in: Martin Wind, Detlef Kröger (Hrsg.): Handbuch IT in der Verwaltung; Springer-Verlag, Berlin Heidelberg 2006, Seite 273 - 292

IT-Sicherheit

Hannes Federrath, Andreas Pfitzmann

Universität Regensburg, TU Dresden

1 Grundlagen

1.1 Begriff

IT-Sicherheit bezeichnet die Funktionen (Abschnitt 2) und Prozesse (Abschnitt 3) zur Schaffung und Erhaltung von Systemzuständen eines informationstechnischen Systems (IT-Systems), in denen Bedrohungen, die auf das IT-System einwirken, keine negativen Auswirkungen auf das System oder dessen Umwelt haben, d.h. das IT-System verbleibt in einem sicheren Systemzustand.

Alle möglichen Maßnahmen zum Schutz eines IT-Systems sind nur Annäherungen an den perfekten Schutz vor jedem möglichen Angreifer [12, S.15]. Die Annäherung wird im Allgemeinen durch Angabe der maximal berücksichtigten Stärke eines Angreifers in Form eines sog. Angreifermodells beschrieben. Ein Angreifermodell beschreibt somit die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus gerade noch sicher ist. Umgekehrt bedeutet dies, dass die Realisierung, Nutzung und Beurteilung einer Sicherheitsfunktion ohne Angabe der Stärke eines Angreifers fragwürdig bzw. wertlos ist.

1.2 Bedrohungen und Schutzziele

In den frühen 80er Jahren wurde IT-Sicherheit durch eine Dreiteilung der Bedrohungen und korrespondierenden Schutzziele
- Unbefugter Informationsgewinn: Verlust der **Vertraulichkeit**,
- Unbefugte Modifikation von Informationen: Verlust der **Integrität**,
- Unbefugte Beeinträchtigung der Funktionalität: Verlust der **Verfügbarkeit**

beschrieben [15]. Hier einige Beispiele für den Bereich Meldewesen, wie diese Schutzziele konkretisiert werden können: Der lesende Zugriff auf Meldedaten durch berechtigte Stellen ist mittels IT-Sicherheitsmechanismen sicherzustellen, und die Übermittlung sollte verschlüsselt erfolgen (Vertraulichkeit). Zur Sicherung der Unversehrtheit darf die Veränderung von Meldedaten ebenfalls nur durch Berechtigte erfolgen (Integrität, teilweise auch Verfügbarkeit). Die Ausfallsicher-

heit und Zuverlässigkeit des Systems kann durch redundante Auslegung der Komponenten (Server, Datenbank) verbessert werden (Verfügbarkeit).

Vertraulichkeit, Integrität und Verfügbarkeit sind heute immer noch aktuelle Schutzziele, allerdings gliedert man die Schutzziele feiner [6]. Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern. Dies gilt jeweils sowohl bzgl. der zu schützenden Inhalte als auch bzgl. der Umstände einer Kommunikation (Tabelle 1).

Tabelle 1. Gliederung von Schutzzielen

	Schutz der Inhalte (Worüber?)	Schutz der Umstände einer Kommunikation (Wer, wann, wo, mit wem, wie lange?)
Unerwünschtes verhindern	Vertraulichkeit von Nachrichteninhalten	gegenseitige Anonymität der Anwender
	Verdecktheit von Nachrichteninhalten	Unbeobachtbarkeit der Anwender
Erwünschtes leisten	Integrität von Nachrichteninhalten	Zurechenbarkeit von Nachrichten zu Absendern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Durch diese Gliederung werden neue Schutzziele explizit, die bisher jeweils unter einem der drei Begriffe Vertraulichkeit, Integrität oder Verfügbarkeit subsumiert wurden. Beispielsweise sind Anonymität und Unbeobachtbarkeit Vertraulichkeitseigenschaften: Die Identität des Urhebers eines Kommunikationsereignisses bleibt vertraulich. Ebenso ist Verdecktheit eine Vertraulichkeitseigenschaft: So wird die Existenz einer vertraulichen Nachricht vor dem Angreifer mit Hilfe von Steganographie verborgen. Zurechenbarkeit bezieht sich auf die unfälschbare Angabe des Urhebers (Verfassers) einer Nachricht und ist somit eine Integritätseigenschaft.

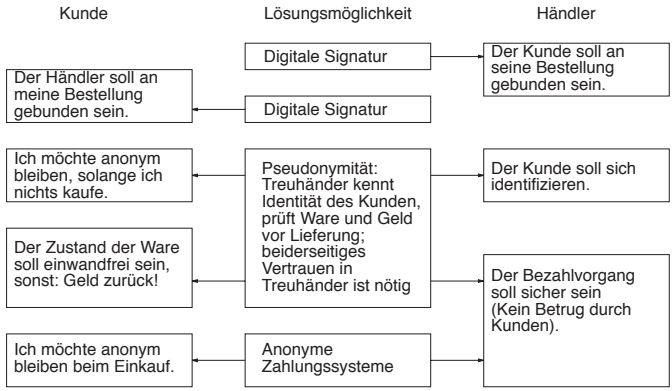

Abb. 1. Kommunikationspartner haben oft unterschiedliche Sicherheitsinteressen (Beispiel Kunde-Händler-Beziehung)

Die Schutzziele der Beteiligten an einer Kommunikation können unterschiedlich oder sogar entgegengesetzt sein (Abb. 1). Das IT-System muss deshalb in der Lage sein, Schutzzielkonflikte zu erkennen und die Aushandlung einer Lösung zwischen den Kommunikationspartnern unterstützen. Systeme, die das leisten, werden als **mehrseitig sicher** [10, 11] bezeichnet.

2 Funktionen zur Realisierung von IT-Sicherheit

2.1 Voraussetzung aller IT-Sicherheit: Existenz eines Vertrauensbereichs

Die maximal erreichbare persönliche Sicherheit des Nutzers eines IT-Systems kann nie größer werden als die Sicherheit des Gerätes, mit dem er physisch direkt interagiert. Es bildet den kleinstmöglichen Vertrauensbereich dieses Nutzers. In diesem Vertrauensbereich kann der Nutzer geheime Berechungen durchführen, vertrauliche Daten (z.B. Verschlüsselungsschlüssel) speichern und ggf. auch erfassen und betrachten, soweit das Gerät auch über ein vertrauenswürdiges Nutzerinterface verfügt.

Definitionsgemäß finden im Vertrauensbereich eines Nutzers keine Angriffe statt. Die Existenz eines Vertrauensbereichs ist die grundsätzliche Voraussetzung für die Realisierung von IT-Sicherheit. Andernfalls könnte der Angreifer dort direkt erfolgreich angreifen (z.B. Klartexte vor deren Verschlüsselung lesen), was natürlich alle weiteren Sicherheitsfunktionen überflüssig macht.

