverwaltung

Seit 2003 wird mit dem Systems-Management-Server von Microsoft ein Produkt angeboten, um Systeme zentral und effizient auf der Seite des Managers zu verwalten. Das Produkt Tivoli von IBM zur Systemverwaltung ist weiter verbreitet. Ein Grund dafür kann sein, daß unter Windows WMI unterstützt wird und zusätzlich für UNIX ein eigenes CIMOM mit Providern bereitsteht. Das Subsystem Tivoli Monitoring dient im Rahmen des Accountings und der Verfügbarkeitsüberwachung speziell der Kontrolle von Betriebssystemen und Anwendungen. Man kann also davon ausgehen, daß CIM in der Industrie unterstützt und eingesetzt wird, auch wenn Microsoft den Transport anders realisiert.
Einen weiterer vielversprechender Ansatz, den die Plattform XA-Suite der Firma XAware [7] bietet, ist die Unterstützung der Service Oriented Information Integration (SOII). Hierbei werden Informationen für andere Systeme über Web-Services verfügbar gemacht. Die Charateristika von SOII sind:

- Lose Kopplung - Verbraucher brauchen nur noch den Ort der zu verwendenden Software zu kennen. Anwendungsfunktionalität und die aufrufenden Programm können beliebig ausgetauscht werden.
- Grobkörnigkeit - Benutzer interagieren mit Systemen durch eine API[8], die auf einer kleinen Menge von Nachrichten basiert.
- Standardbasiert - Integrations-Werkzeuge, die Standards benutzen reduzieren die Kosten für Integration und ermöglichen Entwicklern eine schnelle Einarbeitung und Nutzung der Plattform.

Die XA-Suite bietet lose gekoppelte Datenintegration an. Dabei wird XML genutzt, um metadatenbasierte Modelle der zu integrierenden Informationen bereitzustellen. CIM wird als eine solches Metadaten-Modell angesehen. Durch die CIM-Abstraktion können Informationen zwischen verschiedenen Systemen einfacher ausgetauscht, integriert und wiederverwendet werden. Dadurch verringert sich der Aufwand und die Komplexität von Integrationsprojekten.

8.9 Zusammenfassung

Das Common Information Model (CIM) ist ein ausserordentlich mächtiges und komplexes Informationsmodell zur Verwaltung von Komponenten innerhalb von Systemen und über deren Grenzen hinaus. Es bietet Entwicklern ein ausführliches und dabei flexibles generisches Modell zur Entwicklung spezieller Managementanwendungen.
Die Arbeit an CIM zeigt, dass die Ziele der DMTF erreichbar sind. Darüber hinaus zeigt sich ebenfalls, dass die Ergebnisse dieser Arbeit teilweise Akzeptanz in der Geschäftswelt finden, siehe WMI und Tivoli. Dies kann auf die Nutzung bewährter objektorientierter Techniken und vorhandener Beschreibungs- und Modellierungsstandards wie MOF und

[8] Application Programming Interface

UML zurückzuführen sein.
Das CIM ist nur ein Baustein innerhalb eines komplexen Zusammenspiels vieler verschiedener Protokolle und anderer Standards, ohne die eine Verwirklichung einer funktionierenden Systems-Management-Architektur nicht möglich wäre. Mit Verbesserung und Vereinfachung der verfügbaren Frameworks für die Systemverwaltung, wird sich das CIM auch gewinnbringender einsetzen lassen. Momentan ist die Einführung des Systemmanagement mit Nutzung von CIM noch komplex, langwierig und kostenintensiv. Mit weiterer Verbreitung, auch in kleineren Unternehmen wird es sich hoffentlich durchsetzen.

Literaturverzeichnis

[1] Inc. Distributed Management Task Force. Cim schema: Version 2.8.2 (final), 2003. http://www.dmtf.org/standards/cim/cim_schema_v28.

[2] Distributed Management Task Force, Inc. *DTMF - Distributed Management Task Force*, 2004. http://www.dmtf.org/home.

[3] Distributed Management Task Force, Inc., WBEM Solutions, Inc. *cimtutorial*, 2003. http://www.wbemsolutions.com/tutorials/CIM/.

[4] Klaus Jähne. Diplomarbeit: Management verteilter systeme und anwendungen mit dem common information model, 2003. http://kj.uue.org/papers/cim/cim.html.

[5] MSDN Library. *Die Windows Management Instrumentation in der Praxis*, 2004. http://www.microsoft.com/germany/msdn/library/windows/windowsnt/DieWindowsManagementInstrumentationInDerPraxis.mspx.

[6] Olaf Reuter Thomas Pätzold. Windows management instrumentation, 2004. http://www.rz.rwth-aachen.de/events/kursunterlagen/wb/SoSe04/wmi.pdf.

[7] XAware. *XAware*, 2004. http://www.xaware.com/soii/soii_overview.html.

9 An Overview of Distributed Security Architectures and Integration

Stefan Bartel, Hendrik Horn

Abstract

In diesem Dokument wird der Aufbau von Sicherheitsarchitekturen diskutiert. Dazu werden zuerst verschiedene verfügbare Sicherheitstechnologien vorgestellt. Anschließend wird versucht, eine allgemeine Vorgehensweise für das Erstellen einer Sicherheitsarchitektur vorzustellen.

9.1 Einleitung

Softwaresysteme sind mit der Zeit nicht nur komplexer und unübersichtlicher geworden sondern auch dezentralisierter. Das gilt sowohl in struktureller als auch in geografischer Hinsicht. Ein Großteil des vertraulichen Datenverkehrs verläuft damit durch "feindliches Gebiet".
Doch nicht nur der Datentransfer ist bedroht. In modernen B2C- B2B-Webapplikationen wird ein Teil des Systems zum Kunden bzw. Geschäftspartner ausgelagert. Dies stellt die IT-Sicherheit vor neue Herausforderungen. Es reicht nicht, dass nur die einzelnen Teile des Softwaresystems gesichert werden. Es reicht auch nicht, nur den Datentransfer durch Verschlüsselung zu sichern.
Wie in Abbildung 9.1 dargestellt, greifen aktuelle Anwendungen auf verschiedene Server und dahinterliegende Anwendungen zu. Hierbei kann man die Sicherheitsanforderungen in verschiedene Schichten aufteilen. Bei der `Perimeter-Tier` handelt es sich um die Zugriffe von Clients und Ressourcen über entsprechende Server auf andere Ressourcen, hierbei kommen also Techniken zur Absicherung der Verbindungen zum Tragen. Als zweites existiert die `Mid-Tier`, wobei es sich um die zur Verfügung gestellten Applikationen und deren Sicherheitskonzepte handelt. Die dritte Schicht ist die `Legacy-Tier`, die für die Datenhaltung verantwortlich ist.
Diese verschiendenen Technologien und Sicherheitsmechanismen müssen zu einer ineinandergreifenden Struktur zusammengeführt werden. Verteilte Softwaresysteme bedürfen einer verteilten Sicherheitsarchitektur.

9.2 Überblick über verschiedene Sicherheitstechnologien

9.2.1 Perimeter Tier

Bei den Sicherheitsanforderungen der Perimeter-Tier handelt es sich um den wahrscheinlich wichtigsten Teil: die End-to-End-Absicherung des gesamten Übertragungsweges.

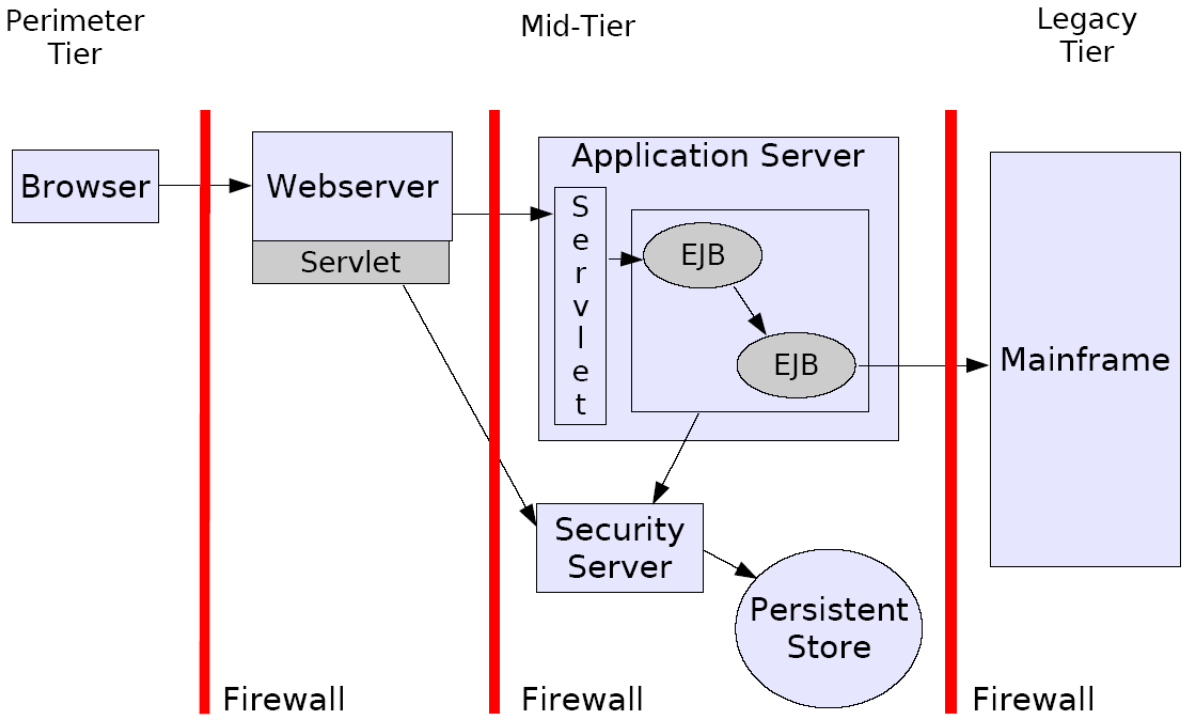

Abbildung 9.1: Verteilte Sicherheit (Quelle: [10])

Dieser muss sich nicht immer nur zwischen einem Browser und einer Anwendung befinden - für eine solche Point-to-Point-Verbindung würde auch eine SSL-Verschlüsselung genügen.
Die Dokumente können dabei auch über mehrere Zwischenstationen durch Netze mit unterschiedliche hohen Sicherheitsanforderungen geroutet werden oder es kann nötig sein, daß ein Partner nur einen Teil eines Dokumentes lesen darf, ein anderer wiederum einen anderen Teil oder das gesamte Dokument.

Die Anforderungen sind vielschichtig. Weshalb Lösungen entwickelt wurden, die möglichst einfach aber trotzdem mächtig genug sind, sowie hersteller- und plattformunabhängig funktionieren können. Wie in Abbildung 9.2 zu sehen, wurden deshalb bereits bestehende Standards wie XML mit Mechanismen zur Verschlüsselung und Signatur erweitert und neue Lösungen, hauptsächlich auf Basis von Markup-Languages, entwickelt.

SAML

Durch SAML, auch `Security Assertion Markup Language` genannt, wird ein XML basierendes Framework beschrieben, welches zum plattform- und herstellerunabhängig Austausch von Sicherheitsinformationen zwischen zwei Anwendungen über das Internet dient.
Ende 2000 wurde durch die Firma Netegrity bei der OASIS (Organization for the Advancement of Structured Information Standards) ein S2ML genannter Vorschlag für ein Sicherheitsframework eingereicht. Ausgehend von diesem Vorschlag wurde von einer OASIS-Arbeitsgruppe mit Mitgliedern wie IBM, Nokia, SAP und SUN die SAML

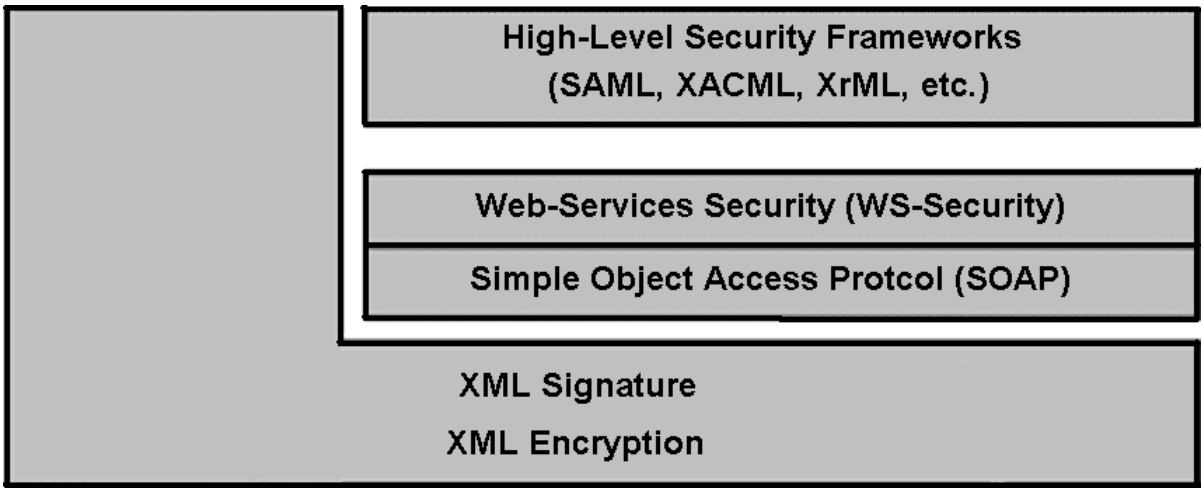

Abbildung 9.2: Sicherheit in der Perimeter-Tier (Quelle: [16])

entwickelt und durch diese in der Version 1.1 standardisiert.

