



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

IT Sicherheit

Allgemeines Ziel des Moduls ist die Vermittlung eines grundlegenden Wissens über wesentliche Sicherheitsprobleme in IT- und Medienanwendungen, organisatorische und technische Lösungsansätze hierfür, grundlegender rechtlicher Rahmenbedingungen sowie der Anwendung ausgewählter praktischer Sicherheitswerkzeuge.

In dem Modul IT-Sicherheit wird ein grundlegendes Verständnis für relevante Sicherheitsaspekte in IT Systemen entwickelt, grundsätzliche organisatorische Konzepte für die Entwicklung von Sicherheitsrichtlinien können wiedergegeben und angewandt werden, Grundlagen von Sicherheitsmodellen und wesentliche Sicherheitsstandards können beschrieben und im Hinblick auf Anwendungsgebiete als auch der adressierten Sicherheitsaspekte eingeordnet werden. Es werden durch die grundlegenden Methoden zudem analytische Vorgehensweisen zur Schwachstellenanalyse vermittelt, welche speziell für Fragestellungen der IT, aber auch in anderen Bereichen wie beispielsweise der betrieblichen Organisationen umgesetzt werden können. Wesentliche juristische Rahmenwerke können benannt, sowie deren Wirkungsweise beschrieben werden. Durch Einführung in Datenschutzrecht wird weiterhin die soziale Kompetenz für diesen Bereich der Persönlichkeitsrechte sensibilisiert. Auf dem Gebiet des Identity Managements werden grundlegende Konzepte zur Verwaltung und Überprüfung von Identitäten in IT Systemen vermittelt und ausgewählte technische Ansätze vertieft. In einem Baustein zu Anwendungen der IT-Sicherheit lernen die Studierenden aktuelle Einsatzgebiete kennen und im Bereich der praktischen IT-Sicherheit werden die erlernten Kenntnisse anhand von konkreten Problemstellungen und deren Lösung mit Sicherheitswerkzeugen vertieft.

Das in der Lehrveranstaltung erworbene Wissen befähigt erfolgreiche Absolventen künftig aktuelle Verfahren zu Erarbeitung und Umsetzung von Sicherheitskonzepten zu bestimmen und umzusetzen. Viele Themen werden hierzu beispielhaft anhand von Fallbeispielen aus praktischen Institutionen aufgearbeitet. In der Berufspraxis wird die Kenntnis der grundlegenden Funktionsweisen die Basis zu Bewertung und Anwendung von Sicherheitsmethoden für Informatiker/innen und Informatiknahen Berufen bilden.

[Nächste »](#)



IT Sicherheit
► Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Bearbeitungshinweise

Dieser Abschnitt enthält Hinweise zur Bearbeitung des Lehrmoduls. Das Lehrmodul besteht aus den folgenden fünf Abschnitten:

1. Einführung und organisatorische Sicherheit
2. Datenschutz und Nicht-technische Datensicherheit
3. Identity Management
4. Angewandte IT Sicherheit
5. Praktische IT Sicherheit

Die einzelnen Abbildungen können zur Vergrößerung angeklickt werden. Es öffnet sich ein neues Fenster mit der Abbildung und deren Bezeichnung. Ein weiterer Klick auf die jeweilige Abbildung vergrößert diese gegebenenfalls auf 100% ihrer Originalgröße. Enthält eine Abbildung mehrere Bilder kann durch diese mit "Vorheriges" rückwärts und mit "Nächstes" vorwärts geblättert werden. Geschlossen wird das Abbildungsfenster über "Schließen".

Jedes der Kapitel enthält Unterkapitel und jeweils einen Abschnitt mit Verständnisfragen, Einsendeaufgaben, Abkürzungen und Bezeichnern und Referenzen.

Verständnisfragen

Es wird empfohlen, nach dem Bearbeiten des Lehrinhaltes zunächst die Verständnisaufgaben zu lösen. Sie sollen dem Studierenden die Möglichkeit geben, das soeben Gelernte anzuwenden. Die Aufgaben beziehen sich auf den Inhalt des jeweiligen Kapitels und sind so gestaltet, dass sie nach dem gründlichen Studium des Textes ohne weitere Literatur- bzw. Online-Recherchen lösbar sind. Zu jeder Aufgabe werden mindestens je zwei Lösungen vorgegeben, von denen mindestens eine die richtige Antwort enthält. Es ist also auch möglich, dass mehrere Antworten zutreffen. Klicken Sie zur Lösung der Aufgaben bitte die Antworten an, die Sie für richtig halten. Falls nötig, lesen Sie den aktuellen Abschnitt (teilweise) noch mal, um die richtigen Antworten zu finden. Unter jeder Aufgabe finden Sie einen Button mit der Aufschrift "Feedback anzeigen", den Sie drücken können, um sich die richtige Lösung anzeigen lassen zu können. Sollten Sie eine Aufgabe falsch beantwortet haben, lesen Sie bitte den entsprechenden Abschnitt erneut.

Einsendeaufgaben

Bitte beginnen Sie mit der Lösung der Einsendeaufgaben erst, wenn Sie die Verständnisaufgaben gelöst bzw. den Grund der gemachten Fehler gefunden und verstanden haben. Die Lösung der Einsendeaufgaben erfordert in den meisten Fällen auch das Studium weiterer Literatur beziehungsweise Online-Referenzen. Setzen Sie sich also gegebenenfalls mit den angegebenen Referenzen auseinander und suchen Sie online nach möglichen Lösungshilfen. Die Lösung der Einsendeaufgaben ist dem Betreuer bis spätestens zum von ihm genannten Abgabedatum zuzusenden.

Abkürzungen und Bezeichner

In diesem Abschnitt werden die im dazugehörenden Kapitel verwendeten Abkürzungen kurz erläutert und die eingeführten Bezeichner noch mal aufgelistet. Dies soll der Übersichtlichkeit dienen und bietet die Möglichkeit, Bezeichner später schnell nachzuschlagen.

Referenzen

Im Abschnitt Referenzen wird die Literatur aufgelistet, die den Studierenden zur Vertiefung des im jeweiligen Kapitel vermittelten Wissens empfohlen werden. Unterschieden wird dabei zwischen gedruckter Literatur (Konferenzbeiträge, Beiträge in Zeitschriften und Bücher) und Online-Referenzen. Dabei ist zu beachten, dass die Aktualität und Erreichbarkeit der Online-Referenzen nicht immer gegeben ist.

Weitere Bemerkungen

Bitte beachten Sie, dass die Online-Version des Lehrmoduls unter Umständen aktueller sein kann, als die druckbare Version im PDF-Format. Grund hierfür ist eine einfachere Anpassung des Online-Moduls bei aktuellen Ereignissen oder neuen Erkenntnissen. Außerdem sind die in der PDF-Version enthaltenen Bilder nur als Vorschaubilder vorhanden. Zusätzlich wird darauf hingewiesen, dass interaktive Komponenten verständlicherweise nicht in der PDF-Version vorhanden sind.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
► Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Literaturempfehlungen



verwendete Literatur

Zum Selbststudium und zur Vertiefung des vermittelten Wissens über den Inhalt des Online-Studienmoduls IT-Sicherheit hinaus werden die folgenden Bücher empfohlen.

[Bish2003] Matt Bishop: Computer Security Art and Science. Addison Wesley, 2003

[Bish2005] Matt Bishop: Introduction to Computer Security; Addison-Wesley, Boston, ISBN 0-321-24744-2; 2005

[Pleg2006] Charles P. Pfleger et al.: Security in Computing, Prentice Hall, 4th edition, 2006

[Ecke2008] Claudia Eckert: IT-Sicherheit, Oldenbourg-Verlag, 2008



vertiefende Literatur

Die nachfolgend aufgelisteten Publikationen dienen der tieferen Einarbeitung in verschiedene Kurseinheiten und werden dort an entsprechender Stelle referenziert.

[Pank2003] Raymond R. Panko: Corporate Computer and Network Security, Prentice Hall, March 2003

[Stal1995] William Stallings: Sicherheit im Datennetz, Prentice Hall, München, London, 1995

[Ande2001] Ross Anderson: Security Engineering, Wiley and Sons, 2001

[RaEf2002] Wolfgang Rankl, Wolfgang Effing: Handbuch der Chipkarten, Carl Hanser Verlag München Wien, 4. Auflage, 2002

[Schn2000] Bruce Schneier: Angewandte Kryptographie - Protokolle, Algorithmen und Sourcecode in C, 2. Aufl., Addison-Wesley, 2000

[Ditt2000] Dittmann: Sicherheit in Medienströmen - Digitale Wasserzeichen, Springer, New York, 2000

[LFBP2000] Peter Lipp, Johannes Farmer, Dieter Bratko, und Wolfgang Platzer: Sicherheit und Kryptographie in Java. Einführung, Anwendung und Lösungen, 1- Aufl., Addison-Wesley, 2000

[Viel2006] Claus Vielhauer: Biometric User Authentication for IT Security: From Fundamentals to Handwriting, Springer, New York, 2006

[Gesc2008] Geschonnek, Alexander: Computer-Forensik – Computerstraftaten erkennen, ermitteln, aufklären, 3., aktualisierte und erweiterte Auflage, 2008



Online-Referenzen

Zusätzlich wird das Studium bestimmter Online-Referenzen empfohlen, wobei hier darauf hingewiesen wird, dass es bei Online-Angeboten immer zu Korrekturen kommen kann, bei denen sich Inhalt, Adresse bzw. Verfügbarkeit der angegebenen Referenz kurzfristig ändern kann.

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen:
Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der
Signaturverordnung (Übersicht über geeignete Algorithmen)

Link: <http://www.bundesnetzagentur.de/media/archive/14953.pdf>

Stand: 17.11.2008

Beschreibung: Katalog mit Algorithmen und Schlüssellängen die zur Erzeugung von
Signaturschlüsseln, zum Hashen zu signierender Daten bzw. zur Erzeugung und Prüfung
qualifizierter elektronischer Signaturen die bis Ende 2015 empfohlen werden

Welcome to CERT

Link: <http://www.cert.org/>

Stand: 29.01.2009

Beschreibung: Beschreibung der CERT-Angriffs-Taxonomie (Computer Emergency
Response Team), die sich mit der Klassifizierung von Angriffen unter verschiedenen
Gesichtspunkten befasst wie z.B. Art des Angreifers, Motivation oder eingesetzte Tools



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacks
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1 Einführung und organisatorische Sicherheit

Die Verwendung und Verbreitung von Technik für Speicherung, Transfer und Verarbeitung von Informationen und zur Kommunikation hat im Laufe der letzten Jahre immer mehr zugenommen, wobei ein Ende der Entwicklung nicht abzusehen ist. Dadurch gewinnt aber auch die Forderung nach Sicherheit der zugrunde liegenden IT-Systeme immer mehr an Bedeutung, da oft Interesse Dritter an der Erlangung und Verwendung verschiedenartiger Informationen besteht. Diese Daten sind häufig von sensibler Natur, wenn sie Informationen über bestimmte Personen oder Personenkreise preisgeben oder mit finanziellen Vorteilen verbunden sind. Beispielhaft können hier die Adresse, persönliche Korrespondenz, Informationen über das Online-Banking, aber auch Vorlieben bei der Nutzung von Online-Angeboten wie das Einkaufsverhalten oder die Suchgewohnheiten eines privaten Nutzers genannt werden. Natürlich gibt es auch sicherheitsrelevante Informationen in anderen Bereichen wie der kommunalen Verwaltung, industriellen oder Dienstleistungsunternehmen. Für jedes der genannten Beispiele existiert eine Vielzahl von Interessenten, die einen Nutzen aus der Gewinnung und Verwertung der Informationen ziehen können. Dabei können potenzielle Angreifer unterschiedliche Ziele verfolgen: Einige nutzen Sicherheitslücken dazu, um Schwachstellen aufzuzeigen und deren Behebung zu motivieren, andere haben das Abfangen, die Löschung oder die Veränderung von Daten zum Ziel während wiederum andere Angreifer Daten sammeln, um sie für kommerzielle Zwecke zu verwenden. Ziel des Forschungs- und Anwendungsbereiches der IT-Sicherheit ist es, IT-Systeme und Informationen zu sichern.

Lehrziel des Moduls IT-Sicherheit ist es, den Teilnehmer für die Problematik der Sicherheit in den Bereichen Datenerzeugung, -speicherung, -transfer und -verarbeitung mit seinen umfangreichen Facetten zu sensibilisieren und Kenntnisse über die Abwehr möglicher Angriffe zu vermitteln. Dabei hervorzuheben ist, dass dieses Studienmodul Sicherheitsbedrohungen und potentielle Schwachstellen motivieren und den Handlungsbedarf aufzeigen soll. Es soll die Fähigkeit erlernt werden, die Sicherheit von IT-Systemen zu überprüfen, einzuschätzen und gegebenenfalls Lösungen für auftretende Probleme zu entwickeln und umzusetzen. Dazu werden dem Studierenden Grundlagen der IT-Sicherheit nahe gebracht, aktuelle Sicherheitsstandards erläutert, technische und nicht-technische beziehungsweise organisatorische Maßnahmen zur Aufrechterhaltung der Sicherheit diskutiert und die Einhaltung beziehungsweise Anwendung rechtlicher Rahmenbedingungen dargelegt. Es sei an dieser Stelle deutlich darauf hingewiesen, dass Handlungen, wie das unbefugte Verschaffen von Zugang (z.B. unter Überwindung von Zugriffssicherungen) zu Daten (§ 202a StGB [StGB2009]), die Sabotage von Datenverarbeitungen (§ 303b StGB [StGB2009]) und das Löschen, Unterdrücken, unbrauchbar machen oder Verändern von Daten (§ 303a StGB [StGB2009]) unter Strafe stehen und verfolgt werden.



Lernziele

Der erste Teil dieses Online-Studienmoduls befasst sich mit einer grundlegenden Einleitung und der Problematik der organisatorischen Sicherheit. Dabei wird auf Grundbegrifflichkeiten, Sicherheitsaspekte und -anforderungen, auf potentielle Sicherheitsrisiken, Sicherheitslücken und Angriffsmöglichkeiten eingegangen. Der Fokus wird vor allem auf Angriffstechniken wie Programmen mit Schadensfunktion, Cross-Site Scripting und SQL Injection und deren Erkennung und Abwehr liegen. Der nächste Unterabschnitt befasst sich mit Sicherheitspolicies und Modellen, wobei wir uns auf eine Einführung in das Sicherheitsmanagement, Vertraulichkeits-, Integritäts- und hybriden Modellen und dem praktischen Zugriffsschutz unter Linux konzentrieren werden. Des Weiteren wird auf unterschiedliche Sicherheitsstandards eingegangen. Der letzte Unterabschnitt des ersten Teils dieses Moduls beschäftigt sich mit einer besonderen Art des Angriffes, dem Social Engineering, dessen Besonderheiten und Methoden zur Abwehr.



Informationen zu Lerneinheit 1

Lerneinheit 1

Bearbeitungszeitraum: Modulwoche 2 - 5

Bearbeitungsdauer: 4 Wochen / 15 Stunden

Verständnisfragen

Anzahl: 8

Einsendaufgaben

Anzahl: 14

Bearbeitungszeitraum: Modulwoche 2 - 5

Bearbeitungsdauer: 4 Wochen / 12 Stunden



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
▶ 1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.1 Security versus Safety

Mit dem Begriff Sicherheit wird im deutschen Sprachraum die Abwesenheit von bzw. der Schutz vor Gefahr verbunden. Gefahren können beispielsweise nicht geplante Ereignisse oder ungewollte aber auch beabsichtigte Handlungen von Personen darstellen. Unterschieden werden können hierbei zwei Arten zur Erzeugung von Gefahren, einerseits solche, die unbeabsichtigt und zufällig entstehen. Dazu zählen natürliche oder durch Fahrlässigkeit ausgelöste Ereignisse. Auf der anderen Seite gibt es Gefahren, die beabsichtigt herbeigeführt werden, um Schaden anzurichten. Im Folgenden werden unbeabsichtigte und beabsichtigte Ursachen für Gefahren auch als Angriffe bezeichnet. Die vor Angriffen zu schützenden Ziele können in zwei Klassen eingeteilt werden, materielle und immaterielle Schutzgüter. Zu den materiellen Schutzgütern zählen zum Beispiel das eigene Leben, die IT-Technik, Gebäude oder die Natur. Daten, Informationen oder das persönliche Ansehen können den immateriellen Schutzgütern zugeordnet werden.

In der englischen Sprache werden in diesem Zusammenhang zwei verschiedene Begriffe verwendet, um Art und Ziel eines Angriffes besser unterscheiden zu können: Security und Safety. Dabei bezieht sich einerseits der Begriff Safety auf die Zuverlässigkeit eines Systems, beispielsweise bezüglich dessen Ausfallsicherheit. Auf der anderen Seite wird der Begriff Security verwendet, wenn es um den Schutz eines Systems vor beabsichtigten Angriffen geht. Zum Beispiel kann ein Sicherheitsgurt (engl. safety belt) oder ein Sicherheitsnetz (engl. safety net) dem Begriff Safety zugeordnet werden. In den Bereich Security können beispielsweise Wachpersonal (engl. security guard) oder Software zur Vermeidung und Beseitigung von Schadsoftware (engl. security suite) eingeordnet werden. Wie in Abbildung 1.1 dargestellt, können beide Begriffe allerdings nicht immer vollkommen unabhängig voneinander betrachtet werden, da sie sich teilweise auch gegenseitig bedingen können. Beim Studium von Fachliteratur sollte darauf geachtet werden, dass einige Autoren diese Unterscheidung nicht oder anders vornehmen.



Abbildung 1.1



Security vs. Safety



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
▶ 1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen

Der Bereich der IT-Sicherheit weist mehrere allgemeine Ziele auf. Unter Prävention versteht man das Implementieren von Schutzmechanismen, die weder der Benutzer selbst noch ein potentieller Angreifer umgehen kann. Diese Schutzmechanismen müssen dabei glaubhaft korrekt und auch unveränderbar umgesetzt sein. Aufgabe einer Detektion ist es, festzustellen, ob momentan ein Angriff auf ein bestehendes System durchgeführt wird bzw. bereits erfolgt ist. Wird ein solches Ereignis festgestellt, muss dieses umgehend an den Benutzer bzw. den zuständigen Systemadministrator gemeldet werden. Ein weiteres Ziel ist die Wiederherstellung bzw. die Sicherstellung der Kontinuität, welche dafür zuständig sind, das korrekte Systemverhalten wiederherzustellen. Dies kann zeitlich nach dem Angriff geschehen, der Idealfall wäre allerdings die Sicherstellung der Funktionsfähigkeit schon während eines Angriffes.

Zur Klassifizierung von Angriffen wurden die Sicherheitsaspekte (siehe z.B. auch [Ditt2000]) eingeführt, welche unterschiedliche Schutzziele beschreiben. Maßnahmen zur Erlangung beziehungsweise Erhaltung eines bestimmten Sicherheitsniveaus erfüllen eines oder mehrere dieser Sicherheitsaspekte.

Die **Integrität** (*engl. Integrity*) ist der Zustand der Unverfälschtheit von Ressourcen wie bspw. Daten, das heißt, Ressourcen können nicht unautorisiert und unbemerkt verändert werden. Um diesen Zustand sicherzustellen existieren unterschiedliche Ansätze. Ein bekanntes Verfahren ist die Verwendung von so genannten Checksummen bei der Übertragung von Daten. Dabei wird über die gesendeten Daten ein eindeutiger Wert berechnet (bspw. mittels Hash-Funktion, siehe auch Abschnitt 5.2). Stimmen die Checksummen vor und nach der Übertragung der Daten nicht überein, so wurde der Inhalt der Daten verändert und deren Integrität verletzt. Ursachen hierfür können Übertragungsfehler oder aber auch beabsichtigte Angriffe sein.

Die **Authentizität** (*engl. Authenticity*) beschreibt die Echtheit von Ressourcen und beinhaltet einerseits die Originalität bezüglich des Erzeugers wie zum Beispiel dem Absender einer Nachricht. Auf der anderen Seite beschreibt die Datenauthentizität die Echtheit von Daten wie zum Beispiel, dass diese von einer bestimmten Kamera aufgenommen oder von einem bestimmten Speichersystem verwaltet werden. Zur Sicherstellung der Authentizität von Nachrichten wird beispielsweise die digitale Signatur (siehe auch Abschnitt 5.2) verwendet. Vereinfacht kann sich das folgende Szenario vorgestellt werden: Mittels eines privaten Schlüssels (eindeutig einer Person zuordenbar) wird der Hash-Wert einer Nachricht verschlüsselt. Mithilfe des öffentlichen Schlüssels derselben Person kann der Hash-Wert entschlüsselt und anschließend mit dem Hash-Wert der empfangenen Nachricht verglichen werden. Sind beide Hash-Werte identisch, stammt die Nachricht vom Inhaber des privaten Schlüssels. Im anderen Fall wurde die Authentizität der Nachricht verletzt. Der Begriff der Authentizität wird auch mit dem Nachweis der Identität (Identifikation) von Subjekten verbunden.

Die **Verfügbarkeit** (*engl. Availability*) ist der Zustand der Erreichbarkeit und Nutzbarkeit von bestimmten Ressourcen wie Daten, Diensten oder Personen in einem definierten Erreichbarkeitsintervall oder Verfügbarkeitsrahmen. Wird zum Beispiel ein Internet-Server (der 24 Stunden täglich zur Verfügung stehen sollte) durch einen Angreifer mit unzähligen gleichzeitigen Anfragen so sehr beschäftigt, dass dieser seinen Aufgaben nicht mehr nachkommen kann (Denial of Service Angriff, DoS), so ist die Verfügbarkeit dieses Servers nicht mehr gegeben.

Unter **Verbindlichkeit** (auch Nachweisbarkeit oder Nicht-Abstreitbarkeit, *engl. Accountability, Non-Repudiation*) versteht man die Beweisbarkeit, dass ein bestimmtes Ereignis oder eine bestimmte Aktion stattgefunden hat. Dies ist zum Beispiel bei Internet-Transaktionen wie Bestell- oder Zahlvorgängen notwendig.

Die **Vertraulichkeit** (*engl. Confidentiality*) beschreibt die Geheimhaltung von Informationen gegenüber Unberechtigten. Ein Beispiel vertraulicher Kommunikation stellt die Verschlüsselung

einer Information durch den Absender dar. Verfügt der Empfänger über den richtigen Schlüssel, ist also berechtigt, die Information einzusehen, so ist er in der Lage, diese zu entschlüsseln und zu nutzen.

Die **Privatsphäre** (*engl. Privacy*) umfasst den Umgang mit personenbezogenen und personenbeziehbaren Daten, so dass die nur für die vorgesehenen Zwecke und von autorisierten Personen genutzt werden können. Dazu zählt beispielsweise die vertrauliche, authentische und integritätsgesicherte Nutzung von persönlichen Informationen von Personen.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
▶ 1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacks
1.3.1 Programme mit Schadensfunktion
1.3.2 Cross-Site Scripting
1.3.3 SQL Injection
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacks

Die Eigenschaft eines Systems, die einen Missbrauch ermöglicht wird als **Schwachstelle** (*engl. Vulnerability*) bezeichnet. Eine solche Schwachstelle kann beispielsweise eine Sicherheitslücke in einer Software sein, die es einem Außenstehenden ermöglicht, Schaden zu verursachen. Als **Bedrohung** (*engl. Threat*) wird jegliches mögliche Vorkommen mit ungewünschten Effekten auf die **Werte** (*engl. Assets*) bzw. **Ressourcen** eines IT-Systems angesehen. Dabei spielt es keine Rolle, ob eine Bedrohung beabsichtigt oder unbeabsichtigt hervorgerufen wird. Ein **Risiko** kann aus einer Schwachstelle in Kombination mit einer passenden Bedrohung entstehen ($\text{Risiko} = \text{Bedrohung} * \text{Schwachstelle}$). Abbildung 1.2 zeigt schematisch wie eine Schwachstelle durch eine Bedrohung ausgenutzt wird, um Assets bzw. Ressourcen eines IT-Systems zu beeinflussen.



Abbildung 1.2



Schwachstelle,
Bedrohung und
Risiko

Die Ausnutzung einer Schwachstelle durch eine Person wird auch als **Angriff** (*engl. Attack*) bezeichnet und diese Person als **Angreifer** (*engl. Attacker*). Es existieren verschiedene Möglichkeiten, die Kommunikation zwischen zwei Partnern (Sender und Empfänger) anzugreifen. In Abbildung 1.3 sind die fünf Basisangriffe bei der Kommunikation zwischen zwei Partnern dargestellt. Dabei wird unterschieden zwischen aktiven und passiven Angriffen. Ein passiver Angreifer ist lediglich am Belauschen (Lesen) der Kommunikation interessiert, in den Datenfluss zwischen dem Sender und Empfänger greift er nicht ein. Ein aktiver Angreifer nimmt Manipulationen an der Kommunikation zwischen Sender und Empfänger vor. So kann er beispielsweise den Datenfluss unterbrechen, Daten abfangen, ändern und modifiziert an den Empfänger weiterleiten oder Daten stehlen.



Abbildung 1.3



5 Basisangriffe auf
eine Kommunikation

Abbildung 1.4 führt gebräuchliche Bezeichnungen für Sender und Empfänger, Angreifer mit verschiedenen Zielen und Instanzen zur Regelung und Überwachung von

Kommunikationsvorgängen ein. In der Abbildung werden nur die Bezeichner eingeführt, die in diesem Modul verwendet werden, weitere sind in der Literatur zu finden (siehe z.B. [Bish2003]).



Abbildung 1.4



Gebräuchliche
Bezeichner zur
Beschreibung von
Kommunikations-
und
Angriffsbeziehungen

Bei der Verwendung von IT-Systemen besteht immer die Gefahr der Infizierung durch Programme mit Schadensfunktion, die als beabsichtigter Angriff angesehen werden. Solche und andere Angriffe werden durchgeführt, um einen oder mehrere Sicherheitsaspekte mit unterschiedlichen Zielen von Seiten des Angreifers zu verletzen.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
▶ 1.3.1 Programme mit Schadensfunktion
1.3.2 Cross-Site Scripting
1.3.3 SQL Injection
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.3.1 Programme mit Schadensfunktion

Eine weit verbreitete Form des Angriffes auf IT-Systeme ist die Verbreitung von Programmen mit Schadfunktion (*engl. malware, malicious code*). Diese Programme können dabei entsprechend der Art ihrer Verbreitung und des angerichteten Schadens in verschiedene Klassen eingeordnet werden.

Die Schadensfunktion von **Computer-Viren** umfasst dabei vor allem das Verfälschen oder Löschen von Daten und Programmen. Sie können nicht kontrollierbare Veränderungen an der Hardware, der Software und dem Betriebssystem vornehmen, die nicht selten bis zum kompletten Funktionsausfall des IT-Systems führen kann. Viele Computer-Viren sind dabei in der Lage, sich selbst zu reproduzieren, sich in andere ausführbare Programme zu integrieren und sich damit unkontrolliert zu verbreiten. Computer-Viren werden aufgrund der Art der Verbreitung bzw. der Infektion klassifiziert. Im Folgenden werden einige Arten von Viren beschrieben, die weit verbreitet sind.

Boot-Viren infizieren den Master Boot Record (MBR) einer Festplatte bzw. den Bootsektor von Festplattenpartitionen und Disketten. MBR als auch Bootsektor enthalten die Software, die direkt nach der Initialisierung des Systems durch BIOS bzw. Firmware gestartet wird (die so genannten Boot-Loader). Das hat zur Folge, dass der Virus noch vor dem Betriebssystem geladen wird bzw. dessen Start verhindert. Damit kann die Schadfunktion des Virus ausgeführt werden, noch bevor Anti-Viren-Programme gestartet werden können.

File-Viren stellen die am weitesten verbreitete Form der Viren dar. Sie infizieren ausführbare Dateien oder Programmbibliotheken indem sie sich an diese Dateien anhängen und deren Programmcode so verändern, dass der Virus beim Start oder das Programm fehlerhaft ausgeführt wird (überschreibende Viren).

Makro-Viren benötigen Anwendungen, die Programmierfunktionen in Form von Makros unterstützen. Ein Makro ist dabei ein frei definierbares Programm, das in ein Dokument eingebettet werden kann, um immer wiederkehrende Befehlsabläufe zu automatisieren. Die Funktionalität von Makros reicht von der einfachen Veränderung von Kommandos der Symbolleiste bis hin zur Ausführung jedes beliebigen Programms, dessen Name und Position bekannt sind.

Weitere Klassen von Viren stellen beispielsweise Java-, Script- oder Stego-Viren dar. Einen guten Schutz vor Viren bieten separate, vorgeschaltete Virens Scanner und deren Einbindung in eine Firewall. Ein Problem stellen verschlüsselte Medien (z.B. verschlüsselte Dateisysteme, siehe Abschnitt 5.2.2) dar, da deren Inhalte nicht von herkömmlichen Virens Scannern untersucht werden können und damit die Feststellung einer potentiellen Infektion nicht möglich ist.

Ein **Wurm** ist ein Programm, welches im Gegensatz zu einem Virus versucht, sich selbst aktiv über vorhandene Netzwerke auf weitere IT-Systeme zu verbreiten. Aktiviert wird es in den meisten Fällen entweder durch den manuellen Start durch den Nutzer oder automatische Startfunktionen innerhalb eines Betriebssystems oder Software (z.B. E-Mail-Client). Ein E-Mail-Client kann beispielsweise so konfiguriert sein, dass Dateianhänge bekannter Anwendungen automatisiert gestartet werden. Dies stellt vor allem bei Programmdateien (z.B. *.exe) ein Problem dar, da damit die Schadfunktion eines enthaltenen Virus, Worms oder ähnlichem vom Anwender unbemerkt gestartet werden kann. Ein aktivierter Wurm versucht, sich selbständig über das Netzwerk auf andere Rechner zu verbreiten. Dies passiert häufig über E-Mail-Programme, indem ein Wurm die Adress- und Kontaktlisten des befallenen Rechners durchsucht, E-Mails erstellt und Kopien von sich selbst an möglichst viele weitere Personen aus diesen Listen versendet.