Niemand, dem der Nutzer nicht vertraut, kann ihm ein vertrauenswürdiges Gerät bereitstellen, das den Vertrauensbereich bildet, ohne dass die Sicherheitsinteressen dieses Nutzers gefährdet wären. In der Realität wird der Nutzer praktisch kaum in der Lage sein, sich ein vertrauenswürdiges Gerät ohne fremde Hilfe zu

bauen, da ihm vermutlich die technischen Voraussetzungen dazu fehlen. Er muss also zumindest noch dem Produzenten des Gerätes vertrauen können. Bei vertrauenswürdigen Geräten sind zwei Situationen zu unterscheiden:

1. Das vertrauenswürdigeGerät verbleibt unter der Kontrolle des Nutzers: Seine physische Sicherheit soll verhindern, dass andere unbefugt in diesen Bereich eindringen. Dies ist beispielsweise der Fall, wenn ein Nutzer seinen (nicht vernetzten) PC in einen verschließbaren Raum stellt oder ein mobiles Endgerät (PDA, Chipkarte) stets bei sich trägt, auf dem er geheime Schlüssel (zur Verschlüsselung oder zur digitalen Signatur) oder andere Geheimnisse speichert. Soweit Daten nicht anderweitig (z.B. durch Verschlüsselung) vor unberechtigtem Zugriff geschützt werden (können), sind sie ebenfalls physisch zu sichern und gehören damit zum Vertrauensbereich des Nutzers. Die physische Sicherheit des Geräte(gehäuse)s selbst schützt insbesondere bei Verlust des Gerätes vor Ausforschung durch den Finder bzw. Dieb.
2. Das vertrauenswürdige Gerät geht dauerhaft oder zeitweise in den Verfügungsbereich eines anderen über, der damit auch die physische Kontrolle über das Gerät erlangt: Beispiele hierfür sind vorausbezahlte Telefonkarten, die ein Telekommunikationsunternehmen ausgibt und Chipkarten zur Nutzung von Pay-TV. Durch physische Schutzmaßnahmen am vertrauenswürdigen Gerät selbst muss das Telekommunikationsunternehmen bzw. der Pay-TV-Anbieter vor Manipulation (z.B. Rücksetzen des Zählers für verbrauchte Gesprächseinheiten) und Ausforschung des Gerätes (z.B. unbefugte Kenntnisnahme und Weitergabe des geheimen Verschlüsselungsschlüssels) durch den Nutzer geschützt werden.

Ausforschungs- und Manipulationssicherheit (Tamper Resistance) sind schwer und bestenfalls auf Zeit zu erreichen, da dem Angreifer u.U. viel Zeit (im Bereich von Monaten oder gar Jahren) zum Angriff zur Verfügung steht und er außerdem in vielen Fällen beim Angriff die Zerstörung des Gerätes riskieren kann, ohne entdeckt zu werden.

Die nächste Generation von PCs wird sehr wahrscheinlich ein ausforschungssicheres Hardwaremodul (Trusted Platform Module, TPM) enthalten, das die Sicherheit für beide der oben genannten Situationen verbessern soll. Erstens soll der Nutzer in die Lage versetzt werden, in einem hardware-gesicherten Bereich auf seinem PC kryptographische Schlüssel und andere geheime Daten abzuspeichern und (in Kombination mit Zugangs- und Zugriffskontrollmechanismen, Abschnitt 2.2 und 2.3) die unbemerkte Verbreitung und Ausführung ungewollter Software (z.B. Viren und Würmer) zu verhindern. Zweitens sollen die Anbieter von Software und Medieninhalten die Möglichkeit erhalten, die Nutzung nur in einer von ihnen bestimmbaren Systemkonfiguration zu erlauben. Hierzu wird beim Systemstart die Integrität (Unversehrtheit) der Ausführungsumgebung (sowohl Hardwareals auch alle aktiven Softwarekomponenten) festgestellt, bevor die geschützte Software bzw. der Medieninhalt benutzt werden dürfen. Dadurch soll das Anfertigen und die Nutzung von Raubkopien deutlich erschwert werden. Die perfekte Absicherung ist allerdings wegen der Vielfalt an Hard- und Softwarekomponenten weder vorgesehen noch zu erwarten. Beispielsweise müsste der Schutz von gesicherten Mediendateien soweit gehen, dass selbst das Abgreifen und Abspeichern

der Medienströme durch einen vom Besitzer des PCs manipulierten Grafik- oder Soundkartentreiber nicht mehr möglich ist.

Eine Initiative zur Spezifikation eines TPM ist die Trusted Computing Group (TCG, http://www.trustedcomputinggroup.org/), der fast alle großen Hard- und Softwareproduzenten angehören.

2.2 Zugangskontrolle zu einem IT-System

Um die unbefugte Inanspruchnahme eines IT-Systems zu verhindern, werden Mechanismen zur Zugangskontrolle eingesetzt. Soweit es sich um ein Mehr-Nutzer-System handelt, fragt das IT-System zunächst nach der Identität des Nutzers oder einem Pseudonym (Nutzerkennung) und erwartet anschließend einen Beweis für die Echtheit. Dieser Beweis kann erbracht werden durch **Wissen** (z.B. Passworte, Antworten auf Fragen), **Besitz** (z.B. Schlüssel, Magnet- oder Chipkarte, maschinenlesbare Ausweise) oder **biometrische Merkmale** (inhärente, messbare Eigenschaft eines Individuums, Abb. 2).

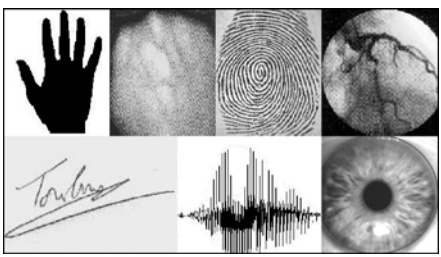

Abb. 2. Beispiele für biometrische Merkmale: Handgeometrie, Handvenenmuster, Fingerabdruck, Retina, Handschrift, Stimme, Iris (Bilder: http://biometrics.cse.msu.edu)

Beispiele:

- Ein (nicht vernetzter) PC, der vor unberechtigtem Zugang zu schützen ist, kann in einem verschließbaren Raum abgestellt werden, zu dem nur Berechtigte mittels eines Schlüssels (Besitz) Zugang haben. Der PC fragt seinen Nutzer nach einem Passwort (Wissen) oder prüft dessen Fingerabdruck (Biometrie), bevor der Nutzer mit dem Gerät arbeiten kann.
- Der Zugang zum Online-Banking wird heute meist mittels PIN (Wissen) geschützt. Innerhalb des Online-Banking-Systems werden besonders kritische Funktionen zusätzlich durch Erfragen eines Einmal-Passworts (Transaktionsnummer, TAN) abgesichert.