Der Hauptgrund für die Entwicklung von SAML war es, eine einheitliche Lösung zu finden, mit welcher ein Domänenübergreifender `SSO` (SingleSignOn) ermöglicht wurde. Bisher war es nur möglich, per Browser Cookies zu hinterlegen, mit welchen der Nutzer daraufhin erkannt bzw. reauthentifiziert werden konnte. Jedoch werden die Cookies beim Nutzer gespeichert und sind somit leicht manipulierbar. Hinzu kommt, daß Cookies nicht zwischen zwei Domänen ausgetauscht werden können.

Die Hauptbestandteile der SAML-Spezifikation sind folgende:

- `Assertions`: Informationen zu Authentifizierung
- `Protokoll`: wie werden SAML-Assertions angefordert und übermittelt
- `Bindings und Profile`: wie werden SAML-Dokumente (Assertions) in Standardtransport- und Messaging-Frameworks eingebunden

Hierbei bilden die Assertions den Kern von SAML, sie stellen vertrauenswürdige Aussagen von Endanwendern oder Web Services dar, die sich über bestimmte digitale Identitäten definieren. Um das den Assertions entgegengebrachte Vertauen abzusichern, werden diese nur von Autoritäten ausgegeben, die zur Veröffentlichung von Bestätigungen bevollmächtigt sind (Assertion Issuing Authorities).
SAML Assertions beinhalten dabei Informationen, von wem und wann sie ausgestellt wurde, eine Assertion-ID, unter welchen Bedingungen sie gültig ist und die Angabe wie sie erstellt wurden.
Insgesamt gibt es drei Arten von Assertions. Zum einen die `Authentication Assertions`, durch welche bestätigt wird, dass bestimmte Benutzer auf geschützte Ressourcen zugreifen dürfen.
Weiterhin gibt es die `Attribute Assertions`. Diese bestätigen, dass ein Benutzer oder Web-Service bestimmten statischen Attributen (Rollen, Funktionen) oder dynamischen Attributen zugeordnet ist. Diese Attributsinformationen spielen dann bei der Zuweisung

von Zugangsberechtigungen eine wichtige Rolle.
Als dritten Typ stehen `Authorisation Decision Assertions` zur Verfügung. Mit diesen wird festgestellt, ob und wie auf eine spezifische Ressource zugegriffen werden darf.

Das eigentliche `SAML-Protokoll` definiert die Interaktion zwischen einem SAML-Requester und einem SAML-Responder. Dabei wird ein Request, welcher Anfragen für Authentifizierung, Attribute und Zugriffsentscheidungen beinhalten kann, von einem SAML-Client gestartet. Daraufhin erfolgt die Response von einem Sicherheitsdienst, die eine oder mehrere Assertions umfasst.

Die bereits angesprochenen `SAML-Bindings` legen fest, wie solche SAML-Request-Response-Nachrichten auf Standard-Übertragungsprotokolle abgebildet werden, beispielsweise mit einem SOAP-over-HTTP-Binding
Mittels `SAML-Profilen` wird spezifiziert, wie SAML Assertions in ein Message Framework oder ein Protokoll eingebunden und wieder extrahiert werden. SAML definiert ein Web Browser-Profil für den Zugriff auf einen Web-Service von einem Client und ein WS-Security-Profil (als Teil der WS-Security-Spezifikation 9.2.1) für die Interaktion zwischen Web-Services.

WS-Security

WS-Security ist eine von Microsoft, IBM und Verisign entwickelte Spezifikation zur Absicherung von SOAP-Nachrichten.

Hierbei werden die Möglichkeiten der Auszeichnungen im Headers von SOAP-Nachrichten um folgende Elemente erweitert:

- UsernameToken
- BinarySecurityToken
- SecurityTokenReference
- XML Digital Signature
- XML Encryption

Diese Auszeichnungen bieten die Möglichkeit, je nach Sicherheitsbedürfnis des Anwenders die verschiedensten - bereits etablierten - Technologien zu verwenden, wie beispielsweise XML-Encryption und XML-Digital Signature, aber auch X.509-Zertifikate oder Kerberos zur Authentifikation. Außerdem kann auch eine PKI (Public Key Infrastructure) verwenden, da in den Tags zusätzliche Daten eingebettet sein können, um auf einen öffentlich Schlüssel, Trustcentern und Ähnlichem zu verweisen.

Durch die Erweiterung des SOAP-Headers mit flexibel einsetzbare Auszeichnungen ermöglicht WS-Security somit die Absicherung der Packete, da das SOAP-Protokoll von sich aus keine Sicherheitsmechanismen enthielt.

XML-Encryption

XML-Encryption definiert einen vom W3C entwickelten Standard zur Verschlüsselung von Dokumenten unter Ausnutzung der XML Struktur.

Dabei gibt es 4 Arten, um Dokumente mit Hilfe von XML-Encryption abzusichern:

- Das gesamte XML-Dokument wird verschlüsselt
- Ein einzelnes Element des Dokumentes wird verschlüsselt
- Nur der Inhalt eines Elementes wird verschlüsselt
- Ein Dokument wird für mehrere Empfänger verschlüsselt

Um diese Arten der Verschlüsselung zu realisieren, wurden folgende Auszeichnungselemente definiert.

- EncryptedData
  - umhüllt verschlüsselten Inhalt des XML Dokumentes
  - Attribut TYPE kennzeichnet Umfang der Verschlüsselung
- EncryptionMethod
  - optionales Element zur Angabe des Verschlüsselungsalgorithmus
- CipherData
  - stellt die verschlüsselten Daten bereit
  - CipherValue und CipherReference sind Untertags
- CipherValue
  - umschließt die verschlüsselten Daten
- CipherReference
  - enthält eine Referenz, verweist beispielsweise auf verschlüsselte Daten
- KeyInfo
  - enthält Informationen über den benutzten Schlüssel, z.B. dessen Namen
- EncryptedKey
  - kennzeichnet den verschlüsselten Session-Key

XML-Digital Signature

Die XML-Digital Signature wurde spezifiziert durch das W3C im XML-Signature Syntax and Processing-Standard im RFC 3275. Festgelegt wurden hier die Regeln und Syntax, wie mit Hilfe digitaler Signaturen die Integrität und Authentizität von Dokumenten sichergestellt wird.

Um dies zu gewährleisten wird die Nachricht mit einem Fingerabdruck, z.B. mittels einer Hash-Funktion, versehen. Um diese Integrität zu gewährleisten, erfüllt die Digitale Signatur mehrere Anforderungen. So haben zwei Nachrichten mit Hilfe eines Timestamps nie den gleichen Fingerabdruck. Ansonsten handelt es sich im wesentlich um eine PKI(Public Key Infrastructure), wobei der private Schlüssel die Nachricht verschlüsselt

und der Empfänger die Nachricht mit dem öffentlichen Schlüssel wieder entschlüsselt. Weiterhin besteht auch die Möglichkeit, einzelne Teile des Dokumentes und/oder Dateien zu signieren.

Folgende Elemente wurden für die XML Signatur festgelegt:

- Signature - Tag für Signaturhülle
- SignedInfo - Information über die Daten und den verwendeten Algorithmus
- CanonicalizationMethod - Kanonisierungsalgorithmus
- SignatureMethod - Signaturverfahren
- Reference - Verweis auf die signierenden Daten
- KeyInfo - Schlüssel für Validierung
- DigestMethod - Hashverfahren
- DigestValue - Wert des Hashverfahrens

Um die XML-Signatur im Dokument zu Integrieren gibt es wiederum mehrere Möglichkeiten. Zum einen die sogenannte `Detached Signature`, wo die Signatur losgelöst vom Dokument ist.
Außerdem gibt es die `Enveloped Signature`, hierbei ist die Signatur in das Dokument eingebettet und schließlich die `Enveloping Signature`. Bei dieser wird die Signatur als Umschlag benutzt und umschließt das gesamte Dokument.

XACML

Um den Zugriff auf Dokumente einzuschränken bzw. zu verwalten gibt es den Standard der `eXtensible Access Control Markup Language`, welcher ebenfalls von der OASIS entwickelt wurde.
Hierbei handelt es sich im Grunde um eine Sicherheitserweiterung für XML, womit Zugriffsrechten auf XML-Dokumente oder Teile davon festgelegt werden können.

Die Kontrolle kann dabei nach verschiedenen Kriterien erfolgen:

- welche Operationen sind erlaubt (Lesen, Schreiben, Kopieren)
- wer hat eine Zugriffsberechtigtigung (z.B. nur Abteilungsleiter und darüber)
- über welche Protokolle darf der Zugriff erfolgen (z.B. nur uber HTTPS)
- welche Art der Authentifizierung wird benötigt (z.B. per Passwort)

Außerdem gibt es ähnlich wie bei SAML 9.2.1 ein Request/Response-Sytem um die benötigten Zugriffsrechte für das Dokument abfragen zu können.

9.2.2 Mid-Tier

Enterprise Java Beans

Das Sicherheitsmodell von Java basiert auf dem Sandkastenprinzip. Jedes Applet hat grundsätzlich nur auf seinen eigenen Arbeitsbereich (die sog. `Sandbox`) Zugriff. Dieser wird durch drei Sicherheitsmechanismen geschützt. Der `Bytecode-Verifyer` prüft die Integrität heruntergeladener Applets. Der `Class-Loader` lädt das Applet ins System und entscheidet, ob etwa eine schon existierende Klasse durch eine im Applet enthaltene Version ersetzt werden soll. Der `Security-Manager` vergibt weitergehende Rechte, die es dem Applet ermöglichen, aus der Sandbox herauszureichen, um z.B. bestimmte Dateien zu lesen oder zu schreiben, andere Programme aufzurufen oder auf Hardwarechnittstellen zuzugreifen. Einerseits ist diese feinkörnige Abstufung von Zugriffsrechten und -beschränkungen gut geeignet seine Java-Umgebung flexibel und individuell angepasst abzusichern, andererseits ist der Verwaltungsaufwand recht hoch, will man diese Sicherheitsmechanismen wirklich ausreizen.
Enterprise Java Beans sind im Grunde erst einmal Java-Applets. Damit stehen ihnen auch alle oben erwähnten Sicherheitsmechanismen zur Verfügung. Zusätzlich werden in einem Bean Sicherheitsrollen definiert, denen der Zugriff auf bestimmte Methoden gewährt oder verwehrt wird. Da diese Sicherheitsrichtlinien innerhalb des Beans bestimmt werden, spricht man auch von `Container-Managed Security`. Dadurch bleibt das Bean unabhängig von der jeweiligen Umgebung. Außerdem ist die Sicherheitskonfiguration des Beans automatisch durch den `Bytecode-Verifyer` vor unerlaubten Veränderungen geschützt. Soll ein EJB verwendet werden, wird dem Benutzer (`Principal`) eine der definierten Sicherheitsrollen zugewiesen.

9.2.3 Legacy Tier

Bei der Legacy-Tier handelt es sich um Netzinterne Reccourcen wie zum Beispiel Datenbanken, Gateways oder Ähnlichem mit welchen die Applikationen verbunden sind. Die Sicherheitskonzepte in dieser Schicht müssen zum einen die Authentifikation der Anwendung beim Mainframe und und zum anderen die Kommunikation zwischen den beiden Komponeten sicherstellen. Da diese Systeme Proprietär sind und kein einheitlicher Standard existiert, gibt es hier die Verschiedensten Möglichkeiten.

Üblich ist allgemein zumindest eine Authetifikation mittels Name und Passwort. Aber auch die Übermittlung von Zertifikaten und anderen Tokens kann implementiert sein, was jedoch seltener umgesetzt wird, da es sich bei der Verbindung zwischen Mid- und Legacy-Tier oft um Firmeninterne Netze handelt. Aus diesem Grund wird ebenso die Absicherung der Kommunikation zwischen den beiden Komponenten der TLS überlassen.

EJB

Für Authentifizierung bei Enterprise Java Beans gegenüber der Legacy-Tier gibt es zwei Möglichkeiten:

- Container-managed:
  Hierbei ist innerhalb des Codes nur eine Anfrage nach der Verbindung zu einer Ressource notwendig, die Loginprozedur wird vom Container übernommen durch eine Abfrage der Logindaten und den Login.

- Bean-managed:
  Bei dieser Möglichkeit wird der Loginvorgang, also auch die Logindaten, direkt vom Bean-Code übernommen.

9.3 Lösungsansätze

Bei den vielen vorhandenen und vorgestellten Techniken und Standards ist es leicht verständlich, daß es keine Lösung geben kann, welche eine komplette Sicherheitsarchitektur umsetzt. Vielmehr wird es dem Anwender ermöglicht, sich eine eigene Lösung nach seinen Anforderungen zusammenzustellen.