Das **Trojanische Pferd** ist ein Programm mit Schadensfunktion, welches sich als nützliche Anwendung tarnt, aber im Hintergrund zusätzliche unerwünschte Funktionen ausführt. Abbildung 1.5 zeigt ein universelles Trojanisches Pferd (nach [Pfit2009]), welches über die Möglichkeit verfügen kann, Anweisungen des Angreifers (z.B. über eine bestehende Internet-Verbindung) entgegenzunehmen und auszuführen. Die Schadensfunktionen eines universellen Trojanischen Pferdes können vielseitig sein. Eine kann das Sammeln von Informationen über

die betroffene Person bzw. deren IT System sein. Diese Informationen werden dann ebenfalls über eine bestehende Internet-Verbindung an den Angreifer weitergegeben. Weitere mögliche Schadensfunktionen beinhalten das Modifizieren von Informationen auf dem Wirtsrechner oder dessen Beeinträchtigung der Funktionalität durch nicht-terminierendes Ausführen von Programmcode (DoS-Angriff).



Abbildung 1.5



universelles
Trojanisches Pferd

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.3.1 Programme mit Schadensfunktion
▶ 1.3.2 Cross-Site Scripting
1.3.3 SQL Injection
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.3.2 Cross-Site Scripting

Die Idee hinter einem Angriff durch Cross-Site Scripting (Abk. XSS) ist es, nicht vertrauenswürdige Informationen in einen Kontext zu überführen, in dem sie als vertrauenswürdige angesehen werden. Ist dies, beispielsweise durch fehlerhafte Programmierung oder Konfiguration eines Web-Servers, möglich, so kann ein Angriff aus diesem vertrauenswürdigen Umfeld heraus durchgeführt werden. Voraussetzungen für einen XSS-Angriff sind eine vertrauenswürdige Web-Applikation, die dynamische Seiten erzeugt und ein Browser, der die Ausführung von Skripten ermöglicht. Web-Applikationen zur Erzeugung von dynamischen Webseiten bieten häufig die Möglichkeit, in der URL Parameter anzugeben, die bei der Erstellung der Seite berücksichtigt bzw. in diese integriert werden. Wird nun an dieser Stelle ein Script übergeben, welches Schadfunktionen enthält, und es wird nicht überprüft, ob der übergebene Parameter im gegebenen Kontext gültig und plausibel ist, wird das Script in die erzeugte Webseite eingebettet. Die so manipulierte Webseite wird dann an den Browser eines oder mehrerer Nutzer weitergeleitet. Erlauben die Einstellungen dieses Browsers die Ausführung des Scripts, wird es gestartet und die enthaltenen (ggf. schadhaften) Befehle ausgeführt.



Beispiel 1.1

Cross-Site Scripting

Handelt es sich beispielsweise, wie in Abbildung 1.6 dargestellt, bei der Script-Sprache um JavaScript und das Script konnte erfolgreich in die Seite eines Online Shops integriert werden, ist das Lesen, Manipulieren oder Löschen von Cookies des Shops möglich. In der Regel ist das Lesen und Verändern von Cookies nur von dem Server aus erlaubt, von dem auch das Cookie stammt. Da der Browser aber das Script von der Seite des Online Shops lädt, darf es auf das Cookie zugreifen, um es zu lesen, zu verändern oder zu löschen.



Abbildung 1.6



Cross-SiteScripting (Beispiel 1.1)

Zur Vermeidung von XSS-Angriffen müssen die Entwickler von Webseiten dafür sorgen, dass kein Schadcode in die betreffenden Seiten eingeschleust werden kann. Dies kann zum Beispiel durch die vollständige Beschreibung und Überprüfung der zulässigen Eingaben durch reguläre Ausdrücke umgesetzt werden. Eine sinnvolle Maßnahme von Seiten des Anwenders ist die Deaktivierung von Scriptsprachen im Internet-Browser.

Das hier gezeigte Beispiel 1.1 soll die Vorgehensweise von XSS-Angriffen nur grundlegend verdeutlichen. Es gibt verschiedene Ausprägungen des Cross-Site Scripting, je nachdem in welcher Weise der schadhafte Skript-Code im Browserkontext zur Ausführung kommt, so z.B. die Varianten Non-persistent (Beispiel 1.1), persistent und DOM-based, für interessierte Leser sei hier beispielsweise auf [Bish2003] verwiesen.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.3.1 Programme mit Schadensfunktion
1.3.2 Cross-Site Scripting
▶ 1.3.3 SQL Injection
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.3.3 SQL Injection

Ein weiterer Angriff, der fehlende bzw. mangelhafte Überprüfung von Eingaben ausnutzt, verbirgt sich hinter dem Begriff SQL Injection. Bei SQL (Structured Query Language) handelt es sich um eine Datenbanksprache, die das Definieren, Abfragen und Verändern von Daten in relationalen Datenbanken ermöglicht. Beim SQL Injection werden Schwachstellen eines Web-Servers ausgenutzt, indem Schadfunktionen über eingeschleuste Datenbankabfragen ausgeführt werden. Bei Erfolg können diese dann Daten auslesen, neue fehlerhafte Daten hinzufügen oder vorhandene Daten manipulieren beziehungsweise löschen. Einen normalen Vorgang bei der Nutzung eines Web-Servers kann man sich vereinfacht wie folgt vorstellen: Über einen Link wird im Browser des Anwenders ein Webformular geöffnet, in das der Anwender Daten eingibt, welche dann nach Absenden des Formulars vom Web-Server in vorbereitete SQL-Anfragen eingesetzt werden. Diese werden dann an die Datenbank weitergeleitet und dort verarbeitet. Werden die aus dem Webformular stammenden Eingaben nicht auf ihre Plausibilität im Kontext der gewünschten Anwendung überprüft, ist es einem Angreifer möglich, durch geschicktes Einfügen von zusätzlichem SQL-Code in die Eingabefelder des Webformulars zusätzliche SQL-Anfragen an die Datenbank zu senden.

Abhängig von den verwendeten Befehlen sind verschiedene Angriffe auf eine Datenbank möglich:

- Lesen von Informationen: z.B. `SELECT`
- Manipulation beziehungsweise Löschen von Informationen: z.B. `DELETE`, `INSERT`, `UPDATE`
- Zerstören von Datenbanken bzw. Tabellen: z.B. `DROP TABLE`, `DROP DATABASE`
- Ausführen von Systembefehlen auf dem Hostsystem: z.B. `System.exec("format c: ")`

Wie beim Cross-Site Scripting ist die Integration einer Eingabeüberprüfung die wichtigste und effektivste Maßnahme zur Vermeidung von SQL Injection Angriffen. Diese sollte wiederum mit einer vollständigen Beschreibung und Überprüfung der zulässigen Eingaben durch reguläre Ausdrücke realisiert werden.



Beispiel 1.2

SQL Injection

Man stelle sich folgendes Szenario vor: In einem Webformular wird die Eingabe eines Altersbereiches verlangt, um die Dauer der Betriebszugehörigkeit der Mitarbeiter einer Firma zu erhalten, die diesem Alter entsprechen. Ein Anwender nimmt folgende Eingaben vor (siehe Abbildung 1.7 a):

Alter

min: 21

max: 65 .

Daraus würde die folgende SQL-Anfrage erstellt und an die Datenbank weitergeleitet werden, um das entsprechende Ergebnis an den Anfragenden zurückzugeben (siehe Abbildung 1.7 b):

```
SELECT name, (akt.Jahr-Einstellungsjahr), alter FROM
personal WHERE alter>=21 AND alter<=65 .
```

Ein Angreifer könnte nun die Eingabe der Altersdaten so manipulieren, dass er die Möglichkeit erhält, weitere Daten auszulesen (siehe Abbildung 1.7 c):

Alter

min: 21

max: 65; SELECT name,adresse,gehalt FROM personal

Die von Web-Server zusammengesetzte SQL-Anfrage wird dann so aussehen:

```
SELECT name,(heute-einstellungsdatum) FROM personal WHERE alter>=21
AND alter<=65;
```

```
SELECT name,adresse,gehalt FROM personal .
```

Damit erhält der Angreifer eine Liste der in der Datenbank eingetragenen Mitarbeiter mit deren Namen, Adressen und dem jeweiligen Gehalt (siehe Abbildung 1.7 d).



Abbildung 1.3.6: SQL Injection (Beispiel 1.2)

a) b) c) d)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
▶ 1.4 Sicherheitspolicies und Modelle
1.4.1 Einführung in das Sicherheitsmanagement
1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula
1.4.3 Integritätsmodelle: Biba, Clark Wilson
1.4.4 Hybride Modelle
1.4.5 Praktischer Zugriffsschutz in UNIX
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.4 Sicherheitspolicies und Modelle

Das Ziel von Sicherheitspolicies und –modellen ist es, den Zugriff auf Ressourcen wie zum Beispiel Daten zu reglementieren und gegebenenfalls einzuschränken. Diese Regeln legen fest, welche **Subjekte** s (Nutzer, Gruppen oder Prozesse) auf **Objekte** o (Prozesse, Dateien, Nutzer, ...) mit welchen **Rechten** r (lesen, schreiben, ausführen, ...) zugreifen dürfen. Im Folgenden wird eine Einführung in das Sicherheitsmanagement gegeben und ausgewählte Modelle und Policies vorgestellt.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
▶ 1.4.1 Einführung in das Sicherheitsmanagement
1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula
1.4.3 Integritätsmodelle: Biba, Clark Wilson
1.4.4 Hybride Modelle
1.4.5 Praktischer Zugriffsschutz in UNIX
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.4.1 Einführung in das Sicherheitsmanagement

Wie in Abbildung 1.8 zu sehen ist, gibt es für IT-Systeme verschiedene Strategien, den Zugriff auf Ressourcen zu beschränken (*engl. Access Control*). Drei Hauptstrategien sind hier Discretionary Access Control, Role-based Access Control und Mandatory Access Control. In diesem Abschnitt wird kurz auf Policies und Modelle der genannten Mechanismen zur Zugriffskontrolle eingegangen. Einige Beispiele werden in den folgenden Abschnitten detaillierter beschrieben.



Abbildung 1.8



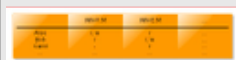
Sicherheitsmodelle

Bei den Verfahren der **Discretionary Access Control** (DAC, *deutsch Benutzerbestimmbare Zugriffskontrolle*) werden Entscheidungen über den Zugriff auf Ressourcen allein über die Identität des Subjektes *s* getroffen.

Bei der Verwendung einer **Access Control Matrix** (ACM, *deutsch Zugriffskontrollmatrix*) wird für jede Kombination von Subjekten *s* und Objekten *o* eine Menge Rechte *r* festgelegt (meist manuell), welche *s* auf *o* hat. Die Menge aller Kombinationen kann in der ACM mit einer Dimension von Anzahl(*s*) * Anzahl(*o*) dargestellt werden. Abbildung 1.9 zeigt eine ACM bei der die Spalten die Zugriffsrechte auf Objekte (hier Dateien) und die Zeilen die Zugriffsrechte der Subjekte (hier Nutzer) angeben. Die Rechte eines Nutzers (hier *r*: read (deutsch lesen), *w*: write (schreiben)) bezüglich einer Datei sind im Schnittpunkt vom jeweiligen Nutzer und der Datei zu finden. Vorteile der Nutzung von ACMs sind die einfache und intuitive Verwendung und die Möglichkeit einer effizienten Suche innerhalb der Matrix. Zu den Nachteilen zählen die Größe der Matrix, gegebenenfalls leere Zellen und der große Aufwand beim Hinzufügen beziehungsweise Entfernen neuer Subjekte oder Objekte.



Abbildung 1.9



Access Control Matrix

Bei einer **Access Control List** (ACL, *deutsch Zugriffskontrollliste*) werden für jedes Objekt o alle Subjekte s gespeichert, die Rechte für den Zugriff besitzen (siehe Abbildung 1.10, Subjekte sind Nutzer und Objekte sind Dateien). Diese Zuordnung kann direkt mit dem Objekt gespeichert werden. Im Gegensatz zur ACM werden hier nur notwendige Einträge gespeichert, dadurch gibt es keine leeren Zellen. Nachteilig ist bei der Verwendung von ACLs die langsamere Suche im Vergleich zu ACMs, wodurch sich beispielsweise die Zusammenstellung aller Rechte eines Subjektes zeitlich aufwändig gestaltet.



Abbildung 1.10



Access Control List

Eine **Capability List** (CAP) enthält für jedes Subjekt s die Objekte o auf die mittels der zugewiesenen Rechte r Zugriff gewährt wird (siehe Abbildung 1.11, Subjekte sind Nutzer und Objekte sind Dateien). Wie bei den ACLs entstehen auch hier keine leeren Zellen. Die Zuordnung der Objekte o und Rechte r zu den Objekten o kann direkt mit den Objekten gespeichert werden, beispielsweise im Nutzeraccount eines Dateisystems. Dies macht eine schnelle Zusammenstellung der Objekte möglich, auf die ein Objekt Zugriff hat. Andererseits gestaltet sich die Auflistung der Objekte, die auf ein bestimmtes Subjekt zugreifen dürfen als langwierig.



Abbildung 1.11



Capability List

Bei Systemen mit **Role-based Access Control** (RBAC, *deutsch Rollenbasierte Zugriffskontrolle*) gibt es keine expliziten Rechte für einzelne Subjekte. Hier werden die Subjekte einer oder mehreren Rollen zugeordnet, die wiederum einer oder mehreren Gruppen zugeordnet werden können. Abbildung 1.12 stellt ein beispielhaftes RBAC für die Verwaltung von Rechten in einem Dateisystem dar (Subjekte sind Nutzer und Objekte sind Dateien). Im dargestellten System gibt es die drei Benutzer Alice, Bob und Carol. Bob sind beispielsweise die Rollen Benutzer und Administrator zugewiesen. Ein Benutzer darf sich an einem Rechner einloggen, da alle Benutzer auch zur Gruppe „Login an Rechner“ angehört. Weiterhin gehört ein Administrator den Gruppen „Darf alles schreiben“ und „Darf alles lesen“ an. Mit diesen Rechten darf sich Bob also an Rechnern einloggen und Dateien und Verzeichnisse lesen und schreiben. Ein großer Nachteil von RBACs liegt darin, keine individuellen Rechte für Subjekte vergeben werden können.



Abbildung 1.12



Role-based Access Control

Die dritte Strategie zur Zugriffskontrolle ist die so genannte **Mandatory Access Control**. Bei Policies und Modellen, die die Mandatory Access Control Strategie benutzen, beruhen die Zugriffsrechte nicht allein auf der Identität des Subjektes sondern auf zusätzlichen Regeln und Eigenschaften des Subjektes und des Objektes.

Die Idee des **Multi-Level Access Control** ist die Einführung einer Hierarchie von Schutzstufen. Basierend auf diesem Konzept wird der Zugriff auf ein Objekt zum einen abhängig gemacht von der Schutzstufe des Subjektes (auch bezeichnet als Freigabe oder engl. clearance) und der des Objektes (auch bezeichnet als Klassifikation oder engl. classification). In den folgenden beiden Abschnitten wird auf das Vertraulichkeitsmodell Bell-LaPadua und die Integritätsmodelle Biba und Clark Wilson eingegangen.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.4.1 Einführung in das Sicherheitsmanagement
1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula
1.4.3 Integritätsmodelle: Biba, Clark Wilson
1.4.4 Hybride Modelle
1.4.5 Praktischer Zugriffsschutz in UNIX
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula

Das Ziel des Bell-LaPadula Modells ist es, die Vertraulichkeit von Informationen zu sichern. Das wird dadurch erreicht, dass es nicht möglich ist, Informationen höherer Schutzstufen als der eigenen zu lesen beziehungsweise Informationen in Objekte mit niedriger Schutzstufe zu schreiben. Daher basiert das Bell-LaPadula Modell auf den folgenden zwei Regeln:

„No-read-up“ (oder Simple Security Property): Es ist nicht möglich, dass ein niedriger eingestuftes Subjekt s_1 Informationen eines höher eingestuften Subjektes s_2 lesen kann. Damit wird vermieden, dass unbefugte Subjekte auf geheime Objekte zugreifen können.

„No-write-down“ (oder *-Property): Es darf einem höher eingestuften Subjekt s_2 nicht möglich sein, Informationen in ein Objekt eines niedriger eingestuften Subjektes s_1 zu schreiben. Diese Regel verhindert die Weitergabe von geschützten Informationen über weniger geschützte Objekte.



Beispiel 1.3

Bell-LaPadula Modell

Abbildung 1.13 zeigt ein Beispiel mit vier Objekten, die wie folgt klassifiziert wurden: Klasse 1 (o_1), Klasse 2 (o_2), Klasse 3 (o_3) und Klasse 4 (o_4). Weiter sei ein Subjekt s_1 mit der Freigabe der Sicherheitsstufe „Klasse 3“ definiert. Der abgebildete Graph zeigt die Richtungen nach dem Bell-LaPadula-Modell an, in die das Subjekt lesen (r) bzw. schreiben (w) kann. Im angegebenen Beispiel darf s_1 die Objekte $o_1 - o_3$ lesen aber nur in die Objekte o_3 und o_4 schreiben.



Abbildung 1.13



Bell-LaPadula-Modell (Beispiel 1.3)

Eine vollständige Definition und eine formale Beschreibung zum Bell-LaPadula-Modell sind beispielsweise in [Bish2005] zu finden.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.4.1 Einführung in das Sicherheitsmanagement
1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula
1.4.3 Integritätsmodelle: Biba, Clark Wilson
1.4.4 Hybride Modelle
1.4.5 Praktischer Zugriffsschutz in UNIX
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.4.3 Integritätsmodelle: Biba, Clark Wilson

Aufgabe des Biba Modells ist die Sicherung der Integrität von Informationen, das heißt, es soll sichergestellt werden, dass die Daten nicht durch Unbefugte manipuliert werden können und den Daten damit vertraut werden kann. Um dieses Ziel zu erreichen, werden die folgenden zwei Regeln verwendet:

„No-read-down“: Jedes Subjekt darf nur innerhalb von Objekten der gleichen oder einer höheren Schutzstufe lesen. Dadurch wird erreicht, dass nur zuverlässige Informationen (da von höherer Stufe geschrieben) verwendet bzw. weitergegeben werden.

„No-write-up“: Schreiben darf ein Subjekt nur in Objekte der gleichen oder einer niedrigeren Schutzstufe. So werden nur Informationen aus einer kompetenteren Quelle an die anderen Stufen weitergegeben.



Beispiel 1.4

Biba-Modell

Gegeben sei eine Klassifizierung von vier Objekten nach dem Biba-Modell wie in Abbildung 1.14 dargestellt: o_1 (Klasse 1), o_2 (Klasse 2), o_3 (Klasse 3) und o_4 (Klasse 4). Ein Subjekt s_1 mit der Freigabe der Sicherheitsstufe „Klasse 3“ hat dann die folgenden Zugriffsrechte auf die Objekte $o_1 - o_4$: s_1 darf lesend auf o_4 zugreifen während auf die Objekte $o_1 - o_3$ lediglich der Schreibzugriff erlaubt ist. Auf diese Weise ist es unmöglich, dass eventuell unzuverlässige Informationen aus den unteren Sicherheitsstufen in eine höhere Stufe gelangt und dort verwendet bzw. verbreitet wird.



Abbildung 1.14



Biba-Modell
(Beispiel 1.4)

Das Clark-Wilson-Modell fokussiert ebenfalls den Schutz der Integrität von Informationen. Es ist ein auf Großrechnern (Mainframes) häufig eingesetztes Modell. Es beschreibt Maßnahmen, die es möglich machen den integeren Zustand eines IT-Systems zu erhalten. Das bedeutet, dass das System von einem gültigen (konsistenten) Startzustand in einen ebenfalls konsistenten Endzustand überführt wird. Übergänge zwischen konsistenten Zuständen können nur durch wenige explizit erlaubte und wohlgeformte Transaktionen erfolgen. Wohlgeformt heißt in diesem Kontext, dass die Konsistenz des Systems bei der Transaktion erhalten bleibt.



Beispiel 1.5: Clark-Willson-Modell – Bank

Für die Kontoführung von Bankkunden seien folgende Eigenschaften gegeben:

S_{in} - Summe des heute eingezahlten Geldes

S_{out} - Summe des heute abgehobenen Geldes

$G_{gestern}$ - Geld auf dem Konto am gestrigen Tag

G_{heute} - Geld auf dem Konto am heutigen Tag

Die Konsistenz kann dann wie folgt beschrieben werden:

$$G_{heute} = G_{gestern} + S_{in} - S_{out}$$

Eine vollständige Definition und eine formale Beschreibung zum Bell-LaPadula-Modell sind beispielsweise in [Bish2005] zu finden.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.4.1 Einführung in das Sicherheitsmanagement
1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula
1.4.3 Integritätsmodelle: Biba, Clark Wilson
▶ 1.4.4 Hybride Modelle
1.4.5 Praktischer Zugriffsschutz in UNIX
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.4.4 Hybride Modelle

Hybride Modelle (auch Multilateral Access Control Modelle) zur Zugriffskontrolle sind auf die Sicherung von Integrität und Vertraulichkeit ausgerichtet. Ziel von Multilateral Access Control Modellen ist es, dadurch Interessenkonflikte zu verhindern. Ein weit verbreitetes Modell ist das Chinese Wall Modell. Hier werden Interessenkonflikte dadurch verhindert, indem Ressourcen bestimmten Konfliktklassen zugeordnet werden. Gehören zwei Objekte unterschiedlichen Konfliktklassen an und will ein Subjekt, welches bereits Zugriff auf eines der beiden Objekte hatte, auf das andere zugreifen, so wird dieser Zugriff verweigert. Das bedeutet, dass die Regeln des Modells zukünftige Zugriffe von Subjekt s_1 auf ein Objekt o_1 verhindern, wenn s_1 in der Vergangenheit bereits Zugriff auf ein Objekt o_2 hatte und o_1 und o_2 derselben Konfliktklasse angehören.



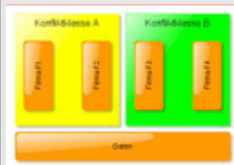
Beispiel 1.6

Chinese Wall Modell in einem Consulting Unternehmen

In Abbildung 1.15 ist ein vereinfachtes Beispiel zu den Regeln des Chinese Wall Modells dargestellt, welches sich auf ein Consulting Unternehmen bezieht. In diesem Unternehmen beraten die Mitarbeiter vier Firmen ($F_1 - F_4$) von denen F_1 und F_2 der Konfliktklasse A und F_3 und F_4 der Konfliktklasse B angehören. Einem Mitarbeiter M, der die Firma F_1 betreut, hat entsprechend den Regeln keinen Zugriff auf Daten der Firma F_2 . Der Grund ist die gemeinsame Konfliktklasse A, zum Beispiel könnten die beiden Firmen im direkten wirtschaftlichen Wettbewerb stehen, und das Wissen um zukünftige Strategien von F_2 könnte diesen zugunsten von F_1 verschieben. Zusätzlich kann M bei entsprechender Betreuung der Firmen entweder auf die Daten von F_3 **oder** F_4 zugreifen, da diese ebenfalls zu einer gemeinsamen Konfliktklasse (hier B) gehören.



Abbildung 1.15



Vereinfachte beispielhafte Darstellung des Chinese Wall Modells (Beispiel 1.6)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.4.1 Einführung in das Sicherheitsmanagement
1.4.2 Vertraulichkeitsmodelle: Bell-LaPadula
1.4.3 Integritätsmodelle: Biba, Clark Wilson
1.4.4 Hybride Modelle
▶ 1.4.5 Praktischer Zugriffsschutz in UNIX
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.4.5 Praktischer Zugriffsschutz in UNIX

Um den Zugriff auf Dateien und Verzeichnisse innerhalb auf UNIX basierender Betriebssysteme zu regeln, wird ein zehnstelliger Buchstabencode zur Rechtevergabe in Kombination mit Nutzern und Nutzergruppen verwendet. Abbildung 1.16 zeigt den Aufbau des Buchstabencodes. Dabei steht der erste Buchstabe für die Art der Ressource ('d' – Verzeichnis (engl. Directory), '-' – Datei (engl. File)). Die nächsten drei Buchstaben geben die Rechte des Besitzers der Ressource an, während die folgenden drei Buchstaben die Rechte der Gruppe, der der Besitzer zugeordnet ist und die letzten drei Buchstaben die Rechte aller übrigen Nutzer beschreiben. Die verwendeten Buchstaben haben dabei die folgende Bedeutung: 'r' – lesen (engl. read), 'w' – schreiben (engl. write), 'x' – ausführen (engl. execute), '-' – Benutzer/ Benutzergruppe darf keine der drei Aktionen ausführen.



Abbildung 1.16



Dateizugriffsrechte
unter UNIX-
Betriebssystemen



Beispiel 1.7

Rechtevergabe unter UNIX-Betriebssystemen

-rw-r--r-- administrator users cv.txt

Datei, vom Besitzer les- und schreibbar, von jedem anderen lesbar (Standard für Benutzerdateien)

-rwxr-xr-x root root kshisen

(Programm-)Datei, vor jedem les- und ausführbar, nur vom Besitzer veränderbar (Standard für Programme)

-rwsr-xr-x root root passwd

von jedem les- und ausführbar, vom Besitzer veränderbar; wird mit den Rechten des Besitzers root ausgeführt (nötig, um Einträge in Passwort-Dateien ändern zu können)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
▶ 1.5 Sicherheitsstandards
1.5.1 ISO 27001
1.5.2 ITIL
1.5.3 COBIT
1.5.4 Common Criteria
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.5 Sicherheitsstandards

Dieser Abschnitt über in der Praxis existierende Sicherheitsstandards stellt nur eine grobe Übersicht dar, da hier häufig Änderungen und Anpassungen durchgeführt werden, um sowohl dem wachsenden Sicherheitsbedürfnis gerecht zu werden als auch der fortlaufenden Anpassungsfähigkeit von Angreifern entgegenzuwirken. Es existiert noch eine Vielzahl weiterer Standards, die in den meisten Fällen branchenspezifisch sind und auf die in diesem Modul nicht eingegangen wird.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
▶ 1.5.1 ISO 27001
1.5.2 ITIL
1.5.3 COBIT
1.5.4 Common Criteria
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.5.1 ISO 27001

ISO 27001 ist eine internationale Norm, die Anforderungen für die Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (engl. Information Security Management System). Es werden Anforderungen spezifiziert, um geeignete Sicherheitsmechanismen umzusetzen, die an die tatsächlichen Gegebenheiten und Risiken der jeweiligen Organisation angepasst werden können. Es werden dabei alle möglichen Arten von Organisationen (bspw. staatliche oder Non-Profit-Organisationen) berücksichtigt.

Die ISO 27001 Norm ermöglicht es, „Qualitätssiegel“ für die Sicherheit von IT-System in Organisationen zu erstellen. Ein Beispiel stellt der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) dar, welches in Abschnitt 5.1 näher besprochen wird. Weiterführende Informationen zur ISO 27001 Norm sind im Internet zu finden (z.B. [ISO27001a], [ISO27001b], [ITGr2009]).

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.5.1 ISO 27001
▶ 1.5.2 ITIL
1.5.3 COBIT
1.5.4 Common Criteria
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.5.2 ITIL

Die IT Infrastructure Library (ITIL) ist eine technologie- und anbieterunabhängige Verfahrensbibliothek zur Gestaltung, Implementierung und zum Management wesentlicher Steuerungsprozesse in der Informationstechnik. Sie stellt einen mittlerweile weltweit akzeptierten Defacto-Standard dar und kann als Bibliothek von Best Practices angesehen werden. Das heißt, die ITIL trägt Erfahrungen aus der Praxis zusammen und vermittelt das zur Anwendung notwendige Wissen und stellt damit eine entscheidende Grundlage für zuverlässige, sichere und wirtschaftliche IT Dienstleistungen dar. Das vermittelte Wissen ist unabhängig von der eingesetzten Hardware, Software und eventuellen Dienstleistern. Die ITIL umfasst ca. 40 englischsprachigen Publikationen und enthält Hinweise zu Verwaltung, Beschreibung und Management von komplexen IT-Infrastrukturen und als Bestandteil davon auch IT-Sicherheitskomponenten. Sie kann mit anderen Sicherheitsstandards kombiniert werden, bietet aber keine Zertifizierung der Sicherheit der nach den gegebenen Vorgehensbeschreibungen gesicherten IT-Komponenten.

In der Literatur und im Internet findet der interessierte Leser weiterführende Informationen zur ITIL ([ITIL2009], [ITIL2005]).

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.5.1 ISO 27001
1.5.2 ITIL
▶ 1.5.3 COBIT
1.5.4 Common Criteria
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.5.3 COBIT

Control Objectives for Information and Related Technology (CobiT) stellt ein international anerkanntes Framework dar, welches die Aufgaben von IT-Systemen in Prozesse und Control Objectives aufteilt. Das Framework konzentriert sich dabei darauf, welche Anforderungen zu erfüllen sind und geht nicht darauf ein, wie diese zu erfüllen sind.

Durch die Umsetzung von geeigneten internen Kontroll-/Steuerungssystemen bzw. Frameworks durch das Management basierend auf CobiT wird dem IT-System ermöglicht, die Geschäftsanforderungen der jeweiligen Organisation zu erfüllen. CobiT ist dabei hilfreich durch:

- eine Verbindung zu den Geschäftsanforderungen,
- die Einbindung von IT bezogenen Aktivitäten in ein allgemein akzeptiertes Prozessmodell,
- die Identifikation von wesentlichen, zu steuernden IT-Ressourcen und
- die Definition von zu berücksichtigenden Control Objectives.

Weitere Informationen zu CobiT findet der interessierte Leser in der Literatur beziehungsweise im Internet (z.B. in [Cobi2009]).