Die Zugangskontrolle kann die Inanspruchnahme eines lokalen IT-Systems, aber auch von vernetzten Systemen kontrollieren. Beides kann sogar kombiniert werden. Beispiele:

1. Die SIM-Karte eines Mobiltelefons erwartet von seinem Nutzer beim Einschalten einen PIN-Code (Wissen).

2. Das Mobilfunknetz überprüft anschließend die Echtheit der für den Nutzer nicht ausforschbaren SIM-Karte (Besitz) mit Hilfe eines kryptographischen Verfahrens (Challenge-Response-Authentikation, Abschnitt 2.5), d.h. zwischen der SIM-Karte und dem Mobilfunknetz werden Nachrichten ausgetauscht, durch die das Mobilfunknetz Gewissheit darüber erlangt, dass es sich unmittelbar um eine befugte SIM und mittelbar um einen befugten Teilnehmer handelt, der das Mobilfunknetz nutzen darf.

Werden biometrische Merkmale zur Identifizierung verwendet, empfiehlt es sich aus Datenschutzgründen, die Referenzwerte individuell auf einem manipulationssicheren Gerät zu speichern, um das Führen einer zentralen Datei zu vermeiden. Zur sogenannten **Selbstauthentifizierung** werden die gemessenen Werte innerhalb des Gerätes mit den Referenzwerten verglichen und das Testergebnis ausgegeben.

2.3 Zugriffskontrolle in einem IT-System

Zugang zu einem System zu haben, bedeutet nicht, alle Rechte auf diesem IT-System zu besitzen. Bei der Zugriffskontrolle wird, nachdem durch die Zugangskontrolle die Identität eines Nutzers festgestellt wurde, kontrolliert, ob ein Subjekt (z.B. der Prozess eines Nutzers) die nötigen Rechte (z.B. Schreibrecht, Leserecht, Ausführungsrecht) hat, um die jeweilige Operation auf einem Objekt (z.B. Prozess, Datei, Peripherie-Gerät) auszuführen.

Zunächst müssen die Rechte an die Subjekte vergeben werden (Autorisierung). Das Ergebnis der Autorisierung ist eine Zugriffskontrollmatrix (Tabelle 2). In der einen Dimension werden die Subjekte aufgetragen, in der anderen die zu schützenden Objekte. Eingetragen werden die jeweiligen Rechte (r: Lesen; w: Schreiben; x: Ausführen), die das Subjekt (s_i) auf dem Objekt (o_j) besitzt.

Tabelle 2. Zugriffskontrollmatrix

	Objekte			
Subjekte	o_1	o_2	o_3	…
s_1	rw		rx	
s_2		rwx		
s_3	r	r		
…				

Bei der Festlegung der Rechte kann restriktiv oder optimistisch vorgegangen werden, was sich in einer Sicherheitspolitik ausdrücken lässt. Entweder es ist alles verboten, was nicht explizit erlaubt ist, d.h. man erteilt Erlaubnisse, oder es ist abgesehen von expliziten Verboten alles erlaubt.

Betrachtet man nur eine Spalte der Zugriffskontrollmatrix, erhält man **Zugriffskontrolllisten** (Access Control List, ACL), wobei die leeren Zellen der Matrix weggelassen werden. Die ACL von o_1 aus Tabelle 2 lautet beispielsweise `s1:rw, s3:r`. Wird die Zugriffskontrollmatrix zeilenweise ausgelesen, erhält

man **Berechtigungslisten** (Capability List, CL). Die CL von s_1 aus Tabelle 2 lautet also `o1:rw, o3:rx`.

Wenn jedes Objekt einen Eigentümer hat und dieser die Matrix-Einträge jeder Objektspalte nach seinen Vorstellungen ändern kann, spricht man von **nutzerbestimmbarem Zugriffsschutz** (Discretionary Access Control). Demgegenüber ist beim **systembestimmten Zugriffsschutz** (Mandatory Access Control) die Vergabe von Rechten entweder dem Systemadministrator vorbehalten oder wird durch systemweite (teilweise dynamische) Mechanismen (z.B. Informationsflusskontrolle) geregelt. Diese Mechanismen sollen beispielsweise verhindern, dass Unberechtigte Zugriff auf Objekte erhalten, wenn ein Interessenskonflikt vorliegt. So wäre es im Verlauf einer stillen Auktion beispielsweise denkbar, nach Abgabe des eigenen Gebots (oder aller Gebote) auch die Höhe der anderen Gebote zu erfahren. Vertreter des systembestimmten Zugriffsschutzes sind das Bell/LaPadula-Modell [2] und das Chinese-Wall-Modell [4].

2.4 Verschlüsselung

Verschlüsselung kann in zwei Bereichen angewendet werden:

1. Um Nachrichten von ihrem Sender zum Empfänger über einen unsicheren Kanal (Übertragungsstrecke) vertraulich zu übermitteln, werden sie verschlüsselt.
2. Inhalte von Dateien, die anderweitig nicht vor Zugriff geschützt werden können, lassen sich durch Dateiverschlüsselung schützen. Der Entschlüsselungsschlüssel darf dabei natürlich nicht ebenfalls im Dateisystem abgelegt werden. Falls beispielsweise der Systemadministrator Leserechte auf allen Dateien besitzt, verhindert Dateiverschlüsselung unbefugte Kenntnisnahme durch ihn.

Man unterscheidet symmetrische und asymmetrische Verschlüsselungsverfahren.

Bei **symmetrischen Verschlüsselungsverfahren** (Abb. 3) besitzen Sender und Empfänger den gleichen – und allen anderen hoffentlich unbekannten – Schlüssel *k* (vom engl. key), der aus einer Zufallszahl gebildet wird. Die bekanntesten Vertreter sind DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) und AES (Advanced Encryption Standard). Die Algorithmen dieser und vieler anderer Verschlüsselungsverfahren werden beispielsweise in [14] anschaulich dargestellt. Symmetrische Verfahren sind sehr effizient realisierbar und eignen sich deshalb zur Verschlüsselung von großen Datenmengen und Multimedia-Strömen.