Identitätsmanagement

Das föderierte Identitätsmanagement spielt eine wesentliche Rolle zur Nutzerauthentifikation und dem rollenbasierten Zugriff auf Ressourcen. Dabei steht das "föderiert" dafür, daß dieser Zugriff und die Authentifikation organisationsübergreifend geschehen kann und somit SSO unterstützt.

Liberty Alliance Project

Bei dem Liberty Alliance Project handelt es sich um einen Zusammenschluß von über 150 Organisationen und Firmen. Diese haben es sich zum Ziel gesetzt, einen offenen Standard für förderiertes Identitätsmanagement zu schaffen, welcher möglichst alle aktuellen Netzwerkschnittstellen unterstützt. Dabei entstehen sogenannte "Liberty Enabled Products" [5], welche nach verschiedenen Spezifikationen des Liberty Alliance Project zertifiziert wurden.
Die Architektur ist dabei so spezifiziert, daß es jeweils Anwender, Service- und Identity-Provider gibt. Die Service- und Identity-Provider kann man dabei zusammenfassen, diese bieten gemeinsam die Services für die Anwender. Die Kommunikation zwischen Service- und Identity-Providern wird wie in Abbildung 9.3 dargestellt über den Anwender geroutet.

1. Anforderung einer Seite vom Service Provider durch den User Agent per HTTP-Request.
2. Service Provider antwortet mit einem Redirect (HTTP-Code 302). Dieser enthält im Header die URI des Identity-Providers und eine zweite eingebettete, welche wieder auf ihn verweist.
3. Der User Agent sendet HTTP-Request and den in Erfahrung gebrachten Identity-Provider mit der Absender-URI des Service-Providers
4. Der Identity-Provider antwortet daraufhin wieder mit einem Redirect, dessen URI ihm der User Agent in Schritt 3 mitgeteilt hat. Zusätzlich kann dieser Redirect noch eine URI zurück zum Identity-Provider enthalten.

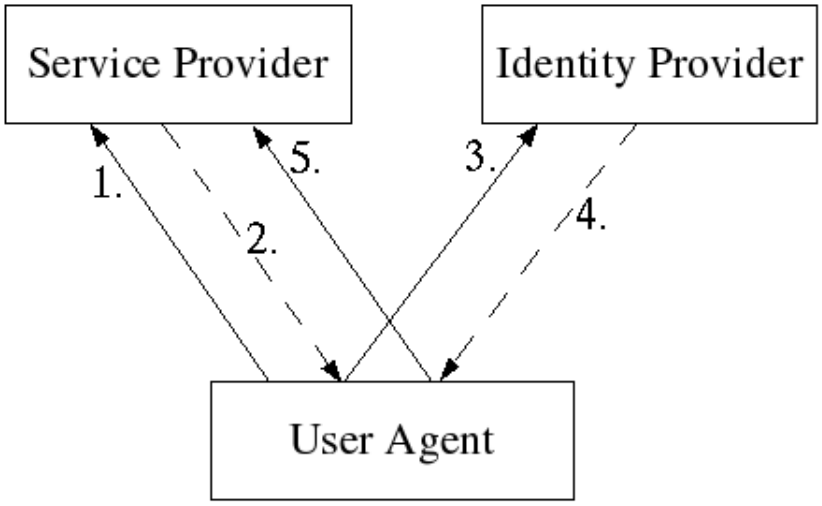

Abbildung 9.3: Liberty Alliance: Redirect-Architektur (Quelle: [23])

5. Der User Agent sendet wieder einen HTTP-Request an den Service-Provider auf die von dem Identity-Provider mitgeteilte URI aus Schritt 4 und wenn dieser noch eine eigene URI mitgeschickt hatte, wird diese dem Service-Provider ebenso mitgeteilt.

Außerdem können mittels der Redirects zusätzlich beliebige andere Daten ausgetauscht werden werden. Wenn zum Beispiel im Redirect-Header die Location http://www.foobar.com/auth?XYZ=1234 eingetragen wurde, dann ruft der User Agent die Adresse http://www.foobar.com/auth auf und übergibt den Parameter “XYZ” mit dem Wert “1234”.
Auf diese Weise können Service- und Identity-Provider beliebige Informationen miteinander austauschen. Beispielsweise gibt der Nutzer auf der Seite des Service-Providers per Auswahlbox seinen Identity-Provider an. Daraufhin wird er mit der Absenderadresse des Service-Providers dorthin geschickt. Kommt der User dann wieder mit der Angabe, daß er eingeloggt ist bzw. es bereits war, von diesem zurück, kann der Service-Provider direkt mit dem Identity-Provider kommunizieren und diesen nach benötigten Nutzer-Daten abfragen.

Shibboleth

Bei einer weiteren Lösung für das Identitätsmanagement handelt es sich um Shibboleth, welches in einem universitären Umfeld enstand und zur Zeit auch hier genutzt wird.
Die Kommunikation verläuft ähnlich wie beim Liberty Alliance Project. Allerdings gibt es bei Shibboleth für den Service-Provider die Möglichkeit einen so genannten WAYF-Service zu nutzen, um festzustellen, bei welchem Identity-Provider der Nutzer registriert ist. WAYF steht für “Where Are You From ?” und ist im Grunde nichts anderes als eine Anfrage (mit einer URI des Servive-Providers als Absender) an den User Agent, bei welchem Identity-Provider er registriert ist. dieser meldet sich dann bei seinem Identity-Provider an oder ist es bereits und übergibt die URI an diesen, worauf er sich über den User Agent ,vergleichbar mit Abbildung 9.3 vom Liberty Alliance Project, beim Service-Provider Meldet.

Die folgende Kommunikation zwischen den beiden Providern erfolgt direkt ohne User Agent und auf Basis von SAML (9.2.1).

9.4 Integration in eine Sicherheitsstruktur

Moderne IT-Systeme werden nicht sicher, indem man wahllos Sicherheittechnologien implementiert. Dazu sind sie viel zu komplex. Vereinzelte abgesicherte Punkte können leicht umgangen werden. Angreifer wählen immer den Weg des geringsten Widerstands. Systeme können außerdem auch sicher sein, aber gegen die falschen Bedrohungen.

9.4.1 Kategorisierung der Schutzmaßnahmen

Schutzmaßnahmen lassen sich auf verschiedene Art und Weise kategorisieren. Ordnet man sie zeitlich, ergeben sich folgende 3 Kategorien:

Vorbeugende Maßnahmen: Firewalls, verschlüsselte Kommunikation, Türschlösser, Elektrozäune

Angriffserkennung: Intrusion Detection Systeme (IDS), Logfiles, Bewegungsmelder, Wachdienst

Reaktion: IDS, Wachdienst, (Strafverfolgung)

Ein Hauptproblem besteht darin, dass die meisten IT-Sicherheitstechnologien in die erste Kategorie fallen und die beiden anderen gern vernachlässigt werden.

Man kann Schutzmaßnahmen auch in verschiedene “Sphären” unterteilen:

- IT-Software/-Hardware
- physischer Schutz
- der Mensch

Auch hier ist es wichtig, dass keine Sphäre ignoriert wird. Die beste Firewall ist nutzlos, wenn ein Angreifer leicht einbrechen kann, und sich direkt ans firmeninterne Intranet anschließt. Man kann IT-Sicherheit also nicht losgelöst von der gesamten Firmensicherheit betrachten. Dementsprechend ist es ein schwerer Fehler, wenn Firmenleitungen IT-Sicherheit einfach wegdelegieren, egal ob an den eigenen Systemadministrator oder externe Spezialisten. Sie muss mit allen anderen Bereichen abgestimmt werden.

9.4.2 Aufbau einer Sicherheitsarchitektur

Um eine sinnvolle Sicherheitsarchitektur zu erstellen sind 3 Schritte notwendig.

1. Risikoanalyse
2. Erstellen einer Sicherheitspolitik
3. Umsetzung dieser Sicherheitspolitik

Eine einmalige Anwendung dieser Schritte reicht allerdings nicht aus. Der Grund dafür ist, dass Punkt 3 das System verändert und damit letztendlich eine neue Risikoanalyse notwendig ist. Dazu kommt, dass die Risikoanalyse nie vollständig sein kann. Deswegen muss dieser Prozess wieder und wieder durchlaufen werden, wenn man auf eine sich ständig ändernde Sicherheitslage reagieren will.

Risikoanalyse

Bevor man eine Sicherheitsarchitektur entwirft, muss man sich einige grundlegende Fragen stellen.

- Welche Angriffsziele bietet mein System?
- Wer sind die Angreifer?
- Welche Mittel stehen ihnen zur Verfügung?
- Wie risikobereit sind sie?

So könnte z.B. ein Konkurrent versuchen,firmeneigene Daten zu entwenden. Ein solcher Angreifer würde recht vorsichtig vorgehen, da er nicht bemerkt werden will. Dafür verfügt er wahrscheinlich über einen beträchtlichen Etat und damit die Möglichkeit Profis für seine Zwecke anzuwerben. Allerdings wird er wirtschaftlich denken und Risiken, Aufwand und Nutzen gegeneinander abwägen. Wollen dagegen Hacker nur für Spaß und Ruhm die Webseite lahmlegen, ist es eher unwahrscheinlich, dass sie dafür große Risiken eingehen. Sie werden sich eher ein anderes Ziel suchen als eine Gefängnistrafe zu riskieren.
Davon ausgehend ergeben sich bestimmte `Bedrohungen` für das eigene IT-System. Damit bezeichnet man bestimmte, konkrete Angriffsformen, z.B. eine Denial-of-Service-Attacke, oder das Belauschen eines Rechners durch eine TEMPEST-Attacke (das Abfangen und Auswerten der elektromagnetischen Strahlung, die jedes elektrische Gerät abgibt). Dem gegenüber sucht man nach `Verwundbarkeiten` im eigenen System, also nach Schwachstellen, die von Angreifern ausgenutzt werden können.
Hat man die für sein IT-System in Frage kommenden Bedrohungen und Verwundbarkeiten aufgelistet, muss man deren Gefahrenpotenzial einschätzen, um sie gegeneinander abwägen zu können und danach gewisse Prioritäten zu setzen. Die Schwierigkeit besteht darin, korrekte Schätzungen abzugeben. Schon kleine Sicherheitslücken können einem gewillten Angreifer eventuell die Möglichkeit geben, immensen Schaden anzurichten.
Bei der `Quantitativen Risikoanalyse` schätzt man die Häufigkeit eines bestimmten Schadensfalles und den Verlust, den das Unternehmen dadurch hinnehmen müsste. Multipliziert ergibt sich daraus die jährliche Schadenserwartung (`ALE: Annual Loss Expectancy`). Als Basis dieser Schätzungen dienen vor allem Statistiken, die allerdings nur so verlässlich sind wie der Erfassungszeitraum der zugrundeliegenden Daten lang ist. Für sich ständig verändernde IT-Systeme greift man deshalb gern auf die `Qualitative Risikoanalyse` zurück. Diese verzichtet auf die Schätzung der Wahrscheinlichkeit eines Schadensfalles. Stattdessen beschränkt man sich darauf, Bedrohungen und vorhandene Verwundbarkeiten gegeneinander abzuwägen, und davon ausgehend das Risiko sozusagen "über den Daumen gepeilt" abzuschätzen. Hierfür ist Expertenwissen in Form von Sicherheitsspezialisten oder speziellen Wissensdatenbanken unabdingbar.

Erstellen einer Sicherheitspolitik

Ausgehend von der Risikoanalyse gilt es, eine Sicherheitspolitik zu entwerfen. Im englischen wird der Begriff meist in der Mehrzahl verwendet, da mit `Security Policy` die einzelnen Richtlinien bezeichnet werden, und weniger das Gesamtgebilde. Eine einzelne Security Policy könnte zum Beispiel so aussehen:

> "Equipment is always to be safeguarded appropriately - especially when left unattended." – RUSecure - Information Security Policies[2]

Die Security Policy besagt, dass Mitarbeiter ihre Hardware vor unerlaubtem Zugriff schützen müssen. Sie gibt jedoch nicht vor, wie dies umgesetzt werden soll, z.B. durch Verwendung eines Bildschirmschoners mit Passwortschutz oder von Kartenlesegeräten. Desweiteren muss eine solche Security Policy immer im Kontext anderer Policies betrachtet werden. So ist diese Regel uninteressant, wenn sowieso nur Befugte in die Nähe der Geräte kommen. Andererseits ist sie nicht ausreichend, wenn Besucher den Angestellten bei der Arbeit über die Schulter schauen können. Es kommt also darauf an, aus einzelnen Security Policies an eine Gesamtstrategie zu formen.
Eine Sicherheitspolitik ist nutzlos, wenn sie nicht angewendet wird. Deshalb ist es notwendig, dass sowohl Angestellte als auch das Management sie kennen und anwenden. Das bedeutet, dass sie auch praktikabel sein muss. Firmen versuchen immer so effizient wie möglich zu arbeiten. Effizienz und Sicherheit sind jedoch Gegenpole. Wie diese gegeneinander abgewogen werden, ist letztendlich Sache der Entscheidungsträger. Es ist also unabdingbar, dass das Management die Sicherheitspolitik nicht nur zur Kenntnis nimmt, sondern direkt in deren Entwicklung involviert wird. Nur so können Sicherheitspolitik und Geschäftsprozesse aufeinander abgestimmt werden. Das ist wichtig, denn die Verwundbarkeiten eines Systems sind immer irgendwie mit einem oder mehreren Geschäftsprozessen verbunden. Einige sind unvermeidbar, ein Onlineshop kann auf einen öffentlich zugänglichen Webserver nicht verzichten. Jedoch kann insbesondere die Vertraulichkeit der Daten durch die Optimierung der Geschäftsprozesse verbessert werden. Je weniger Mitarbeiter Zugang zu bestimmten Information benötigen, desto sicherer wird das Gesamtsystem.