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.5.1 ISO 27001
1.5.2 ITIL
1.5.3 COBIT
▶ 1.5.4 Common Criteria
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.5.4 Common Criteria

Common Criteria for Information Technology Security Evaluation (kurz Common Criteria oder auch nur CC) ist ein internationaler Standard, welcher Kriterien zur Bewertung und Zertifizierung der Sicherheit von IT-Systemen vorgibt. Ein Hauptziel von CC ist die Vermeidung von Mehrfachzertifizierungen von IT-Systemen bzw. IT Komponenten in unterschiedlichen Ländern.

Die dabei zugrunde liegende Bewertung wird in die Bewertung von Funktionalität (Funktionsumfang) und Bewertung der Vertrauenswürdigkeit des zu zertifizierenden Systems bzw. Komponente unterteilt.

Die CC umfassen drei Teile:

Teil 1: Einführung und allgemeines Modell (engl. Introduction and General Model)

Teil 2: Funktionale Sicherheitsanforderungen (engl. Functional Requirements)

Teil 3: Anforderungen an die Vertrauenswürdigkeit (engl. Assurance Requirements)

Die Evaluierung von IT-Systemen bzw. IT-Komponenten gemäß der CC, welche von eigens akkreditierten Prüfstellen durchgeführt werden muss, ist aufwändig und nimmt daher viel Zeit in Anspruch. Eine Zertifizierung erfolgt durch das BSI (im Ausland durch entsprechende Partnerorganisationen) und muss in regelmäßigen Abständen erneuert werden. Vertiefende Informationen zu den CC sind auch im Internet auf der offiziellen Homepage zu finden ([Comm2009]).

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
▶ 1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

1.6 Social Engineering

Ziel des Social Engineering ist das Ausspähen bzw. „in Erfahrung bringen“ von vertraulichen Daten. Üblicherweise handelt es sich dabei um sicherheitsrelevante Informationen wie beispielsweise Zugangsinformationen (Nutzername und Passwort), für Online-Banking notwendige persönliche Identifikations- (PIN) und Transaktionsnummern (TAN) oder (Firmen-) Geheimnisse. Durchgeführt wird diese Art von Angriffen auf nicht-technischem Wege, wobei aber auch technische Hilfsmittel eingesetzt werden können. Ziel ist das Umgehen von (technischen) Sicherheitsvorkehrungen auf sozialer Ebene. Grundsätzlich wird eine Kommunikation zwischen dem Angreifer und dem Opfer hergestellt, deren Ziel die beabsichtigte oder unbeabsichtigte Herausgabe der gewünschten Informationen von Seiten des Opfers ist. Unterschieden wird dabei zwischen Human-based und Computer-based Social Engineering. Beim **Human-based Social Engineering** tritt der Angreifer direkt mit dem Opfer in Verbindung. Dies kann über direkten Kontakt oder auch über das Telefon passieren. Eine Kontaktaufnahme über die verschiedenen Möglichkeiten des Computers wird als **Computer-based Social Engineering** bezeichnet. Typische Beispiele sind hier das Versenden von E-Mails oder das Kontaktieren in Chats.

Beim Social Engineering werden unterschiedliche Schwachstellen einer Person durch den Angreifer ausgenutzt. Dabei kann es sich beispielsweise um (übertriebene) Hilfsbereitschaft, Gutgläubigkeit/Naivität, Gefühlen wie Angst (z.B. vor Unannehmlichkeiten), Unwissenheit (z.B. bzgl. einer Problematik oder der Sensibilität von Informationen), Unachtsamkeit oder auch Vergesslichkeit handeln. Diese, nicht zwangsläufig negativen, Eigenschaften einer Person helfen dem Angreifer, Ansatzpunkte zu finden und auszunutzen, um an die gewünschten Ressourcen zu gelangen. Die folgenden zwei Beispiele sollen unterschiedliche Vorgehensweisen und Zielsetzungen verdeutlichen.



Beispiel 1.8

Telefonanruf eines vermeintlichen IT-Administrators

Angreifer: Guten Tag, mein Name ist Hans Meyer, und ich Administrator des IT-Systems in unserer Firma. Spreche ich mit Frau Stefanie Müller?

Opfer: Ja.

Angreifer: Sie arbeiten im Archiv und ihr Büro befindet sich in Raum 016?

Opfer: Ja.

Angreifer: Ihre Telefonnummer ist die 20123?

Opfer: Ja.

Angreifer: Laut meiner Liste ist ihr Benutzername für unser IT-System SMueller und ihr Passwort ist pw1109.

Opfer: Nein, mein Passwort ist waldi27.

Der Angreifer versucht durch sein umfangreiches Wissen über das Opfer diesem glaubwürdig zu vermitteln, dass er vertrauenswürdig ist. Dieses Wissen kann er beispielsweise über die Webseite der Firma oder Social Engineering bei anderen Mitarbeitern erlangt haben. Dabei bringt er das Opfer in eine Situation, in der das Opfer versucht, möglichst schnell und vor allem richtig auf die Fragen des Anrufers zu antworten. Dabei rutscht dem Opfer das aktuelle Passwort heraus, wodurch dem Angreifer die Möglichkeit gegeben wird, in das IT-System zu gelangen, um dort Schaden anzurichten. Bei diesem Beispiel handelt es sich um Human-based Social Engineering.



Beispiel 1.9

Phishing Mail

„Werter Kunde, um die Nutzbarkeit und die Sicherheit unseres Onlinebanking-Portals für Sie weiter zu verbessern, haben wir weit reichende Änderungen an unserem Onlinebanking-System vorgenommen. Damit auch Sie von den neuen Merkmalen des Systems profitieren können, muss dieses von Ihnen aktiviert werden. Klicken Sie dazu bitte auf den Link <https://onlinebanking.ihrebank.be> und melden sie sich mit ihrem Benutzernamen, Passwort und der Eingabe von fünf Transaktionsnummern (TAN) an.“

Mittels dieser Mail versucht ein Angreifer an die Zugangsdaten von Bankkunden zu gelangen, um diese dann zu seinen Gunsten einzusetzen. Dazu erstellt er eine Webseite, die unter dem angegebenen Link zu erreichen ist. Diese nimmt dann sensible Daten des Bankkunden entgegen und speichert sie. Der Angreifer verfügt damit bei einem erfolgreichen Angriff über den Benutzernamen, das Passwort und fünf Transaktionsnummern, mit denen er beispielsweise fünf Überweisungen auf beliebige Konten durchführen kann. Vertrauen wird dadurch aufgebaut, dass die Mail und die Webseite dem gewohnten Layout der tatsächlichen Seite der Bank nachempfunden sind und der Kunde auf vermeintliche Verbesserungen bzgl. der Sicherheit des Onlinebankings seiner Bank hingewiesen wird. Bei dieser Art des Angriffes handelt es sich um Computer-based Social Engineering.

Ein Angriffsbaum (oder Bedrohungsbaum, engl. Attack Tree) dient der Erfassung und Analyse möglicher Bedrohungen eines IT-Systems. Das Angriffsziel (die Bedrohung) wird als Wurzel des Baumes dargestellt. Die danach folgenden Zweige stellen Zwischenziele des Angreifers dar, während die einzelnen Blätter jeweils einem Angriffsschritt entsprechen. Mehrere Zwischenziele können dabei durch UND (müssen gleichzeitig erfüllt sein) oder durch ODER (mindestens eins muss erfüllt sein) verbunden sein.

Abbildung 1.17 zeigt einen Angriffsbaum mit dem Ziel, das Passwort einer bestimmten Person zu erlangen. Dazu sind verschiedene Herangehensweisen möglich, von denen nur eine Auswahl im abgebildeten Baum zu sehen ist. Die Zwischenziele sind hier ausschließlich über ODER verbunden. Das Passwort der Person P kann entweder mit deren Mitwirken (bewusst oder unbewusst) oder ohne deren Mitwirken erlangt werden. Nehmen wir beispielsweise an, dass der Angreifer sich für die Variante ohne Mitwirken von P entscheidet. Hier gibt es dann verschiedene Möglichkeiten, das Passwort herauszufinden. Beim Lexikon-Angriff wird sukzessive versucht, ob das Passwort einem bekannten bzw. existierenden Wort entspricht. Der Brute Force-Angriff versucht, jede mögliche Kombination von Zeichen als Passwort zu verwenden, um das tatsächliche zu ermitteln. Beide Varianten können zeitaufwändig sein. Daher bietet das Erraten des Passworts eine Erfolg versprechende Alternative. Um dies zu vereinfachen, kann der Angreifer versuchen, zusätzliche Informationen über P zu bekommen. Dafür kann er beispielsweise Personen um Umkreis von P befragen, um die Namen bzw. Geburtsdaten von P und dessen Angehörigen, Freunden oder Haustieren zu erfahren. Andere Wege, um an persönliche Informationen zu gelangen, sind, die Post oder gar den Müll von P zu durchwühlen. Die linke Seite des Angriffsbaumes kann entsprechend der eben diskutierten rechten gelesen werden.



Abbildung 1.17



Angriffsbaum zur
Erlangung des
Passworts einer
Person P

Maßnahmen zur Verhinderung von Social Engineering sind zum Beispiel das Aufbauen eines Gefahrenbewusstseins von Mitarbeitern in Schulungen oder die Reduzierung von frei verfügbaren Informationen auf ein notwendiges Minimum. Ein frei zugängliches Online-Verzeichnis aller Mitarbeiter, welchen Informationen wie E-Mail-Adresse, Durchwahl und Büronummer zu entnehmen sind, birgt die Gefahr, dass zu viele Informationen preisgegeben werden, die ein Angreifer für Social Engineering ausnutzen kann (siehe auch Beispiel – Telefonanruf eines vermeintlichen IT-Administrators).

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
► Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Verständnisfragen



Verständnisfragen 1

1. Welchem der beiden Begriffe Security und Safety kann der Sicherheitsgurt in einem Flugzeug zugeordnet werden?

Security

Safety

2. Ist eine Software zur Abwehr von Angriffen aus dem Internet dem Begriff Security oder eher Safety zuzuordnen?

Security

Safety

3. Welcher Sicherheitsaspekt wird bei einem Angriff auf einen Server durch Denial of Service (DoS) verletzt?

Integrität

Vertraulichkeit

Verfügbarkeit

4. Welcher Sicherheitsaspekt wird verletzt, wenn eine Nachricht von Alice an Bob während der Übertragung von Eve gelesen wird?

Authentizität

Privatsphäre

Integrität

5. Ist es richtig, dass ein Angriff aus Fahrlässigkeit auf die Gesundheit eines Menschen dem Begriff Security zugeordnet werden kann?

richtig

falsch

6. Welches Sicherheitsmodell sollte eingesetzt werden, wenn verhindert werden soll, dass militärische Befehle, die einer Sicherheitseinstufung von 3 zugeordnet wurden, nicht von Personen einer niederen Stufe gelesen werden dürfen?

Bell-

LaPadula

7. Bitte wählen Sie die Antwort, die den angegebenen Rechten eines Objektes in einem UNIX-Dateisystem entspricht!

d rwx rw- r--

Der Besitzer kann die Datei lesen, in die Datei schreiben und sie ausführen. Die Gruppenmitglieder können nur lesen und schreiben. Alle anderen können die Datei nur lesen.

Der Besitzer kann in das Verzeichnis wechseln, den Inhalt auflisten und Dateien oder Verzeichnisse darin anlegen. Die Gruppenmitglieder können nur auflisten und anlegen. Alle anderen können nur auflisten.

8. Welche der angegebenen Maßnahmen können die Gefahr des Social Engineering sinnvoll verringern?

Mitarbeiterschulung

Unterbinden sämtlicher Kommunikation

Verhindern von direkten Kontakten der Mitarbeiter mit externen Personen

Schaffung von Gefahrenbewusstsein

Bewusstes Hinterfragen von Tätigkeiten

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Einsendeaufgaben

Aufgabe 1.1 – Sicherheitsaspekte

Nennen Sie für jeden der Ihnen bekannten fünf Sicherheitsaspekte einen möglichen Angriff, der diesen Aspekt verletzt!

Aufgabe 1.2 – Anwendung der Sicherheitsaspekte

Mit welchem der Begriffe „Vertraulichkeit“, „Integrität“ oder „Authentizität“ assoziieren Sie die folgenden Vorgänge und Objekte?

Fingerabdruck

„Knopf im Ohr“ (Steiff-Teddies)

Siegel auf Dokumenten

Durch die Sahne kunstvoll verzierter Schokoladenpudding

Keuschheitsgürtel

TÜV-Plakette

Aktenkoffer mit Zahlenschloss

Verplomben eines Zimmers

Aufgabe 1.3 – „Safety“ und „Security“

Worin unterscheiden sich Safety und Security voneinander? Nennen Sie je zwei Beispiele, die diese Unterschiede veranschaulichen.

Aufgabe 1.4 – Programme mit Schadfunktion

Nennen Sie Beispiele für Programme mit Schadensfunktion, welche (a) einen Wirt benötigen und (b) wirtsunabhängig arbeiten.

Aufgabe 1.5 – Definitionen

Definieren sie die Begriffe „Schwachstelle“, „Bedrohung“ und „Risiko“!

Aufgabe 1.6 – Sicherheit als Risikomanagement

"Sicherheit als Risikomanagement" bedeutet, nur solche Sicherheitsmaßnahmen zu ergreifen, bei denen der zu erwartende Sicherheitsgewinn größer ist als Kosten der Sicherheitsmaßnahmen. Nennen Sie zu den folgenden Sicherheitsmaßnahmen je ein Anwendungsbeispiel, bei dem sie genutzt bzw. nicht genutzt werden und tragen Sie Ihre Antworten in die nachstehende Tabelle ein!

Virens Scanner einsetzen

Feste minimale Passwortkomplexität (z.B. mindestens 7 Zeichen, mindestens ein Sonderzeichen) fordern

Bestätigung aller Anfragen/Aktionen durch mindestens zwei Benutzer

Sicherheitspersonal zur Bewachung der Computer bereitstellen

Maßnahme	Benutzen bei	Nicht Benutzen bei
Virens Scanner		
Lokale Firewall		
Festgelegte Passwortkomplexität		
Bestätigung aller Aktionen durch mindestens zwei Benutzer		

Sicherheitspersonal zur Bewachung der Hardware		
--	--	--

Aufgabe 1.7 – Sicherheitseinstellungen von Internetbrowsern

Welche Gefahren gehen von den folgenden Einstellungen des Firefox aus?

Einstellung	Gefahr
History	
Formulardaten speichern	
Passwörter speichern	
Download History	
Cookies aktivieren	
HTML Cache aktivieren	
Popup Fenster aktivieren	
Java aktivieren	
JavaScript aktivieren	
Installation von Anwendungsprogrammen erlauben	

Aufgabe 1.8 – Grundlegende Sicherheitsmodelle

Worin unterscheiden sich „Discretionary Access Control, DAC “ und „Mandatory or Rule-based Access Control (MAC)“?

Aufgabe 1.9 – Vergleich von Sicherheitsmodellen

Wovon hängt ab ob ein Sicherheitsmodell für ein bestimmtes Szenario geeignet ist?

Aufgabe 1.10 – Sicherheitsmodelle – Zugriffsmatrix

Auf der Hauptbrücke eines Raumschiffes gibt es verschiedene Konsole für die Kontrolle der unterschiedlichen Schiffssysteme. Die verschiedenen Mannschaftsmitglieder haben unterschiedliche Rechte an den Konsolen. Legen sie mit Hilfe des Zugriffsmatrix-Modells die Zugriffsrechte der beteiligten Besatzungsmitglieder zu den Konsolen fest. Gegeben sind:

Besatzungsmitglieder: {Kapitän, Fähnrich, Wissenschaftsoffizier, Taktischer Offizier (Waffen), Steuermann, Medizinisches Personal}

Konsolen: {Navigation, Sensoren, Taktisch (Zielerfassung und Waffen), Selbstzerstörung, medizinisch }

Rechte: { lesen/einsehen, schreiben/benutzen}

	Navigation	Sensoren	Taktisch	Selbstzerstörung	Medizinisch
Kapitän					
Fähnrich					
Wissenschaftsoffizier					
Taktischer Offizier					
Steuermann					
Medizinisches Personal					

Aufgabe 1.11 – Zugriffskontrolle unter UNIX

Erklären Sie verbal die folgenden UNIX Dateizugriffsrechte:

a) Datei a: d rwx rw- r--

b) Datei b: - r-x r-- ---

c) Sind diese UNIX Dateizugriffsrechte genauso mächtig wie ACLs? Beweisen sie diese Behauptung oder geben sie ein Gegenbeispiel an!

Aufgabe 1.12 – Social Engineering

Welche Arten von Social Engineering wurden in der Vorlesung behandelt? Nennen Sie für jede Art jeweils zwei Beispiele!

Aufgabe 1.13 – Social Engineering

Nennen Sie Schutzmaßnahmen gegen Social Engineering!

Aufgabe 1.14 – Social Engineering, Angriffsbaum

Erstellen Sie einen Angriffsbaum, dessen Ziel die Erlangung geheimer firmeninterner Informationen ist. Gehen Sie dabei auch (aber nicht nur) auf Aspekte des Social Engineering ein, und kennzeichnen Sie die entsprechenden Teile des Baumes farblich.

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
► Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Abkürzungen und Bezeichner



Abkürzungen und Bezeichner 1

A - Alice
 ACL - Access Control List
 ACM - Access Control Matrix
 B - Bob
 BIOS - Basic Input Output System, die Firmware des Personal Computers
 BSI - Bundesamt für Sicherheit in der Informationstechnik
 C - Carol
 CAP - Capability List
 CC - Common Criteria for Information Technology Security Evaluation
 CobiT - Control Objectives for Information and Related Technology
 D - Dave
 E - Eve
 IT - Informationstechnologie, Information Technology
 ITIL - IT Infrastructure Library
 M - Mallory, Marvin, Mallet
 MBR - Master Boot Record
 o - Objekt (Access Control Szenarien)
 r - Recht (Access Control Szenarien)
 RBAC - Role-based Access Control
 s - Subjekt (Access Control Szenarien)
 SQL - Structured Query Language
 URL - Uniform Resource Locator
 XSS - Cross-Site Scripting



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
1.1 Security versus Safety
1.2 Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
1.3 Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
1.4 Sicherheitspolicies und Modelle
1.5 Sicherheitsstandards
1.6 Social Engineering
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Referenzen



Konferenzbeiträge, Beiträge in Zeitschriften, Bücher

[Bish2003] Matt Bishop: Computer Security Art and Science. Addison Wesley, 2003

[Bish2005] Matt Bishop: Introduction to Computer Security; Addison-Wesley, Boston, ISBN 0-321-24744-2; 2005

[Ditt2000] Jana Dittmann: Digitale Wasserzeichen. Grundlagen, Verfahren, Anwendungsgebiete. Springer-Verlag: Berlin; Heidelberg; New York, 2000

[Ecke2008] Claudia Eckert: IT-Sicherheit, Oldenbourg-Verlag, 2008

[Viel2006] Claus Vielhauer: Biometric User Authentication for IT Security: From Fundamentals to Handwriting, Springer, New York, 2006



Online-Referenzen

An dieser Stelle wird darauf hingewiesen, dass es bei Online-Angeboten immer zu Korrekturen kommen kann, bei denen sich die Adresse bzw. die Verfügbarkeit bestimmter Inhalte kurzfristig ändern kann.

[ISO27001a] ISO 27000 - ISO 27001 and ISO 27002 Standards, <http://www.27000.org/index.htm>, Letzter Aufruf: 23.05.2009

[ISO27001b] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Prüfschema für ISO 27001-Audits, http://www.bsi.bund.de/gshb/zert/ISO27001/Pruefschema_V.2.1.pdf, 2008, letzter Aufruf: 23.05.2009

[ITIL2009] ITIL.org - ITIL, <http://www.itil.org/de/vomkennen/itil/index.php>, Letzter Aufruf: 23.05.2009

[ITIL2005] ITIL und Informationssicherheit – Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management, <http://www.bsi.de/literat/studien/ITinf/itil.pdf>, 2005, letzter Aufruf: 23.05.2009

[ITGr2009] IT-Grundschutz – Startseite, <http://www.bsi.de/gshb/index.htm>, letzter Aufruf: 01.06.2009

[Cobi2009] CobiT 4.0, Control Objectives – Management Guidelines – Maturity Models, Deutsche Ausgabe, <http://www.isaca.at/Ressourcen/CobiT%204.0%20Deutsch.pdf>, letzter Aufruf: 01.06.2009

[Pfit2000] Andreas Pfitzmann: Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme, Vorlesungsskript, TU Dresden, <http://dud.inf.tu-dresden.de/~pfitza/Skript.pdf>, letzter Aufruf: 27.07.2009

[Comm2009] Common Criteria - The Common Criteria Portal, <http://www.commoncriteriaportal.org/>, letzter Aufruf: 27.07.2009

[StGB2009] Strafgesetzbuch (StGB), <http://bundesrecht.juris.de/bundesrecht/stgb/gesamt>.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

2 Datenschutz und Nicht-technische Datensicherheit

Ziel des Datenschutzes ist, jedes Individuum vor Beeinträchtigungen seines Rechtes auf informationelle Selbstbestimmung zu schützen, die durch den Umgang mit seinen personenbezogenen Daten entstehen können. Durch die Verwendung von IT Systemen zur Erfassung und Speicherung von personenbezogenen Daten wird es in letzter Zeit immer einfacher, diese Daten zu sammeln und zu speichern. Bundesdatenschutzgesetz (BDSG, [BDSG2009]) und die Landesdatenschutzgesetze (LDSG) regeln den Umgang mit diesen personenbezogenen Daten, um deren Besitzer (in den Gesetzestexten als Betroffener bezeichnet) vor dem Missbrauch der Daten schützen.

Das Bundesverfassungsgericht definiert das Recht auf informationelle Selbstbestimmung wie folgt: „Jeder Mensch kann selbst darüber entscheiden, wer wann was über ihn wissen und seine Daten verwenden darf. Dieses Recht ist jedoch nicht im Sinne einer absoluten, uneingeschränkten Herrschaft über seine Daten gewährt. Ausnahmen bedürfen einer gesetzlichen Basis, die im Allgemeininteresse begründet sein muß.“ Das Bundesdatenschutzgesetz (BDSG, §3 Abs.(1)) definiert personenbezogene Daten als „... Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person ...“.

Beispielsweise speichern Online Shops neben dem Namen eines Kunden und dessen bestellten Artikeln auch sensible Daten wie Adresse, Geburtstag und Bankverbindung. Basierend auf diesen Daten könnte der Shop-Betreiber oder auch (unseriöse) Dritte Persönlichkeitsprofile anlegen und damit beispielsweise Kunden gezielt angepasste Werbung zu Geburtstagen für vermeintlich bevorzugte Artikel zusenden. Abbildung 2.1 zeigt eine beispielhafte Auswahl von öffentlichen und nicht-öffentlichen Stellen, die personenbezogene Daten aus verschiedenen Gründen erfassen und verarbeiten.



Abbildung 2.1



Wer sammelt und verarbeitet unsere Daten



Lernziele

Im zweiten Teil werden Grundlagen des Datenschutzes auf Basis rechtlicher Bestimmungen und des nicht-technischen Datenschutzes gegeben. Dabei wird inhaltlich auf rechtliche und soziale Datenschutzgesetze auf Bundes- und Landesebene, auf das Telemediengesetz und die Telekommunikationsüberwachung, auf die Vorratsdatenspeicherung und auf die Urheberrechte eingegangen.



Informationen zu Lerneinheit 2

Lerneinheit 2

Bearbeitungszeitraum: Modulwoche 6

Bearbeitungsdauer: 1 Woche / 6 Stunden

Verständnisfragen

Anzahl: 4

Einsendeaufgaben

Anzahl: 6

Bearbeitungszeitraum: Modulwoche 6

Bearbeitungsdauer: 1 Wochen / 4 Stunden

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
▶ 2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG

Das Bundesdatenschutzgesetz ([BDSG2009]) bezieht sich auf die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch öffentliche Stellen des Bundes und der Länder (soweit es keine entsprechenden Regelungen in den Landesdatenschutzgesetzen gibt) und nicht-öffentliche Stellen. Die Erhebung, Verarbeitung und Nutzung der Daten sind nur zulässig, wenn der Betroffene dem zustimmt oder wenn das Datenschutzgesetz oder eine andere Rechtsvorschrift diese erlaubt bzw. anordnet. Ein Grundprinzip der Datenschutzgesetze ist das generelle Verbot der Erfassung von personenbezogenen Daten mit Erlaubnisvorbehalt. Das bedeutet, das Verbot wird unwirksam, wenn dieses durch Rechtsvorschriften aufgehoben wird oder eine explizite Erlaubnis des Betroffenen vorliegt.

Dem Betroffenen werden dabei wichtige Rechte zugesprochen, von denen er bezüglich seiner personenbezogenen Daten und deren Erhebung und Verarbeitung gebrauch machen kann. Auskunft: Die verantwortliche Stelle ist verpflichtet, dem Betroffenen zu den folgenden Punkten Auskunft zu erteilen: alle zu dem Betroffenen gespeicherten Daten, Herkunft und Empfänger oder Kategorien von Empfänger und Zweck der Speicherung.

Berichtigung: Die verantwortliche Stelle muss unrichtig gespeicherte Daten des Betroffenen auf seinen Antrag hin kostenlos berichtigen.

Löschung: Personenbezogene Daten müssen gelöscht werden, wenn ihre Speicherung unzulässig ist bzw. wenn sie für die verantwortliche Stelle nicht mehr erforderlich sind.

Sperrung: Sollte es Gründe geben, die einer Löschung entgegenstehen, so können die Daten des Betroffenen auch gesperrt werden. Gründe hierfür können beispielsweise sein, dass es gesetzliche oder vertragliche Aufbewahrungsfristen gibt oder eine Löschung nicht oder nur mit sehr hohem Aufwand möglich ist.

Schadenersatz: Wird einem Betroffenen Schaden durch eine unzulässige oder unrichtige Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten zugefügt, so ist die verantwortliche Stelle zu Schadenersatz verpflichtet, sofern sie den entstandenen Schaden zu verantworten hat (LDSG Sachsen-Anhalt, [LDSG2005]).

Widerspruch: Der Betroffene kann der Nutzung und Übermittlung seiner personenbezogenen Daten zu bestimmten Zwecken, wie zum Beispiel zur Werbung, widersprechen.

Bei der Speicherung der personenbezogenen Daten sind technische Vorkehrungen zu treffen, um deren Missbrauch durch Dritte zu verhindern. Möglichkeiten bieten Anonymisierung, Pseudonymisierung, Kryptographie (z.B. Verschlüsselung, siehe auch Abschnitt 5.2), verdeckte Kommunikation (z.B. Steganographie, siehe auch Abschnitt 4.2.2) oder die digitale Signatur. Das Bundesdatenschutzgesetz beinhaltet einen Maßnahmenkatalog, welcher umgangssprachlich auch als die zehn Gebote des Datenschutzes bezeichnet wird. In Tabelle 2.1 sind diese zehn Regeln mit einer kurzen Beschreibung und Beispielen aufgelistet.



Tabelle 2.1: Die zehn Gebote des Datenschutzes

Gebot	Beschreibung	Beispiel
Zugangskontrolle	Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, ist Unbefugten zu verwehren	Türsicherung, Verschluss von Datenträgern, Überwachungs- und Alarmanlagen
Datenträgerkontrolle	Lesen, Kopieren, Verändern und Entfernen von Datenträgern verhindern	Datensafes, kontrolliertes und protokolliertes Kopieren, Vernichten

Speicherkontrolle	Verhindern unbefugter Eingabe, Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten	Trennung von Programm- und Datenbereichen verschiedener Nutzer, sicheres Löschen von Datenträgern
Benutzerkontrolle	Verhinderung der Nutzung von Datenübertragungseinrichtungen durch Unbefugte	Authentifizierungsverfahren, Kontrolle der Netzverbindungen
Zugriffskontrolle	Benutzer dürfen nur auf Daten gemäß ihrer Zugriffsberechtigung zugreifen	Festlegen und Prüfen von Berechtigungen, Protokollierung
Übermittlungskontrolle	Feststellen, ob und an welche Stellen personenbezogene Daten übertragen werden dürfen	Definition von Empfängern und Art der zu übermittelnden Daten, Protokollierung
Eingabekontrolle	Feststellbar, welche Daten wann von wem in das Datenverarbeitungssystem eingegeben werden	Unbefugte Eingabe verhindern, manipulationssichere Protokollierung
Auftragskontrolle	Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden	Protokollierung über Auftrag und Erledigung, Vertrag eindeutig gestalten
Transportkontrolle	Daten dürfen bei Transport/Übertragung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden	Festlegung von Boten, Transportwegen, Transportkoffer, Verschlüsselung
Organisationskontrolle	Organisation der verantwortlichen Stelle so gestalten, dass sie dem Datenschutz gerecht wird	Verantwortlichkeiten regeln, Planung, Funktionstrennung



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

2.2 TMG, Telekommunikationsüberwachung

Das Telemediengesetz (TMG, [TMG2008]) regelt den Umgang mit so genannten Telemedien. Dieser Begriff umfasst Informations- und Kommunikationsdienste. Dazu zählen (fast) alle Angebote im Internet, wie beispielsweise Online-Shops, Online-Auktionshäuser oder Suchmaschinen. Nicht Teil des TMG sind Telekommunikationsdienste nach dem Telekommunikationsgesetz (TKG, [TKG2009]), welches die rechtlichen Grundlagen für die Übertragung von Signalen regelt. Vor Inkrafttreten des TMG wurde unterschieden zwischen Telediensten (Waren und Dienstleistungen im Netz) und Mediendiensten (Meinungsdienste im Netz). Tabelle 2.2 listet einige Beispiele und deren Zuordnung zu TMG, TKG und RStV (Staatsvertrag für Rundfunk und Telemedien, [RStV2009]) auf.