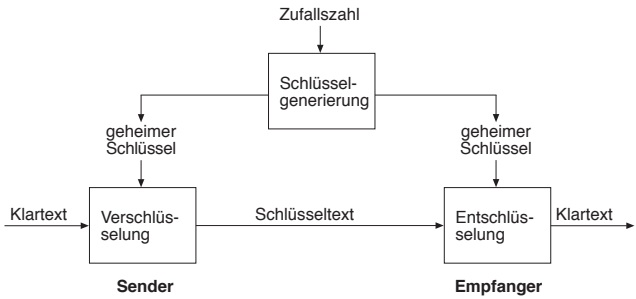

Abb. 3. Symmetrisches Verschlüsselungssystem

Bekannte **asymmetrische Verschlüsselungsverfahren** (Abb. 4) sind RSA (Rivest, Shamir, Adleman) und ElGamal. Im Vergleich zu symmetrischen Systemen sind sie deutlich rechenaufwendiger (etwa Faktor 100 bis 10000), vereinfachen jedoch die Schlüsselverteilung erheblich, da zum Ver- und Entschlüsseln jeweils verschiedene Schlüssel e und d benutzt werden, die der Empfänger erzeugt. Der öffentliche Verschlüsselungsschlüssel e (encryption key) dient zum Verschlüsseln. Dieser Schlüssel darf jedem bekannt sein und wird vom späteren Empfänger gewöhnlich in einem öffentlichen Schlüsselverzeichnis allgemein zugänglich gemacht. Zum Entschlüsseln benutzt der Empfänger den privaten Entschlüsselungsschlüssel d (decryption key), der nur ihm bekannt ist. Damit man e tatsächlich nicht geheim halten muss, darf d nicht mit vernünftigem Aufwand aus e zu bestimmen sein. Jeder, der den öffentlichen Verschlüsselungsschlüssel einer Person kennt, kann ihr nun verschlüsselte Nachrichten schicken, die nur sie wieder entschlüsseln kann.

Der Sender einer Nachricht muss sich sicher sein können, dass e tatsächlich dem Empfänger zugeordnet ist. Diese Zuordnung wird durch ein Schlüsselzertifikat (Abschnitt 2.6) bestätigt. Andernfalls könnte der Angreifer ein Schlüsselpaar erzeugen und behaupten, der öffentliche Schlüssel gehöre einer anderen Person P. Der unwissende Sender, der dieser Person P eine vertrauliche Nachricht schickt, weiß nicht, dass der Angreifer den zugehörigen Entschlüsselungsschlüssel besitzt und somit die Nachricht entschlüsseln kann.

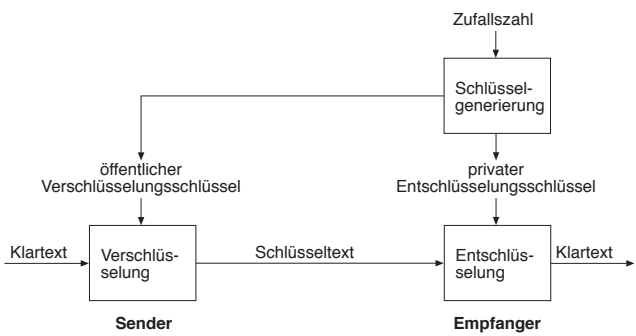

Abb. 4. Asymmetrisches Verschlüsselungssystem

In der Praxis wird meistens eine Kombination von asymmetrischen und symmetrischen Systemen eingesetzt (**hybride Verschlüsselung**). Wegen der im Vergleich zum symmetrischen Verfahren geringen Effizienz der asymmetrischen Verfahren wird mit dem asymmetrischen Verfahren lediglich ein symmetrischer Sitzungsschlüssel verschlüsselt, während der Nachrichteninhalt effizient mit einem symmetrischen Verfahren und dem Sitzungsschlüssel verschlüsselt wird.

Die hybride Verschlüsselung wird beispielsweise bei Secure Sockets Layer (SSL), das beim Zugriff auf https-Webseiten verwendet wird, und bei den im Internet weit verbreiteten Verschlüsselungsprogrammen Pretty Good Privacy (PGP) und Gnu Privacy Guard (GnuPG) eingesetzt.

2.5 Symmetrische Authentikation

Authentikation dient der Integritätssicherung mittels eines **Authentikationssystems**. Bei symmetrischer Authentikation haben Sender und Empfänger wieder einen geheimen Schlüssel k ausgetauscht. Symmetrische Authentikationssysteme findet man sehr oft in zwei Anwendungsbereichen:

1. Der Empfänger einer Nachricht soll erkennen, ob die Nachricht unverfälscht übermittelt wurde. Hierzu wird sie vom Sender mit einem Message Authentication Code (MAC) versehen und zusammen mit ihm übermittelt. Der Empfänger bildet aus k und der Nachricht ebenfalls den MAC, vergleicht ihn mit dem übermittelten und hat bei Übereinstimmung der beiden MACs die Gewissheit, dass die Nachricht unverfälscht ist (Abb. 5).
2. In einem Zugangskontrollsystem soll der Prüfende feststellen können, ob das Subjekt, das Zugang erlangen möchte, ein Geheimnis K besitzt, ohne dieses Geheimnis selbst übertragen zu müssen (Abb. 6). Nur der Besitzer des Geheimnisses kann die Zugangskontrolle passieren. Da das Geheimnis selbst jedoch nicht übertragen wird, kann die Kommunikation während der Authentikation unverschlüsselt erfolgen. Dies ist gegenüber passwortbasierten Verfahren ein Vorteil. Aus einer vom Netzbetreiber an ein persönliches Gerät (Abschnitt 2.1) gesendeten Zufallszahl (genannt Challenge oder RAND) und K wird mittels eines kryptographischen Algorithmus eine Antwort (Response RES) berechnet und mit der erwarteten Antwort (Expected Response XRES) verglichen. RES (und XRES) kann nur berechnen, wer den für jeden Teilnehmer individuellen Authentisierungsschlüssel K kennt.

Beim Einsatz symmetrischer Authentikationssysteme ist zu beachten, dass sowohl der Sender als auch der Empfänger den MAC bzw. RES bilden können. Dies ist ein wichtiger Unterschied zu den im Folgenden beschriebenen digitalen Signatursystemen.