9.5 Zusammenfassung

Bruce Schneier schreibt in seinem Buch "Secret & Lies"[8]: "Sicherheit ist ein Prozess." Man kann nicht ein IT-System aufbauen, es anschließend mit jeder Menge Sicherheitstechnologie versehen und erwarten, dass es sicher ist. Das hat damit zu tun, dass Sicherheit keine feste Größe ist. Angreifer werden immer neue Wege finden, in einen Computer oder ein Netzwerk einzubrechen. Dem kann man nur entgegentreten, indem man flexibel ist und seine Gegenmaßnahmen und Schutzmechanismen den neuen Gegebenheiten anpasst. Dazu kommt die immer weiter fortschreitende technische Entwicklung. Schnellere Rechner erleichtern Brute-Force-Attacken auf Kryptographie. Ständige Softwareupdates und Programmerweiterungen bergen neue Sicherheitslücken, die möglichst vor eventuellen Angreifern gefunden werden müssen. Das Hauptproblem liegt jedoch in der stetig steigenden Komplexität der zu schützenden IT-Systeme. Schon heute ist es unmöglich auch ein nur durchschnittlich komplexes System in allen Konfigurationen zu testen. Zertifikate wie ITSEC oder Common Criteria helfen, können aber nie vollständig sein. IT-Systeme werden wohl also in Zukunft unsicherer werden.

Literaturverzeichnis

[1] *Introduction to Security Risk Analysis & Security Risk Assessment*, 2001. http: http://www.security-risk-analysis.com.

[2] RUSecure - Information Security Policies Evaluation. 2001. http://www.information-security-policies-and-standards.com.

[3] *SUN Java Homepage*, 2004. http://java.sun.com.

[4] Liberty Alliance Project. *Liberty Alliance Homepage*, 2004. http://www.projectliberty.org.

[5] Liberty Enabled Products. *Liberty Alliance Homepage*, 2004. http://www.projectliberty.org/about/enabledproducts.php.

[6] shibboleth Project. *Shibboleth Homepage*, 2004. http://shibboleth.internet2.edu/.

[7] Björn Waide. SAML - Security Assertion Markup Language. 2003. http://www.ibr.cs.tu-bs.de/lehre/ss03/svs/ausarbeitungen/saml.pdf v.

[8] Bruce Schneier. *Secrets and Lies - IT-Sicherheit in einer vernetzten Welt*. dpunkt.verlag, 2001. ISBN 3-89864-302-6.

[9] Cover Pages - Online ressource for markup language technologies. Security Assertion Markup Language (SAML). Dezember 2004. http://xml.coverpages.org/saml.html.

[10] Don Flinn, Ted Burghart. An Overview of Distributed Security Architectures and Integration. 2002. http://www.omg.org/news/meetings/workshops/DOCsec-2002_Proceedings/02-1_Burghart-Flinn_DOCSec2002tutorial.pdf.

[11] Dr. Marcus Dormanns. E-Business Systemarchitekturen. 2002. http://kbs.cs.tu-berlin.de/teaching/ws2001/ebusiness/folien1fach/008_Sichere_Arch.pdf.

[12] Dr. Reinhard Riedl. Digitale Identitäten und Identitätsmanagement. *Verteilte Applikationsarchitekturen mit J2EE und .NET*, Oktober 2004. http://www.ifi.unizh.ch/egov/lectures/j2ee_ws04/IDMgmt041025.pdf.

[13] Eve Maler. SAML basics. http://www2002.org/presentations/maler.pdf.

[14] Georgi Todorov, Peter Jacobi. Sicherheit für Web Services. *Aktuelle Trends in Kommunikationsnetzen*, Januar 2003. http://www.nm.ifi.lmu.de/Hauptseminare/ws0203/handouts/ws-sicherheit-folien.pdf.

[15] Jan Steinkraus. EJB Sicherheit. 2003. http://www.inf.fu-berlin.de/lehre/WS02/sss/slides/EJB-Ausarbeitung.pdf.

[16] Marc Chanliau. Web Services-Sicherheit und die SAML. *XML & Web Services Magazin*, Januar 2004. http://www.entwickler.com/itr/online_artikel/psecom,id,468,nodeid,69.html.

[17] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, Ed Simon. XML-Signature Syntax and Processing. *W3C Recommendation*, Februar 2002. http://www.w3.org/TR/xmldsig-core/.

[18] OASIS Consortium. WSS Technical Commitee Homepage. 2004. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.

[19] Prof. Dr. Stefan Fischer. Sicherheit für Web Services. *Enterprise Applications*, 2004. http://www.ibr.cs.tu-bs.de/lehre/ss04/ea/EntApps-SS04-Kap10-WS-Security-3S.pdf.

[20] Scott Cantor. Shibboleth Architecture - Protocols and Profiles, Working Draft 05. *Shibboleth Homepage*, November 2004. http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-05.pdf.

[21] Scott Seely. Grundlegendes zu WS-Security. *Microsoft Homepage*, Juni 2004. http://www.microsoft.com/germany/ms/msdnbiblio/show_all.asp?siteid=559977.

[22] Takeshi Imamura, Blair Dillaway, Ed Simon. XML Encryption Syntax and Processing. *W3C Recommendation*, Dezember 2002. http://www.w3.org/TR/xmlenc-core/.

[23] Thomas Wason. Liberty ID-FF Architecture Overview. *Liberty Alliance Homepage*, 2004. http://www.projectliberty.org/specs/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf.

10 Multilateral Security - Mehrseitige Sicherheit

Johannes Orgis, Jörgen Kosche

Abstract

In dieser Ausarbeitung wird das Konzept der mehrseitigen Sicherheit (multilateral security) diskutiert. Dabei geht es darum, dass nicht mehr länger nur ein Teilnehmer in einem Prozeß geschützt wird, sondern nach Möglichkeit alle. Dies erlangt im Rahmen immer größerer Ansammlungen von persönlichen Daten zunehmend an Bedeutung.
Das Dokument geht auf die Ziele der mehrseitigen Sicherheit und deren technische Realisierung an. Weiterhin wird an Beispielen erklärt, wie es zu Konflikten zwischen diesen Zielen kommen kann, und wie man diese möglicherweise lösen kann.

10.1 Definitionen

Einige gängige Definitionen von mehrseitiger Sicherheit:

Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen aller beteiligten Parteien.
Kai Rannenberg: Kriterien und Zertifizierung Mehrseitiger IT-Sicherheit. Dissertation, Universität Freiburg, Wirtschaftswissenschaftliche Fakultät, 1997.

Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.
Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 83-104.

Während in den klassischen Sicherheitsmodellen die Sicht des Netzbetreibers im Vordergrund steht, berücksichtigt die mehrseitige Sicht auch und gerade die Sicht der Benutzer. Neben dem Schutz, den die Netze ihren Benutzern bieten, werden die Benutzer auch Mechanismen zum Selbstschutz benötigen, um die Abhängigkeit von anderen zu reduzieren. Damit schützen sich Telekooperationspartner nicht nur gegen Angriffe aus dem Netz, sondern sie wahren auch ihre Interessen gegeneinander, so wie Käufer und Verkäufer Geld und Quittung austauschen, manchmal sogar unter notariellen Augen.
G. Gattung, R. Grimm, U. Pordesch, M.J. Schneider: Persönliche Sicherheitsmanager in der virtuellen Welt, in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, Seite 182

Mehrseitige Sicherheit: Wo bisher bei der Einführung neuer Kommunikationsmedien und -dienste die Sicherheit des Betreibers (z.B. gegen unberechtigte Benutzung und Eintreibung der angefallenen Kosten) im Vordergrund stand, soll jetzt auch die Sicherheit des Benutzers eines neuen Dienstes Beachtung finden.
Andreas Bertsch, Herbert Damker, Hannes Federrath, Dogan Kesdogan, Michael J. Schneider: Erreichbarkeitsmanagement. PIK Praxis der Informatonsverarbeitung und Kommunikation 4/95 231-234

10.2 Einleitung

Mehrseitige Sicherheit ist ein Konzept, bei dem die Sicherheitsbedürfnisse aller an einem Prozeß beteiligten Parteien berücksichtigt werden. Dazu kann jede Partei ihre Sicherheitsbedürfnisse festlegen, treten Konflikte auf, müssen diese durch Aushandeln der Parameter beigelegt werden oder der Prozeß wird nicht durchgeführt. Grundlegend ist, dass jede Partei die technischen Vorraussetzungen besitzt, um selbst die Einhaltung seiner Sicherheitsbedürfnisse zu prüfen, sich als in der Beziehung nicht auf andere verlassen muss.
Es gilt also:

- Jeder Beteiligte hat Sicherheitsinteressen.
- Jeder Beteiligte kann seine Interessen formulieren.
- Konflikte werden erkannt und Lösungen ausgehandelt.
- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

Der Grundsatz hierbei ist, dass jede Partei nur minimales Vertrauen in Andere setzen muss. Bei herkömmlichen Sicherheitskonzepten ist. der Anwender immer der 'Gnade' Anderer ausgeliefert, da deren Sicherheitsbelange vorrangig durchgesetzt werden oder sie die Mittel zur Durchsetzung der Sicherheitsbelange kontrollieren. Somit ist der Anwender in diesem Fall nicht in der Lage seine Interessen gebührend zu wahren und durchzusetzen. Dies ist bei dem Konzept der Mehrseitigen Sicherheit nicht der Fall. Vorraussetzung hierfür ist, dass alle Parteien ihre Bedürfnisse formulieren können und die Möglichkeit haben ihre Schutzbedürfnisse zu wahren. Bei Widersprüchlichen Ansprüchen (z.B: steht das Bedürfnis nach Privatsphäre und Anonymität dem nach Wissen über den Partner entgegen) müssen Kompromisse zwischen den einzelnen Parteien ausgehandelt werden.

10.3 Schutzziele in der Mehrseitigen Sicherheit

Neben den klassischen Schutzzielen der IT Sicherheit wird bei der Mehrseitigen Sicherheit mehr Rücksicht auf die persönlichen Bedürfnisse der Parteien gelegt. Im Prinzip kann man die Schutzziele in zwei Gruppen einteilen: 'Unerwünschtes verhindern' und 'Erwünschtes leisten'.

10.3.1 Unerwünschtes verhindern

Wie bei den meisten klassischen Sicherheitsprinzipien geht es auch bei der Mehrseitigen Sicherheit darum, unerwünschte Effekte zu verhindern und so verschiedene Ansprüche zu realisieren.

Vertraulichkeit

Geheimhaltung von Daten während der Übertragung. Der Inhalt einer Kommunikation sollte nur den beteiligten Kommunikationspartnern bekannt sein. Weder der Betreiber des Netzes noch unerwünschte Lauscher sollen die Möglichkeit haben die Kommunikation zu verfolgen. Realisiert werden kann dies zum Beispiel durch Verschlüsselung der Kommunikation. Dabei sollte die Verschlüsselung/Entschlüsselung auf Seiten der Kommunikationspartner erfolgen, nicht unter der Kontrolle des Netzbetreibers oder einer weiteren Partei.

Verdecktheit

Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.
Um das Risiko eines Angriffs auf die Vertraulichkeit einer Kommunikation zu minimieren, sollte kein Aussenstehender bemerken, dass diese überhaupt erfolgt. Darüberhinaus kann auch das Wissen um die Existenz einer solchen Kommunikation vertraulich sein. Die Kommunikation sollte also ohne Mithilfe Aussenstehender initiiert und durchgeführt werden können.

Anonymität

Der Nutzer möchte gegebenenfalls Dienste und Ressourcen benutzen ohne, dass seine Identität bekannt ist. Dies kann zum Beispiel bei unverbindlichen Anfragen oder Gesprächen der Fall sein. Selbst der Kommunikationspartner soll gegebenenfalls die Identität des Benutzers nicht kennen. Dies ist zum Beispiel durch die Nutzung von Anonymisierungsdiensten welche die IP verbergen möglich, wobei hierbei wieder dem Betreiber dieses Dienstes ein gewisses Vertrauen geschenkt werden muss.

Unbeobachtbarkeit

Ähnlich wie bei der Verdecktheit möchte man verhindern, dass die Benutzung von Diensten und Ressourcen beobachtet werden kann, da die Existenz der Benutzung dieser ebenfalls als vertrauliche Information angesehen werden kann. Dritte sollen nicht die Möglichkeit haben, dass versenden und empfangen von Daten zu bemerken.

10.3.2 Erwünschtes leisten

Natürlich steht neben der Einschränkung von verschiedenen Aspekten auch die Gewährleistung von gewissen Bedingungen im Vordergrund.

Integrität

Damit Daten aus der Kommunikation auch als Beleg verwendet werden können und ihre Authentizität sichergestellt ist, müssen Modifikationen der kommunizierten Inhal-

te (Absender eingeschlossen) durch den Empfänger erkannt werden. Dies erreicht man beispielsweise durch die Verwendung digitaler Signaturen.