Tabelle 2.2: Zuordnung von Diensten zu TMG, TKG und RStV

Dienst	Zuordnung
Access-Providing	Telekommunikationsgesetz
Mehrwertdienste (z.B. 0900-Nummern)	Telekommunikationsgesetz
Voice-over-IP	Telekommunikationsgesetz
Internet-Suchmaschinen	Telemediengesetz
Anonymisierungsdienste	Telemediengesetz
Versenden von Werbemails	Telemediengesetz
Teleshopping	Telemediengesetz
Fernseh- und Radiotext	Telemediengesetz
Livestreaming, Webcasting	Staatsvertrag für Rundfunk und Telemedien
Video on Demand	Telemediengesetz
Private Homepage (persönliche und familiäre Zwecke)	Nicht Telemediengesetz



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
▶ 2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

2.3 Vorratsdatenspeicherung

Mit dem in Kraft treten des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG ([Gese2007]) sind seit dem 01.01.2009 Telekommunikationsanbieter und Internetprovider verpflichtet, Daten über den Telekommunikationsverkehr (Telefon, Telefax, E-Mail, Internet) zu speichern. Nach dem Gesetz müssen die Daten sechs bis maximal sieben Monate lang auf Vorrat gespeichert werden. Bis zu diesem Zeitpunkt war eine Höchstspeicherfrist von 80 Tagen möglich, wenn diese für die Abrechnung erforderlich war.

Im Folgenden werden die zu speichernden Informationen aufgeteilt nach genutztem Dienst aufgelistet, dabei ist zu beachten, dass bei allen aufgeführten Diensten auch Verbindungsversuche protokolliert werden:

Telefon, Mobilfunk und Internet-Telefonie

- Rufnummern von Anrufer und Angerufenem (inklusive von allen beteiligten Anschlüssen bei evtl. eingerichteten Um- und Weiterleitungen)
- Anfang und Ende der Verbindung (Datum und Uhrzeit mit Angabe der zugrunde liegenden Zeitzone)
- Während der Verbindung genutzte Dienste
- Bei Verbindung über ein Mobilfunkanbieter
 - Internationale Kennung des anrufenden und angerufenen Anschlusses
 - Internationale Kennung des anrufenden und angerufenen Endgerätes
 - Bezeichnung der Funkzellen, die während der Verbindung genutzt wurden
- Internet-Telefonie
 - IP-Adresse des anrufenden und angerufenen Teilnehmers

Nutzung von E-Mail

- Beim Senden:
 - Kennung von Absender und jedes Empfängers
 - IP-Adresse des Absenders
- Beim Empfangen:
 - Kennung von Absender und jedes Empfängers
 - IP-Adresse der absendenden Telekommunikationsanlage
- Beim Zugriff:
 - Kennung und IP-Adresse des Zugreifenden
- Anfang und Ende der Nutzung (Datum und Uhrzeit mit Angabe der zugrunde liegenden Zeitzone)

Nutzung von Internetzugängen

- Dem Teilnehmer zugewiesene IP-Adresse
- Eindeutige Kennung des genutzten Anschlusses
- Anfang und Ende der Nutzung (Datum und Uhrzeit mit Angabe der zugrunde liegenden Zeitzone)

Von den gesetzlichen Regelungen sind auch Privatpersonen betroffen, die kostenlos einen öffentlichen WLAN-Zugang oder einen E-Mail-Service anbieten. Nicht betroffen sind Anbieter von Webseiten, Webspace (Hosting), Foren und Chats.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
▶ 2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

2.4 Urheberrechte

Das Urheberrecht schützt geistiges Eigentum vor unbefugter wirtschaftlicher Verwertung und Verletzung der ideellen Interessen. Zum Gegenstand dieser gesetzlichen Regelungen ([Urhe2008]) zählen neben Werken der Literatur, Wissenschaft und Kunst auch Computerprogramme, Multimedia-Produktionen, technische Dokumentationen und Datenbanken. Das Recht auf Urheberschaft an einer geistigen Schöpfung gilt automatisch vom Moment der Entstehung des Werkes. Es gibt dem Urheber alle notwendigen Rechte an der Verwertung seines Werkes. Dies umfasst die Vervielfältigung, die Verbreitung, die Ausstellung, die öffentliche Wiedergabe und die Bearbeitung. Ausgenommen vom Schutz durch das Urheberrecht sind triviale Kreationen, die eine gewisse Schöpfungshöhe unterschreiten. Als Schöpfungshöhe wird das Ausmaß an Individualität des Werkes bezeichnet. Das Urheberrecht erlischt 70 Jahre nach dem Tode des Urhebers bzw. des längstlebenden Urhebers bei Gemeinschaftsschöpfungen.

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
▶ Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Verständnisfragen



Verständnisfragen 2

1. Ist das Aufnehmen von personenbezogenen Daten generell erlaubt oder verboten?

erlaubt

verboten

2. Das im Bundesdatenschutzgesetz gewährte Recht auf Berichtigung bedeutet, dass:

die verantwortliche Stelle in regelmäßigen Abständen die Richtigkeit der personenbezogenen Daten überprüfen und gegebenenfalls berichtigen muss?

die verantwortliche Stelle die personenbezogenen Daten auf Antrag des Betroffenen berichtigen muss?

3. Unter der Speicherkontrolle versteht man

die Kontrolle zur Verhinderung der unbefugten Eingabe, Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten.

die regelmäßige Kontrolle der Funktionstüchtigkeit der zur Speicherung von personenbezogenen Daten eingesetzter Datenträger (z.B. Festplatten, CDs, DVDs).

4. Das Urheberrecht schützt jede geistige Schöpfung! Ist diese Aussage richtig oder falsch?

richtig

falsch

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
► Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Einsendeaufgaben

Aufgabe 2.1 – Rechtlicher Datenschutz

Nennen Sie die Grundprinzipien des rechtlichen Datenschutzes!

Aufgabe 2.2 – Rechtlicher Datenschutz

Nach welchen Kriterien dürfen Daten erhoben, gespeichert, übertragen, verändert und genutzt werden?

Aufgabe 2.3 – Rechtlicher Datenschutz

Welche Rechte haben die so genannten Betroffenen, also die Bürger?

Aufgabe 2.4 – Rechtlicher Datenschutz

Nehmen Sie mindestens 5 von den in Abbildung 2.1 gezeigten öffentlichen und nicht öffentlichen Stellen in die nachstehende Tabelle auf. Machen Sie sich Gedanken über die Art der jeweils aufgenommenen Daten und geben Sie an, ob diese Daten kritisch sind in Bezug auf das Bundesdatenschutzgesetz und nennen Sie mögliche Gründe warum beziehungsweise warum nicht.

öffentliche/ nicht öffentliche Stelle	erfasste Daten	Finden Sie die Aufnahme der erfassten Daten kritisch für den Betroffenen?	Warum? bzw. Warum nicht?

Aufgabe 2.5 – Gesetzliche Regelungen

Welche Aktionen stellen die Paragraphen §§ 202a, 202b, 202c, 263a, 303a, 303b StGB im Kontext der IT unter Strafe? Nennen sie Beispiele! Welche ähnlichen Aktionen werden nicht unter Strafe gestellt?

Bitte beachten Sie: Dies ist eine Recherche-Aufgabe. Bitte nutzen zur Beantwortung die entsprechenden Gesetzestexte.

Aufgabe 2.6 – Überwachung im Alltag

Dokumentieren Sie stichpunktartig für einen Tag, wann, wo und durch welche nicht von ihnen kontrollierbaren Geräte und/oder Überwachungseinrichtungen Ihr Tagungsablauf protokolliert wird.

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
► Abkürzungen und Bezeichner
Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Abkürzungen und Bezeichner



Abkürzungen und Bezeichner 2

BDSG - Bundesdatenschutzgesetz
 LDSG - Landesdatenschutzgesetz
 RStV - Staatsvertrag für Rundfunk und Telemedien (kurz Rundfunkstaatsvertrag)
 TKG - Telekommunikationsgesetz
 TMG - Telemediengesetz

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
2.1 Rechtlich/Soziale Datenschutzgesetze: BDSG, LDSG
2.2 TMG, Telekommunikationsüberwachung
2.3 Vorratsdatenspeicherung
2.4 Urheberrechte
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
► Referenzen
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Referenzen



Online-Referenzen

An dieser Stelle wird darauf hingewiesen, dass es bei Online-Angeboten immer zu Korrekturen kommen kann, bei denen sich die Adresse bzw. die Verfügbarkeit bestimmter Inhalte kurzfristig ändern kann.

[Gese2007] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Bundesgesetzblatt Jahrgang 2007 Teil I Nr. 70, Bonn, 2007

[StGB2009] Strafgesetzbuch (StGB), <http://bundesrecht.juris.de/bundesrecht/stgb/gesamt.pdf>, Stand: 29.6.2009, letzter Aufruf: 30.07.2009

[BDSG2009] Bundesdatenschutzgesetz (BDSG), http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf, Stand:05.02.2009, letzter Aufruf: 08.08.2009

[LDSG2005] Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA), Stand: http://www.sachsen-anhalt.de/LPSA/fileadmin/Elementbibliothek/Bibliothek_Politik_und_Verwaltung/Bibliothek_LFD/PDF/binary/Vorschriften/Land/dsg-lsa/dsg-lsa.pdf, Stand:18.12.2005, letzter Aufruf: 08.08.2009

[TMG2008] Telemediengesetz (TMG), <http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf>, Stand: 25.12.2008, letzter Aufruf: 08.08.2009

[TKG2009] Telekommunikationsgesetz (TKG), http://bundesrecht.juris.de/bundesrecht/tkg_2004/gesamt.pdf, Stand: 29.04.2009, letzter Aufruf: 08.08.2009

[RStV2009] Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV –), http://www.alm.de/fileadmin/Download/Gesetze/RStV_aktuell.pdf, Stand: 01.06.2009, letzter Aufruf: 08.08.2009

[Urhe2008] Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz), <http://bundesrecht.juris.de/bundesrecht/urhg/gesamt.pdf>, Stand: 17.12.2008, letzter Aufruf: 08.08.2009



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
▶ 3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3 Identity Management

In der heutigen technisierten Welt ist es nicht mehr immer möglich, dass Menschen gegenseitig von Angesicht zu Angesicht die Identität des anderen feststellen können. Dies liegt beispielsweise in der Entfernung zwischen zwei Parteien begründet, die durch ein Computernetzwerk (z.B. Internet) überbrückt wird. Die Feststellung und Sicherung der Identität der an einem Prozess beteiligten Personen wird zunehmend durch automatische Systeme vorgenommen. Der Nachweis bzw. die Bestimmung der Identität einer Person wird als Authentifikation bezeichnet. Genutzt wird sie beispielsweise zur Zugangskontrolle für Räume bzw. Häuser, als Zugriffskontrolle für Computer, Kommunikations- bzw. Zahlungssysteme oder zur Sicherung von Fahrzeugen.



Lernziele

Mit Identity-Management beschäftigt sich der dritte Abschnitt des Moduls. Hier werden Grundlagen, Wissen zu Techniken und Anwendungsbereichen sowie Vor- und Nachteile verschiedener Authentifizierungsmethoden vermittelt. Schwerpunkte liegen dabei auf den Grundlagen der Benutzerauthentifizierung, Authentifizierungsmethoden auf Basis von Wissen, Besitz und Biometrie sowie der Kombination verschiedener Faktoren und unterschiedlichen Single-Sign-On-Systemen.



Informationen zu Lerneinheit 3

Lerneinheit 3

Bearbeitungszeitraum: Modulwoche 7 - 10

Bearbeitungsdauer: 4 Woche / 13 Stunden

Verständnisfragen

Anzahl: 4

Einsendeaufgaben

Anzahl: 8

Bearbeitungszeitraum: Modulwoche 7 - 10

Bearbeitungsdauer: 4 Wochen / 8 Stunden



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
▶ 3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.1 Grundlagen der Benutzerauthentifizierung

Bishop beschreibt die Authentifikation als die Bindung einer Identität an ein Subjekt [Bish2005]. Weiter gibt er die folgenden fünf Komponenten für ein System zur Benutzerauthentifizierung an:

1. Eine Menge von aktuellen Authentifizierungsdaten dient als Grundlage für spezielle Informationen, mit der eine Person ihre Identität nachweisen will.
2. Eine Menge von Referenzdaten ist im System gespeichert und wird zur Überprüfung der Identität genutzt.
3. Eine Menge von Funktionen, die die Authentifizierungsdaten in das gleiche Format wie die Referenzdaten überführt, um einen Vergleich zu ermöglichen.
4. Eine Menge von Authentifizierungsfunktionen, die die Identität überprüfen.
5. Eine Menge von Funktionen, die es einer Person erlauben, Authentifizierungs- bzw. Referenzdaten zu erzeugen oder zu ändern.

In Abbildung 3.1 ist ein allgemeines Schema eines Authentifizierungsprozesses dargestellt. Dieser besteht in den meisten Fällen aus vier Prozessmodulen: Datenaufnahme-, Merkmalsextraktions-, Vergleichs- und Entscheidungsmodul. Ein Authentifizierungsversuch läuft folgendermaßen ab: Zum Zeitpunkt der Datenaufnahme wird das Authentifizierungsobjekt dem System präsentiert (z.B. Passwort, Schriftprobe). Die Rohdaten werden dann an die Merkmalsextraktion übergeben. Hier werden aus den Daten Merkmale berechnet, die die Grundlage für den Vergleich darstellen. Im Vergleichsmodul werden die Merkmale des aktuell präsentierten Authentifizierungsobjektes mit den im System hinterlegten Daten (Referenzdaten, Referenz) verglichen. Basierend auf dem Ergebnis des Vergleichs wird eine Entscheidung bezüglich der Authentizität getroffen.



Abbildung 3.1



Schema – Allgemeine Benutzerauthentifizierung

Die gebräuchlichsten Authentifizierungsverfahren basieren auf geheimem Wissen („Was weiß ich?“), persönlichem Besitz („Was habe ich?“), Biometrie („Was bin ich?“ oder „Was kann ich?“) und Standort („Wo bin ich?“). In den folgenden Abschnitten werden unterschiedliche Möglichkeiten der Benutzerauthentifizierung beschrieben.

Die **Authentifizierung** kann in zwei Methoden unterteilt werden, die Verifikation und die Identifikation. Von einer **Verifikation** spricht man, wenn die aktuell präsentierten Authentifizierungsdaten einer Person mit den Referenzdaten derselben Person verglichen werden, um zu überprüfen, ob diese diejenige ist, die sie vorgibt zu sein. Es findet also ein 1:1 Vergleich statt. Bei der **Identifikation** werden die aktuellen Daten mit den Referenzdaten aller registrierten Personen verglichen (1:n-Vergleich). Das Ergebnis ist entweder die Angabe der Person, deren Referenzdaten mit den aktuell präsentierten übereinstimmen oder die Information, dass es keine solche Person gibt. Zur Vereinfachung wird im Folgenden eine Verifikation angenommen, sofern nicht anders angegeben. Aus Sicht der Authentifizierung kann die Sicherheit eines IT-Systems dahingehend beeinträchtigt werden, dass Angreifer unberechtigten Zugriff auf gesicherte Bereiche gelangen können, indem er die Identität einer registrierten Person annimmt. Abhängig von deren Autorisierung kann ein Angreifer Schaden in verschiedenem Ausmaß anrichten.

Als **Autorisierung** wird im IT Bereich die erfolgreiche Zuweisung von bestimmten Rechten innerhalb von IT-Systemen verstanden. Sie erfolgt meistens nach einer erfolgreichen Authentifizierung. Zum Beispiel wird ein erfolgreich authentifizierter Nutzer eines Betriebssystems für verschiedene Handlungen innerhalb des Betriebssystems autorisiert. Das können Nutzungsrechte für Hardware, Dateien und Verzeichnisse oder auch Dienste sein.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
▶ 3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.

Wissensbasierte Authentifizierung (auch Authentifizierung durch geheimes Wissen) nutzt Informationen, die anderen Personen nicht bekannt sind, wie beispielsweise PIN, Passwort oder Passphrase. Diese muss sich der Nutzer merken und bei Aufforderung an das System übergeben (z.B. über die Tastatur). Das geheim halten des Wissens ist dabei die wichtigste Komponente zur Wahrung der Sicherheit des entsprechenden Systems. Zusätzlich sollten beispielsweise Passwörter aus einer möglichst großen Menge von Zeichen bestehen, Sonderzeichen und Zahlen enthalten und nicht in einem Wörterbuch zu finden sein. Außerdem sollten PIN, Passwort bzw. Passphrase in regelmäßigen, nicht allzu großen Abständen erneuert werden. Diese Anforderungen führen jedoch dazu, dass sich der Nutzer unter Umständen mehrere (sinnlose) lange Zeichenkombinationen merken muss, die dazu noch ständig wechseln. Die Nutzung des geheimen Wissens ist jedoch für die automatische Authentifikation die am einfachsten zu lösende Variante. Dadurch findet sie eine große Verbreitung, z.B. bei der Anmeldung bei Betriebssystemen oder bei Onlineshops. Ein großer Nachteil ist, dass das geheime Wissen durch Vergessen verloren gehen oder durch Verraten weitergegeben werden kann. Auch ein Ausspähen durch Kameras oder durch heimliches Protokollieren der Tastatureingaben ist möglich.

Zur Veranschaulichung stellt Abbildung 3.2 das allgemeine Schema zur Benutzerauthentifizierung der beispielhaften Authentifizierung mittels Passwort gegenüber. Das Authentifizierungsobjekt ist in diesem Fall das Passwort, welches über eine Tastatur aufgenommen wird. Während der Merkmalsextraktion wird mittels eines so genannten Hash-Verfahrens (für weitere Erläuterungen hierzu siehe auch Abschnitt 5.2) ein eindeutiger Wert aus dem Passwort generiert und an das Vergleichsmodul weitergegeben. Hier wird der gerade generierte Hash mit dem im System hinterlegten Hash des Nutzers verglichen. Sind beide Werte identisch, dann gilt die Person als identifiziert, im anderen Fall nicht.



Abbildung 3.2



Schema –
Benutzerauthentifizierung
durch Wissen
(Passwort)

Das One-Time-Pad (siehe auch [Ecke2008]) nutzt ebenfalls geheimes Wissen, um eine symmetrische Verschlüsselung (siehe auch Abschnitt 3.6.1) durchzuführen und gilt bis heute als theoretisch nicht brechbar. Es wurde 1917 von M.J. Mauborgne und G. Vernam entwickelt. Die folgenden Bedingungen machen das One-Time-Pad Verfahren einerseits sicher, andererseits sind sie auch die Begründung für die schwierige Umsetzung in der Praxis:

1. Der Schlüssel wird nur einmal verwendet.
2. Die Länge des Schlüssels muss mindestens der Länge der Nachricht entsprechen.
3. Der Schlüssel ist unvorhersagbar zufällig.
4. Der Schlüssel ist nur dem Sender und dem Empfänger bekannt.

Bei der Übertragung einer Nachricht benötigen Sender (Alice) und Empfänger (Bob) das gleiche geheime Passwort (auch Schlüssel, siehe Exkurs Symmetrische Verschlüsselung). An dieser Stelle wird angenommen, dass dieser bereits sicher zwischen Alice und Bob ausgetauscht wurden und nur ihnen bekannt ist. Das One-Time-Pad basiert auf der binären Codierung (Verschlüsselung) des Klartextes mit dem Schlüssel durch die XOR-Operation ($0 \text{ XOR } 0 = 0$, $1 \text{ XOR } 1 = 0$, $0 \text{ XOR } 1 = 1$, $1 \text{ XOR } 0 = 1$). Die so verschlüsselte Nachricht kann dann beispielsweise per E-Mail übertragen werden. Ein potentieller Angreifer kann ohne den Schlüssel die Nachricht nicht entschlüsseln, dies kann nur Bob, welcher im Besitz des Schlüssels ist.

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
▶ 3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positionsbasierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.3 Besitzbasierte Authentifizierung: Smartcards & RFID

Der persönliche Besitz eines Merkmals ermöglicht die Authentifizierung einer Person über einen physischen Gegenstand, wie z.B. Schlüssel oder SmartCard und ermöglicht so beispielsweise den Zugang zu nicht öffentlichen Räumen oder Computersystemen. Der Nutzer muss durch das Aufweisen des physischen Gegenstandes seine Berechtigung nachweisen. Durch den Verlust (z.B. durch Diebstahl oder Verlieren) des Gegenstandes ist eine Gefährdung des zu sichernden Raumes bzw. Systems möglich.

Der Authentifizierungsprozess mittels eines Schlüssels ist in Abbildung 3.3 dargestellt. Dabei ist der Schlüssel das Authentifizierungsobjekt und wird dem System durch einstecken in das Schloss präsentiert. Die Länge und Form des Schlüsselbarts mit Auskerbungen, Erhöhungen und Bohrungen stellen die Merkmale dar. Ein Vergleich findet in der Form statt, dass die Merkmale des Schlüssels der physischen Struktur des Schlosses entsprechen müssen. Ist dies der Fall, kann der Schlüssel gedreht und damit das Schloss geöffnet werden.



Abbildung 3.3



Schema –
Benutzerauthentifizierung
durch Besitz (Schlüssel)

Es ist zu beachten, dass es sich beispielsweise beim Notieren eines Passwortes nicht mehr um geheimes Wissen handelt, sondern vielmehr um persönlichen Besitz. Ein weiterer Nachteil beider Authentifizierungsmerkmale ist die beabsichtigte Weitergabe an eine dritte Person.

Geht ein geheimes Wissen durch Vergessen oder Ausspähen verloren, ist es möglich, den sicheren Zustand durch Sperren der alten und Erzeugen neuer Daten wiederherzustellen. Genauso kann die Gültigkeit verlorener oder gestohlener physischer Gegenstände aufgehoben werden. Der betroffenen Person kann dann ein neuer Gegenstand zur Authentifizierung zur Verfügung gestellt werden.

Die Verwendung von **Smart Cards** ist eine weit verbreitete Methode der besitzbasierten Authentifizierung. Die gebräuchlichsten Formen von Smart Cards werden durch die ISO-Formate ID-000 (SIM-Karten, z.B. eingesetzt in Mobiltelefonen) und ID-1 (Scheckkartenformat, z.B. EC-Karte) beschrieben. Es sind aber auch andere Formate im Einsatz, beispielsweise existieren Smart Cards die in USB-Sticks integriert sind. Allgemein handelt es sich dabei um einen Chip, der Logik-Hardware, Speicher und teilweise auch einen eigenen Prozessor enthält. Sie werden zum Beispiel eingesetzt für den bargeldlosen Zahlungsverkehr oder zur Zugangssicherung von Gebäuden oder IT-Systemen.

RFID (Radio Frequency Identification, deutsch Funkerkennung oder Identifizierung mit Hilfe von elektromagnetischen Wellen) ist ein technisches Verfahren, das es ermöglicht, Daten zu lesen und zu schreiben, ohne den Datenträger zu berühren. Dazu wird der Gegenstand, der durch die Daten auf dem RFID-Chip authentifiziert werden soll, mit einem so genannten Transponder

versehen. Dieser reagiert auf Anfragen eines Lesegerätes, welche per Funk übertragen werden, dadurch ist kein Kontakt zwischen Gegenstand und Lesegerät notwendig. Die Anwendungsbereiche von RFID-Technik sind vielfältig, sie wird beispielsweise eingesetzt, um Informationen über Waren (Kleidung, Lebensmittel, Autos etc.) zu speichern und bei Bedarf zu übertragen, um den Warenfluss kontrollieren zu können. Sie dienen mittlerweile auch dazu, Tiere oder Menschen zu authentifizieren. So werden RFID-Chips auch in Reisepässen eingesetzt, wo unter anderem biometrische Informationen wie der Fingerabdruck und das Gesicht des Inhabers gespeichert werden, die bei Bedarf abgerufen werden können.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
▶ 3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.4 Biometrische Authentifizierung

Ein wichtiger Aspekt der wissens- und besitzbasierten Authentifizierung ist, dass hier nicht überprüft werden kann, ob sich eine bestimmte Person dem System gegenüber authentifiziert. Es wird nur festgestellt, ob das vorgewiesene Authentifizierungsobjekt (geheimes Wissen bzw. persönlicher präsentierte Gegenstand) zum Zugang zum geschützten Bereich berechtigt oder nicht. Das bedeutet, die Identität der Person, die Zugang verlangt, kann nicht überprüft werden. Anders verhält es sich bei der Verwendung von biometrischen Merkmalen zur Benutzerauthentifizierung. Wie in Abbildung 3.4 zu sehen ist, sind diese Charakteristiken (auch Modalitäten) fest mit dem Körper (statisch, offline, physisch) oder dem Verhalten (dynamisch, online, verhaltensbasiert) eines Menschen verbunden. Bekannte Beispiele sind hier die Nutzung des Fingerabdruckes (statisch), der Iris (statisch) oder der Handschrift (dynamisch). Die biometrischen Verfahren basieren also auf der Tatsache des Vorhandenseins der berechtigten Person, wogegen bei den oben genannten Verfahren nur die Präsenz eines bestimmten Wissens oder Gegenstandes überprüft werden kann.



Abbildung 3.4



Beispiele für
statische und
dynamische
biometrische
Modalitäten

Die oben angeführten Nachteile von Authentifizierungsmerkmalen, die auf geheimem Wissen bzw. Besitz basieren, zeigen deutlich, dass eine Gefährdung der Sicherheit hauptsächlich auf Vergessen, Verlieren, Diebstahl und Weitergabe basieren. Durch die Verwendung biometrischer Merkmale wird versucht, diesen Umstand zu umgehen.

Während die nicht biometrische Authentifikation auf einer genauen Übereinstimmung des benutzten Merkmals basiert, ist dies bei der biometrischen Authentifikation nicht möglich. Der Grund dafür ist, dass die Qualität des Merkmals schwankt. Das kann beispielsweise durch unterschiedliche Erfassungshardware, Verletzungen oder auch durch das aktuelle Befinden der Person hervorgerufen werden.

Die Authentifikation in der Biometrie dient der Überprüfung bzw. Ermittlung der Identität einer Person, die zu einem gesicherten Bereich oder Computersystem Zugang verlangt. Die Überprüfung der Identität wird als Verifikation bezeichnet. Dabei wird sichergestellt, ob die Person diejenige ist, für die sie sich ausgibt. Dazu werden die aktuell aufgewiesenen Daten mit den in der Datenbank hinterlegten Referenzdaten verglichen, die sich auf einen bestimmten Identifikator (d.h. der behaupteten Identität, z.B. Nutzernamen) beziehen. Stimmen diese in ausreichendem Maße überein, wird der Person Zugang auf das gesicherte System gewährt. Im anderen Fall wird sie abgewiesen. Soll im Verlauf einer Authentifizierung die Identität einer Person ermittelt werden, spricht man von einer Identifikation. Hierbei werden die Eingabedaten der zunächst unbekannten Person mit den Referenzdaten aller dem System bekannten Personen verglichen. Im Falle einer Übereinstimmung mit einem vorhandenen Datensatz innerhalb vorgegebener Grenzen gilt die Person als identifiziert und erhält Zugang zum geschützten System.



Abbildung 3.5



a) Fingerabdruck



b) Handschrift (hier: PIN)

Bei der biometrischen Authentifikation wird mindestens ein biologisches Merkmal des Nutzers („Wer bin ich?“ bzw. „Was kann ich?“) zur Identifikation bzw. Verifikation genutzt. Vorteil ist hier, dass die verwendeten Merkmale nicht oder nur sehr selten verloren gehen können. Dabei gibt es eine Vielzahl biologischer Eigenschaften eines Menschen, die verwendet werden können. Zu den gebräuchlichsten gehören der Fingerabdruck oder auch die Handschrift (siehe Abbildungen 3.5).

Im vorherigen Abschnitt wurde festgestellt, dass bei einem nicht biometrischen System nur das Wissen bzw. der Gegenstand authentifiziert wird. Das ist bei biometrischen Systemen nicht der Fall. Hier wird, begründet durch den Umstand, dass das biologische Merkmal Bestandteil der Person ist, die Person selbst authentifiziert. Um zu verhindern, dass dem System vom Körper abgetrennte Merkmale (z.B. Finger) oder künstliche Kopien (z.B. Silikon-Finger, Fotos) angeboten werden, verfügen die meisten Systeme über eine Lebenderkennung. Diese überprüft durch Merkmal typische Tests (z.B. auf winzige Bewegungen der Iris), ob das Merkmal von der lebenden Person stammt, die in diesem Moment vom System authentifiziert werden soll. Eine Lebenderkennung ist vor allem bei statischen biometrischen Merkmalen notwendig, da die Nutzung dynamischer Merkmale eine aktive Mitwirkung der betroffenen Person voraus setzt.

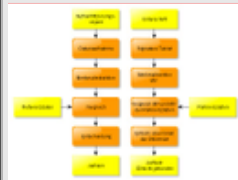
Im Gegensatz zur nicht biometrischen Authentifikation können biologische Merkmale unter normalen Umständen nicht verloren gehen, gestohlen oder weiter gegeben werden. Eine große Gefahr liegt jedoch im Diebstahl und der Veränderung der Daten der beschreibenden Merkmale der biologischen Eigenschaft. So können beispielsweise Referenzdaten abgeschwächt werden, um einen Angriff zu erleichtern. Solche Angriffe können zum Beispiel durch Abfangen und Veränderung der Daten während der Datenübertragung zwischen der Aufnahmehardware und dem Computer stattfinden. Ist ein Diebstahl der Daten eines biometrischen Merkmals erfolgreich gewesen, ist dessen Einsatz zur Authentifikation nicht mehr sicher. Es kann aber auch nicht, wie zum Beispiel bei einem Passwort, ohne weiteres ersetzt werden. Im Fall des Fingerabdruckes stehen noch andere Finger zur Verfügung, sofern nicht ein bestimmter Finger vom System gefordert wird. Werden aber beispielsweise die Daten zur Erkennung eines Gesichtes gestohlen, kann die betroffene Person unter Umständen nicht mehr mit dem Authentifizierungssystem arbeiten. Auch eine Nachahmung dynamischer biometrischer Merkmale ist denkbar. Beispielsweise kann durch aufwändiges Training versucht werden, die Unterschrift einer anderen Person zu fälschen. Dies ist jedoch sehr schwierig, da dabei nicht nur das Schriftbild zu reproduzieren ist. Vielmehr sind viele andere Faktoren, zum Beispiel Schreibdauer oder Druckverlauf, zu beachten, um eine erfolgreiche Fälschung zu erzeugen. Geht die Unterschrift einer Person als Authentifizierungsobjekt verloren, zum Beispiel durch einen der oben erwähnten Angriffe, kann sie im Normalfall nicht mehr ersetzt werden. Es gibt aber inzwischen Ansätze, die die Verwendung anderer Semantiken neben der Unterschrift vorschlagen. Vielhauer untersucht beispielsweise die Verwendung von Unterschriften, Passwörtern, Passphrasen und Symbolen [Viel2006]. Er zeigt, dass eine Authentifizierung über andere Semantiken als die Unterschrift grundsätzlich möglich ist. Weiter wird nachgewiesen, dass auch so genannte globale Semantiken, bei denen alle Nutzer inhaltlich das gleiche schreiben, zur Authentifikation herangezogen werden können. Dies wahrt die Anonymität des Schreibers. Allerdings führt die Verwendung von globalen Semantiken zurzeit noch zu höheren Fehlerraten als bei der Nutzung der Unterschrift oder individueller Inhalte.