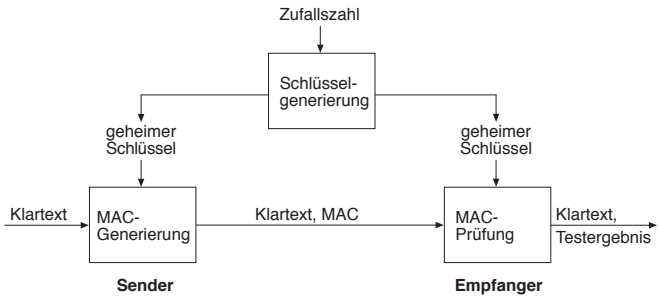

Abb. 5. Message Authentication Code

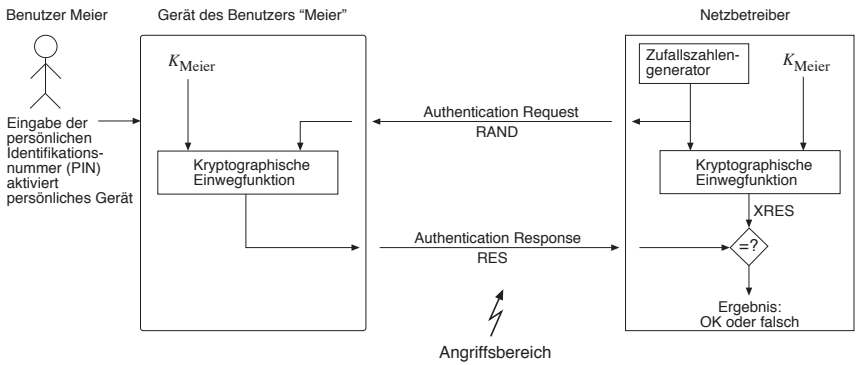

Abb. 6. Challenge-Response-Authentikation

2.6 Digitale Signatur

Digitale Signatursysteme (Abb. 7) sind asymmetrische Authentikationssysteme. Mit ihnen kann nicht nur die Unversehrtheit einer Nachricht festgestellt werden, was bereits mit einem symmetrischen Authentikationssystem (Abschnitt 2.5) möglich ist, sondern auch die **Zurechenbarkeit** der Nachricht zu ihrem Urheber. Der Sender einer Nachricht erzeugt sich zwei verschiedene, aber zusammengehörende Schlüssel s und t. Der private Signierschlüssel s wird vom Absender geheim gehalten. Mit s und dem Signieralgorithmus erzeugt er die Signatur zu einer Nachricht. Bekannte Signieralgorithmen sind RSA (ebenfalls für asymmetrische Verschlüsselung einsetzbar) und DSS (Digital Signature Standard). Den öffentlichen Testschlüssel t lässt sich der Sender von einer Zertifizierungsstelle beglaubigen. Diese Beglaubigung ist der Nachweis, dass der Testschlüssel zu einer ganz bestimmten Person gehört. Sie wird (ggf. zusammen mit weiteren beglaubigten Eigenschaften, z.B. Volljährigkeit der Person) als digitales **Schlüsselzertifikat** veröffentlicht.

Um zu überprüfen, ob eine Nachricht tatsächlich vom Absender stammt, besorgt sich der Tester das Schlüsselzertifikat und kann dann überprüfen, ob die Nachricht tatsächlich vom Absender stammt.

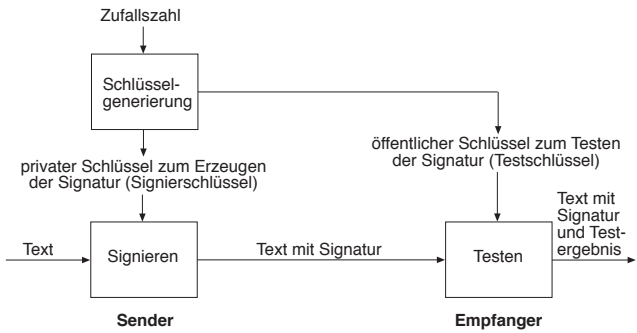

Abb. 7. Digitales Signatursystem

Der Empfänger einer Nachricht kann jedem beweisen, dass die Nachricht vom Sender stammt. Da nur der Sender seinen privaten Signierschlüssel *s* kennt, kann niemand außer ihm selbst eine gültige Signatur erzeugt haben. Kommt es zwischen dem Sender und Empfänger zum Streit, kann auch durch eine dritte Partei die Urheberschaft einer Nachricht festgestellt werden, da der Testschlüssel *t* öffentlich ist.

Ganz ohne Vertrauen kommt man allerdings auch bei der digitalen Signatur nicht aus:

1. Der Signierschlüssel, mit dem rechtsverbindliche digitale Signaturen geleistet werden, darf keinesfalls von anderen Personen nutzbar sein – denn das käme dem nicht erkennbaren Fälschen der eigenhändigen Unterschrift gleich. Wird der Signierschlüssel auf einer Chipkarte gespeichert, muss er vor unberechtigter Verwendung und Kenntnisnahme durch Fremde geschützt sein. In der Praxis sollte der Signierschlüssel deshalb möglichst auf der Karte erzeugt werden und diese – soweit physische Sicherheit (Abschnitt 2.1) angenommen werden kann – niemals verlassen.
2. Alle Beteiligten müssen darauf vertrauen, dass sich die Zertifizierungsstelle ausreichend von der Identität des Inhabers des Schlüsselzertifikats überzeugt hat, damit nur authentische Testschlüssel, d.h. solche, die eindeutig und fehlerfrei einer Person zugeordnet sind, im Umlauf sind.

Das Datenformat der meisten Schlüsselzertifikate entspricht dem Standard X.509 [9] der International Telecommunications Union (ITU). Ein **X.509-Zertifikat** enthält folgende Datenfelder:

- die X.509-Versionsnummer (heute meist v3),
- eine Seriennummer des Zertifikats,
- eine Kennung des verwendeten Signieralgorithmus,
- die Gültigkeitsdauer des Zertifikats,
- den Namen des Ausstellers (Zertifizierungsstelle),
- den Namen des Inhabers,

- den öffentlichen Schlüssel des Inhabers,
- ID-Nummern für Inhaber und Aussteller,
- ggf. Angaben zur Art und zum Anwendungsbereich des Zertifikats, alternative Namen für Nutzer und Aussteller, Informationen bzgl. Sperrlisten und schließlich private ausstellerspezifische Erweiterungen,
- sowie eine digitale Signatur des Ausstellers.

Nachdem sich der Empfänger einer Nachricht das Schlüsselzertifikat des Senders besorgt hat, überprüft er zunächst die Gültigkeit und dann die Echtheit des Schlüsselzertifikats:

1. Das Schlüsselzertifikat ist gültig, wenn der aktuelle Zeitpunkt innerhalb der Gültigkeitsdauer des Zertifikats liegt und das Zertifikat nicht vorfristig für ungültig erklärt wurde. Hat der Inhaber beispielsweise seine Chipkarte verloren oder besteht der Verdacht, dass der private Signierschlüssel kompromittiert ist, kann der Nutzer das Zertifikat in eine Sperrliste eintragen lassen.
2. Die Überprüfung der Echtheit des Zertifikats geschieht durch Testen der digitalen Signatur des Ausstellers unter dem Zertifikat. Hierzu besorgt sich der Tester den öffentlichen Testschlüssel der Zertifizierungsstelle. Selbstverständlich muss auch die Gültigkeit und Echtheit dieses Zertifikats geprüft werden usw. (Zertifikatskette).

In vielen Programmen (insb. bei Browsern, Abb. 8) werden die Zertifikate der wichtigsten Zertifizierungsstellen bereits bei der Softwareinstallation vorinstalliert und a priori als gültig angenommen. Insoweit muss auch dem Softwareproduzenten vertraut werden, dass er nur Zertifikate von vertrauenswürdigen Zertifizierungsstellen mit aufnimmt. Zwar kann der Nutzer jederzeit die ihm nicht vertrauenswürdigen Zertifikate aus der Software entfernen – aber das wird kaum praktiziert.