Zurechenbarkeit

Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden. Dies benötigt man möglicherweise zur Stellung einer Rechnung oder zum Durchsetzungen von Haftungsansprüchen. Spam mit gefälschten Absenderadressen ist ein Beispiel für die Folgen des Fehlens dieser Bedingung.

Verfügbarkeit

Nutzbarkeit von Diensten und Ressourcen muss immer ermöglicht werden, wenn ein Teilnehmer sie benutzen will. Dies schliesst die Bereitstellung ausreichender Rechenleistung zur Beibehaltung der Verfügbarkeit auch während Stosszeiten ein.

Erreichbarkeit

Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht. Der Zugang kann also nicht von Dritten eingeschränkt oder kontrolliert werden, sondern ist jederzeit uneingeschränkt verfügbar.

Verbindlichkeit

Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen. Dies setzt Zurechenbarkeit voraus und bedingt eine rechtliche Absicherung der Dienste.

10.3.3 Konflikte

Diese Bedingungen schliessen sich teilweise gegenseitig aus. So kann Anonymität und Zurechenbarkeit nicht gleichzeitig erfüllt werden. Konflikte müssen in für alle Beteiligten akzeptablen Kompromissen gelöst werden.

10.4 Beispiel: Handelsplattform

Als Beispiel zur Illustration verwenden wir eine Handelsplattform im Internet. Ein Anbieter stellt diese Plattform bereit und verlangt Provisionen für getätigte Handelsabschlüsse. Beliebige Personen oder Firmen können diese Plattform benutzen, um Waren oder Dienstleistungen anzubieten. Kunden können über die Handelsplattform auf die Angebote zugreifen.
Bei diesem Projekt gibt es drei beteiligte Parteien: der Anbieter der Handelsplattform, die Händler und die Kunden. Jede diese Parteien hat gewisse Sicherheitsbedürfnisse.

Anbieter:

Provision Die Provision wird gezahlt.

Händler:

Bezahlung Die Ware wird sicher bezahlt. Dies entspricht dem Ziel der Zurechenbarkeit, der Anbieter muss die Handelspartner identifizieren können, um ihnen eine Rechnung zu stellen.

Anonymität Die Kunden und der Anbieter der Handelsplattform kennen die Identität des Händlers nicht.

Kunde:

Lieferung Die Ware wird sicher geliefert.

Haftbarkeit Die Händler können im Zweifelsfall haftbar gemacht werden.

Anonymität Die Händler und der Anbieter der Handelsplattform kennen die Identität des Kunden nicht.

10.4.1 Konflikte

Einige dieser Ansprüche stehen offensichtlich im Widerspruch.

Anonymität(Händler) vs Haftbarkeit(Kunde)

Der Kunde hat das Bedürfnis die Identität des Händlers zu kennen damit er ihn im Falle von Schadenersatzforderungen haftbar machen kann.

Bezahlung (Händler) vs Anonymität(Kunde)

Der Händler möchte natürlich die Identität des Kunden kennen um ihm eine Rechnung zustellen und gegebenenfalls Schritte bei Nichtbezahlung unternehmen zu können.

10.4.2 Lösung

Um die Konflikte aufzulösen müssen alle beteiligten Partner einen praktikablen Kompromiss ausarbeiten der möglichst viele Bedürfnisse erfüllt. Als Lösung könnte man dem Anbieter der Handelsplattform eingeschränkt Vertrauen schenken. Dieser kennt die Identität von Kunden und Händler und sichert die Erfüllung der jeweiligen Ansprüche ab. So kann die Transaktion (sowohl der Versand der Ware, als auch der des Geldes) über die Handelsplattform abgewickelt werden. Der Händler schickt also die Ware an den Plattformbetreiber, der Kunde überweist dorthin sein Geld. Sobald beides eingetroffen ist, leitet der Plattformbetreiber beides weiter an den jeweiligen Handelspartner. Dabei kann auch gleich die Provision abgezogen werden. Trifft eines von beiden nicht rechtzeitig ein, wird die Transaktion abgebrochen und der ehrliche Partner erhält seine Ware oder Geld zurück. Bei Haftungsansprüchen des Kunden, setzt der Plattformbetreiber diese für den Kunden durch.

10.5 Beispiel: E-Mail

Als 2. Beispiel zur Erläuterung verwenden wir das Prinzip der E-Mail. Der Bereich der elektronischen Post weitet sich immer mehr aus und wird zu einem festen Bestandteil unseres Lebens. Leider sind viele Sicherheitsbedürfnisse auf diesem Gebiet nicht erfüllt.

10.5.1 Ansprüche der Benutzer

Ein kurzer Abriss über einige Bedürfnisse die ein Benutzer dieses Dienstes stellen könnte.

Zurechenbarkeit Erhaltene E-Mails sollen eindeutig einem Absender zuzuordnen sein.

Anonymität Der Sender einer E-Mail möchte anonym bleiben.

Vertraulichkeit Der Inhalt der E-Mail soll nur dem Empfänger zugänglich sein.

Integrität Der Inhalt einer E-Mail muss dem entsprechen was der Absender gesendet hat.

Verfügbarkeit Ich muss jederzeit E-Mails senden und empfangen können.

Eingangskontrolle Der Benutzer möchte bestimmen von wem er E-Mails erhält (SPAM)

Verlässlichkeit Der Absender möchte sichergehen, dass seine E-Mail ankommt.

10.5.2 Konflikte

Auch hier tun sich in einigen Bereichen Konflikte auf vor allem wenn man betrachtet wofür verschiedenen Anwender dieses Medium benutzen wollen.

Zurechenbarkeit vs Anonymität

Der Wunsch nach Zurechenbarkeit wird deutlich wenn man sich den Anteil an SPAM-Mails im heutigen E-Mail Verkehr vor Augen führt (und aus eben diesem Grund wird der Versender eben dieser gerne Anonym bleiben). Zwingend wird er spätestens im Fall von Drohungen/Beleidigungen über dieses Medium.

Vertraulichkeit

Auch wenn es sich bei diesem Bedürfnis nicht unbedingt um einen Konflikt handelt so muss im Hinblick auf das Prinzip der multilateralen Sicherheit betrachtet werden wer die Vertraulichkeit garantiert.

Integrität

Ebenso bei diesem Punkt ist zu betrachten wer diesen Punkt gewährleisten soll.Kritisch in dieser Beziehung ist die Veränderung von E-Mails durch Viren.

Eingangskontrolle vs Verlässlichkeit

Dem Wunsch nach einer Regulierung des E-Mail Empfangs z.B. um bestimmte Absender auszuschliessen steht das Bedürfnis nach einer verlässlichen Zustellung der Mail entgegen.

10.5.3 Lösungen

Wir versuchen einige mögliche Lösungen für die genannten Konflikte zu nennen.

Zurechenbarkeit vs Anonymität

Eine Möglichkeit für die Lösung dieses Konfliktes wäre, E-Mail Konten fest an Reale Personen (Personengruppen e.c.t.) zu binden die Daten darüber jedoch verschlüsselt beim Anbieter des Kontos zu belassen, so dass die Anonymität des Benutzers im normalen Verkehr gewahrt bleibt und im Bedarfsfall (z.B. zur Einleitung rechtlicher Schritte) vom Anbieter erfragt werden kann. Dies setzt jedoch vorraus, dass das Versenden von E-Mails nur von registrierten Benutzerkonten aus erfolgen kann.

Vertraulichkeit

Da beim Prinzip der Multilateralen Sicherheit jede Partei soweit möglich ihre Bedürfnisse selbst befriedigen können soll bietet sich hierbei die Verschlüsselung des E-Mail Verkehrs an (so beide Kommunikationspartner den jeweiligen Schlüssel kennen). So müssen die Benutzer nicht auf die Sicherheit der Datenleitungen und Systeme des Anbieters vertrauen.

Integrität

Immer wieder kommt es vor, dass E-Mails durch Viren verändert werden (unerwünschte Anhänge e.c.t.) oder ohne das Wissen des Benutzers versandt werden. Als Lösung bietet sich neben der Verwendung von Checksummen auch der Einsatz eines Virenscanners auf der Seite des Empfängers an. (Minimales benötigtes Vertrauen in den Kommunikationspartner)

Eingangskontrolle vs Verlässlichkeit

Eingangskontrolle wird heutzutage schon verstärkt durchgeführt vor allem in Form von Filtern welche den Anwender vor unerwünschten E-Mails schützen sollen. Eine Mögliche Lösung wäre ein zentraler Dienst für dringende Nachrichten welcher eine genaue Identifikation des Senders zulässt. So können dringende Nachrichten sicher gesendet werden und die Filter des Adressaten können aktiv bleiben.

10.5.4 Fazit Beispiel E-Mail

Man sieht unschwer, dass sich bei genauerem Hinsehen auch in diesem einfachen Beispiel verschiedenste Konflikte und Lösungen ergeben. Der Vorteil des Konzepts der Multilateralen Sicherheit ist hierbei, dass in einigen Bereichen (z.B. Filter,Virenscanner,Verschlüsselung) dem Benutzer überlassen ist in welchem Umfang er eine Absicherung benötigt. Dies hat noch grössere Wichtigkeit im Hinblick darauf, dass das momentane Konzept der E-Mail fast keine Sicherheitsaspekte berücksichtigt.

10.6 Zusammenfassung

Mehrseitige Sicherheit ist ein Konzept, bei dem die Sicherheitsbedürfnisse aller an einem Prozeß beteiligten Parteien berücksichtigt werden. Dazu kann jede Partei ihre Sicherheitsbedürfnisse festlegen, treten Konflikte auf, müssen diese durch Aushandeln der Parameter beigelegt werden oder der Prozeß wird nicht durchgeführt. Grundlegend ist, dass jede Partei die technischen Vorraussetzungen besitzt, um selbst die Einhaltung seiner

Sicherheitsbedürfnisse zu prüfen, sich also in der Beziehung nicht auf andere verlassen muss.

Literaturverzeichnis

[1] Dr. Helmut Bäumler. IT-Sicherheit - für wen? *Vortrag auf dem 5. Deutschen IT-Sicherheitskongreß des BSI am 30. April 1997 in Bonn*, 1997. http://www.datenschutzzentrum.de/material/themen/divers/itsichfw.htm.

[2] Kai Rannenberg. Multilateral Security - A concept and examples for balanced security.

[3] Sebastian Clauß, Marit Köhntopp. Identity management and its support of multilateral security. http://drim.inf.tu-dresden.de/literatur/ClKoe_01CompNetworks.pdf.

11 Distributed Security Framework for Multimedia Transmissions

Henrik Hinrichs, Christian Förster

Abstract

Im folgenden Dokument wird über die Entwicklungen im Bereich der Sicherung multimedialen Datentransfers und die Implementation solcher Mechanismen am Beispiel des Distributed Security Framework for Multimedia Transmissions berichtet.

11.1 Einleitung

In den letzten Jahren gab es gewaltige Fortschritte in den Bereichen von Multimedia-Streaming-Technologien. Durch die Steigerung der Leistungsfähigkeit aktueller Rechner, die immer bessere Kompressionsverfahren ermöglichten, und die immer größere Verbreitung von breitbandigen Internetanschlüssen wird der Transfer von digitalem Content in immer bessere Qualität möglich. Dabei macht es immer weniger Unterschiede ob nur Ton oder auch Bild an eine große Anzahl von Clients übertragen werden soll, ob diese nun im selben Gebäude über ein lokales Netz, oder weltweit verteilt durch das Internet verbunden sind. Aber bei all diesen neuen Entwicklungen darf man die Sicherheit der so übertragenen Daten nicht vernachlässigen.

So tauchen mehrere Probleme auf, die alle bewältigt werden müssen, die Authentifizierung der Clients, die sichere Datenübertragung, der Copyrightschutz und die Bestätigung der Herkunft der Daten. All diese Probleme können über verschiedene Protokolle und Standards gelöst werden, jedoch ist es wichtig ein komplettes integriertes und flexibles Paket zu liefern, das es einfach ermöglicht all das genannte unter einen Hut zu bekommen.

11.2 Sicherheit bei Multimedialem Datentransfer

11.2.1 Einleitung

Um zu einem Sicherheitspakt bei Multimediadatenübertragung wie Video-Streaming zu kommen muss man sich zuerst fragen wo security nötig ist, woher Gefahren drohen und wie man ihnen entgegen treten kann. Man unterscheidet Sicherheitskonzepte in zwei Ebenen: die des Netzes und die der Anwendung. Die erstgenannte beschäftigt sich mit dem Zugang zum Netz dabei geht es um Firewalls, Paketfilter, Routerkonfigurationen

usw. um dieses soll es hier jedoch nicht gehen. Ferner werden Sicherheitsmechanismen auf der Anwendungsebene behandelt. Sicherheitsfragen sind nicht die Netzeigenschaften vielmehr hat man es mit Objekten und Benutzern zu tun.

Die zunehmende Nutzung des Mediums Video erleichtert die Speicherung und Austauschbarkeit der Daten. Dies hat zu folge das Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit stärker werden. In diesem Zusammenhang gewinnt der Schutz der digitalen Daten durch eine Vielzahl von aufeinander abgestimmten Sicherheitsmaßnahmen an Bedeutung.