Das Schema der Authentifizierung durch die Biometrie Unterschrift ist in Abbildung 3.6 dargestellt. Hier werden die Daten von einem Graphic Tablet aufgenommen, wie es beispielsweise zur Bildverarbeitung verwendet wird. Dieses liefert als Rohdaten physikalische

Werte wie X- und Y- Position, Druck an der Stiftspitze und gegebenenfalls Höhen- und Seitenwinkel des Stiftes. Aus diesen Werten werden statistische Werte berechnet, welche in einem Merkmalsvektor gespeichert werden. Der Merkmalsvektor der aktuell präsentierten Unterschrift wird dann mit dem in der Referenzdatenbank gespeicherten Merkmalsvektor der Zugriff verlangenden Person verglichen. Sind diese in einem vorherdefinierten Ausmaß ähnlich zueinander, gilt die Person als authentifiziert.



Abbildung 3.6



Schema –
Benutzerauthentifizierung
durch Biometrie
(Unterschrift)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
▶ 3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.5 Multifaktorielle Authentifizierung

Zur Erhöhung der Sicherheit ist es möglich, Authentifizierungsmethoden zu kombinieren. Eine weit verbreitete Kombination ist zum Beispiel die Verwendung einer SmartCard in Verbindung mit einer Geheimzahl (PIN). Diese Möglichkeit wird seit einigen Jahren zum bargeldlosen Zahlungsverkehr genutzt. Wie in Abbildung 3.7 dargestellt, ist auch eine Kombination von Handschrift und PIN denkbar ([Viel2006]). Dadurch ergeben sich aber neue Probleme, wie zum Beispiel die Möglichkeit des Mitlesens durch eine dritte Person. Es würde in diesem Fall nur noch die Handschrift zur Sicherheit beitragen, da es kein geheimes Wissen mehr gibt. Solche und ähnliche Probleme müssen bei Planung, Entwurf und Bau von Authentifikationssystemen berücksichtigt werden.



Abbildung 3.7



Kombination von
Biometrie
(Handschrift) und
geheimem Wissen
(PIN)

Es gibt verschiedene Möglichkeiten, Authentifizierungsmethoden miteinander zu kombinieren. Vereint man in einem System zwei oder mehr Methoden so spricht man von einer multifaktoriellen Authentifizierung. Zusätzlich wird in der Biometrie die Kombination von mehreren biologischen Eigenschaften als multi-modale biometrische Authentifizierung bezeichnet. Beide Arten der Kombination können wiederum miteinander kombiniert werden, dabei handelt es sich dann um eine multifaktorielle, multi-modale Authentifizierung. Ein Beispiel dafür wäre die Nutzung einer Smart Card mit einer Handschrifterkennung und einer Fingerabdruckerkennung.

Werden die Daten eines biometrischen Merkmals gestohlen oder verändert, ist dieses Merkmal im Normalfall für die Authentifikation nicht mehr nutzbar. Abhilfe könnten hier unter anderem multi-biometrische Systeme schaffen (siehe auch [ScVD2005]), bei denen mehrere voneinander unabhängige biometrische Verfahren verschiedene biologische Merkmale erfassen und auswerten. Die Kombination der Systeme kann dabei an mehreren Stellen innerhalb der einzelnen Subsysteme erfolgen. Bei multibiometrischen Systemen ist das heimliche Aufzeichnen aller biometrischen Daten während der Aufnahme aber auch das Wiedereinspielen der Daten in das System (Replay-Angriff) schwierig. Außerdem müssen dem System mehrere unterschiedliche biometrische Daten einer Person übergeben werden. Es ist ebenfalls möglich, die Daten nicht vorhandener oder gestohlener (d.h. nicht mehr sicherer) Merkmale für die betreffende Person auszuschließen.

Für vertiefende und weiterführende Studien zum Thema Biometrie sei der interessierte Leser auf die Literatur (z.B. Handschrift [Viel2006], multi-biometrische Authentifizierung [RoNJ2006]) und das Internet verwiesen (z.B. Grundlagen [Brom2009a], Fingerprint [Brom2009b], Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren [Krit2006]).



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
▶ 3.6 Single-Sign-On Systeme
3.6.1 Kerberos
3.6.2 LDAP
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.6 Single-Sign-On Systeme

Die große Menge an Authentifizierungsanfragen, mit denen ein Nutzer eines IT-Systems täglich konfrontiert wird, kann enorm sein. Eine Möglichkeit, den Aufwand für den Nutzer gering zu halten, bieten Single-Sign-On Systeme. Diese ermöglichen einem Anwender nach einmaliger Authentifizierung den Zugriff auf alle Ressourcen (z.B. Rechner, Dienste oder Daten) für deren Zugriff der Anwender autorisiert ist. Zu den Vorteilen von Single-Sign-On Systemen zählen, dass durch nur einmalige Verwendung des Authentifizierungssystems Zeit eingespart werden kann, der Nutzer nur ein einziges Authentifikationsobjekt (z.B. Passwort) benötigt und pro Authentifizierungsvorgang nur ein Passwort einmalig übertragen werden muss. Ein wesentlicher Nachteil von Single-Sign-On Systemen liegt darin, dass ein potentieller Angreifer Zugriff auf alle Ressourcen gelangt, für deren Nutzung ein Anwender autorisiert ist, wenn er an dessen Authentifizierungsobjekt gelangt (z.B. Passwort). Um die Arbeitsweise von Single-Sign-On Systemen zu verdeutlichen, werden im Folgenden die Applikationen Kerberos und LDAP beispielhaft vorgestellt.

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
▶ 3.6.1 Kerberos
3.6.2 LDAP
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.6.1 Kerberos

Kerberos ist ein Protokoll zur Authentifikation innerhalb von Netzwerken welches am MIT Mitte der 80er Jahre entwickelt wurde. Kerberos basiert auf einem Authentifizierungsdienst, dem der Nutzer seine Identität nachweisen muss, um ohne weitere Authentifikation Ressourcen nutzen zu können. Es steht dem Anwender sowohl kommerzielle als auch freie Software zur Verfügung. Eine Kerberos-Implementierung sollte verschiedene Eigenschaften aufweise. Der Nutzer soll nichts von der Authentifizierung mitbekommen (Transparenz). Das System soll zuverlässig sein, da sowohl die Nutzer als auch die dem System angeschlossenen Ressourcen davon abhängig sind (Zuverlässigkeit). Ein Angreifer soll aus den Datenflüssen keine Informationen ableiten können, mit denen die Übernahme der Identität eines registrierten Nutzers bzw. die unautorisierte Nutzung der Ressourcen möglich ist (Sicherheit). Die Eigenschaft der Skalierbarkeit beschreibt die Möglichkeit, dass dem System jederzeit neue Nutzer und Ressourcen hinzugefügt werden können.

Da das beschriebene System in einigen Arbeitsschritten symmetrische Verschlüsselung verwendet, wird an dieser Stelle ein kurzer Exkurs zu diesem Thema gegeben.



Exkurs: Symmetrische Verschlüsselung

Allgemeines Ziel der Verschlüsselung ist es, Informationen geheim zu halten und sie nur autorisierten Personen zu offenbaren. Die ursprüngliche Information m wird als Nachricht oder auch Klartext bezeichnet. Das verschlüsselte Ergebnis c ist das Chiffre oder der Geheimtext. Die Funktion, die m in c überführt, wird als Verschlüsselung E (engl. *Encryption*) bezeichnet, während man die umgekehrte Richtung (aus c wird m berechnet) als Entschlüsselung D (engl. *Decryption*) bezeichnet. Zur Parametrisierung von Ver- und Entschlüsselung wird jeweils ein Schlüssel (engl. *Key*) K_1 bzw. K_2 benötigt. Das bedeutet:

$$c = E(m, K_1) \text{ und } m = D(c, K_2).$$

Bei den meisten symmetrischen Verschlüsselungsverfahren gilt:

$$K = K_1 = K_2.$$

Das hat zur Folge, dass vor dem Austausch von Nachrichten beide Kommunikationspartner K sicher miteinander tauschen müssen und diesen geheim halten müssen. Im Kapitel 5 gibt es einen weiteren Exkurs zum Thema asymmetrische Verschlüsselung. Weitere Information zu beiden Arten der Verschlüsselung sind unter anderem in [Ecke2008] zu finden.



Abbildung 3.8



Kerberos

Die Grundidee des Kerberos ist, dass für alle Aktionen so genannte Tickets notwendig sind. Im Folgenden wird die Funktionsweise eines Kerberos-Systems vereinfacht dargestellt (siehe auch Abbildung 3.8). Dabei werden folgende Abkürzungen benutzt:

C – Client, IT-System von dem aus auf eine Ressource zugegriffen werden soll
Alice – auf C eingeloggter Nutzer
 A_{Alice} – Authentikator, der die Authentizität von Alice nachweist (enthält Name und IP-Adresse von C und einen Zeitstempel)
KDC – Key Distribution Center, zuständig für die Vergabe und Überprüfung von Schlüsseln
TGS – Ticket Granting Server, stellt bei gültigem Nachweis der Authentizität von Alice Tickets für Ressourcen her
R – Ressource, auf die aktuell zugegriffen werden soll
 $MK_{\text{Alice}}, MK_{\text{TGS}}, MK_{\text{R}}$ – Masterschlüssel von Alice, TGS bzw. R
 $K_{\text{Alice,TGS}}, K_{\text{Alice,R}}$ – Sitzungsschlüssel von Alice und TGS bzw. Alice und R
 $T_{\text{Alice,TGS}}, T_{\text{Alice,R}}$ – Ticket für die Anfrage des TGS bzw. den Zugriff auf R durch Alice (enthält Name des beanspruchten Servers und des Anfragenden, seine IP-Adresse, Zeitstempel, Anfangs- und Endwert der Lebenszeit des Tickets und den Sitzungsschlüssel von C und R)

Vereinfachte Funktionsweise (Nummerierung entspricht den Schritten in Abbildung 3.8):

1. Der Client C stellt eine Anfrage an KDC. Diese Nachricht enthält den Namen des Benutzers, der von C (Alice) zugreifen will und die Ressource auf die C als nächstes zugreifen will, den TGS (Ticket Granting Server).
2. Ist Alice registriert, stellt der KDC ein Ticket für den TGS aus, welches mit dem geheimen Schlüssel MK_{TGS} des TGS verschlüsselt ist. Zusätzlich wird der vom KDC erzeugte Sitzungsschlüssel $K_{\text{Alice,TGS}}$ für die Kommunikation zwischen Alice und TGS mit dem Masterpasswort MK_{Alice} von Alice verschlüsselt. Beide Daten werden dann an C übertragen.
3. Der Client C schickt dann eine Nachricht an TGS, der einen Authentikator A_{Alice} der Anfragenden (Alice) enthält, verschlüsselt mit dem Sitzungsschlüssel $K_{\text{Alice,TGS}}$ von Alice und TGS. Dieser weißt die Authentizität von C nach. Weiter enthält die Nachricht das mit dem Masterpasswort MK_{TGS} des TGS verschlüsselte Ticket und die ID der beanspruchten Ressource R.
4. Das Ticket wird vom TGS mit seinem Schlüssel entschlüsselt, damit verfügt TGS jetzt ebenfalls über den gemeinsamen Sitzungsschlüssel $K_{\text{Alice,TGS}}$ mit Alice. Mit diesem wird der Authentikator entschlüsselt und über dessen Zeitstempel die Aktualität überprüft. Ist dieser gültig, wird ein Sitzungsschlüssel $K_{\text{Alice,R}}$ für Alice und die angeforderte Ressource und ein Ticket $T_{\text{Alice,R}}$ zum Zugriff auf diese erzeugt. Der Schlüssel wird mit dem Sitzungsschlüssel $K_{\text{Alice,TGS}}$, das Ticket mit dem Masterschlüssel MK_{R} der Ressource verschlüsselt. Beide Chiffre werden an C geschickt.
5. Das gerade erzeugte Ticket wird an R übertragen und kann von R mit dem eigenen Masterpasswort entschlüsselt werden. R gewährt Alice entsprechend den Angaben im Ticket Zugriff.

Ein tieferer Einblick in die Funktionsweise von Kerberos-Systemen wird unter anderem von Eckert in [Ecke2008] gegeben.

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.6.1 Kerberos
▶ 3.6.2 LDAP
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.6.2 LDAP

LDAP (Lightweight Directory Access Protocol) ist eine Client-Server-Anwendung, die bei Verzeichnisdiensten zum Einsatz kommt. Es beschreibt die Kommunikation zwischen einem LDAP-Client und einem LDAP-Server. Letzter stellt eine Verzeichnisstruktur zur Verfügung, aus der über Anfragen Informationen ausgelesen werden können. Diese Informationen können beispielsweise Adressen sein. Ein solches Adressverzeichnis kann die Personeninformationen zu einer E-Mailadresse ausgeben, wenn es zu dieser vom Client angefragt wird. Das Protokoll stellt alle für die Funktionalität wichtigen Kommandos bereit. Diese ermöglichen die Anmeldung am Server, die Suchanfragen und die Modifikation der Daten. In neueren Versionen besteht auch die Möglichkeit, Daten zwischen verschiedenen Verzeichnissen zu synchronisieren.

Detaillierte Informationen zu LDAP sind zum Beispiel hier zu finden [LDAP2009].

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
▶ 3.7 Positionsbasierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

3.7 Positionsbasierte Authentifizierung

Es gibt auch Ansätze, die Authentifizierung über den Standort einer Person durchzuführen. Danning und MacDoran [DeMa1996] beschreiben beispielsweise ein System zur Benutzerauthentifizierung, welches auf dem Global Positioning System (GPS) basiert. GPS kann eine Position auf wenige Meter und einige Millisekunden genau feststellen. Der physische Standort einer Person wird durch eine Positionssignatur beschrieben, die von den GPS-Satelliten stammt. Sie ist einzigartig durch die Position und die Zeit zu ihrer Erfassung. Die Signatur wird übertragen, um einen Nutzer zu authentifizieren. Der Host verfügt über einen eigenen Sensor zur Bestimmung der Signatur (location signature sensor – LSS) und ermittelt eine entsprechende Signatur für den Standort des Nutzers. Unterscheiden sich die Signaturen von GPS-Signal und von LSS voneinander, schlägt der Authentifizierungsversuch fehl. Stimmen sie überein, war die Authentifizierung erfolgreich und die Person erhält Zugang zum gesicherten System. Für den Fall, dass der Sensor gestohlen wird, müsste sich der Dieb für einen Angriff geografisch innerhalb eines autorisierten Bereiches befinden. Sollte eine Positionssignatur abgefangen werden, ist eine Verwendung innerhalb des sehr kurzen Zeitfensters, in dem sie gültig ist (wenige Millisekunden), nicht möglich. Eine räumliche Einschränkung der Möglichkeit zur Authentifizierung, zum Beispiel auf ein Gebäude oder eine Stadt, ist mit diesem System ebenfalls möglich.

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
▶ Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Verständnisfragen



Verständnisfragen 3

1. Handelt es sich bei einem mit einem Stift auf einen Zettel geschriebenen Passwort um:

Geheimes Wissen

persönlichen
Besitz

Biometrie

2. Womit muss gerechnet werden, wenn man biometrische Verfahren kombiniert?

Längere Laufzeit des biometrischen Systems

Höhere Anforderungen an den Nutzer bei der Bedienung des Systems

Verschlechterung der Erkennungsgenauigkeit

3. Welche Verfahren zur Benutzerauthentifizierung werden beim Bezahlen an der Kasse eines Supermarktes per EC-Karte und Geheimzahl genutzt?

Geheimes Wissen

Persönlicher
Besitz

Biometrie

4. Single-Sign-On bedeutet in der IT:

Das Verwenden des gleichen Passwortes für die Logins verschiedener Anwendungen/Dienste/etc.

Das einmalige Einloggen zur Nutzung mehrerer Anwendungen/Dienste/etc.



IT Sicherheit

Bearbeitungshinweise

Literaturempfehlungen

1 Einführung und organisatorische Sicherheit

2 Datenschutz und Nicht-technische Datensicherheit

3 Identity Management

3.1 Grundlagen der Benutzerauthentifizierung

3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.

3.3 Besitzbasierte Authentifizierung: Smartcards & RFID

3.4 Biometrische Authentifizierung

3.5 Multifaktorielle Authentifizierung

3.6 Single-Sign-On Systeme

3.7 Positionsbasierte Authentifizierung

Verständnisfragen

► Einsendeaufgaben

Abkürzungen und Bezeichner

Referenzen

4 Angewandte IT Sicherheit

5 Praktische IT Sicherheit

Stichwortverzeichnis

Einsendeaufgaben

Aufgabe 3.1 Benutzerauthentifizierung

Benennen und erläutern Sie die drei grundlegenden Benutzerauthentifizierungsmethoden!

Aufgabe 3.2 Benutzerauthentifizierung

Erläutern Sie die Begriffe Authentifikation, Verifikation, Identifikation und Autorisierung und grenzen Sie sie voneinander ab.

Aufgabe 3.3 Benutzerauthentifizierung

In der nachfolgenden Tabelle sind in den Spalten 2-5 die drei gebräuchlichsten Authentifizierungsmethoden aufgeführt. Geben sie zu jeder Zeile jeweils mindestens eine Antwort.

	geheimes Wissen	persönlicher Besitz	Biometrie
Möglichkeiten des Verlustes			
Übertragung an eine andere Person			
Ersatz des Authentifizierungsobjektes			
Beispiele			

Aufgabe 3.4 Biometrische Benutzerauthentifizierung

Nennen Sie 5 biometrische Modalitäten, auf die nicht detailliert im Script eingegangen wurde und ordnen Sie sie den Klassen statisch und dynamisch zu und erläutern Sie kurz Ihre Entscheidung.

Aufgabe 3.5 Biometrische Benutzerauthentifizierung

Wählen Sie 5 biometrische Modalitäten und geben Sie jeweils eine mögliche Kombination der Modalität mit geheimem Wissen an. Erläutern Sie jeweils kurz, ob die von Ihnen gewählte Kombination einfach oder schwer umzusetzen ist.

Aufgabe 3.6 Biometrische Benutzerauthentifizierung

Kann die Handschrift in der Biometrie als statische und als dynamische Modalität angesehen werden? Begründen Sie Ihre Antwort.

Aufgabe 3.7 Kerberos

Kerberos basiert auf der Annahme, dass sich die Server einer Infrastruktur gegenseitig vertrauen. Welchen Einfluss auf Sicherheit des Gesamtsystems hat es, wenn

- Der Authentication Server kompromittiert wird
- Der Ticket-Granting Server kompromittiert wird
- Ein Dienst-Server kompromittiert wird

Aufgabe 3.8 Kerberos

Welche Folgen hat es für die Verfügbarkeit, wenn in einer Kerberos-Umgebung:

- Der Authentication Server ausfällt
- Der Ticket-Granting Server ausfällt
- Ein Server eines Dienstes ausfällt

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
► Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Abkürzungen und Bezeichner



Abkürzungen und Bezeichner 3

A - Authentikator (Kerberos)
 C - Client (Kerberos)
 c - Geheimtext, Chiffretext (Kryptographie)
 D - Entschlüsselungsfunktion, Decryption (Kryptographie)
 E - Verschlüsselungsfunktion, Encryption (Kryptographie)
 GPS - Global Positioning System
 K - Schlüssel (Kryptographie)
 KDC - Key Distribution Center (Kerberos)
 LDAP – Lightweight Directory Access Protocol
 m - Klartext, Nachricht, Message (Kryptographie)
 MK - Masterschlüssel, Masterkey (Kerberos)
 PIN - Persönliche Identifikationsnummer
 R - Ressource (Kerberos)
 RFID - Radio Frequency Identification
 T - Ticket (Kerberos)
 TGS - Ticket Granting Server (Kerberos)

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
3.1 Grundlagen der Benutzerauthentifizierung
3.2 Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
3.3 Besitzbasierte Authentifizierung: Smartcards & RFID
3.4 Biometrische Authentifizierung
3.5 Multifaktorielle Authentifizierung
3.6 Single-Sign-On Systeme
3.7 Positions-basierte Authentifizierung
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Referenzen



Konferenzbeiträge, Beiträge in Zeitschriften, Bücher

[Bish2005] Matt Bishop: Introduction to Computer Security; Addison-Wesley, Boston, ISBN 0-321-24744-2; 2005

[DeMa1996] Dorothy E. Denning, Peter F. MacDoran: Location-Based Authentication: Grounding Cyberspace for Better Security; Computer Fraud & Security, February 1996, Elsevier Science Ltd.

[Ecke2008] Claudia Eckert: IT-Sicherheit, Oldenbourg-Verlag, 2008

[RoNJ2006] A. Ross, K. Nandakumar, A.K. Jain, "Handbook of Multibiometrics". Springer-Verlag New York, 2006

[ScVD2005] Tobias Scheidat, Claus Vielhauer, Jana Dittmann: Distance-Level Fusion Strategies for Online Signature Verification; In: Proceedings of the IEEE International Conference on Multimedia and Expo (ICME); Amsterdam, The Netherlands, 2005, ISBN: 0-7803-9332-5

[Viel2006] Claus Vielhauer: Biometric User Authentication for IT Security: From Fundamentals to Handwriting, Springer, New York, 2006



Online-Referenzen

An dieser Stelle wird darauf hingewiesen, dass es bei Online-Angeboten immer zu Korrekturen kommen kann, bei denen sich die Adresse bzw. die Verfügbarkeit bestimmter Inhalte kurzfristig ändern kann.

[Bromba2009a] Biometrie FAQ, <http://www.bromba.com/faq/biofaqd.htm>, Letzter Aufruf: 12.06.2009

[Bromba2009b] Fingerprint FAQ, <http://www.bromba.com/faq/biofaqd.htm>, Letzter Aufruf: 12.06.2009

[KritKat2006] Kriterienkatalog – TeleTrust Deutschland e.V., <http://www.teletrust.org/publikationen/fachartikel/kriterienkatalog/>, Letzter Aufruf: 12.06.2009

[LDAP2009] LDAP Howtos, LDAP Links, LDAP Whitepapers (DNS, BIND Nameserver, DHCP, LDAP and Directory Services), <http://www.bind9.net/ldap>, Letzter Aufruf: 17.06.2009



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
▶ 4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.2 Einführung in die Mediensicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4 Angewandte IT Sicherheit

Die Verwendung von digitalen Medien in fast allen alltäglichen Bereichen bringt neben vielen unbestreitbaren Vorteilen auch neue Nachteile mit sich, die analoge Medien nicht haben. Solche Nachteile können beispielsweise durch Schadsoftware (siehe auch Abschnitt 1.3.1 Programme mit Schadensfunktion) entstehen oder dadurch, dass Kopien möglich sind, die von den Originalen in Qualität bzw. Funktionalität nicht zu unterscheiden sind. Weiter bieten vernetzte IT-Systeme meist viele Schwachstellen, die für Angriffe ausgenutzt werden können. Oft ist es schwer, festzustellen, ob bzw. was auf einem solchen System gestohlen (z.B. unerlaubte Kopien sensibler Daten) oder zerstört wurde (z.B. Löschen von wichtigen Daten). Ziel der IT Sicherheit ist es, Schwachstellen zu entdecken und zu schließen, aber auch, festzustellen was hat der Angreifer auf dem System getan und wer war der Angreifer.

Mit diesen Teilbereichen der IT-Sicherheit befassen sich die IT-Forensik und die Mediensicherheit, zu denen in den folgenden beiden Abschnitten jeweils eine Einführung gegeben wird.



Lernziele

Der vierte Teil befasst sich mit angewandter IT-Sicherheit und gibt dabei Einblicke in die Bereiche der IT-Forensik und der Mediensicherheit. Der Abschnitt IT-Forensik beschäftigt sich schwerpunktmäßig mit der Gegenüberstellung von Online und Post-Mortem Analyse, dem forensischen Vorgehensmodell nach Casey und einer Auswahl von computerforensischen Werkzeugen. Im Rahmen der Mediensicherheit werden dem Studierenden unterschiedliche Mechanismen wie das Erreichen von Anonymität durch Mixen, Steganographie und Wasserzeichenverfahren nahe gebracht.



Informationen zu Lerneinheit 4

Lerneinheit 4

Bearbeitungszeitraum: Modulwoche 11 - 14

Bearbeitungsdauer: 4 Woche / 12 Stunden

Verständnisfragen

Anzahl: 4

Einsendeaufgaben

Anzahl: 7

Bearbeitungszeitraum: Modulwoche 11 - 14

Bearbeitungsdauer: 4 Wochen / 8 Stunden



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
▶ 4.1 Einführung in die IT Forensik
4.1.1 Online vs. Post-Mortem Analyse
4.1.2 Das forensische Vorgehensmodell nach Casey
4.1.3 Computerforensische Werkzeuge
4.2 Einführung in die Mediensicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4.1 Einführung in die IT Forensik

Die gerichtsverwertbare Beweissicherung von Daten auf IT-Systemen und in Netzwerken wird als IT-Forensik bezeichnet. Dazu müssen digitale Spuren gesichert, analysiert und ausgewertet werden. Der Fokus liegt in diesem Abschnitt auf der IT-Forensik, die sich allgemein mit der Untersuchung von Daten befasst, die auf dem angegriffenen als auch dem IT-System des Angreifers zu finden sind. Der Aspekt der Netzwerkforensik, welche sich mit der Analyse von Daten beschäftigt, die im Vorfeld und Verlauf eines Sicherheitsvorfalles in einem Netzwerk aufgezeichnet wurden, wird hier nicht eingehend behandelt.

Die grundlegende Vorgehensweise bei der Untersuchung eines Vorfalles beinhaltet die folgenden Schritte:

- Sichern der Beweise, ohne dass das Original beschädigt oder verändert wird,
- Sicherstellen, dass die gesicherten Beweise und die beschlagnahmten Originale identisch sind und
- Analyse der Daten, ohne dass die Originale verändert oder beschädigt werden.

Dabei sind verschiedene Zusammenhänge zu klären, die in fünf Fragen zusammengefasst werden können:

- Was ist passiert?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?
- Wer hat es verursacht?

Um diese Fragen beantworten zu können, gibt es verschiedene Vorgehensmodelle, von denen hier eine der gebräuchlichsten beschrieben wird. Weitere Informationen findet der interessierte Leser online oder in der Literatur (z.B. [KCGN2006], [MaPP2003], [Gesc2008]). In den folgenden Abschnitten wird auf den Zeitpunkt der Analyse, ein oft verwendetes Vorgehensmodell und kurz auf spezielle Werkzeuge eingegangen.

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
▶ 4.1.1 Online vs. Post-Mortem Analyse
4.1.2 Das forensische Vorgehensmodell nach Casey
4.1.3 Computerforensische Werkzeuge
4.2 Einführung in die Mediensicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4.1.1 Online vs. Post-Mortem Analyse

Bei einer **Online Analyse** arbeitet der IT-Forensiker am laufenden IT-System, um Informationen sicherzustellen, die nach dem Ausschalten des IT-Systems nicht mehr zur Verfügung stehen. Dies kann beispielsweise notwendig sein, wenn der Inhalt des Arbeitsspeichers gesichert oder direkt analysiert werden muss, da dieser beim Ausschalten des Systems verloren geht und damit potentielle Beweise.

Eine **Post-Mortem Analyse** basiert auf den einem Duplikat eines sichergestellten Datenträgers und wird nach dem eigentlichen Angriff durchgeführt. Zur Erstellung eines solchen Duplikates wird eine bitweise Kopie des Datenträgers erstellt. Für die eigentliche Untersuchung können je nach Bedarf beliebig viele digitale Kopien erstellt werden, mit denen der IT Forensiker in Ruhe und ohne versehentliche Zerstörung des Originals arbeiten kann.

[« Vorheriges](#) | [Nächste »](#)



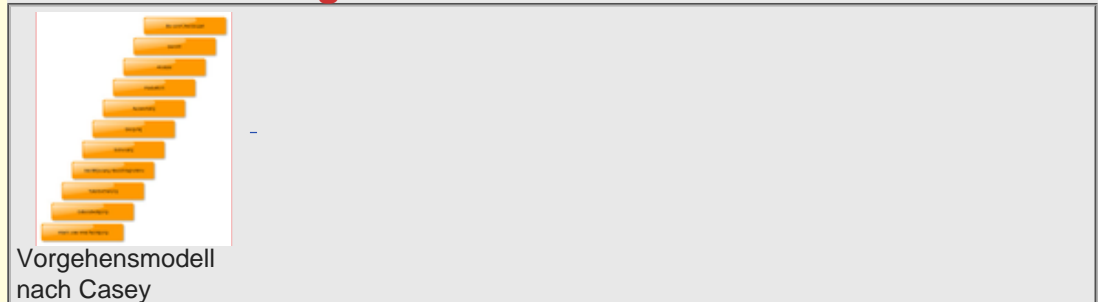
IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.1.1 Online vs. Post-Mortem Analyse
▶ 4.1.2 Das forensische Vorgehensmodell nach Casey
4.1.3 Computerforensische Werkzeuge
4.2 Einführung in die Mediensicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4.1.2 Das forensische Vorgehensmodell nach Casey

Das forensische Vorgehensmodell nach Casey stellt eine Auflistung von Arbeitsschritten zur Durchführung von digitalen Untersuchungen dar (siehe auch [Case2004]). Dabei werden nicht nur die eigentlichen Aufgaben eines IT-Forensikers berücksichtigt, sondern auch die Aufgaben eines polizeilichen Ermittlungsbeamten am Tatort. Dieses Modell stellt einen de facto Standard dar. Es besteht aus elf Phasen, welche als Treppe dargestellt werden (siehe Abbildung 4.1).