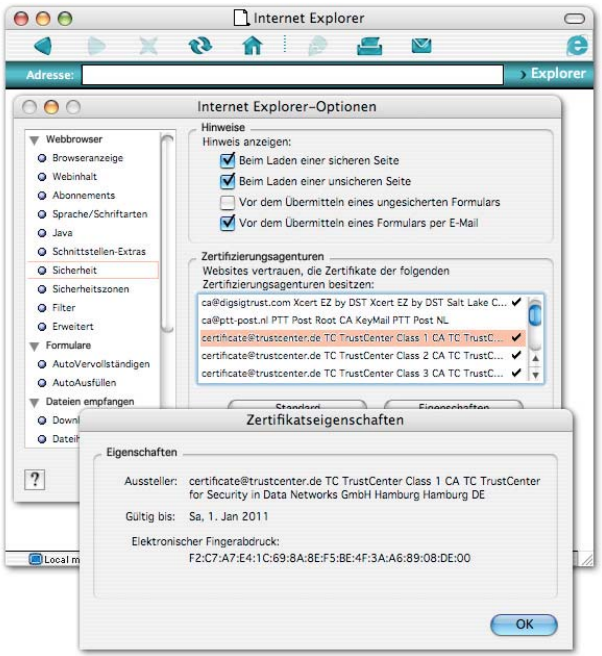

Abb. 8. Zertifikate im Internet Explorer für MacOS X

Nach dem deutschen Signaturgesetz (SigG) werden drei Stufen von Signaturen unterschieden, von denen nur zwei mit digitalen Signatursystemen realisiert sind:

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Hierbei handelt es sich nicht notwendigerweise um digitale Signaturen. Beispielsweise werden die üblicherweise an E-Mails angehängten Kontaktdaten (Abb. 9) als elektronische Signaturen nach SigG angesehen. Streng genommen kann hier von Authentizität keine Rede sein, da problemlos falsche Angaben gemacht werden können und die Daten außerdem auch unbemerkt bei der Übertragung verfälscht werden können.

Dagegen werden fortgeschrittene und qualifizierte elektronische Signaturen mit Hilfe digitaler Signatursystem erstellt. Dementsprechend müssen **fortgeschrittene elektronische Signaturen** folgende Bedingungen erfüllen:

1. Die Signaturen sind ausschließlich dem Signaturschlüssel-Inhaber zugeordnet.
2. Die Identifizierung des Signaturschlüssel-Inhabers ist möglich.
3. Die Signaturen werden mit Mitteln erzeugt, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann.
4. Die Signaturen sind mit den Daten, auf die sie sich beziehen, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Qualifizierte elektronische Signaturen sind im Prinzip fortgeschrittene elektronische Signaturen. Zusätzlich sind jedoch zwei weitere Forderungen zu erfüllen:

1. Die Signatur beruht auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat (beispielsweise einem X.509-Zertifikat).
2. Die Signatur wurde mit einer sicheren Signaturerstellungseinheit (§§ 17 und 23 SigG) erzeugt.

Elektronische Signatur	Fortgeschrittene Signatur	Qualifizierte Signatur
Beispiel: E-Mail mit "Signatur"	Beispiel: PGP-signierte E-Mail	wie fortgeschrittene Signatur, zusätzlich:
From: Hannes Federrath Subject: Beispiel Das ist der Text. -- Hannes Federrath Uni Regensburg Sicherheitsmanagement 93040 Regensburg	-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 Das ist der Text. -----BEGIN PGP SIGNATURE----- Version: PGP 8.0.2 iQA/AwUBP6wDdOFAIGFJ7x2EEQK9VgCg2Q 4eQAztVIHP0HNFQ10eaXte96sAnR2p 53T/SdevjXIuX6WOF5IXA44S =K3TO -----END PGP SIGNATURE-----	Zertifikatausstellung nach Identitätsüberprüfung und sichere Signaturerstellungseinheit 

Abb. 9. Arten von Signaturen nach dem Signaturgesetz (SigG)

3 Prozesse zur Schaffung und Erhaltung von IT-Sicherheit

3.1 Sicherheitsmanagement

Je mehr Funktionen eine Organisation mit Hilfe von IT-Systemen erledigt, umso abhängiger wird sie von der fehlerfreien und verlässlichen Funktion der Systeme. Das IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe und unbeabsichtigte Ereignisse zu schützen.

Mit der wachsenden Bedeutung der IT im Unternehmen wächst natürlich auch die Bedeutung der IT-Sicherheit. Während vor einigen Jahren die Verantwortung für die Gewährleistung von IT-Sicherheit meist innerhalb der IT-Abteilung lag, wird heute IT-Sicherheit mehr und mehr als Managementaufgabe verstanden. Damit wird auch den veränderten Bedingungen in der Datenverarbeitung der letzten 20 Jahre Rechnung getragen. So dominieren heute offene, dezentralisierte, vernetzte Systeme die IT-Landschaft, während früher größtenteils auf gut bewachten Großrechnern gearbeitet wurde, die – wenn überhaupt – über Standleitungen miteinander verbunden waren. Heute vernetzt man IT-Systeme kostengünstig über das unsichere Internet. Bei derartigen Rationalisierungsmaßnahmen sind jedoch die Kosten für den Schutz der Systeme und Daten gegenzurechnen. Die Aufgabe des Sicherheitsmanagements besteht nun in der Lösung eines Optimierungsproblems: Bei minimalen Kosten für Sicherheitsmaßnahmen ist akzeptabler Schutz über einen gegebenen Zeitraum zu gewährleisten. Das verbleibende Restrisiko wird entweder abgewälzt (z.B. auf eine Versicherung) oder selbst getragen (Abb. 10).

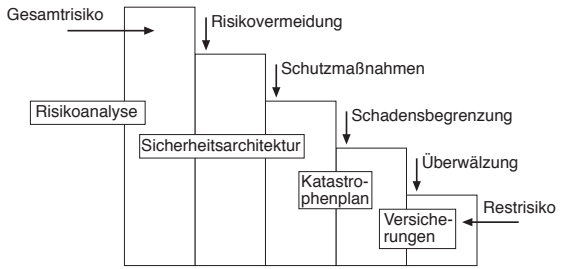

Abb. 10. Risiko-Management für IT-Systeme (nach [13, S.35])

Sicherheitsmanagement beginnt im Unternehmen oder in der Behörde mit dem Schaffen der Stelle eines **IT-Sicherheitsbeauftragten**, in größeren Organisationen zusätzlich mit der Bildung einer Arbeitsgruppe Sicherheitsmanagement, in der alle relevanten Bereiche der Organisation vertreten sind. Anschließend formuliert die Organisation eine **Sicherheitsleitlinie** (Security Policy), die den Stellenwert der IT-Sicherheit im Unternehmen definieren soll. Der zeitintensivste Schritt ist die Erstellung und Umsetzung eines **Sicherheitskonzeptes** sowie begleitend hierzu die Definition von Maßnahmen zur **Erhaltung** des erreichten Sicherheitsniveaus im laufenden Betrieb.