Folgende Sicherheitsaspekte spielen hier eine Rolle:

- Datenauthentizität:
  Unter Datenauthentizität versteht man den Nachweis, von wem die Daten stammen.
- Vertraulichkeit:
  Die Vertraulichkeit verhindert, dass unberechtigte Dritte Daten lesen können.
- Integrität:
  Die Integrität dient den Nachweis, dass Daten nicht verändert wurden.
- Nachweisbarkeit:
  Unter Nachweisbarkeit ist zu verstehen, daß die Möglichkeit besteht, das nicht nur der Datenempfänger, sondern auch berechtigte Dritte Authentizität und Integrität der Daten prüfen können.

Neben den bereits bekannten Sicherheitsmechanismen erfordert die Verwendung von Video und Audio in Multimediakommunikationsdiensten wie Electronic Publishing, video-on-demand und Konferenzsystemen eine spezielle Sicherheitsfunktionalität und Dienste. Eines der größten Anforderungen ist die Forderung der Originalität, da es sehr viel einfacher geworden ist die digitale Repräsentation eines Bildes oder Videos nachzubearbeiten und zu manipulieren so das etwas Falsches repräsentiert wird, obwohl es wie in der Realität aussieht. Somit erscheint die Notwendigkeit, einen neuen Dienst einzuführen, der die Originalität der digitalen Daten, die Unverfälschtheit und die Benennung des Erstellers/Urhebers sicherstellt. Die Kryptograpie, bietet hier Abhilfe. Jedoch hat man es bei Multimediadaten mit weit aus größeren Datenmengen zu tun, so dass ein Schutz mit herkömmlichen Methoden der Krypthographie, bei den gegenwärtigen Rechnerleistungen und Übertragungsraten der Netzwerke bei gleichzeitiger Echtzeitanforderung von verteilten Multimedia-Applikationen nicht realisierbar ist. Es gilt immer Sicherheit gegen Benutzbarkeit abzuwägen.

11.2.2 Ausgewählte Verfahren

Mechanismen für Integrität und Vertraulichkeit

Es gibt folgende Anforderungen an die Mechanismen für die Gewährleistung von Integrität und Vertraulichkeit bei Multimedialen Daten:

- Bei der Verwendung von Echtzeitprotokollen ist bei der Konzeption und Realisierung der Mechanismen auf eine möglichst hohe Perfomanz zu achten, das Ver- bzw. Entschlüsseln der Daten muss möglichst synchron erfolgen.

- Bei der Verwendung von Daten, die auf Massenspeichern zur Verfügung stehen, ergibt sich die Möglichkeit die Entschlüsselung auf Kosten der Verschlüsselung zu optimieren.
- Die Mechanismen müssen kryptographisch sicher sein.
- Die Mechanismen für den Integritätsschutz müssen den besonderen Anforderungen hochvolumiger Daten gerecht werden, es sollten Alternativen zu den bestehenden Methoden benutzt werden.
- Die Mechanismen sollten in einer Art und Weise zu konfigurieren sein, so dass sie den unterschiedlichen Anforderungen angepasst werden können.

Integrität

Um prüfen zu können, ob eine empfangene Nachricht dem Original entspricht, benötigt der Empfänger zusätzliche Informationen welche als Prüfsumme, Fingerabdruck oder Message-Authentication-Code (MAC) bezeichnet werden. Der Sender erstellt diese Information mit einem Verfahren, welches auch dem Empfänger bekannt sein muss und versendet diese zusätzlich zur eigentlichen Nachricht. Diese Verfahren sind in der Praxis öffentlich bekannt, so dass diese Information nicht ungesichert übertragen werden können, deshalb werden sie mit kryptographischen Methoden zusätzlich verschlüsselt. Analog zur handschriftlichen Unterschrift ist dies dann die digitale Unterschrift.

Verfahren zur Fehlererkennung basieren meist auf Prüfsummen und werden schon seit langer Zeit angewandt und dienen hauptsächlich dazu, Fehler während der Übertragung zu erkennen. Bei kleineren Übertragungseinheiten lassen sich mit dieser Methode Fehler mit hoher Wahrscheinlichkeit erkennen, bei größeren Blöcken ist aber die Möglichkeit gegeben, bei verschiedenen Nachrichten die gleiche Prüfsumme zu erhalten. Damit ist eine Entscheidung, ob eine Nachricht authentisch ist, nicht mehr möglich. Die verwendeten Verfahren zur Berechnung eines MAC sollten kryptographisch sicher sein. d.h. es sollte praktisch unmöglich sein, zu einem gegeben MAC eine passende Nachricht zu finden. Außerdem sollte es praktisch in nicht akzeptabler Zeit möglich sein, zwei verschieden Nachrichten zu finden, die denselben MAC haben. Diese werden als Einweg-Hashfunktionen bezeichnet. Diese Funktionen berechnen einen MAC von einer festen Länge aus einer beliebig langen Nachricht, Es sollte ein minimaler Hashwert von 128 Bit eingesetzt werden, mit dem der MAC von allen Zeichen der Nachricht abhängig ist.

Vertraulichkeit

Die Vertraulichkeit verhindert, dass unberechtigte Dritte Daten lesen können. Sie ist durch geeignete Maßnahmen, z.B. kryptographische Verfahren sicherzustellen. Diese werden hinsichtlich des Verschlüsselungsvorganges unterschieden.

- symmetrische Verfahren:
  Dabei haben Sender und Empfänger einen gemeinsamen geheimer Schlüssel.
- asymmetrische Verfahren:
  Sender und Empfänger haben jeweils einen öffentlichen und einen privaten Schlüssel.

Die Nachricht wir mit dem Öffentlichen Schlüssel vom Empfänger verschlüsselt und kann nur mit dem Privaten Schlüssel, der nur dem Empfänger bekannt ist, entschlüsselt werden.

Die Vertraulichkeit basiert darauf, dass die entsprechenden Schlüssel sicher und geheim sind, da die Verfahren zur Verschlüsselung öffentlich bekannt sind.

Praktische Realisierungen

Hierbei muss vor allem auf eine hohe Effizienz und eine ausreichende Sicherheit geachtet werden. Dies steht aber im Widerspruch zueinander. Wünscht man eine hohe Effizienz, so müssen Abstriche bei der Qualität der Sicherheitsanforderungen gemacht werden, da die Sicherheitsmechanismen zusätzlichen Zeitaufwand für die Verschlüsselung oder ein höheres Datenvolumen erfordern. In der Praxis gibt es Mechanismen, die auf bekannte Videodatenformate aufbauen, diese erweitern und mit zusätzlichen Diensten versehen. MPEG-2 ist der erste der vielen Mulitmedia-Video-Definitionen- und -Standards, in dem auch der Bereich der Sicherheit (Vertraulichkeit und Integrität) mit einbezogen wurde.

Die Datenformate lassen sich in zwei Klassen einteilen:

- Format mit einer festen Framegröße (z.B. SMP)
- Format mit einer variablen Framegröße (z.B. MPEG)

Im Hinblick auf das Einfügen von Sicherheitsinformationen ist diese Unterteilung nötig. Bei Formaten mit einer festen Framegröße wird diese Information hinter jedem Frame eingefügt. In diesem Fall besteht diese Information nur aus dem MAC, weitere Informationen werden nicht benötigt. Bei den Formaten mit einer variablen Framelänge muss die benötigte Sicherheitsinformation jeweils vor dem Frame eingefügt werden, da neben dem MAC auch noch der Offset des folgenden Frames gesichert werden muss. Weitere zusätzliche Informationen können zugefügt werden, wenn je nach Format noch unterschiedliche Kompressionsverfahren pro Frame angwendet werden.

In der Praxis werden Sicherheitsinformationen jeweils einem Frame zugeordnet. Alle Sicherheitsinformationen der ursprünglichen Datei- bzw. Streamheader und zusätzliche Informationen in dem möglichen Sicherheitsheader sind verschlüsselt.

Copyright-Schutz

Neben der Problematik des Abhörens und Verfälschens von Daten spielt auch das illegale Anfertigen von Kopien digitaler Daten eine immer größere Rolle. Mit Methoden der Zugriffskontrolle kann zwar der unautorisierte Zugriff auf Daten verhindert werden, hat ein Benutzer jedoch einmal die notwendigen Zugriffsrechte erworben, so ist keine Kontrolle seiner Aktionen mehr möglich. Gerade die digitale Repräsentation der Daten erlaubt das einfache Anfertigen von identischen Kopien. Um diesen Missbrauch einzudämmen, sind spezifische Maßnahmen notwendig, um einerseits den Eigentümer einer Datei, andererseits auch den Verbreiter illegaler Kopien eindeutig identifizieren zu können. Nicht ausreichend ist das bloße Anfügen einer digitalen Signatur oder das Einfügen einer sichtbaren Information in das Videomaterial. Diese Informationen können problemlos wieder

entfernt werden.

Ein geeigneter Ansatz ist, die Copyright-Information so in die Daten zu integrieren, dass diese dem Benutzer nicht sichtbar ist und nur mittels eines geheimen Schlüssels rekonstruiert werden kann. Für Bilddaten liegen bereits Ansätze für solche Verfahren vor. Der zur Rekonstruktion der Copyright-Information benötigte Schlüssel wird bei einer vertrauenswürdigen Instanz aufbewahrt, so dass Unstimmigkeiten über Urheberrechte an einem Bild durch Herauslesen der Copyright-Information beseitigt werden können. Ein Beispiel für ein solches System ist SysCop. Bisher ist dieses Verfahren noch nicht für bewegte Bilder implementiert, bietet jedoch Ansatzpunkte auch für das Videodatenformat. In analoger Weise kann auch eine Information über den Benutzer im Bild kodiert werden, so dass der Erzeuger illegaler Kopien ermittelt werden kann.

Steganographie

Mit den herkömmlichen Verschlüsselungsmethoden möchte man vor allem den Inhalt einer geheimen Nachricht verbergen. Will man jedoch die Daten offenlegen und gleichzeitig zum Beispiel Informationen anfügen, um gewisse Rechte zum späteren Zeitpunkt geltend zu machen, muss eine anderes Verfahren herangezogen werden. Diese Technik nennt sich Steganographie und ist eine Art und Weise der Kommunikation, die die Existenz der geheimen Kommunikation verbirgt.

Das Ziel der Steganographie ist, geheime Nachrichten in harmlosen Nachrichten zu verbergen, so dass ein Angreifer nicht erkennt, dass eine zweite geheime Nachricht vorhanden ist. Diese Algorithmen, die geheime Nachrichten sozusagen unsichtbar machen, basieren auf Prinzipien nicht unähnlich denen von Verschlüsselungsalgorithmen. Die geheimen Nachrichten werden versteckt mit einem geheimen Schlüssel, so dass nur der Eigentümer des korrekten Schlüssels die Existenz von geheimen Nachrichten feststellen und beweisen kann. In der Praxis existieren Verfahren, die darauf basieren, dass sie eine verrauschte Komponente der digitalen Nachricht mit einer verschlüsselten, geheimen Nachricht ersetzen. Diese Art von Verfahren werden substitutionale Steganographie genannt.

SysCop - System zum Copyrigth-Schutz

SysCop ist ein Werkzeug, welches erlaubt, unsichtbare Copyright-Labels in Multimedia-Daten robust zu integrieren. Das können Ursprungsdaten, Eigentumsinformationen, Inhaltsdaten, Rechte, Integritätsinformationen oder Zielinhalte sein. Um eine Copyright-Fälschung, Mißbrauch und Verletzung zu vermeiden, muss die eingebundene Information unsichtbar, unlöschbar, unerkennbar und unabänderbar sein. Vor allem muss es auch Verfahren überstehen, die zum Beispiel die Qualität des Datenmaterial verschlechtern. Ein erster Prototyp für statische Images wurde bereits implementiert. Die eingebundenen Markierungen erscheinen als ob sie ein natürlicher Teil des Originalbildes sind. Das System besteht aus zwei grundsätzlichen Funktionen für das Schreiben und Lesen der Markierungen. Der erste Schritt erstellt den aktuellen Copyright-Code und eine zufällige Sequenz für die Positionen der einzubringenden oder abzurufenden geheimen Nachricht. Diese Komponente benutzt bestehende Verschlüsselungs- und Pseudozufallszahlengenerierungstechniken.

Der zweite Schritt liest oder bindet die erzeugte geheime Nachricht an den im ersten Schritt ermittelten Positionen ein. Die Einfügemethoden sind abhängig vom verwendeten Datenformat. Für die Grau-Skala und Farb-Bilder wurde eine JPEG-basierte Methode entwickelt. Eine Sequenz von 8x8-Blocks werden pseudo-zufällig, abhängig von einem benutzerspezifischen Schlüssel und dem Datenmaterial, selektiert. Im derzeitigen Mechanismus wird nur die Höhe und Breite des Bildes für die Positionsgenerierung verwendet, so dass eine Skalierung des Bildes nachdem die Copyright-Information eingebunden wurde, das Erkennen der Copyrightinformation unmöglich macht. Dies ist bisher noch ein Schwachpunkt des Verfahrens und muss noch verbessert werden. Die Änderungen sind nur schwach visuell erkennbar. Da das Verfahren für JPEG-Bilder implementiert wurde, konnte es auch für das MPEG-1-Video-Format erweitert werden, da hier auch auf das JPEG-Format im Intra-Frame zurückgegriffen wird.