Abbildung 4.1



In den nachfolgenden Abschnitten wird auf die einzelnen Stufen eingegangen, um die Vorgehensweise beispielhaft zu demonstrieren.

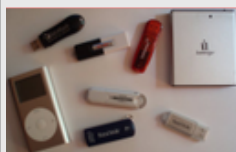
- Alarm und Anschuldigung:** Der Vorgang der Untersuchung beginnt mit der Meldung eines Vorfalles. Dafür sollten an der entgegennehmenden Stelle Vorkehrungen getroffen werden, um bestimmte Informationen aufzunehmen. Von Bedeutung können hier beispielsweise Informationen über die Art des Angriffes sein, z.B. um was für ein IT-System handelt es sich.
- Güterabwägung:** In dieser Stufe wird abgeschätzt, ob sich, verglichen mit dem entstandenen Schaden, der Aufwand und die Kosten einer Verfolgung lohnen. Gegen eine Verfolgung sprechen in der Praxis einerseits oft ein hoher Ressourcenverbrauch, die zu erwartende Dauer des Ausfalls des betreffenden IT-Systems oder negative Medienberichte über den Vorfall. Auf der anderen Seite kann ein Interesse an der Verfolgung bestehen, zum Beispiel mit den Zielen Abschreckung, Erlangung von Schadenersatz oder Verbesserung der Sicherheit durch Abwehr beziehungsweise Vermeidung künftiger Vorfälle.
- Tatortsicherung:** Im Idealfall sollte der Tatort weiträumig abgesperrt werden. Leider kann dieser im Fall der IT-Sicherheit auch Netzwerke wie Intra- und Internet betreffen. Hier ist ein Absperrern natürlich nicht oder nur sehr begrenzt möglich. Am Tatort sollten alle brauchbaren Spuren gesichert werden, dabei sollte man sich nicht nur auf digitale Spuren beschränken sondern auch auf herkömmliche forensische Hinweise achten, die bei der digitalen Untersuchung hilfreich sein könnten.
- Beschlagnahme:** Es müssen alle digitalen Geräte die am Tatort vorgefunden werden mitgenommen werden. Dabei sollte man sich nicht auf Computer beschränken, sondern auch periphere Hardware berücksichtigen. Das für die Beschlagnahme an IT-Tatorten zuständige Personal muss für diesen Fall gesondert geschult werden, um es in die Lage zu versetzen, die für den IT-Forensiker relevanten Geräte zu erkennen, fachgerecht am Tatort zu entfernen und mitzunehmen. Abbildung 4.2 zeigt beispielsweise eine kleine Auswahl verschiedener Speichermedien, die an einen handelsüblichen Computer per USB-Port angeschlossen werden können. Diese können dazu verwendet werden, um Schadsoftware auf bzw. sensible Daten von einem Computer zu kopieren oder um Software zu starten, ohne etwas an der aktuellen Software oder der Konfiguration auf dem betreffenden Computer zu verändern. Abbildung 4.3 zeigt einen IT-Arbeitsplatz mit Peripheriegeräten, Dokumenten und Datenträgern, die bei der Beschlagnahme zu berücksichtigen sind. Leitfäden zur Untersuchung von IT-Tatorten sind für den interessierten Leser unter anderem in [NIJ2008] und [USDJ2002] zu finden.
- Sicherung:** In diesem Bereich muss sichergestellt werden, dass die Beweise nach ihrer

Beschlagnahme unverändert bleiben, um einerseits deren Beweiskraft zu erhalten und andererseits eine Untersuchung durch den IT-Forensiker zu ermöglichen. Dazu werden Kopien von Datenträgern und gegebenenfalls Abbilder von Speicherinhalten erstellt. Um sicherzustellen, dass die originalen Daten die Grundlage der Untersuchung waren, werden von Original und Kopien kryptographische Hash-Werte (siehe auch Abschnitt 5.2) erstellt. Zur Erhaltung der Beweiskraft der Untersuchung sollte der IT-Forensiker vertrauenswürdige Tools verwenden. Das bedeutet, dass diese in der Community der IT-Forensik anerkannt sind und deren Funktionalität bekannt ist.

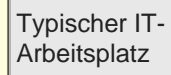
6. **Bergung:** Dieser Schritt beinhaltet die Wiederherstellung von Daten, die gelöscht, versteckt, getarnt oder auf andere Weise unbrauchbar gemacht wurden. An dieser Stelle können andere Beweismittel sehr hilfreich sein, die am Tatort sichergestellt wurden, beispielsweise Notizzettel mit Passwörtern für Betriebssysteme oder verschlüsselte Dateien.
7. **Auswertung:** Da die sichergestellten Daten in den meisten Fällen sehr umfangreich sind, müssen diese für die Untersuchungen organisiert werden. Hilfreich können an dieser Stelle der Hash-Wert und die Metadaten von Dateien sein, nach denen diese geordnet werden können. Dazu können beispielsweise Dateityp oder Datum/Uhrzeit (Erstellung, letzte Änderung, letzter Zugriff) verwendet werden.
8. **Reduktion:** In dieser Stufe wird die Menge der vorhandenen Daten auf die wesentlichen Informationen reduziert. Dazu kann zum Beispiel wiederum die Dateierweiterung herangezogen werden. Ist man auf der Suche nach bestimmten Dateien, kann die Untersuchung auf die entsprechenden Typen eingeschränkt werden (z.B. unter der Anschuldigung auf Besitz von Kinderpornographie könnten dies Bilddateien wie *.GIF oder *.JPG sein). Eine gute Hilfe sind dabei Datenbanken mit Hash-Werten von bekannten Dateien. In diesem Fall können automatisiert Hash-Werte der verdächtigen Dateien erstellt und mit den in der Datenbank gespeicherten Hashes verglichen werden. Wurden allerdings (geringfügige) Änderungen an den Dateien vorgenommen, ändert sich auch der Hash und ein automatischer Vergleich ist nicht mehr möglich. Spezielle Informationen über Dateien werden im NIST National Software Reference Library (NSRL) Project (siehe [NIST2009]) gesammelt, um Untersuchungen im Bereich Computerkriminalität zu unterstützen.
9. **Analyse:** Die Analyse von gefundenen Informationen beinhaltet als wichtigen Aspekt das Herstellen von Verbindungen zu anderen Informationen und Personen und das Feststellen von Verantwortlichkeiten. Dazu werden auch Inhalt und Kontext der untersuchten Informationen betrachtet. Weiterhin können Experimente durchgeführt werden, um undokumentiertes Verhalten nachzuvollziehen bzw. neue Methoden zu entwickeln. Im Allgemeinen ist dieser Analyseschritt nicht-linear und aufwändig. Als hilfreich bei der Analyse hat sich eine neue Organisation der Daten nach der Reduktion erwiesen, die oft auf der Anfertigung von Indizes und Übersichten basiert.
10. **Bericht:** Im Bericht werden die Ergebnisse präsentiert und die Wege zu deren Erlangung dokumentiert. Dabei wird der Dokumentation, welche (anerkannten) Standards und Regeln verwendet wurden, eine hohe Bedeutung zugemessen. Gezogene Schlüsse sollten verständlich und nachvollziehbar begründet und alternative Erklärungsmodelle erörtert werden.
11. **Bezeugen:** Die Tätigkeiten des Bezeugens und Überzeugens kann von Seiten des IT-Forensikers zum einen darin liegen, dass er als Gutachter vor Gericht aussagt. Auf der anderen Seite können sie sich auf Gespräche mit dem Auftraggeber beschränken, um ihn über die Ursachen, den/die Verantwortlichen, den angerichteten Schaden, die zu erwartenden Kosten und Maßnahmen zur Verhinderung zukünftiger Vorfälle zu informieren.



Abbildung 4.2



Auswahl von USB-Speichermedien



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.1.1 Online vs. Post-Mortem Analyse
4.1.2 Das forensische Vorgehensmodell nach Casey
▶ 4.1.3 Computerforensische Werkzeuge
4.2 Einführung in die Mediensicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4.1.3 Computerforensische Werkzeuge

In der IT Forensik werden neben speziellen kommerziellen Werkzeugen auch Tools eingesetzt, die bereits vom Betriebssystem angeboten werden oder als Freeware oder Open Source Software verfügbar sind. Dieser Abschnitt soll einen kleinen Einblick geben, welche Werkzeuge verfügbar sind und wozu man diese einsetzen kann. Dabei gibt es einige Werkzeuge, die bereits vom Betriebssystem zur Verfügung gestellt werden (z.B. fdisk). Tabelle 4.1 stellt eine Auswahl frei verfügbarer beziehungsweise mit den Betriebssystemen Linux oder Windows mitgelieferter Tools dar, die für grundlegende IT-forensische Datensicherung und Untersuchungen verwendet werden können. Detaillierte Informationen sind in den jeweiligen Dokumentationen zu finden.



Tabelle 4.1

Computerforensische Werkzeuge

Einordnung	Name
Administrative Werkzeuge	Linux: fdisk, fsck, tar, etc. Windows: fdisk, chkdsk, etc.
Laufwerksbackup	Linux: Dd, dcfldd, AIR, Grab Windows: Dd, SafeBack, truelmage
Forensische Werkzeuge	Linux: The Coroner's Toolkit, Sleuthkit Windows: EnCase, ILook
Textsuche	Linux: strings, grep Windows: strings, dtSearch, textSearch
Dateiwiederherstellung	Linux: dcat & icat, foremost, lazarus Windows: UnErase, R-Undelete, Restorer
Hex-Editoren	Linux: ht, khexedit Windows: Diskedit, Hex Workshop, WinHex
Netzwerkforensik	Linux, Windows: Wireshark, Snort, netstat
Bootfähige CDs	Knoppix, Sleuthkit, F.I.R.E., Helix
RAM-Analyse	Dumpchk, dd, memdump

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
▶ 4.2 Einführung in die Mediensicherheit
4.2.1 Anonymität mit Mixen
4.2.2 Steganographie und Wasserzeichenverfahren
Verständnisfragen
Einsendaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4.2 Einführung in die Mediensicherheit

Beim Surfen im Internet hinterlässt der Nutzer Datenspuren, beispielsweise in Form von Logdateien, die verschiedene Möglichkeiten der Auswertung ermöglichen. Es gibt verschiedenen Strategien, die Rückschließbarkeit auf den einzelnen Nutzer zu verhindern. Eine solche so genannte Anonymisierung macht beispielsweise Sinn bei Online-Beratungsangeboten (z.B. Seelsorge, Bürgerberatungsbüro), bei Review-Prozessen zur Auswahl von wissenschaftlichen Artikeln zur Veröffentlichung oder bei Abstimmungen beziehungsweise Wahlen.

Das Kopieren von digitalen Mediendaten ist in der Regel sehr einfach und, im Gegensatz zu analogen Medien (z.B. VHS-Videos), ohne Verlust von Informationen, Qualität und Funktionalität möglich. Hersteller digitaler Medien sehen darin ein großes Problem und die Ursache für den Rückgang von Gewinnen. Weiterhin ermöglicht eine Vielzahl von Tools die Manipulation digitaler Medien (z.B. Bilder, Videos). Dabei sind die Entdeckung und der Nachweis der Manipulation meist unmöglich oder sehr schwierig.

[« Vorheriges](#) | [Nächste »](#)



4.2.1 Anonymität mit Mixen

Ziele der Vermeidung der Rückschließbarkeit auf eine bestimmte Person bei der Nutzung des Internets können mit den folgenden Begriffen beschrieben werden:

- **Unbeobachtbarkeit:** Ein Beobachter kann nicht erkennen, wer die Daten sendet bzw. empfängt.
- **Anonymität:** Bei der Auswertung aller Ereignisse kann ein Beobachter die Identität der an der Kommunikation beteiligten Personen nicht feststellen.
- **Unverkettbarkeit:** Die Verkettung von Ereignissen bezüglich eines Merkmals ist für einen Beobachter nicht möglich.
- **Pseudonymität:** Eine Person tritt unter einem anderen Namen auf.
- **Modell eines mächtigen Angreifers:** Dieser mächtige Angreifer ist in der Lage, (zumindest theoretisch) alle Verbindungen im Netz zu beobachten.

Tabelle 4.2 zeigt Informationen, die der Betreiber einer besuchten Webseite auslesen kann (ermittelt auf <http://www.anonym-surfen.com/anonym-surfen/test/>, letzter Aufruf: 20.06.2009). Basierend auf diesen Angaben und dem Einsatz von Cookies ist es möglich, das Surf-Verhalten eines Nutzers zu beobachten und zu protokollieren. Einige Webseiten nutzen diese Informationen beispielsweise, um einen Besucher wieder zu erkennen mit dem Ziel, ihm die Webseite entsprechend vermeintlicher Vorlieben oder der aktuellen Konfiguration seines Computers zu präsentieren. Es lassen sich aber auch Benutzerprofile anlegen, die zusätzlich zu den in Tabelle 4.2 angegebenen Informationen das Klick- oder Konsumverhalten der Anwender erfassen. Dies ermöglicht beispielsweise bekannte Angaben in Online-Shops wie „Kunden die diesen Artikel gekauft haben, haben sich auch für die Artikel A, B und C interessiert.“ Oder „Sie haben Artikel X bei uns gekauft, daher könnte Artikel Y ebenfalls für Sie von Interesse sein.“



Tabelle 4.2

Beim Internet-Surfen erfasste Daten

Schlüssel	Wert	Info
Daten des aktuellen Servers		
IP	82.165.106.227	IP-Adresse des Servers
Datum	24.08.2009 11:59 Uhr	Aktuelles Datum auf dem Server. Wichtig um den genauen Verlauf Ihres Besuches festhalten zu können.
Daten über Sie		
IP	88.51.127.101	Dies ist Ihre aktuelle IP Adresse über die Sie auf verschiedenen Projekten wiedererkannt werden können.
Auflösung	1280*1024 Pixel	Ihre aktuelle Bildschirmauflösung. Kann Aufschluss über Ihren Monitor (z.B. Flachbild) geben.
ActiveX	deaktiviert	Über Microsofts Browsererweiterung ActiveX sind zahlreiche Sicherheitslücken bekannt. Es sollte zwingend deaktiviert sein.
JavaScript	aktiviert	Ca. 98% der Internetnutzer haben JavaScript aktiviert.

Betriebs-system	Windows XP	Das Betriebssystem steckt in der Signatur Ihres Besuches.
Browser	Opera	Der Browser ebenso.
Akzeptanz	text/html application/xml;q=0.9 application/xhtml+xml image/png image/jpeg image/gif image/x-bitmap */*;q=0.1	Sog. Mime-Types die Ihr Browser unterstützt (z.B. durch Plugins).
Provider		Dies ist Ihr Zugangsprovider über den Sie in das Internet gehen.
Proxy	keiner	Falls Sie über einen Proxy / LAN in das Internet gehen.
Ihr Host	annamaria.cs.uni-magdeburg.de	Der Hostname den Sie von Ihrem Provider zugeteilt bekommen haben. Er wechselt bei jedem neuen Verbindungsaufbau, sofern Sie keine feste IP Adresse besitzen.
Besuchte Seiten	3	So viele Seiten haben Sie bisher mit dieser Browserinstanz betrachtet.
Onlinezeit	undefined	So lange sind Sie nun mit dieser Browserinstanz online.

Eine Möglichkeit, Kommunikationsbeziehungen vor der Beobachtung durch eine dritte Partei zu sichern, stellt die Verwendung von Anonymisierungsmethoden dar. Durch das Umleiten der zu transferierenden Daten über Zwischenstationen und deren Verschlüsselung über einen Teil des Weges, schützen solche Methoden die Kommunikation.

Proxies zur Anonymisierung

Eine relative einfache und schnelle Möglichkeit zur Einschränkung der Beobachtbarkeit stellt die Verwendung von so genannten anonymisierenden Proxy-Servern dar. Diese Dienste werden mit einem normalen Browser über eine Adresse (z.B. <http://anonymouse.org/>, <http://behidden.com/>, letzter Aufruf: 20.06.2009) aufgerufen. Die vom Nutzer gewünschte Adresse wird dann in ein Webformular eingegeben und der anonymisierende Proxy ruft die entsprechende Webseite mit seinen eigenen Angaben auf. Auf diese Weise erhält der Server der abgerufenen Webseite keine Informationen über die Person, die die Seite nutzt. Ein Hauptproblem anonymisierender Proxies ist, dass der Betreiber sowohl die IP-Adresse des Nutzers als auch das Ziel kennt und diese protokollieren kann. Ein weiterer Nachteil ist, dass anonymisierende Proxies keinen Schutz vor einem mächtigen Angreifer bilden. Überwacht dieser alle bzw. große Teile des Internets, verfügt er über die Information, zu welchem Zeitpunkt eine Anfrage über einen anonymisierenden Proxy gestellt wurde. Weiter kennt der mächtige Angreifer auch den Zeitpunkt, zu dem ein Nutzer eine Anfrage an den Proxy gestellt hat. Leitet dieser die Anfrage unmittelbar weiter, kann der mächtige Angreifer beide Informationen miteinander verbinden. Ein wichtiger Vorteil der anonymisierenden Proxies ist, dass keine Installation von Software notwendig ist, da die Dienste von einem beliebigen Webbrowser aus aufgerufen werden können.

VPN-Anonymisierer

VPN-Anonymisierer basieren auf dem gleichen Konzept wie anonymisierende Proxies, erfordern allerdings

die Installation einer speziellen Software. Diese stellt eine verschlüsselte Verbindung zu einem Proxy-Server auf. Vorteil dieser Methode ist, dass die Daten zwischen dem IT-System des Nutzers und dem anonymisierenden Proxy verschlüsselt ausgetauscht werden. Dadurch erhält der Internet-Service-Provider keine Informationen über die übertragenden Daten. Allerdings bleiben die bei den anonymisierenden Proxies beschriebenen Nachteile bestehen.

Mixe

Die so genannten Mixe stellen eine Weiterentwicklung der anonymisierenden Proxies dar und umgehen deren angesprochenen Nachteile. Als Mix wird eine Zwischenstation bei der Übertragung von Daten bezeichnet. Um die Möglichkeit der Beobachtung und Verknüpfung der eingehenden und ausgehenden Daten durch einen mächtigen Angreifer zu verhindern, sammelt ein Mix die eingehenden Daten. Diese werden dann umkodiert, mit dem Ziel einer Zuordnung der Daten mittels ihres Aussehens entgegenzuwirken. Die Verschlüsselung wird mittels öffentlichen Schlüssels des Mixes (siehe auch Exkurs Asymmetrische Verschlüsselung in Abschnitt 5.2) durchgeführt. Der Mix kann mit seinem privaten Schlüssel die eingehenden Nachrichten entschlüsseln und diese gemeinsam mit anderen Nachrichten weiterleiten. Um das Problem des Vertrauens zu lösen, werden alle Nachrichten durch eine Folge von Mixen transportiert. Die Nachrichten werden dann von jedem Mix umkodiert und neu gemischt. Dazu müssen die Nachrichten vor dem Versenden mit den jeweiligen öffentlichen Schlüsseln der zu durchlaufenden Mixe verschlüsselt werden. Übertragen auf den herkömmlichen Postweg kann man sich diesen Vorgang so vorstellen: Der Absender legt seine Nachricht in einen Briefumschlag, der an eine Zwischenstation adressiert ist, diesen legt er in einen weiteren entsprechend adressierten Umschlag usw. Die aktuell adressierte Zwischenstation entfernt den an sich gerichteten Umschlag und findet einen neuen Umschlag vor, der an die nächste Station adressiert ist. Nur die letzte Station, also der Empfänger, kann den letzten Umschlag öffnen und die Nachricht verwenden. Die Verwendung von Mixen zur Anonymisierung erfordert die Verwendung von speziellen Programmen auf dem IT-System des Anwenders. Bekannte leistungsfähige Anonymisierungsdienste auf Basis der Mix-Technik sind beispielsweise JAP (Java Anon Proxy, <http://anon.inf.tu-dresden.de/index.html>, letzter Aufruf: 20.06.2009) und TOR (<https://www.torproject.org/>, letzter Aufruf: 20.06.2009).



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.2 Einführung in die Mediensicherheit
4.2.1 Anonymität mit Mixen
4.2.2 Steganographie und Wasserzeichenverfahren
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

4.2.2 Steganographie und Wasserzeichenverfahren

Wie bereits in der Einleitung dieses Kapitels beschrieben, ist das Kopieren digitaler Medien im Gegensatz zu analogen Medien allgemein nicht mit einem Qualitätsverlust verbunden. Das bedeutet auch, dass Kopien der Kopien immer noch mit dem Original identisch sind.

Steganographie

Als Steganographie bezeichnet man die verdeckte Übertragung von Informationen. Versendet Alice eine Nachricht an Bob unter der Verwendung steganographischer Verfahren, würde Eve als Beobachter der Kommunikation zwar den Austausch von Daten bemerken, die Übertragung der eigentlich verdeckten Information würde ihr jedoch verborgen bleiben.

Eine gute Möglichkeit, Informationen bei ihrer Übertragung zu verstecken, bieten beispielsweise Dateien mit einem gewissen Grad an Irrelevanz und Redundanz. Diese können genutzt werden, um Informationen einzubetten. Dies müssen nicht zwangsläufig geheime Nachrichten sein, andere Anwendungsbereiche sind hier zum Beispiel im Bereich von digitalen Bildern, Videos oder Musik Angaben über das Copyright, Zeitpunkt der Aufnahme oder Seriennummer des Aufzeichnungsgerätes.

Der Einbettalgorithmus bringt die geheim zu haltenden Informationen in das Trägermedium ein (siehe auch Abbildung 4.4). Dabei wird ein symmetrischer Schlüssel verwendet, was zur Folge hat, dass die eingebetteten Daten nur ausgelesen werden können, wenn der Empfänger den Schlüssel kennt. Dieser nutzt den Auslesealgorithmus, um die versteckte Information zu extrahieren.

Damit ein steganographisches Verfahren sinnvoll nutzbar ist, muss es die folgenden zwei Voraussetzungen erfüllen:

Nicht-Detektierbarkeit: Das Vorhandensein der eingebetteten Daten darf nicht detektierbar sein, beispielsweise durch Anwendung verschiedener statistischer Analysen auf das Trägermedium ohne und mit eingebetteter Information.

Hohe Kapazität: Die Kapazität beschreibt die Größe der Nachricht, die vom Trägermedium aufgenommen werden kann. Die maximale Kapazität wird von der Nicht-Detektierbarkeit bestimmt.



Abbildung 4.4



Schematische
Einbett- und
Auslesevorgang bei
steganographischen
Verfahren

Steganographische Verfahren können entsprechend der zugrunde liegenden Vorgehensweise unterteilt werden:

Substitutionale Steganographie: Hier werden Bereiche im Trägermedium durch die meist verschlüsselte Nachricht ersetzt, in denen Änderungen visuell oder akustisch (je nach Trägermedium) nicht wahrgenommen werden können.

Konstruktive Steganographie: Diese Verfahren bilden Signale des Trägermediums basierend auf dem Modell des Originalsignals nach, um die Informationen einzubetten.

Eine oft eingesetzte Methode in der Steganographie stellt das LSB-Verfahren (Least Significant Bit) für RGB-Bilder dar. Dabei wird das Trägermedium verändert, indem die Informationen in das jeweils letzte Bit der Farbinformationen eingebettet werden. Dieses Verfahren bietet verglichen mit der Dateigröße eine hohe Kapazität, und die durch die Einbettung hervorgerufenen Veränderungen werden im Normalfall vom allgemein vorhandenen Bildrauschen verdeckt.

Wasserzeichenverfahren

Prinzipiell basieren Wasserzeichenalgorithmen auf steganographischen Verfahren, verfolgen jedoch eine andere Zielsetzung. Dafür existieren unterschiedliche Eigenschaften, die mittels Wasserzeichenverfahren umgesetzt werden können. Im Folgenden werden einige der wichtigsten Eigenschaften aufgelistet und jeweils kurz erläutert:

Robustheit: Die Eigenschaft, dass eingebettete Informationen wieder aus dem Trägermedium ausgelesen werden können, wird als Robustheit bezeichnet. Es stellt damit eine Widerstandsfähigkeit der eingebetteten Informationen gegenüber beabsichtigten und unbeabsichtigten Veränderungen des Trägermediums dar. Dies können beispielsweise verlustbehaftete Komprimierung, Größenveränderung, Rotation oder Formatkonvertierungen sein.

Nicht-Detektierbarkeit: Diese Eigenschaft schließt die Erkennbarkeit des Wasserzeichens aus. Das ist der Fall, wenn das markierte Trägermedium konsistent zum ursprünglichen Trägermedium ohne eingebettete Informationen ist.

Nicht-Wahrnehmbarkeit: Hier wird die visuelle bzw. akustische Wahrnehmbarkeit der eingebrachten Daten bezüglich der entsprechenden menschlichen Sinne adressiert. Das bedeutet, dass das menschliche Seh- bzw. Hörvermögen nicht in der Lage ist, zwischen originalem und markiertem Trägermedium zu unterscheiden.

Security: Als sicher (engl. secure) wird ein Wasserzeichenalgorithmus eingestuft, wenn es unmöglich ist, die eingebrachte Information zu zerstören, aufzuspüren bzw. zu fälschen. Dabei ist dem Angreifer der Algorithmus bekannt und er verfügt über mindestens eine markierte Datei aber nicht über den verwendeten Schlüssel.

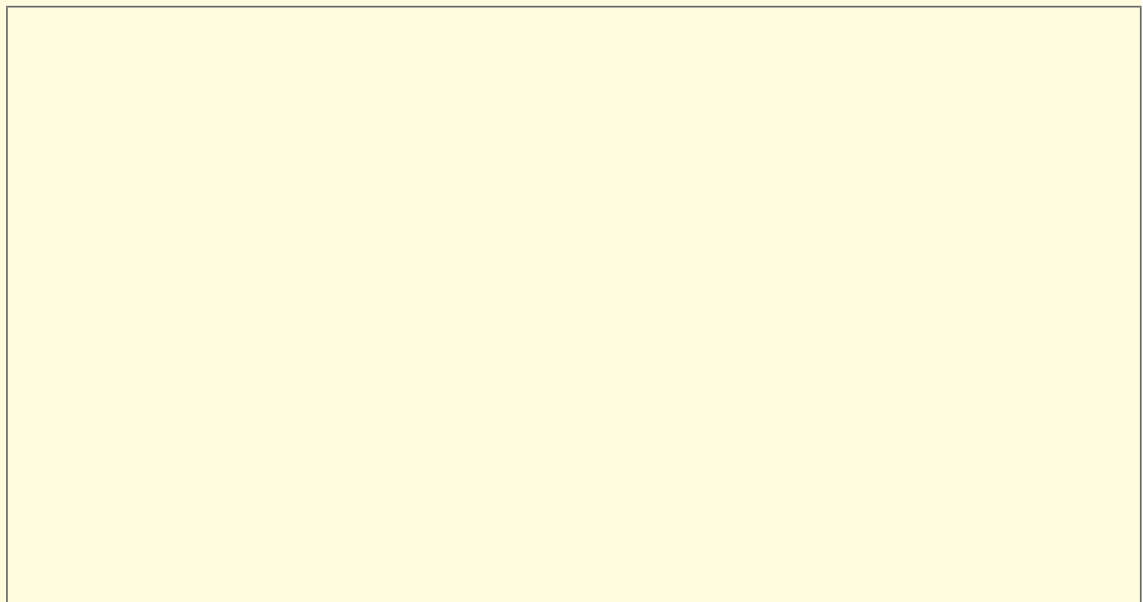
Komplexität: Der zu erbringende Aufwand zur Einbettung und zum Auslesen der Wasserzeicheninformationen, wird als Komplexität bezeichnet. Von Bedeutung ist diese Eigenschaft, wenn die Echtzeitfähigkeit des Algorithmus wichtig ist.

Kapazität: Die Kapazität gibt an, in welchem Umfang Informationen in ein Trägermedium eingebettet werden können bzw. wie viel Wasserzeichen in einem Original parallel möglich bzw. zugelassen sind.

Geheime/öffentliche Verifikation: Eine geheime Verifikation des Wasserzeichens liegt vor, wenn es nur der Urheber oder eine dedizierte Personengruppe auslesen kann. Im anderen Fall spricht man von einer öffentlichen Verifikation.

Eine gleichzeitige Optimierung aller genannten Eigenschaften ist nicht möglich. Zum Beispiel können nicht die Nicht-Detektierbarkeit, Nicht-Wahrnehmbarkeit und Robustheit optimiert werden, wenn eine große Menge an Informationen in ein Trägermedium eingebracht werden soll. Das hat zur Folge, dass für einen zu implementierenden Wasserzeichenalgorithmus ein gemeinsames Optimum der gewünschten Eigenschaften gefunden oder eine geeignete Parametrisierung der jeweiligen Eigenschaften ermöglicht werden muss.

Abbildung 4.6 zeigt das Ergebnis der Einbettung eines Wasserzeichens in das in Abbildung 4.5 dargestellte Originalbild. Dabei wurden nur in drei Bereiche des Bildes Informationen eingebettet mit dem Ziel der Nicht-Wahrnehmbarkeit. Bei der Einbettung von Informationen in Abbildung 4.8 war das Ziel die Unterbringung von möglichst viel Information. Die Störungen, die dadurch auftreten, sind deutlich mit dem bloßen Auge wahrnehmbar. Die Abbildungen 4.7 und 4.9 stellen die Differenzbilder zu den Abbildungen 4.6 beziehungsweise 4.8 dar. Änderungen zwischen dem Originalbild und den mit Wasserzeichen markierten Bildern sind dabei durch weiße Pixel dargestellt.