3.2 Standards

Es existieren inzwischen mehrere Standards, die Vorgehensmodelle für das Sicherheitsmanagement beschreiben. Die wichtigsten sind ISO 17799, das Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und ISO 13335.

Der Standard **ISO 17799** [7] beschreibt einen Best-Practice-Ansatz zur Schaffung unternehmensweiter Informationssicherheit. Mit seinem geringen Umfang von knapp 80 Seiten ist der Standard jedoch nur auf die Beschreibung konzeptioneller Maßnahmen beschränkt.

Das **Grundschutzhandbuch** (GSHB, [5], siehe Abschnitt 3.4) definiert auf seinen ca. 2500 Seiten neben dem Vorgehen zur Schaffung von angemessener Sicherheit auch sehr umfangreich die umzusetzenden technischen und organisatorischen Maßnahmen. Methodisch arbeitet das GSHB mit einem Soll-Ist-Vergleich, d.h. es werden die bereits umgesetzten Maßnahmen mit den noch umzusetzenden in Beziehung gesetzt. Das GSHB wird halbjährlich überarbeitet und aktualisiert und steht kostenlos unter http://www.bsi.bund.de/gshb/ zur Verfügung. Es ist auch in einer engl. Fassung erhältlich.

Der Standard **ISO 13335** [8] liegt bzgl. seiner Beschreibungstiefe zwischen ISO 17799 und dem Grundschutzhandbuch. ISO 13335 leistet sowohl konzeptionell als auch konkret einen Beitrag zur Schaffung von IT-Sicherheit. Ein wesentlicher Unterschied von ISO 13335 im Vergleich zum Grundschutzhandbuch liegt in der stärkeren Orientierung auf das Risikomanagement.

3.3 Rechtliche Rahmenbedingungen

Dass Sicherheitsmanagement heute mehr und mehr als Managementaufgabe verstanden wird, hat auch seinen Grund in der Umsetzung von rechtlichen Vorgaben an die Sicherheit in einer Organisation.

Wenn das Fortbestehen eines Unternehmens vom Funktionieren der IT abhängt, ist dieses möglicherweise gesetzlich verpflichtet, Maßnahmen zu treffen, um Schäden von der IT abzuwenden. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG, am 1. Mai 1998 in Kraft getreten, [3]) verpflichtet in § 91 Aktiengesetz (AktG) die betroffenen Unternehmen, ein Überwachungssystem zur Früherkennung existenzgefährdender Entwicklungen einzurichten. Damit wird die Geschäftsführung gesetzlich verpflichtet, ein unternehmensweites Risikomanagement zu implementieren. So sind allgemein Vorkehrungen zur Verhinderung von Vermögensschäden zu treffen. Dies betrifft bei Abhängigkeit des Unternehmens von IT-Systemen auch entsprechende Vorkehrungen zum Schutz der Informationssysteme.

Speziell für das Bankwesen hat der Baseler Ausschuss für Bankenaufsicht Rahmenbedingungen für das Risikomanagement in Banken geschaffen [1]. Wesentliches Ziel dieses als „Basel II“ bezeichneten Dokuments ist die Sicherung einer angemessenen Eigenkapitalausstattung von Banken. Die finanziellen Risiken durch Ausfall von und Angriffe auf IT-Systeme werden von Basel II als operative Risiken erfasst. Somit muss das Finanzdienstleistungsunternehmen angemessene Maßnahmen zur Erhaltung der IT-Sicherheit realisieren, um den Anforderungen von Basel II gerecht zu werden. Basel II tritt Ende 2005 mit einer einjährigen Einführungsphase in Kraft.

Daneben werden durch Datenschutzbestimmungen (insb. das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze) konkrete Anforderungen an die IT-Sicherheit gestellt. So hat der betriebliche oder behördliche Datenschutzbeauftragte die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme zu überwachen und in bzgl. Datenschutz sensiblen Datenverarbeitungsprozessen eine Vorabkontrolle durchzuführen, d.h. die Einhaltung der Datenschutzvorschriften vor Einführung eines neuen Datenverarbeitungsprozesses zu prüfen. Solche Prüfungen werden durch ein systematisches Vorgehen bei der Realisierung neuer Datenverarbeitungsprozesse erheblich erleichtert.

3.4 Beispiel: Grundschutzhandbuch

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem Grundschutzhandbuch eine Methodik zur Schaffung von IT-Sicherheit in Unternehmen und Behörden geschaffen. Ausgehend von allgemeinen organisatorischen Maßnahmen (z.B. Infrastruktur, Personal, Gebäude, Vernetzung) werden für verschiedene technische Komponenten (z.B. Arbeitsplatz-PC, Webserver) und Systeme (z.B. Windows, Unix, Novell) konkrete Maßnahmen- und Gefährdungskataloge angegeben. Das GSHB ist etwa folgendermaßen untergliedert:

- Einstieg und Vorgehensweise: Hier wird die Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach dem GSHB beschrieben.
- Bausteine: Sie enthalten die sog. Gefährdungslage und die Maßnahmenempfehlungen für verschiedene Komponenten, Vorgehensweisen und IT-Systeme, die jeweils in einem Baustein zusammengefasst werden.
- Gefährdungskataloge: Hier findet man ausführliche Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden.
- Maßnahmenkataloge: Dies sind die in den Bausteinen genannten IT-Sicherheitsmaßnahmen, wobei jeder Maßnahme eine Priorität zugeordnet (als Anhaltspunkt für eine anzustrebende Reihenfolge bei der Umsetzung fehlender Maßnahmen) oder sie als optional gekennzeichnet wird.

Das Vorgehen nach GSHB ist von folgender Idee geprägt: Anstelle einer traditionellen **Risikoanalyse**, bei der zunächst die Gefährdungen ermittelt und mit Eintrittswahrscheinlichkeiten versehen werden, um anschließend die entsprechenden Maßnahmen auszuwählen und das verbleibende Restrisiko zu bewerten, wird bei der **Grundschutzanalyse** ein Soll-Ist-Vergleich zwischen den geforderten und bereits umgesetzten Maßnahmen durchgeführt und erst bei zusätzlichem (signifikant höherem) Schutzbedarf eine ergänzende Sicherheitsanalyse durchgeführt.