Transparente Verschlüsselung

Eine weitere Anforderung ist digitales Bildmaterial zwar zur Verfügung zu stellen, so dass sich der Interessent einen ersten Eindruck vermitteln kann, aber so lange nicht in den Genuss der vollen Qualität kommt, bevor er nicht einen entsprechenden Preis oder bestimmte Konditionen erfüllt hat. Diese Problematik führt dazu, dass die Daten nicht wie herkömmlich vollständig und sogar unleserlich verschlüsselt werden, sondern nur teilweise und in schlechter Qualität dargestellt werden. Mit einem nach Bezahlung erhaltenen Schlüssel soll es dann möglich sein, das Bildmaterial in voller Qualität anzusehen.

TIE - Tool for Image Encryption

Ein bei dem Frauenhofer-Institut für Graphische Datenverarbeitung entwickelten Werkzeug TIE - Tool for Image Encryption[5] - stellt einen ersten Ansatzpunkt zum Verschlüsseln von Rasterbildern zur Verfügung. Hier können Teile des Bildes verschlüsselt werden, welche dann zum Beispiel in niedriger Auflösung oder als schwarzer Kasten erscheinen. Die zu ersetzenden Bildbereiche werden bei TIE in sogenannten Application Extension Blocks abgelegt. Zur Sicherheit werden diese Daten mit dem DES verschlüsselt, für den der Anwender einen Schlüsselraum der Größe 2 bis 56 frei wählen kann.

Bisher wurde dieses Verfahren für GIF und JPEG Bildformate implementiert. Die Implementierung für JPEG wurde anschließend für MPEG-1-Video erweitert. Grundsätzlich ist jedes Bildformat geeignet, sofern es in seinem Dateiaustauschformat einen frei definierbaren Erweiterungsblock besitzt.

11.2.3 Zusammenfassung

Wie man in den vorangegangen Ausführungen gesehen hat, bestehen oft Probleme, alle möglichen Angriffspunkte abzustecken und in den verwendeten Methoden zu berücksichtigen. Ein weiteren Problembereich stellt die eigentliche Verschlüsselung mit dem geheimen Schlüssel dar. Die Verschlüsselungsroutinen müssen einerseits so in die Anwendung eingebettet werden, so dass der geheime Schlüssel keinesfalls in die Hände eines Angreifers gelangen kann oder ausgespäht werden könnte. Dasselbe betrifft auch die Übermittlung

der geheimen Schlüssel zum Beispiel zur Verfikation der Copyright-Markierung oder im TID-System zur Freischaltung digitaler Daten zur vollen Qualität. Desweitern müssen natürlich kryptographisch sichere Schlüssel für die verwendeten Verfahren erzeugt werden. Um spätere Ansprüche zum Beispiel auf Urheberrechte geltend machen zu können, müssen die geheimen Schlüssel außerdem noch bei einer vertrauenswürdigen Instanz, dem sogenannten notwendigen Dritten, hinterlegt werden. In diesem Zusammenhang spricht man auch von Trust-Funktionen die wahrgenommen werden müssen. Kryptographie hält zwar Auswege bereit, sie schafft jedoch allein noch keine Abhilfe für alle Problemfelder und es meist eine sichere Kommunikation weiter Dritter bedarf, welcher wiederum ein Sicherheitsrisiko darstellen kann.

Trotz aller Ansätze für mehr Sicherheit bleiben noch eine Reihe ungelöster Probleme. Vor allem im Bereich des Urheberrechts existieren noch keine befriedigenden Lösungen. Gerade hier sind auch Aktivitäten von Seiten des Gesetzgebers nötig, da derzeit auch keine klare gesetzliche Grundlage für die Urheberschaft an digitalen, insbesondere multimedialen Daten existiert. In jedem Fall sollte man sich darüber im Klaren sein, dass eine hundertprozentige Sicherheit nicht erreicht werden kann, verursacht durch die eingesetzten Verfahren oder durch organisatorische Lücken und Schwächen.

11.3 Das Distributed Security Framework for Multimedia Transmissions

11.3.1 Einleitung

Um all die Probleme die bei der sicheren Übertragung multimedialer Inhalte auftauchen könnten, soll sich das Distributed Security Framework for Multimedia Transmissions (DSFMT) [12], welches von Raghavendra Vinayak Prabhu als Master Thesis an der University of Illinois im Jahre 2002 entwickelt wurde, kümmern.

Das DSFMT ist ein objektorientiertes Framework, welches benutzt werden kann um verschiedene Sicherheitsprotokolle, Ver-/Entschlüsselungschemata, Netzwerkprotokolle und multimediale Anwendungen flexibel zu kombinieren. Dabei kann das DSFMT so konfiguriert werden, dass es verschiedene Szenarien - hohe Sicherheit, multiple Sender (militärische Videokonferenz); mittlere Sicherheit, aber eine hoch-performante kommerzielle Single-Sender Video-On-Demand-Lösung; eine intelligente Lösung, mit mehreren Empfängern bei unterschiedlichert Bandbreite (oder/und unterschiedlich hoher Sicherheit) und so weiter.

Dabei kann das DSFMT als eine black-box API oder als ein white-box objekt-orientiertes Framework benutzt werden. Als Kleinstmögliches was eine multimediale Anwendung tuen muss, um die Sicherheits-Features vom DSFMT zu nutzen, ist es auf die DSFMT-Sockets für die Kommunikation umzusteigen. Dennoch ist es Entwicklern auch jederzeit möglich die einzelnen Komponenten vom DSFMT selbst zu implementieren, wenn das Standard-Verhalten des DSFMT nicht genügen sollte.

Im Folgenden wird zuerst auf die Designgedanken hinter DSFMT eingegangen, danach ein wenig über die Implementierung und abschließend über die vorhandenen/fehlenden

Features und Schlüsse daraus berichtet.

11.3.2 Design und Architektur

Um eine vernünftige Applikation zu garantieren wurde beim DSFMT besonders viel Wert auf ein konsistentes Design gelegt, um früh feststellen zu können, welche Funktionalitäten ein Framework für die sichere Übertragung von multimedialen Inhalten unbedingt benötigt und wie diese bestmöglichst und gleichzeitig flexibel zu nutzen sind.

Designfragen

Dabei stellt sich Prabhu einige Fragen, die bei der Entwicklung einer sicheren Anwendung für multimedialen Datentransfer auftauchen, und beantwortet diese, um seine Designentscheidungen zu treffen.

Im folgenden wird kurz auf die Fragen eingegangen.

- **Welches Sicherheitsprotokoll wird gewählt?**
  Es gibt eine große Menge an Protokollen, alle mit unterschiedlicher Effizienz (Bandbreite, Rechenintensität...). Für den Designer wäre es am einfachsten wenn er einfach aus einer Menge von Protokoll-Plugins wählen könnte, oder noch einfacher, wenn er nur die Anforderungen angibt (Bandbreite, Sicherheitsstufe, Anzahl Clients...) und die Auswahl automatisch wäre.
- **Wie wird das Protokoll eingebunden?**
  Zumeist wird die Sicherheit nachträglich hinzugefügt, auch wenn dieses Vorgehen nicht empfehlenswert ist. Dieser Vorgang muss durch ein einfaches übersichtliches Design unterstützt werden.
- **Wie lässt sich ein Protokoll modifizieren/wechseln?**
  Die Anforderungen an die Sicherheit einer Applikation können sich schnell zu einem späteren Zeitpunkt ändern, verschiedene Protokolle erfüllen verschiedene Anforderungen. Durch ein Trennen von Anwendung und Sicherheitsschicht kann das einfach ermöglicht werden.
- **Wie kann die Sicherheitsstufe modifiziert werden?**
  Manche Anwendungen brauchen mehr Performance und weniger Sicherheit, dies kann durch weniger Schlüsselwechsel und eine andere Verschlüsselungsart geändert werden. Damit dies nachträglich möglich ist, ist auch hier das Trennen von Anwendung und Ver/Entschlüsselung und Schlüsselverteilung hilfreich.
- **Wie kann die Trennung von Netzwerk und Netzwerkprotokoll vollführt werden?**
  Wenn man nicht gut acht gibt, kann leicht Anwendungscode mit Netzwerkprotokollspezifischem Code vermischt werden. Besonders multicast benötigt eine spezielle Betrachtung und macht den späteren Wechsel nicht leicht. Auch hier kann eine Trennung der betrachteten Komponenten helfen.

Zusammengefasst soll ein erweiterbares Framework entstehen, welches leicht in bestehende Anwendungen einzugliedern ist, und auch ein einfaches nachträgliches Wechseln/-modifizieren von gewählten Komponenten (Protokoll, Verschlüsselungssystem, Sicherheitsstufe...) ermöglicht. Dabei sollen alle veränderbaren Teile in separaten Modulen vorkommen, möglichst viele Protokolle eingebunden werden und dabei eine einfache Socket-Schnittstelle für Anwendungen produziert werden.

Aus diesen Designvorgaben lassen sich erste Komponenten identifizieren.

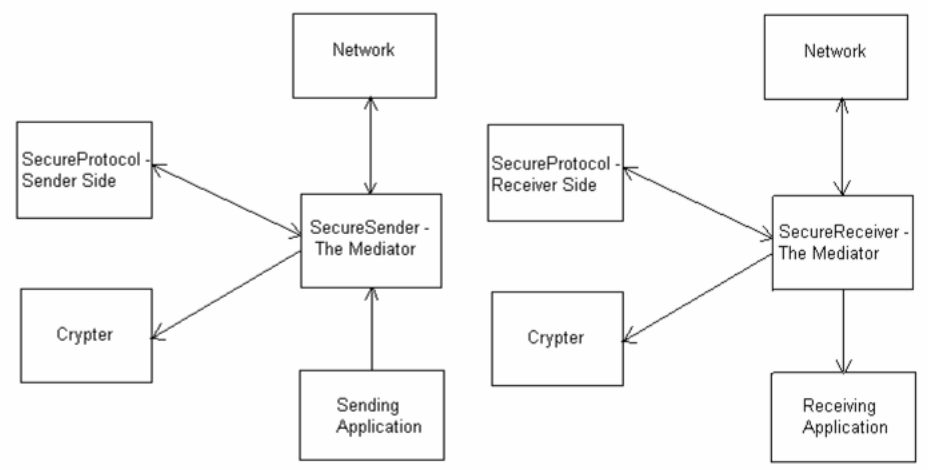

Abbildung 11.1: Designkomponenten

Dabei existieren 5 Komponenten :

Komponentenname	Funktion
SecureSender/SecureReceiver	Kapselt Quelle und Empfänger der gesicherten Kommunikation
SecureProtocol	Kapselt das benutzte Protokoll, kümmert sich um die Schlüsselvergabe
Crypter	Kümmert sich um Ver- und Entschlüsselung[1]
Network Component	Kapselt die Netzwerk Implementation[2]

Tabelle 11.1: Komponenten-Tabelle

Architektur

Aus den Designfragen baut Prabhu unter weiteren Überlegungen die Architektur auf.

Auch für die Architektur betrachtet Prabhu die Notwendigen Entscheidungen und benötigten Features für eine multimediale Datenübertragungsanwendung. Das DSFMT soll es ermöglichen die Kontrolle über die Schlüsselvergabe auf einzelne Untergruppen zu verteilen, da zentralisierte Ansätze leicht zu einem Flaschenhals in der Kommunikation führen können, weiterhin muss es möglich sein, daß verschiedene, unabhängige Clients gleichzeitig senden

können. Zu guter Letzt soll die Möglichkeit existieren zwischen verschiedenen Untergruppen unterschiedliche Protokolle oder Sicherheitsstufen benutzen zu können.

Die Gruppenverwaltung wird dabei im DSFMT in die Hände des sendenden Knotens gelegt, da offentlich ist, das der Knoten sich selber stärker vertrauen kann als einer dritten Partei. Dadurch das der Sender sämtliche Untergruppen verwaltet, kann er für diese unterschiedliche Protokollen/Sicherheitseinstellungen wählen. Dennoch ist es, falls ein Protokoll dies benötigen sollte, möglich ein Authentifizierung/Versendung über eine dritte Partei einzubauen.

11.3.3 Implementationsdetails

Da allein durch das Design und die Architektu der ungefähre Aufba des DSFMT klar geworden sein sollte, wird hier stärker auf die Features des DSFMT und die darausfolgenden Schlussfolgerungen für die Performance des Systems eingegangen.

Features

Das DSFMT benutzt in seiner Beispielsimplementation zur Verschlüsselung die Microsoft Windows CryptoAPI, eine Bibliothek die 56-bit DES, 112-bit triple DES und 168-bit triple DES unterstützt. Eine Portierung auf andere Betriebssysteme, oder nicht von der CryptoAPI unterstützte Ver/Entschlüsselungsalgorithmen muss erst selbst durchgeführt werden.