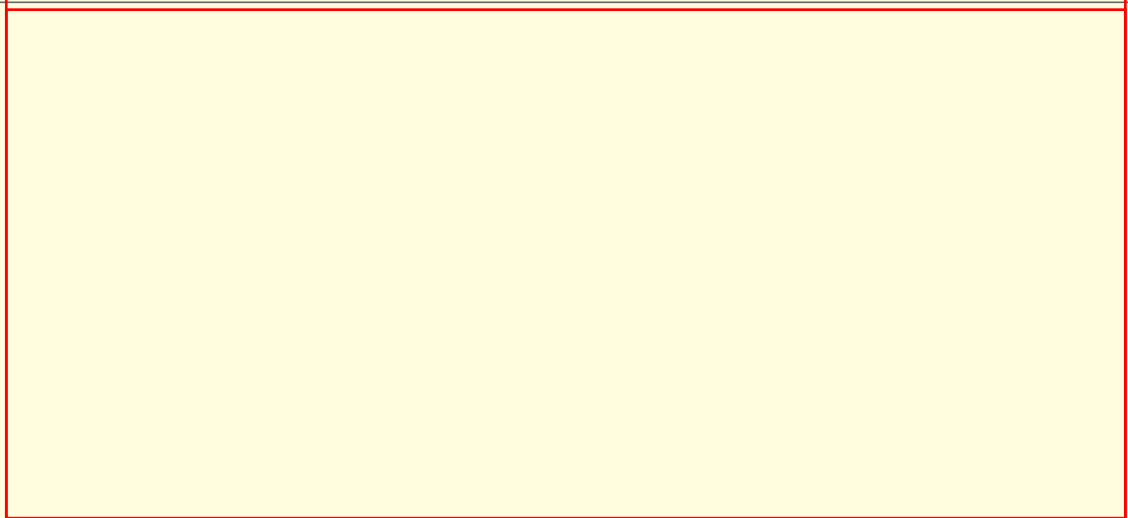
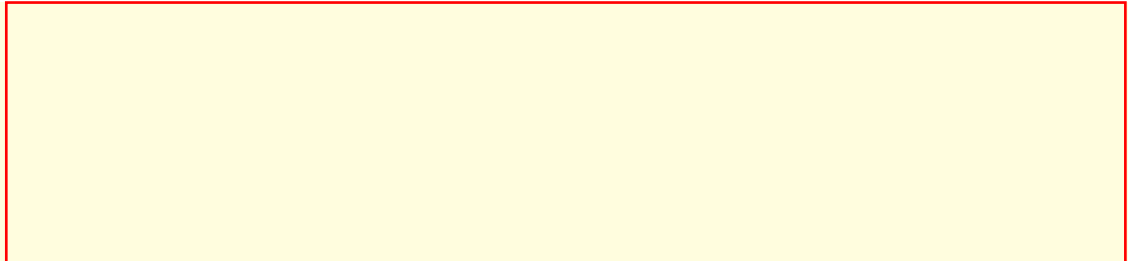


Abbildung 4.5: Originalbild



Abbildung 4.6: Markiertes Bild mit einem Wasserzeichen mit geringer Kapazität

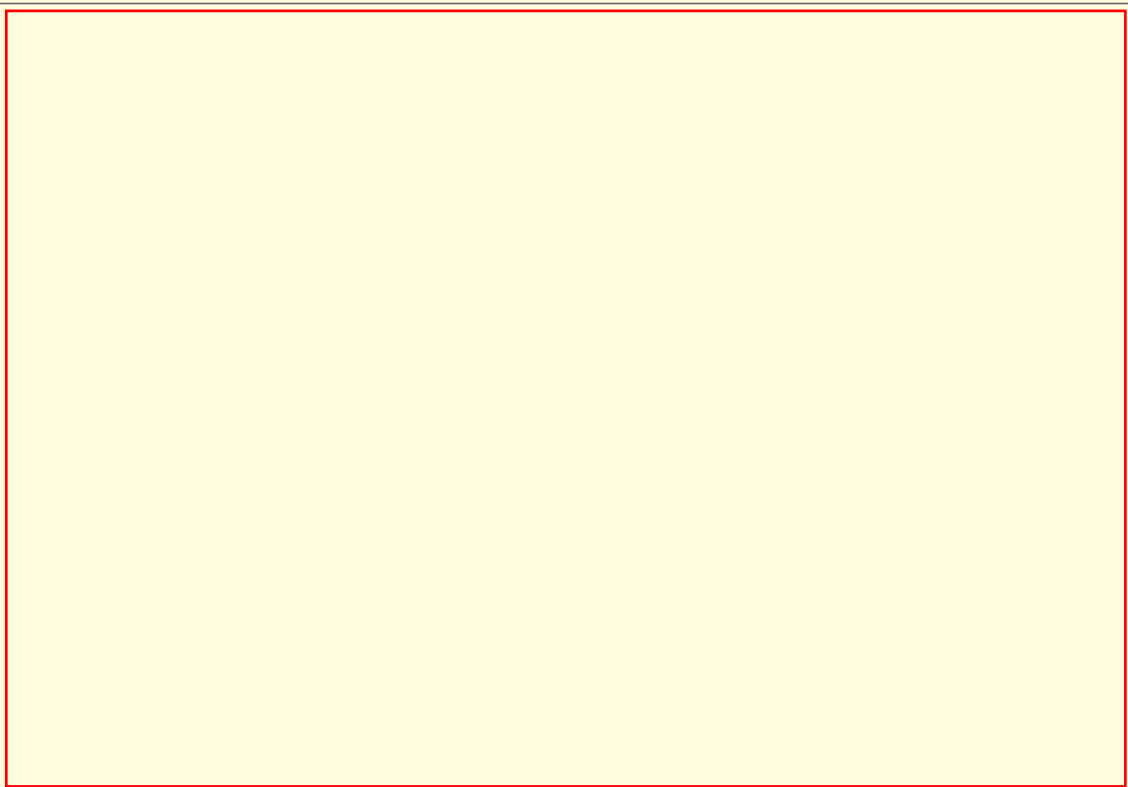


Abbildung 4.7: Differenzbild zwischen Abb. 4.5 und Abb. 4.6






Abbildung 4.8: Markiertes Bild mit einem Wasserzeichen mit hoher Kapazität

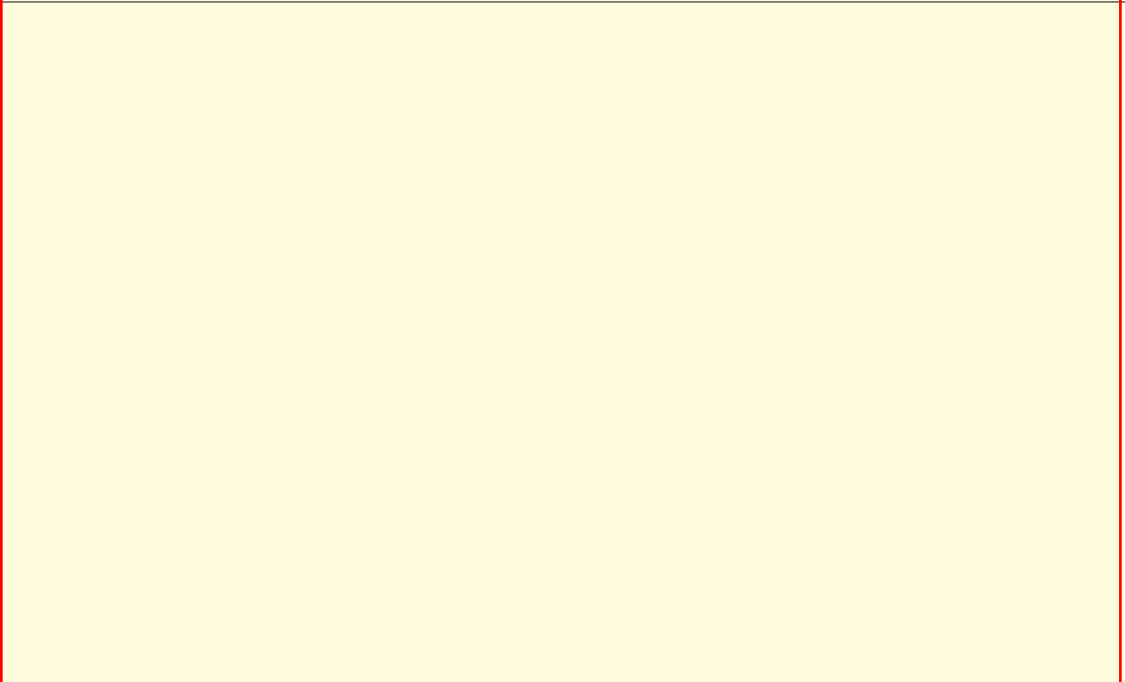


Abbildung 4.9: Differenzbild zwischen Abb. 4.5 und Abb. 4.8

Zur Vertiefung der Themen Steganographie und digitale Wasserzeichenverfahren wird der interessierte Leser an die Literatur verwiesen, zum Beispiel [Ditt2000].



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.2 Einführung in die Mediensicherheit
▶ Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

Verständnisfragen



Verständnisfragen 4

1. Ziel der IT-Forensik kann sein,

herauszufinden, welche Daten auf einem IT-System einer Firma unerlaubt kopiert wurden.

Fingerabdrücke von Kriminellen zu digitalisieren und in einer Datenbank zum automatischen Vergleich zu speichern.

digitale Hinweise auf einem zum Datendiebstahl verwendeten IT-System zu sichern.

2. Welche Informationen kann der Betreiber einer Webseite beim Besuch mittels Internet-Browser über Sie und Ihr IT-System in Erfahrung bringen?

Aktuelle IP-Adresse

Installierte Spielesoftware

Momentan laufende Anwendungssoftware

Eingestellte Auflösung des Monitors

Ob JavaScript aktiviert ist

Verwendetes Betriebssystem

Inhalte der in der aktuellen Sitzung versandten E-Mails

Name des verwendeten Internet-Browsers

Aktueller vom Provider vergebener Hostname

Datei-Anhänge der in der aktuellen Sitzung versandten E-Mails

Ob ActiveX aktiviert ist

Name und Version des Virenschanners

3. Auf welche Weise wird versucht, die Anonymität eines Nutzers zu wahren, wenn Mixe eingesetzt werden:

durch Mischen von Dateien

durch Mischen von Datenpaketen

durch Mischen von
Verzeichnisebenen

4. Alice möchte ein selbst fotografiertes Bild auf ihrer Webseite veröffentlichen. Um später gegebenenfalls nachweisen zu können, dass es von ihr stammt, bettet sie

ihren Namen, die Kamera-ID und das Aufnahmedatum ein. Handelt es sich hierbei um Steganographie oder um ein digitales Wasserzeichen?

Steganographie

Wasserzeichen



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.2 Einführung in die Mediensicherheit
Verständnisfragen
► Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

Einsendeaufgaben

Aufgabe 4.1 – IT-Forensik

Geben Sie mindestens drei Gegenstände, Geräte usw. an, die ein IT-Forensiker von einem gewöhnlichen IT-Arbeitsplatz mitnehmen sollte, wenn dieser für eine Computerstraftat genutzt wurde. Erläutern Sie jeweils, warum dieses Objekt wichtig sein könnte.

Aufgabe 4.2 – IT-Forensik

Skizzieren Sie das Vorgehensmodell nach Casey für den forensischen Prozess und identifizieren Sie die wesentlichen technischen Phasen, die für den Informatiker relevant sind.

Aufgabe 4.3 – IT-Forensik

Erläutern Sie die Begriffe „Post-Mortem Analyse“ und „Online Analyse“ sowie deren Vor- und Nachteile!

Aufgabe 4.4 – Anonymität

Erläutern Sie für jeden Schlüssel in Tabelle 4.2 des Skriptes in welchem Maße die Kenntnis des zugehörigen Wertes die Anonymität eines Nutzers beeinflussen kann.

Schlüssel	Sicherheitsrelevanz	Erklärung
IP		
Auflösung		
ActiveX		
JavaScript		
Betriebssystem		
Browser		
Akzeptanz		
Provider		
Proxy		
Ihr Host		
Besuchte Seiten		
Onlinezeit		

Aufgabe 4.5 – Mediensicherheit

Skizzieren Sie im Blockdiagramm das Prinzip von steganographischer Einbettung / digitaler Wasserzeichenverfahren.

Aufgabe 4.6 – Mediensicherheit

Durch welche Eigenschaften unterscheiden sich steganographische und Wasserzeichenverfahren?

Aufgabe 4.7 – Mediensicherheit

Welche Sicherheitsaspekte können mittels Wasserzeichen erfüllt werden, welche mittels Steganographie?

[« Vorheriges](#) | [Nächste »](#)

IT Sicherheit

Bearbeitungshinweise

Literaturempfehlungen

1 Einführung und organisatorische
Sicherheit

2 Datenschutz und Nicht-technische
Datensicherheit

3 Identity Management

4 Angewandte IT Sicherheit

4.1 Einführung in die IT Forensik

4.2 Einführung in die Mediensicherheit

Verständnisfragen

Einsendaufgaben

► Abkürzungen und Bezeichner

Referenzen

5 Praktische IT Sicherheit

Stichwortverzeichnis

Abkürzungen und Bezeichner



Abkürzungen und Bezeichner 4

NIST – National Institute of Standards and Technology

NSRL – NIST National Software Reference Library Project

VPN – Virtual Private Network

[« Vorheriges](#) | [Nächste »](#)



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
4.1 Einführung in die IT Forensik
4.2 Einführung in die Mediensicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
► Referenzen
5 Praktische IT Sicherheit
Stichwortverzeichnis

Referenzen



Konferenzbeiträge, Beiträge in Zeitschriften, Bücher

[Case2004] Eoghan Casey: Digital Evidence and Computer Crime. 2nd Ed., Academic Press, 2004

[Ditt2000] Dittmann: Sicherheit in Medienströmen - Digitale Wasserzeichen, Springer, New York, 2000

[Gesc2008] Geschonnek, Alexander: Computer-Forensik – Computerstraftaten erkennen, ermitteln, aufklären, 3., aktualisierte und erweiterte Auflage, 2008

[KCGD2006] Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang: Guide to Integrating Forensic Techniques into Incident Response, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD. NIST Special Publication 800-86, 2006

[MaPP2003] Kevin Mandia, Chris Prosise, Matt Pepe: Incident Response & Computer Forensics. 2nd Ed., McGraw-Hill, 2003



Online-Referenzen

An dieser Stelle wird darauf hingewiesen, dass es bei Online-Angeboten immer zu Korrekturen kommen kann, bei denen sich die Adresse bzw. die Verfügbarkeit bestimmter Inhalte kurzfristig ändern kann.

[NIJ2008] Electronic Crime Scene Investigation: A Guide for First Responders, <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>, April 2008, letzter Aufruf: 22.06.2009

[NIST2009] National Software Reference Library, <http://www.nsl.nist.gov/>, letzter Aufruf: 27.07.2009

[USDJ2002] United States Department of Justice: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, <http://www.cybercrime.gov/s&smanual2002.pdf>, 2002, letzter Aufruf: 24.06.2009



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
▶ 5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5 Praktische IT Sicherheit



Ziele

Die praktische IT-Sicherheit steht im Mittelpunkt des fünften Abschnittes und vermittelt Wissen zur Anwendung von gegebenen Sicherheitskonzepten sowie Ausblicke auf den kryptographischen Schutz von Informationen basierend auf dem Einsatz von speziellen Tools (z.B. Pretty Good Privacy (PGP)) oder von verschlüsselten Dateisystemen und auf die Netzwerksicherheit, wobei insbesondere auf Paketfilter und Application Level Gateways eingegangen wird.



Informationen zu Lerneinheit 5

Lerneinheit 5

Bearbeitungszeitraum: Modulwoche 15 - 17

Bearbeitungsdauer: 3 Wochen / 11 Stunden

Verständnisfragen

Anzahl: 8

Einsendeaufgaben

Anzahl: 8

Bearbeitungszeitraum: Modulwoche 15 - 16

Bearbeitungsdauer: 3 Wochen / 8 Stunden



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
▶ 5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch

Die heutige technisierte Welt ist auf vielfältige Arten von Informationen angewiesen, die generiert, gespeichert, transferiert und verarbeitet werden. Da viele Prozesse, beispielsweise im industriellen, Dienstleistungs-, kommunalen oder auch privaten Bereich, ohne IT-Technik nicht mehr durchführbar sind, ist es besonders wichtig, die Informationen als auch die entsprechende IT-Technik zu schützen. Die IT-Grundschutz-Kataloge des BSI ([BSI2009]) bieten eine strukturiert Grundlage, um den Schutz von Informationen einer Organisation sicher zu stellen. Mit der Version 2005 wurde eine Umbenennung des BSI IT-Grundschutzhandbuch in IT-Grundschutz vorgenommen. Dabei handelt es sich um einen ganzheitlichen Ansatz, bei dem basierend auf einer geeigneten Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein bestimmtes, pauschalisiertes Sicherheitsniveau erreicht werden soll. Dieser Grundschutz basiert auf einer Kombination der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2 [BSI2008a]) und den IT-Grundschutz-Katalogen ([BSI2008b]), welche Sicherheitsmaßnahmen und eine entsprechende Methodik zur Auswahl und Adaption geeigneter Maßnahmen zum sicheren Umgang mit verschiedenartigen Informationen zur Verfügung stellen. Die IT-Grundschutz-Kataloge bieten dazu verschiedene Beschreibungen von relevanten IT-Komponenten (Bausteine), Beschreibungen möglicher Gefahren (Gefährdungskataloge), erforderliche Maßnahmen (Maßnahmenkataloge) und unterschiedliche Hilfsmittel zur Umsetzung von Sicherheitsstrategien im IT-Bereich. Im Folgenden wird ein Überblick über die IT-Grundschutz-Kataloge gegeben.

Abbildung 5.1 zeigt die verschiedenen Phasen des Sicherheitsprozesses basierend auf dem IT-Grundschutz. Während der Initialisierung des Sicherheitsprozesses müssen unterschiedliche organisatorische Elemente geklärt werden. Dazu gehört die Klärung der Verantwortung der Leitungsebene, die Konzeption und Planung, die Erstellung einer Leitlinie zur Informationssicherheit, der Aufbau einer Informationssicherheitsorganisation, die Bereitstellung von Ressourcen und die Einbindung aller Mitarbeiter. Basierend darauf kann ein entsprechendes Sicherheitskonzept erstellt werden, welches den Ansprüchen der jeweiligen Organisation entspricht. Diese Konzeption muss dann umgesetzt, daran anschließend aufrechterhalten und laufend verbessert werden. Die drei zuletzt genannten Module bilden einen Kreislauf mit dem Ziel, ein hohes Sicherheitsniveau auch bei wechselnden Anforderungen oder fortschreitender Entwicklung aufrecht zu erhalten.



Abbildung 5.1



Phasen des Sicherheitsprozesses nach dem IT-Grundschutz

Bausteine

Die Bausteine des IT-Grundschutzes werden zur Modellierung der vorhandenen und zu sichernden IT-Systeme verwendet. Um eine Sicherheitskonzeption zu erstellen, ist diese

Modellierung des zugrunde liegenden IT-Systems notwendig. Dies wird im folgendem auch als Informationsverbund bezeichnet. Ein Informationsverbund kann dabei aus verschiedenen IT-Komponenten (Bausteinen) bestehen, die jeweils mindestens einmal durchlaufen werden. Abbildung 5.2 zeigt, wie Zusammenhänge zwischen den Bausteinen und den sicherheitsrelevanten Aspekten abgebildet werden. Basierend auf einem existierenden oder geplanten Informationsverbund wird eine Strukturanalyse durchgeführt, dann der erforderliche Schutzbedarf festgestellt und dann ein Modell erstellt. Dieses Modell kann einerseits als Prüfplan verwendet werden, um die Sicherheit eines existierenden Informationsverbundes zu gewährleisten. Andererseits kann das Modell auch bei der Planung und Entwicklung eines noch nicht existierenden Informationsverbundes eingesetzt werden.



Abbildung 5.2



Ergebnis der
Modellierung nach
IT-Grundschutz

Bausteine umfassen zu den betrachteten Komponenten, Vorgehensweisen und IT-Systemen jeweils eine Kurzbeschreibung und eine Sammlung von Informationen über die Gefährdungslage und die entsprechenden Maßnahmenempfehlungen. Die Bausteine sind wie folgt strukturiert:

- B 1: Übergreifende Aspekte der Informationssicherheit
- B 2: Sicherheit der Infrastruktur
- B 3: Sicherheit der IT-Systeme
- B 4: Sicherheit im Netz
- B 5: Sicherheit in Anwendungen

Um ein ausreichendes Sicherheitsniveau zu etablieren und aufrecht zu erhalten, ist ein Informationssicherheitsmanagement (auch IS-Management) notwendig. Dieses ist für die Planung und Durchführung der Maßnahmen zur Sicherung der Informationen und der damit verbundenen IT-Technik und Prozesse zuständig. Da ein effizientes IS-Management für die Schaffung eines ausreichenden Sicherheitsniveaus unablässig ist, wird dessen Aufbau und Organisationsstruktur in B 1 beschrieben. Darüber hinaus enthält dieser Abschnitt unter anderem Informationen über organisatorische Maßnahmen, verschiedene Konzepte (bspw. zu Notfallvorsorge, Datensicherung, Kryptographie), Hard- und Software-Management und Standardsoftware.

Baustein B 2 befasst sich mit der Infrastruktur einer Organisation, die direkt mit der Sicherheit der Informationen verbunden sind. Dazu zählen zum Beispiel Gebäude, spezielle Räumlichkeiten (z.B. Büro, Serverraum) oder die elektrotechnische Verkabelung.

B 3 gruppiert die vorhandenen Arten von IT-Systemen einerseits nach ihrer Verwendung (bspw. Server, Client, Internet-PC, Laptop, Firewall). Weitere Unterteilungen werden vorgenommen bezüglich des verwendeten Betriebssystems (wie z.B. Unix, Windows). Zusätzlich werden auch Telekommunikationsanlage, Faxgeräte, Anrufbeantworter, Mobiltelefon, PDAs und Drucker, Scanner und Multifunktionsgeräte berücksichtigt.

Die verschiedenen Aspekte der Vernetzung von IT-Systemen werden in Baustein B 4 betrachtet. Gegenstand dieses Bausteins sind Heterogene Netze, Netz- und Systemmanagement, Modem, VPN, LAN-Anbindungen eines IT-Systems über ISDN, WLAN und VoIP.

Der fünfte Baustein B 5 behandelt Anwendungen, die auf IT-Systemen eingesetzt werden. Dazu gehören beispielsweise E-Mail, Webserver oder Datenbanken. Teilweise wird auch auf spezielle häufig verwendete bzw. weit verbreitete Anwendungen wie Exchange 2000/Outlook 2000 oder Apache Webserver eingegangen.

Gefährdungskataloge

Die Gefährdungskataloge enthalten ausführliche Beschreibungen von möglichen Gefahren für die einzelnen Bausteine. Basierend darauf, ob diese nicht beeinflussbar auftreten bzw. durch menschliche oder technische Fehler entstehen wird dabei zwischen den nachfolgenden Gefährdungen unterschieden:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

In Katalog G 1 werden Gefahren durch höhere Gewalt zusammengefasst. Dazu zählen neben Gefährdungen wie Blitz, Feuer, Wasser und Sturm auch der Datenverlust durch starke magnetische Felder oder starkes Licht oder Ausfall bzw. die Störung eines Funknetzes.

Organisatorische Mängel werden in G 2 abgedeckt. Dazu zählen unter anderem fehlende und unzureichende Regelungen bzw. deren unzureichende Kenntnis, ungenügende Kontrolle der IT-Sicherheitsmaßnahmen aber auch die Verwendung unsicherer Protokolle in öffentlichen Netzen. Insgesamt enthält dieser Katalog 140 Gruppen von möglichen Gefährdungen durch organisatorische Mängel.

Der Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer, die fahrlässige Zerstörung von Gerät oder Daten und die Nichtbeachtung von IT-Sicherheitsmaßnahmen sind nur wenige typische Beispiele für menschliche Fehlhandlungen. Diese sind in G 3 eingeordnet und umfassen in der aktuellen Version 92 Gruppen.

Unter technisches Versagen (siehe G 4) fallen zum Beispiel Ausfälle der (internen) Stromversorgung, der internen Versorgungsnetze, der vorhandenen Sicherheitseinrichtungen oder auch unsichere kryptographische Algorithmen. Insgesamt werden insgesamt 71 verschiedene Kategorien in diesem Katalog aufgeführt.

G 5 fasst vorsätzliche Handlungen in 145 Gruppen zusammen. Dazu zählen unter anderem Diebstahl, Vandalismus, Abhören von Räumen, verschiedene Typen von Programmen mit Schadensfunktion oder der unberechtigte Anschluss von IT-Systemen an ein Netz.

Maßnahmenkataloge

Die Maßnahmenkataloge empfehlen geeignete Schritte zur Verhinderung von Gefahren bzw. zur Reaktion auf bereits eingetretene Vorfälle. Diese Maßnahmen sind wie folgt strukturiert:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

Der erste Maßnahmenkatalog (M 1) umfasst Anweisungen die den Bereich der Infrastruktur einer Organisation betreffen und ist in 69 Kategorien gegliedert. Es werden beispielsweise Maßnahmen zu Blitzschutzeinrichtungen, Einbruchsschutz, Klimatisierung oder Videoüberwachung gegeben.

Die empfohlenen organisatorischen Maßnahmen werden unter M 2 in 430 Gruppen unterteilt angegeben. Dazu zählen Schritte wie die Verwaltung von Betriebsmitteln oder Datenträgern, die Vergabe bestimmter Rechte (z.B. Zutritt, Zugang, Zugriff) oder ein Nutzungsverbot für nicht freigegebene Hard- und Software.

In M 2 werden Maßnahmen in Bezug auf das Personal gegeben. Unter anderem fallen darunter Schulungen, Einweisungen bzw. Einarbeitung der Mitarbeiter bezüglich der Bedienung der verschiedenen IT-Komponenten wie beispielsweise Hard- und Software. Dieser Katalog ist aufgeteilt in 66 Kategorien.

Konkrete Hinweise zur Abwehr von Gefahren bzgl. der Hard- und Software werden im Katalog M 3 in 324 Kategorien aufgelistet. Wesentliche Punkte dabei sind beispielsweise der geeignete

Passwortschutz für verschiedene IT-Systeme, die Verwendung von Bildschirmsperren, der regelmäßige Einsatz eines Anti-Viren-Programms oder der geeignete Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern.

Unter dem Begriff Kommunikation werden im Katalog M 4 Maßnahmen in Bezug auf verschiedenartige Vernetzung von IT-Systemen empfohlen, welche in 150 Gruppen unterteilt wurden. Diese Maßnahmen befassen sich zum Beispiel mit der Netzverwaltung, der Rechtevergabe, der Absicherung von Remote-Zugängen oder der sicheren Konfiguration von Mail-Clients.

Der sechste Maßnahmenkatalog M 6 stellt Empfehlungen zur Vorsorge von Notfällen in 109 Kategorien zusammen. Dazu zählen etwa die Erstellung einer Übersicht über Verfügbarkeitsanforderungen bezüglich der IT-Komponenten einer Organisation, die Definition des Begriffes Notfall und die Festlegung des Verantwortlichen bei dessen Eintreten oder das Abschließen geeigneter Versicherungen.

Hilfsmittel

Weiterhin enthält der IT-Grundschutz unterschiedliche Hilfsmittel. Dazu gehören Checklisten und Formulare, Muster und Beispiele, IT-Grundschutz-Beispielprofile, Dokumentationen und Studien, Informationen externer Anwender und ein Archiv mit älteren Informationen, die trotz nicht aktuellem technischen Stand auch weiterhin Gültigkeit haben.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
▶ 5.2 Ausblick kryptographischer Schutz
5.2.1 Pretty Good Privacy (PGP)
5.2.2 Verschlüsselte Dateisysteme
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.2 Ausblick kryptographischer Schutz

Dieser Abschnitt beschäftigt sich mit Anwendungen basierend auf kryptographischen Verfahren. Um das Verständnis der Unterabschnitte 5.2.1 und 5.2.2 zu ermöglichen, wird vorher ein kurzer Überblick über relevante kryptographische Verfahren gegeben.

Bereits im vorhergehenden Kapitel wurde ein Exkurs zur symmetrischen Verschlüsselung von Informationen gegeben. Wichtige Aspekte waren dabei, dass die Informationen mittels eines geheimen Schlüssels codiert wurden, die nur mit demselben Schlüssel wieder decodiert werden können. Das bedeutet, dass jeder an einer Kommunikation berechtigter Beteiligter über diesen Schlüssel verfügen muss und diesen auch geheim halten muss. Aus dieser Konstellation ergibt sich das Problem der sicheren Verteilung der Schlüssel an den Personenkreis, der Zugang zu einer verschlüsselten Nachricht erhalten soll. Im folgenden wird als Alternative die asymmetrische Verschlüsselung erläutert.



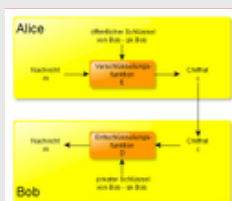
Exkurs: Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung wird ein individuelles Schlüsselpaar von jedem beteiligten Kommunikationspartner verwendet. Bei den Schlüsselpaaren wird zwischen einem **geheimen** (engl. **secret Key**, sk) und einem **öffentlichen Schlüssel** (engl. **public Key**, pk) unterschieden. Während der secret Key vom Besitzer geheim zu halten ist, ist der public Key über eine öffentlich zugängliche Datenbank für jeden frei verfügbar. Abbildung 5.3 zeigt ein vereinfachtes Schema der asymmetrischen Verschlüsselung. Alice möchte Bob eine vertrauliche Nachricht m zukommen lassen. Zur Verschlüsselung des Klartextes m nutzt sie die Codierungsfunktion E mit dem public Key von Bob (pk_{Bob}) und versendet die verschlüsselte Nachricht c an Bob. Um die empfangene Nachricht lesen zu können, muss Bob diese vorher mittels Decodierungsfunktion D und seinem secret Key (sk_{Bob}) entschlüsseln.