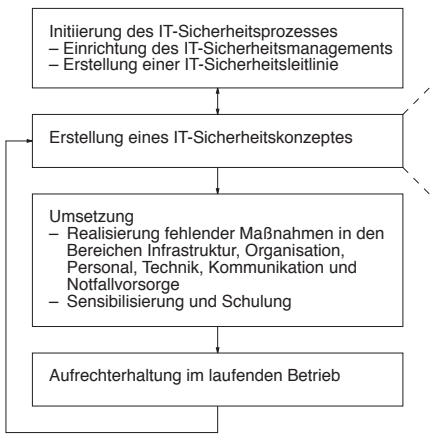

Abb. 11. Arbeitsschritte zur Realisierung von IT-Grundschutz nach GSHB, Maßnahme M 2.191

Die wesentlichen Schritte zur Schaffung von IT-Grundschutz nach GSHB sind in Abb. 11 dargestellt. Zur Initiierung des IT-Sicherheitsprozesses wird das IT-Sicherheitsmanagement-Team (bestehend aus dem IT-Sicherheitsverantwortlichen und ggf. einer speziell gebildeten Arbeitsgruppe) eingesetzt. Diese Gruppe verfasst nun die IT-Sicherheitsleitlinie, auf deren Grundlage im zweiten Schritt ein Sicherheitskonzept für die Organisation erstellt wird. Das Vorgehen hierfür ist ebenfalls detailliert vom GSHB vorgegeben (Abb. 12). Schließlich wird das Sicherheitskonzept umgesetzt. Begleitend hierzu sind Sensibilisierungs- und Schu-

lungsmaßnahmen vorzusehen. Für die Aufrechterhaltung der Sicherheit im laufenden Betrieb schlägt das GSHB u.a. regelmäßige und anlassbezogene Prüfungen und ggf. Korrekturen der Systeme vor. Darüber hinaus soll der aktuelle Status in einem Managementreport dokumentiert werden.

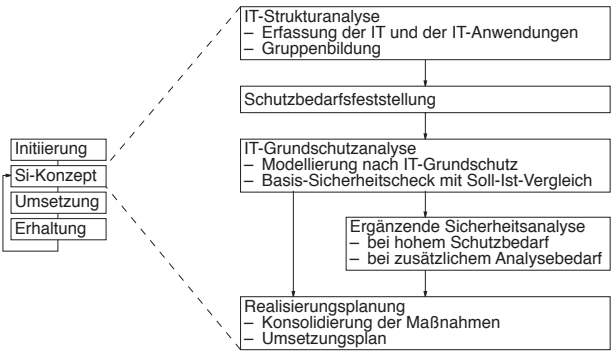

Abb. 12. Erstellung des Sicherheitskonzeptes nach GSHB, Maßnahme M 2.195

Für die Erstellung des Sicherheitskonzepts (Abb. 12) schlägt das GSHB folgendes vorgehen vor:

IT-Strukturanalyse: Selbstverständlich sind zunächst alle IT-Systeme und -Anwendungen zu erfassen. Durch Gruppenbildung wird anschließend eine Komplexitätsreduktion angestrebt.

Schutzbedarfsfeststellung: Die identifizierten Systeme werden bzgl. ihres Schutzbedarfs in eine der drei Kategorien „niedrig bis mittel“ (begrenzte), „hoch“ (beträchtliche) oder „sehr hoch“ (katastrophale Schadensauswirkung) eingeordnet.

IT-Grundschutzanalyse: Nun wird für jedes System im GSHB nachgeschlagen, welchen Bedrohungen es ausgesetzt ist. Für jede Bedrohung nennt das GSHB Maßnahmen, die umzusetzen sind. Anschließend werden die geforderten Maßnahmen mit dem Ist-Zustand verglichen.

Ergänzende Sicherheitsanalyse: Soweit bzgl. eines Systems nur begrenzte Schadensauswirkungen zu erwarten sind, kann die Umsetzung der fehlenden Maßnahmen sofort geplant werden. Bei höherem Schutzbedarf (beträchtliche oder katastrophale Schadensauswirkung) sind ergänzende Analysen (z.B. eine deutlich aufwändigere Risikoanalyse oder Penetrationstests) notwendig, da der vom GSHB angestrebte Grundschutz für diese Systeme (wegen des erhöhten Schutzbedarfs) nicht mehr ausreichend ist.

Realisierungsplanung: Die erkannten Defizite (fehlenden Maßnahmen) werden in eine Prioritätenliste eingetragen, damit deren Beseitigung (Umsetzung der fehlenden Maßnahmen) zielgerichtet erfolgen kann.

Das GSHB gibt auch dem wenig erfahrenen Sicherheitsbeauftragten die Möglichkeit einer Bestandsaufnahme der IT-Sicherheit. Die vorgeschlagene Vorgehensweise ist kanonisch, und die Anwendung des GSHB bleibt trotz des großen Umfangs recht überschaubar. Allerdings bleibt die Beurteilung des Schutzbedarfs eines Systems weitgehend subjektiv.

Die fehlerfreie Modellierung erfordert sehr viel Erfahrung, um nicht zu verdeckten Unsicherheiten zu führen. Versierte Sicherheitsbeauftragte sind jedoch dank ihrer Erfahrung selten auf die Maßnahmenkataloge des GSHB angewiesen. Für diese Nutzergruppe eignet sich das GSHB aber gut als Nachschlagewerk.

Soweit alle geforderten Maßnahmen umgesetzt sind, kann darüber hinaus eine Zertifizierung durch das BSI erfolgen (Grundschutz-Zertifikat).

Literatur

[1] Basler Ausschuss für Bankenaufsicht: Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework. Basel Committee Publications No. 107, June 2004, http://www.bis.org/publ/bcbs107.htm

[2] D. Bell, L. Lapadula: Secure computer systems: Unified exposition and MULTICS interpretation. Technical report ESD-TR-75-306, MITRE Corporation, 1975.

[3] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). BGBl I 1998/24.

[4] David F. C. Brewer, Michael J. Nash: The Chinese Wall security policy. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, California, May 1989, 206-214.

[5] Bundesamt für die Sicherheit in der Informationstechnik (BSI): Grundschutzhandbuch. Version Oktober 2003.

[6] Hannes Federrath, Andreas Pfitzmann: Gliederung und Systematisierung von Schutzzielen in IT-Systemen. Datenschutz und Datensicherheit DuD 24/12 (2000) 704-710.

[7] ISO/IEC 17799 Information technology -- Code of practice for information security management, 2000.

[8] ISO/IEC TR 13335-x Information technology -- Guidelines for the management of IT Security -- Parts 1-5, 1996-2001.

[9] International Telecommunication Union: Recommendation X.509 - Information technology - Open Systems Interconnection - The Directory: Authentication framework, 1997

[10] Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997.

[11] Günter Müller, Kai Rannenberg (Ed.): Multilateral Security in Communications, Addison-Wesley-Longman 1999.

[12] Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Heidelberg 1990.

[13] Ingrid Schaumüller-Bichl: Sicherheitsmanagement: Risikobewältigung in informationstechnischen Systemen. BI-Wiss.-Verl., Mannheim, 1992.

[14] Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, (2nd ed.) New York 1996. (Die deutsche Übersetzung ist bei Addison-Wesley-Longman erschienen.)

[15] Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols. ACM Computing Surveys 15/2 (1983) 135-171.