Das DSFMT beherrscht zwei Arten der Schlüsselverteilung, manuell und hierarchisch, bei der letzteren kümmern sich vorher festgelegte Grupenführer um die Verteilung der Schlüssel in der Gruppe. Der Schlüssel wird unter verschiedenen Bedingungen gewechselt:

- **Eine Gruppe wird gegründet**
  Damit er nicht einen zuvor aufgezeichneten Teil der Transmission dekodieren kann
- **Ein neuer Client betritt die Gruppe**
  Damit er nicht einen zuvor aufgezeichneten Teil der Transmission dekodieren kann
- **Ein Client verlässt die Gruppe**
  Damit er nicht weitere Teile der Transmission dekodieren kann
- **Ein Schlüsseltimeout tritt ein**
  Je nach Sicherheit eines Schlüssels braucht es ein bestimmte Zeit um ihn zu errechnen, davor muss der Schlüssel gewechselt werden.

Dabei findet der Schlüsselwechsel asynchron zum multimedialen Datenstrom statt, sobald alle Mitglieder diesen Schlüssel bestätigt haben, oder ein Timeout eingetreten ist, wird auf den neuen Schlüssel gewechselt.

Das DSMFT bietet leider keinerlei Authentifizierungsverfahren, genausowenig wie eine Verifizierung der Herkunft der Daten, gegen Man-In-The-Middle Angriffe wurden keinerlei Vorkehrungen getroffen. Eine digitale Rechteverwaltung wurde von Prabhu nicht einmal angedacht.

Benchmarks

Das DSFMT gibt zwar keine Echtzeitgarantien, jedoch ist der Overhead nach Prabhus Benchmarks recht gering. Für die genauen Benchmarks soll nur auf die Master Thesis[12] verwiesen werden, hier wird nur kurz auf die Ergebnisse eingegangen.

Als Testrechner sind vier, heutzutage bereits recht veraltete Rechner gewählt worden. Die Perfomance reichte von einem Pentium II mit 400Mhz bis zu einem Athlon Mobile 4 mit 1 Ghz. Dabei waren diese Rechner über ein 100 Mbit LAN verbunden. Jedoch wurden keine Test über das Internet oder langsamere DialUp Verbindungen ausgeführt. Die Schlüsselneverteilung war bie 4 Clients mit 34ms mehr als aktzeptabel und der Zeit-Overhead selbst bei diesen langsamen Rechnern sehr gering, so das flüssige 30fps Videokommunikation möglich war.

Leider geht Prabhu nicht auf den Datenoverhead ein, und da Testfälle für nicht LAN-Anwendungen und eine größere Anzahl an Clients oder auch mehrfachen Sendern fehlen sind diese Benchmarks nicht sehr aussagekräftig und bei der Entscheidungsfindung ob man das DSFMT benutzen will, nicht wirklich hilfreich.

11.3.4 Zusammenfassung

Insgesamt versucht das DSFMT eine flexible Basis für den Transfer von multimedialen Streams zu bieten. Die Interfaces sind einfach gehalten und lassen sich leicht nachnutzen, dabei lassen sich auch leicht zur Laufzeit bzw. nach der Konzeption und Implementierung einer sicheren Anwendung die einzelnen Komponenten austauschen, sprich das Protokoll/die Sicherheitsstufe wechseln.

Jedoch wird sich nicht um die besondere Natur von multimedialen Daten gekümmert, deren Header zumindest wiederholt ähnlich aussehen, und ein einfacheres Knacken der Schlüssel fördern. Eigentlich handelt es sich nicht wirklich um ein Multimedia-Transmissions Framework, der Ansatz ist zu generisch, und ermöglicht natürlich auch das Versenden anderer zu verschlüsselnder Daten. Die einzig besonderen Features die das DSFMT dabei bietet ist die Protokollunabhängkeit und die Möglichkeit an multiple Empfänger zu senden, sowie seine Flexibilität. Das Militär wird aber nicht ohne weitere Änderungen auf ein solches System umsteigen, allein die fehlende Authentizifierung und die feste Bindung an die Windows Crypto API, deren Quellcode und eventuelle Lücken/Hintertüren nicht offenliegen, machen das DSFMT eher zu einem Sicherheitsrisiko.

Die Benchmarks hinterlassen auch einen faden Beigeschmack, die Testcases waren zu wenige und zu undifferenziert, etliche interessante Answendungen, von denen Prabhu zuvor mehrfach schwärmt werden nicht untersucht, geschweige denn erwähnt.

11.4 Andere Lösungen

11.4.1 Einleitung

Das Interesse an sicher multimedialer Datenübertragung steigt immer weiter. Die Bandbreite erhöht sich stetig, und damit auch das Interesse normaler Kunden Video-On-Demand und ähnliche Lösungen auszuprobieren. Gleichzeitig sollen dabei natürlich keine illegalen Kopien entstehen oder unauthorisierte Betrachtungen stattfinden. Auch in großen Firmen oder beim Militär muss immer globaler gehandelt werden, das verlangt nach sicheren, stabilen Lösungen. Wichtig sind hier große Sicherheitsfirmen wie Nortel, obwohl einzelne, größere Konzerne sicher auf In-House Lösungen oder VPNs setzen werden.

11.4.2 Systeme im Vergleich

Hier werden ein paar, dem DSFMT ähnliche, Systeme verglichen.

Multimedia Communication Server

[10] Eine komplette Multimedia-Anwendung die die Kollaboration über Videokonferenzen und verteilte Präsentationen. Gedacht für große Firmen die mit ihren Kunden oder entfernten Mitarbeitern zusammenarbeiten. Für Großkunden gedacht, hohe Sicherheit zu einem hohen Preis.

SECMPEG

Das Sicherheitsformat für MPEG-I-Video-Ströme basiert auf den Forschungen innerhalb des Projektes SSicherheit in verteilten Systemenän der TU Berlin. Das dort entwickelte Format SECMPEG ist eine Basisentwicklung welches mit DES und CRC implementiert wurde, um Vertraulichkeit und Integrität zu gewährleisten. Die Sicherheitsmechanismen für Videodaten beruhen auf dem formatübergreifenden Prinzip, nur Teile des Datenstromes in Abhängigkeit zu den verwendeten Kompressionsverfahren zu schützen.

Die dafür benutzten Basismechansimen für die Verschlüsselung und Integrität sind konfigurierbar, so dass bei Bekanntwerden eines Sicherheitsrisikos auf höhere Sicherheitsniveaus umgeschaltet werden kann und die Algorithmen ausgetauscht werden können. Um die Sicherheit der Algorithmen zu beurteilen, muss man nachweisen, dass aus den ungeschützten Anteilen des Datenstromes, keine Rekonstruktion der verschlüsselten Informationen möglich ist, bzw. nur mit einem sehr hohen Aufwand zu realisieren ist.

Ein thoeretischer Nachweis ist von den Entwicklern dieses neuen Sicherheitsdatenformates bisher nicht erfolgt. Es wird lediglich darauf hingewiesen, dass es sich um einen sehr hohen Aufwand handeln wird, diese Informationen aus den unverschlüsselten Daten zu extrahieren.

MPEG-2

MPEG-2 ist der erste der Standards und Formatspezifikationen im Bereich Multimedia und Video, in dem auch der Bereich der Sicherheit, Vertraulichkeit und Integrität, von Anfang an mit konzipiert wurde. Das Format ist robust gegen Bitfehler und Zellverlust. Die Verwendung von Integritätschecks erlaubt die Erkennung von Übertragungsfehlern, die ansonsten den Abspielvorgang unterbrechen oder blockieren könnten. Für den Bereich Security soll auf eine Realisierung im Rahmen des Projektes Digital Video Broadcasting (DVB) eingegangen werden. Hier wird eine Methode verwendet, die die Verschlüsselung dazu benutzt, um übertragene Videosignale nur für berechtigte Empfänger verfügbar zu machen. Man spricht in diesem Zusammenhang von einem Common Scrambling System, welches auf der Senderseite das Programmsignal in einem Scrambler verschlüsselt, auf der Empfängerseite können die Daten nur wahrgenommen werden, wenn das Empfangsgerät im Besitz der Entschlüsselungsanleitung ist.

Das verwendete Konzept besteht dabei aus zwei Verschlüsselungsverfahren, die hintereinander geschaltet werden. Das erste Verfahren dient der Vermischung der Daten von 8 Bit Größe, während das darauf folgende Verfahren eine bitweise Vermischung vornimmt. Das MPEG-2-Format bietet zwei Ebenen, in denen eine Verschlüsselung stattfinden kann. Das sind zwei Ebenen des System Layers, welcher der ISO-Transport-Schicht entspricht. Nähere Informationen können unter [13] entnommen werden.

11.4.3 Zusammenfassung

Allgemein lässt sich erkennen, das nicht die Flexibiltät sondern die Sicherheit beim sicheren Datentransfer das Wichtigste ist. Dabei wurde jedoch nicht der größte Wert beim DSFMT gelegt, wenn man die Beispiele aus Kapitel 2 in Kapitel 3 wiederzufinden sucht. Es scheint so als hätte Prabhu über seinen Designentscheidungen vergessen sich auf dem Markt nach ähnlichen Lösungen umzuschauen, oder zumindest die Bedürfnisse genau zu erkennen. So wird sein Framework nur für kleinere Projekte nutzen, wenn es wirklich um Geld und Sicherheit geht, werden sich die wenigsten für das DSFMT entscheiden.

11.5 Fazit

Insgesamt lässt sich, wie gesagt, keine Lösung finden die wirklich zu einhundert Prozent sicher ist. Besonders bei Video-On-Demand für Copyright geschützte Materialen muss nicht nur die Übertragung gesichert sein, es muss auch die Berechtigung des Benutzers überprüft und verwaltet werden. Hier hat sich Prabhu mit seiner Aussage, dass es sich 'einfach implementieren lässt' aus der Affäre gezogen, zeigt aber auch damit, dass seine Master Thesis sich nur um den puren Transfer aber kaum um die Logik dahinter kümmert, und damit nicht wirklich auf die besonderen Eigenschaften multimedialer Daten eingeht.

Somit ist das DSFMT nur eine flexible Verschlüsselungsbibliothek für Streambaren Content unter Windows-Systemen, für alles mehr muss erst das System eigenhändig modifiziert werden.

Glossar

ABI Ein Application Binary Interface (ABI, Anwendungsbinärschnittstelle) definiert die konkrete Realisierung einer Schnittstelle einer API für ein bestimmtes System.

API Application Programming Interface. Ein API ist die Schnittstelle, die ein Betriebssystem oder auch ein anderes Softwaresystem anderen Programmen zur Verfügung stellt. Im Gegensatz zu einem ABI definiert ein API nur die Verwendung der Schnittstellen, nicht aber deren Realisierung.

DSFMT Distributed Security Framework For Multimedia Transmission

Framework Frameworks werden durch die Anwendung objektorientierter Designprinzipien erstellt. Das Hauptziel eines Frameworks ist es, wiederverwendbar zu sein. Es ist besonders sinnvoll, wenn Teile eines Anwendungsgebiet existieren, die sich im Kern gleichen. Eine Gruppe von Komponenten kann dann für ein bestimmtes Problem/System entwickelt werden, und bei einem anderen weiter benutzt werden. Ein Framework ist eigentlich auch nur ein einfaches Programm, aber eines das einfach erweitert werden kann, um für eine ganze Gruppe von Anwendungen benutzt werden zu können. Ein Framework ist also Design und Quelltext zugleich.

Literaturverzeichnis

[1] Wolfenstetter Beutelsbacher, Schwenk. *Moderne Verfahren der Kryptographie*. Vieweg Verlag, 1995.

[2] Caronni. Assuring ownership rights for digital images. *Proceedings der GI-Fachtagung VIS'95*, 1995.

[3] Wikipedia Community. *Wikipedia, die freie Enzyklopädie*. None, 2004. http://www.wikipedia.org.

[4] Jana Dittmann. Homepage jana dittmann. 2004. http://www.ipsi.fraunhofer.de/~dittmann/.

[5] Frauenhofer-Institut für Graphische Datenverarbeitung. Informationsblatt tie. *Informationsblatt TIE*, 1995. http://www.igd.fhg.de/www/igd-a8/projects/tie/tie.htm.

[6] Frauenhofer-Institut. Mediensicherheit in it (merit). 2004. http://www.ipsi.fraunhofer.de/merit/.

[7] Meyer Gadegast. *Securitymechanisms for Mutlimedia-Data with the Example MPEG-I-Video*. Vieweg Verlag, 1994. http://white.yeungnam.ac.kr/~dhlee/mpeqfaq/mpe7621.html.

[8] Meyer Gadegast. Sicherheitsmechanismen für multimedia-daten, studienarbeit. *TU-Berlin*, 1994.

[9] Zhao Koch, Rindfrey. Copyright protection for multimedia data. *Proceedings der GI-Fachtagung VIS'95*, 1994. http://www.igd.fhg.de/~ekoch/publications.html.

[10] Nortel. Multimedia communication server 5200. *Nortel Homepage*, 2004. http://www.nortelnetworks.com/products/01/mcs52/index.html.

[11] University of Illinois. Multimedia security - dsfmt. *None*, 2003. http://cairo.cs.uiuc.edu/security/dsfmt.htm.

[12] Prabhu, Raghavendra Vinayak. *Distributed Security Framework For Multimedia Transmission*. None, 2002. http://cairo.cs.uiuc.edu/security/dsfmt_thesis.pdf.

[13] Ulrich Reimers. *Digitale Fernsehtechnik: Datenkompression und Übertragung für DVB*. Springer Verlag, 1995.