Ein großer Vorteil der asymmetrischen gegenüber der symmetrischen Verschlüsselung liegt darin, dass keine Schlüssel zwischen den Kommunikationspartnern ausgetauscht werden müssen. Wichtig ist dabei allerdings die Authentizität des public Key. In unserem Beispiel muss also sichergestellt werden, dass der public Key auch wirklich Bob gehört und nicht durch einen Angreifer durch dessen public Key ausgetauscht wurde.



Abbildung 5.3



Schematische Darstellung einer asymmetrischen Verschlüsselung

Verbreitete Verfahren für die Asymmetrische Verschlüsselung sind das RSA-Verfahren (benannt nach den Entwicklern Ronald L. Rivest, Adi Shamir und Leonard Adleman) und das

Elgamal-Verfahren. Bei RSA hängen die Schlüssel von einem Paar großer Primzahlen ab, welche im Normalfall mehr als 100 Stellen besitzen. Daher beruht die Sicherheit des Verfahrens auf der Schwierigkeit der Faktorisierung großer Zahlen. Die Sicherheit von RSA konnte bisher weder bewiesen noch widerlegt werden.

Ein Problem asymmetrischer Verschlüsselung stellt vor allem bei großen Datenmengen der rechnerische Aufwand dar. Symmetrische Systeme sind zwar in den meisten Fällen sehr schnell, hier besteht aber das Problem des sicheren Schlüsselaustausches. Bei der Kombination beider Verfahren zu so genannten hybriden Verschlüsselungssystemen sollen Nachteile beider Verfahren umgangen und Vorteile genutzt werden. Das folgende Beispiel beschreibt eine hybride Verschlüsselung zum sicheren Austausch eines symmetrischen Schlüssels.



Beispiel 5.1

Hybride Verschlüsselung zum sicheren Austausch eines symmetrischen Schlüssels

Wir nutzen an dieser Stelle wieder das bekannte Szenario, in dem Alice Bob eine geheime Nachricht m schicken will. Die Verschlüsselung der Nachricht soll dabei symmetrisch erfolgen. Im ersten Schritt muss Alice also Bob den symmetrischen Schlüssel k zukommen lassen. Wie in Abbildung 5.4 im ersten Schritt dargestellt, verwendet Alice den öffentlichen Schlüssel von Bob (pk_{Bob}), um den symmetrischen Schlüssel k mittels asymmetrischer Verschlüsselung E_a zu codieren. Das Ergebnis stellt c_k dar. c_k wird dann an Bob gesendet. Bob kann dann mit seinem geheimen Schlüssel sk_{Bob} und der asymmetrischen Dekodier-Funktion D_a den symmetrischen Schlüssel k wieder herstellen. Im zweiten Schritt codiert Alice die Nachricht m mit dem gemeinsamen Schlüssel k und der symmetrischen Codier-Funktion C_s zum Geheimtext c_m und sendet diesen an Bob. Da Bob über den Schlüssel k verfügt, kann er die Nachricht mit diesem und der symmetrischen Dekodier-Funktion D_s entschlüsseln und lesen.



Abbildung 5.4



Hybride
Verschlüsselung
zum sicheren
Austausch eines
symmetrischen
Schlüssels

Da in der IT und der IT-Sicherheit, hier vor allem beim Umgang mit Passwörtern und in der Kryptographie, häufig Hash-Funktionen verwendet werden, wird im folgenden Exkurs näher darauf eingegangen.



Exkurs: Hash-Funktionen

Hash-Funktionen sind Einwegfunktionen, die Eingabedaten einer nicht festgelegten Größe

auf Ausgabedaten mit fixer Länge abbilden, wobei eine Umkehrung dieser Operation nicht oder nur mit höchstem Aufwand möglich ist. Eine Hash-Funktion h muss dabei die folgenden vier Eigenschaften aufweisen:

Reproduzierbarkeit: Sind zwei Eingabewerte a und a' identisch, so sollen auch die beiden durch ein und dieselbe Hash-Funktion h berechneten Werte $h(a)$ und $h(a')$ identisch sein.

Kollisionsresistenz: Sind zwei Eingabewerte a und a' ungleich, dann müssen auch die durch eine Hash-Funktion h berechneten Hash-Werte $h(a)$ und $h(a')$ ungleich sein.

Unumkehrbarkeit: Es sollte rechnerisch nicht möglich sein, aus dem durch die Hash-Funktion h erzeugten Hash-Wert $h(a)$ wieder den Ausgangswert a zu bestimmen.

Bitsensibilität: Kleine Änderungen der Eingabedaten a sollten zu möglichst großen Veränderungen der Ausgabedaten $h(a)$ führen.

Einsatzbereiche für Hash-Funktionen sind beispielsweise die sichere Speicherung von Passwörtern oder das Erzeugen von Referenzwerten. Hash-Werte können beispielsweise aus den Passwörtern für den Anmeldevorgang eines Betriebssystems erzeugt werden, welche dann gespeichert werden. Bei der Anmeldung eines Benutzers gibt dieser seinen Benutzernamen und sein Passwort ein. Das System berechnet dann den Hash-Wert des Passwortes und vergleicht ihn mit dem zum angegebenen Nutzernamen gespeicherten Wert. Sind beide Hash-Werte identisch, wird die Person vom System zugelassen, anderenfalls wird der Zugriff verweigert. Die Erzeugung von Referenzwerten mittels Hash-Funktionen wird häufig verwendet, um sicherzustellen, dass eine zum Download angebotene Datei sich in einem vom Anbieter definierten Zustand befindet. Dazu wird der Hash-Wert der Datei berechnet und zusammen mit der Datei auf einer Webseite zur Verfügung gestellt. Ein Nutzer kann dann diese Datei herunterladen, den Hash-Wert berechnen und mit dem originalen Wert vergleichen. Sind beide Werte identisch, wurde die Datei nicht verändert. Folglich sichert diese Art der Anwendung von Hash-Funktionen die Integrität der Datei.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
▶ 5.2.1 Pretty Good Privacy (PGP)
5.2.2 Verschlüsselte Dateisysteme
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.2.1 Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) ist eine Software zum Verschlüsseln und Unterschreiben (Signieren) von Daten. Kostenlose und kommerzielle Softwarelösungen stehen für verschiedene Betriebssysteme zur Verfügung. Zum Leistungsumfang von PGP gehören Funktionen zur vertraulichen Übermittlung von eMails, zum Nachweis des Urhebers einer Nachricht über Signaturen, zur Sicherung von Authentizität und Integrität von eMails oder das Verschlüsseln von Dateien. PGP-Softwarelösungen stellen dabei nur die notwendigen kryptographischen Dienste zur Verfügung, zum Beispiel als Plug-In für gängige E-Mail-Clients.

Grundlage für PGP bieten asymmetrische Verschlüsselungsverfahren. Der öffentliche Schlüssel des Empfängers wird durch den Sender zur Verschlüsselung der Nachricht genutzt. Der Empfänger nutzt seinen privaten Schlüssel (der in der Regel durch ein Passwort geschützt wird), um die Nachricht zu entschlüsseln. Da wie schon in Abschnitt 5.2 erwähnt, die Verschlüsselung großer Datenmengen mit asymmetrischen Verfahren zu rechenintensiv ist, verwenden PGP-Softwarelösungen hybride Verschlüsselung (siehe auch Beispiel 5.1) für die Kommunikation. Zur Verschlüsselung der Daten wird ein zufällig erzeugter symmetrischer Schlüssel (Sitzungsschlüssel, engl. Session Key) verwendet, welcher durch asymmetrische Verschlüsselung geschützt versendet wird.

Die Hauptaufgaben von PGP beinhalten das Signieren von Daten und deren Verschlüsselung und Entschlüsselung:

Signatur: Um die Authentizität und Integrität einer Nachricht sicherzustellen, kann der Sender (Alice) eine so genannte digitale Signatur erstellen. Dazu wird ein Hash-Wert der zu sendenden Nachricht erstellt, der als eindeutiger Fingerabdruck der Nachricht (engl. Message Digest) angesehen werden kann. Anschließend wird die digitale Signatur erzeugt, indem der Hash-Wert mit dem privaten Schlüssel von Alice verschlüsselt wird.

Verschlüsselung: Die digitale Signatur und die Nachricht werden dann (nach einer eventuellen Komprimierung) und mit dem zufällig generierten symmetrischen Sitzungsschlüssel verschlüsselt. Der Sitzungsschlüssel wird, wie oben schon beschrieben, asymmetrisch verschlüsselt an den Empfänger (Bob) gesendet. Der aus der eigentlichen Nachricht und dem daraus berechneten Hash-Wert bestehende Geheimtext wird ebenfalls an Bob geschickt.

Entschlüsselung: Im ersten Schritt wird Bob den Sitzungsschlüssel mit seinem privaten Schlüssel decodieren. Mit ihm kann dann der Geheimtext entschlüsselt werden. Nun liegen Bob die Nachricht und deren digitale Signatur vor. Im letzten Schritt wird sichergestellt, dass die Nachricht vom angegebenen Sender kommt (Authentizität) und während der Übertragung nicht verändert wurde (Integrität). Dazu wird aus der Nachricht mittels desselben Hash-Verfahrens der Hash-Wert bestimmt und die digitale Signatur mit dem öffentlichen Schlüssel von Alice entschlüsselt. Stimmen beide Hash-Wert überein, kann Bob davon ausgehen, dass die Nachricht von Alice geschickt und nicht verändert wurde.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.2.1 Pretty Good Privacy (PGP)
▶ 5.2.2 Verschlüsselte Dateisysteme
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.2.2 Verschlüsselte Dateisysteme

Verschlüsselte Dateisysteme dienen der sicheren Speicherung von sensiblen Daten. Dabei werden die Daten in einem bestimmten Bereich hinterlegt, auf den man nur mit der entsprechenden Autorisierung Zugriff erhält. So ein Bereich kann beispielsweise eine Festplattenpartition oder ein Ordner des Dateisystems des Betriebssystems sein. Verbreitete Betriebssysteme bieten bereits Tools zur Verschlüsselung von Dateien. Windows stellt zum Beispiel in den Versionen ab Windows 2000 das EFS (Encrypting File System, deutsch verschlüsselndes Dateisystem) zur Verfügung. Damit ist es möglich, Dateien für den aktuell angemeldeten Nutzer zu verschlüsseln. Versucht ein anderer Benutzer, eine derart verschlüsselte Datei zu öffnen, ist dies nicht möglich. Unter Linux ist ebenfalls die Arbeit mit verschlüsselten Dateisystemen mit Tools wie beispielsweise Cryptoloop oder Loop-aes möglich.

Es gibt zwei generelle Möglichkeiten der Nutzung von verschlüsselten Dateisystemen: die Betriebssystem-Ebene und die Anwendungsebene. Während im erst genannten Fall das verschlüsselte Dateisystem Teil des vorhandenen Dateisystems ist und vom Betriebssystem selbst verwaltet wird, wird bei der zweiten Möglichkeit das Dateisystem simuliert. Letzteres hat den Vorteil, dass das verschlüsselte Dateisystem portabel und teilweise plattformunabhängig (erforderliche Treiber und Software vorausgesetzt) genutzt werden kann.

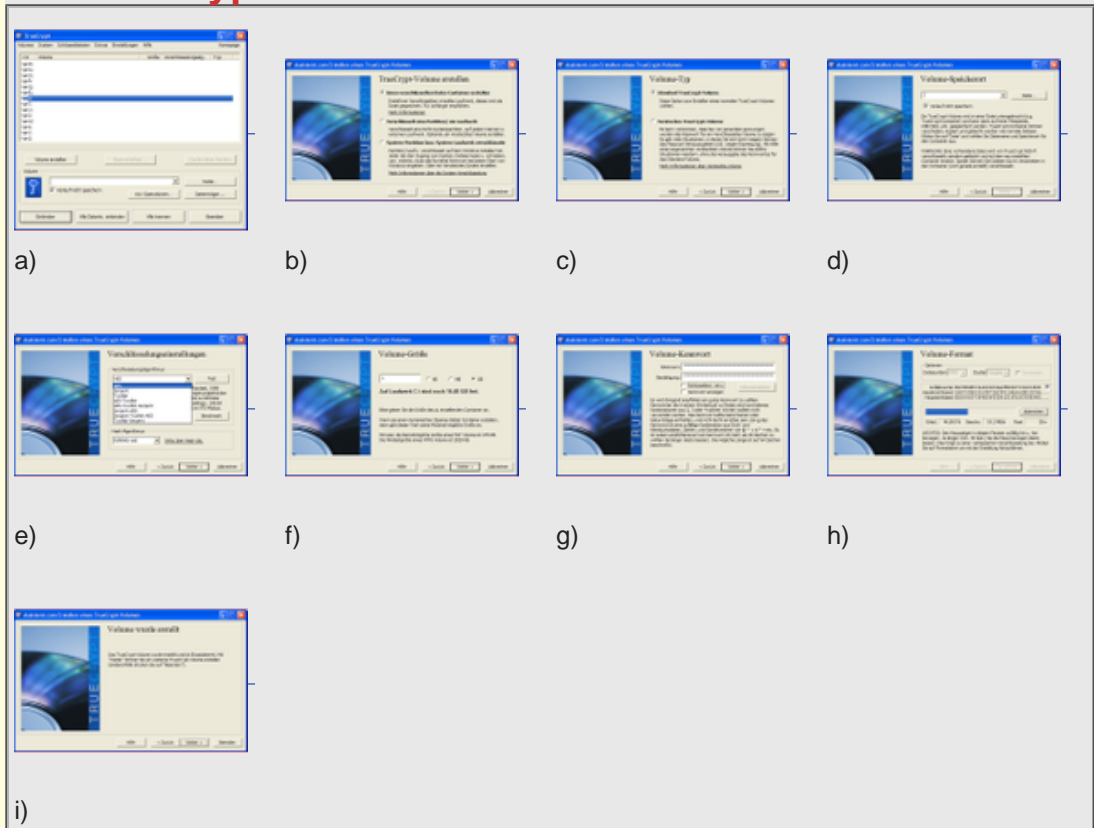
Im Folgenden wird beispielhaft das Anlegen und anschließende Öffnen eines verschlüsselten Dateisystems mittels TrueCrypt (siehe [True2009]) gezeigt. TrueCrypt ist eine OpenSource-Software zur Erstellung, Nutzung und Verwaltung von verschlüsselten Dateisystemen, die auf so genannten Containern basieren. Ein Container ist eine einzelne verschlüsselte Datei, in der das Programm ein Dateisystem verwaltet. Diese Container sollten verwendet werden, wenn sie auf einer ansonsten unverschlüsselten Partition oder zum mobilen Einsatz verwendet werden sollen. Diese Container werden beim Öffnen unter Windows und Mac OS X als zusätzliches Laufwerk und unter Linux und Mac OS X als Ordner angezeigt. Eine andere Möglichkeit, auf die hier nicht weiter eingegangen werden soll, ist das Anlegen einer verschlüsselten Partition. Bei beiden Varianten werden Daten beim Lesen und Schreiben für den Nutzer transparent (engl. On-The-Fly) ent- bzw. verschlüsselt.

Nach dem Start von TrueCrypt wird das Hauptfenster angezeigt (Abbildung 5.5 a), in welchem alle verfügbaren Funktionen mittels Menü oder Buttons gestartet werden können. Zum Anlegen eines Containers wird der Button „Volume erstellen“ angeklickt, worauf sich der Assistent zum Erstellen von TrueCrypt-Containern mit dem in Abbildung 5.5 b gezeigten Fenster öffnet. An dieser Stelle muss der Anwender entscheiden, ob er einen verschlüsselten Datei-Container erstellen bzw. eine Partition oder ein System-Laufwerk bzw. eine System-Partition verschlüsseln will. Wir wählen in diesem Fenster den Datei-Container und klicken auf „weiter“. Im darauf folgenden Schritt des Assistenten (Abbildung 5.5 c) muss entschieden werden, ob ein Standard TrueCrypt-Volume oder ein verstecktes TrueCrypt-Volume erstellt werden soll. Im ersten Fall wird eine normale Datei für den Container generiert. Unter einem versteckten TrueCrypt-Volume versteht der Hersteller einen Container, der innerhalb des freien Speicherplatzes eines anderen Containers versteckt wird. Wird der Anwender beispielsweise gezwungen, sein Passwort preiszugeben und verrät nur das für den äußeren Container, so kann nur dieser geöffnet werden und der innere Container bleibt unentdeckt. Dies trägt zur Sicherheit geheimer Daten bei, wenn der äußere Container keine Dateien mit sensiblen Inhalten enthält, diese aber im inneren gespeichert werden. Wir wählen in diesem Dialog das Standard TrueCrypt-Volume, betätigen den Button „weiter“ und gelangen so in den Dialog zur Auswahl des Speicherortes und Dateinamens der Container-Datei (Abbildung 5.5 d). Dieser wird über den entsprechenden Standard-Öffnen-Dialog des Betriebssystems ausgewählt. In diesem Beispiel nutzen wir den Ordner „container“ auf dem Laufwerk C und benennen unsere Container-Datei mit „arbeit.tc“. Anschließend gelangen wir über den Button „weiter“ in den Dialog zur Auswahl der Verschlüsselungseinstellungen (Abbildung 5.5 e). In diesem Fenster kann der Algorithmus zur symmetrischen Verschlüsselung der Daten ausgewählt werden. Außerdem ist die Auswahl eines Hash-Algorithmus möglich, welcher zur Generierung von Zufallszahlen zur Erstellung der Container-Datei benötigt wird. Nach Wahl von „AES-Twofish“ zu Verschlüsselung und „RIPEMD-160“ als Hash-Algorithmus gelangen wir über den Button „weiter“ in das Fenster zur Auswahl der Größe der Container-Datei (Abbildung 5.5 f). Hier kann der Anwender entscheiden, wie groß der Speicherplatz des anzulegenden verschlüsselten Dateisystems sein soll. Grenzen werden dabei von der maximal erlaubten Dateigröße des

verwendeten Betriebssystems gesetzt. In unserem Beispiel haben wir eine Container-Dateigröße von 1 GB gewählt und setzten die Erstellung mit einem Klick auf „weiter“ fort. Im nächsten Schritt gelangen wir in den Dialog zur Angabe des gewünschten Passworts zur symmetrischen Verschlüsselung (Abbildung 5.5 g). Hier sollte ein ausreichend sicheres Passwort gewählt werden. Hinweise dazu werden im unteren Bereich des Dialog-Fensters gegeben. Zusätzlich ist es möglich, eine beliebige Datei als Schlüsseldatei zu verwenden. Das bedeutet, dass diese Datei als Ergänzung zum Passwort als zusätzlicher Schlüssel verwendet wird. Der Vorteil besteht darin, dass sowohl Passwort als auch Schlüsseldatei zum Öffnen des Containers benötigt werden. Nachteilig dabei ist, dass diese Schlüsseldatei nicht gelöscht oder verändert werden darf, da dadurch Veränderungen herbeigeführt werden. Die Erzeugung des Beispiel-Containers wurde mit einem einfachen Passwort (dreimalige Wiederholung der Ziffern 0-9) und ohne Verwendung einer Schlüsseldatei durchgeführt. Im darauf folgenden Fenster (Abbildung 5.6 h) kann das Dateisystem und die verwendete Clustergröße des Containers gewählt werden. Dieser Dialog bietet auch die Möglichkeit, die Erzeugung von Zufallszahlen für die Generierung von Zwischenschlüsseln aktiv zu beeinflussen, indem die Maus innerhalb des Fensters bewegt wird. Als Einstellung wurde für das Beispiel als Dateisystem „NTFS“ und für Cluster „Vorgabe“ gewählt. Mit einem Klick auf den Button „Formatieren“ wird die Erstellung der Container-Datei gestartet. Dies nimmt je nach gewählter Größe der Datei eine gewisse Zeit in Anspruch. Nach Abschluss der Generierung des Containers teilt der darauf folgende Dialog (Abbildung 5.5 i) die Fertigstellung mit. Geschlossen wird das Fenster auf einen Klick auf den Button „Beenden“. Damit ist der Vorgang zur Erstellung einer Container-Datei abgeschlossen.



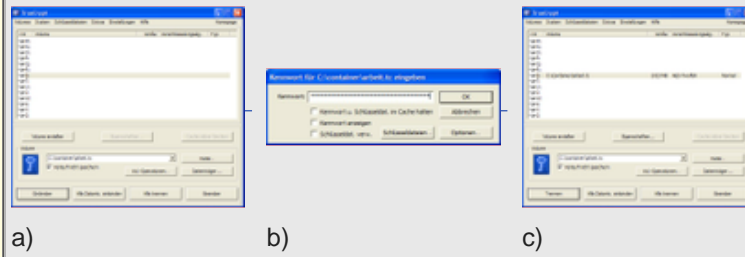
Abbildung 5.5: Erstellen einer Container-Datei mit TrueCrypt



Um die gerade erstellte Container-Datei zu nutzen, muss diese im Hauptfenster (Abbildung 5.6 a) über den Button „Datei“ geöffnet werden. Dann wird im darauf folgenden Dialog die Datei (im Beispiel „C:\container\arbeit.tc“) ausgewählt und geöffnet. Im nächsten Schritt wird ein Laufwerk gewählt, unter dem das verschlüsselte Dateisystem angesprochen werden soll. Hier ist es Laufwerk S. Anschließend wird der Button „Mount“ betätigt und es öffnet sich das Fenster zur Eingabe des Passwortes und zur Angabe einer möglicherweise verwendeten Schlüsseldatei (Abbildung 5.6 b). Sind die angegebenen Informationen korrekt, wird der Container geöffnet und dem gewählten Laufwerksbuchstaben zugewiesen (Abbildung 5.6 c). Nun kann der verschlüsselte Inhalt wie gewohnt als Laufwerk verwendet werden. Die Ver- und Entschlüsselungsvorgänge im Hintergrund laufen transparent ab und werden vom Nutzer nicht wahrgenommen.



Abbildung 5.6: Öffnen einer mit TrueCrypt erstellten Container-Datei





IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
▶ 5.3 Ausblick Netzsicherheit
5.3.1 Paketfilter
5.3.2 Application Level Gateways
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.3 Ausblick Netzsicherheit

Zur Absicherung von Netzwerken werden häufig so genannte Firewalls verwendet. Der Begriff stammt aus dem Englischen und beschreibt eine feuerfeste Wand zwischen zwei Gebäuden, wobei die Öffnungen zwischen den Gebäuden durch feuerfeste Abschlüsse verschließbar sind. In der IT-Sicherheit bezeichnet Firewall den alleinigen Übergang zwischen zwei Netzen mit unterschiedlichen Sicherheitsanforderungen (z.B. Internet und privates Heimnetzwerk). Dabei wird die Risikozone auf wenige bzw. ein einzelnes System beschränkt, welche durch Kontroll- und Überwachungsmethoden überprüft werden. Dafür werden meist mehrere Hard- und Softwarekomponenten eingesetzt, die individuell konfiguriert werden können, abhängig von der verfolgten Sicherheitsstrategie bzw. dem Sicherheitsbedarf. Personal Firewalls sind Softwarekomponenten, die auf dem zu schützenden Rechner installiert werden. Diese ermöglichen es, einzelnen Programmen und Diensten Verbindungen aufzubauen oder dies zu verbieten.

In der IT-Sicherheit wird ein Netzwerk meistens wie folgt betrachtet: Es gibt eine Innensicht, die meist aus einem einzelnen PC oder einem internen Netzwerk besteht. Die Außensicht entspricht externen PCs oder Netzwerken, die nicht von der Innensicht erfasst werden. Abbildung 5.2 stellt diese Sichtweise für einen einzelnen Heim-PC und das Internet dar. Als Schutz für den PC soll eine Firewall dienen, die in die Verbindung zwischen PC und Internet (z. B. in der DSL-Hardware) geschaltet wird. Aufgabe der Firewall ist es jeglichen Datenverkehr zu verhindern, mit Ausnahme der explizit erlaubten Kommunikation.



Abbildung 5.2



Innen- und
Außenansicht von
Netzwerken

In den folgenden Abschnitten wird einführend auf zwei Hauptmethoden bei der Umsetzung von Firewalls eingegangen, den Paketfilter und den Applikationsfilter. Dieser Abschnitt stellt nur eine kurze Einführung in den wichtigen Bereich Netzsicherheit dar. Für eine Vertiefung dieses Themas sei hier auf einschlägige Lehrmodule (z. B. zum Thema Rechner-/ Kommunikationsnetze) verwiesen.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
▶ 5.3.1 Paketfilter
5.3.2 Application Level Gateways
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.3.1 Paketfilter

Aufgabe von Paketfiltern (engl. Network Level Firewall, Screening Router) ist es, Datenpakete bei ihrer Übertragung über ein Netzwerk basierend auf vordefinierten Regeln zu filtern. Die davon betroffenen Protokolle sind IP (Internat Protocol), TCP (Transmission Control Protocol) und UDP (User Datagram Protocol). Die Entscheidung über die Weiterleitung der Datenpakete basiert dabei auf den IP-Headern der jeweils verwendeten Protokolle. Darauf aufbauend können Paketfilter Datenpakete typischerweise basierend auf den folgenden Informationen filtern:

- IP-Adresse von Absender bzw. Empfänger
- Portnummer von Absenders bzw. Empfänger
- Protokolle/Typ des Pakets (TCP, UDP)
- Flags im TCP-Header

Die Filterung der Datenpakete basiert auf drei Kernfunktionen, die aus der Auswertung der Regel und der entsprechenden Reaktion bestehen:

Pass: Diese Funktion leitet ein Datenpaket weiter, wenn keine der Regeln des Paketfilters verletzt wird.

Drop: Für den Fall, dass eine Bedingung verletzt wird, wird das entsprechende Datenpaket nicht weitergeleitet. Je nach Einstellung wird dem Empfänger eine Fehlermeldung gesendet. Als Default-Regel wird immer Drop verwendet, um unerwünscht Kommunikation auszuschließen.

Log: Die Log-Funktion protokolliert abgewiesene Pakete. Dieses Protokoll kann gegebenenfalls für das Feststellen von Angriffen (engl. Intrusion Detection) verwendet werden.

Von Vorteil sind die einfache technische Umsetzung von Paketfiltern und deren schnelle Abarbeitung der einzelnen Regeln bei geringem Ressourceneinsatz. Paketfilter werden in der Praxis meistens nur als Vorfilter für andere Schutzmaßnahmen eingesetzt. Ein Nachteil des Verfahrens liegt darin, dass Protokolle, die gleichzeitig mehr als eine logische TCP-Verbindung nutzen (z.B. FTP, H323), Probleme bereiten. Auch ist eine Täuschung des Paketfilters durch die Manipulation von IP-Fragmenten möglich, beispielsweise durch das Vortäuschen einer falschen Portnummer. Ein wesentlicher Nachteil ist, dass die Daten nicht nach Inhalt gefiltert werden können, was zur Folge hat, dass die Übertragung von Schadsoftware, z.B. durch E-Mail-Anhänge, nicht erkannt und abgewiesen werden kann.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
5.3.1 Paketfilter
▶ 5.3.2 Application Level Gateways
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

5.3.2 Application Level Gateways

Applikationsfilter (engl. Application Level Gateways) bestehen aus einer oder mehreren Softwarekomponenten, die den Austausch von Informationen über bestimmte Protokolle auf Anwendungsebene kontrollieren können. Sie verfügen also über Kenntnisse bezüglich der jeweiligen Applikation, für die die Informationen gefiltert werden sollen. Daher sind sie in der Lage, anwendungsspezifische Kontrollen durchzuführen. Das bedeutet auch, dass Applikationsfilter auch die Kontrolle des gesendeten Inhalts ermöglichen. So können beispielsweise Kommandos gefiltert werden, die aus Sicherheitsgründen für die entsprechende Applikation nicht zugelassen sind. Dazu ist es allerdings erforderlich, dass Applikationsfilter für die Inhaltsprüfung eine Vielzahl von Netzwerkdatenpaketen zu logischen Datenobjekten zusammenfügen, auf welchen dann die Sicherheitskontrollen durchgeführt und ggf. Schutzmaßnahmen eingeleitet werden. So muss z.B. bei einem Dateidownload durch einen PC im internen Netz der Applikationsfilter zunächst alle zu der angeforderten Datei gehörigen Datenpakete einsammeln, in der richtigen Reihenfolge anordnen, die Dateiinhalte aus den Datenpaketen dekodieren und kann dann erst eine Kontrolle (z.B. durch Virens Scanner) durchführen. Falls die Kontrolle keinen Verdacht auf schadhafte Inhalte liefert, muss anschließend das Applikationsfilter dann den umgekehrten Prozess durchführen, d.h. die Dateidaten wieder in Datenpakete kodieren und diese schließlich durch die Netzwerkschnittstelle an den anfordernden PC weiterleiten. Da somit offensichtlich die Kontrolle bei Applikationsfilter auf Anwendungsebene durchgeführt wird, im Gegensatz zu Paketfiltern, wo dies auf Datenpaketebene erfolgt, erklärt sich die Namensgebung Applikationsfilter. In der Netzwerktechnik spricht man im Übrigen auch von Layer 5-7 Filterung für Applikationsfilter, bzw. Layer 3-4 für Paketfilter, Bezug nehmend auf das so genannte ISO/OSI Schichtenmodell für Rechnernetze.

Ein Nachteil der Applikationsfilter ist, dass sie sehr aufwändig konfiguriert werden müssen und sehr rechenintensiv sind. Zu den Vorteilen der Applikationsfilter gehört neben der inhaltsbasierten Prüfmöglichkeit zudem die Möglichkeit der Durchführung differenzierter Authentifikationen und Überprüfungen. Weiterhin ermöglichen sie die frühzeitige Erkennung auffälliger Zugriffsmuster und erkennen so Angriffsversuche auch den zu schützenden Bereich. Als Konsequenz können dann weitere zukünftige Zugriffe des jeweiligen Nutzers automatisch blockiert werden. Applikationsfilter ermöglichen auch die anwendungsspezifische Protokollierung von Zugriffen. Eine Nutzungsmöglichkeit stellt hier die Abrechnung von Dienstleistungen dar, die in Anspruch genommen wurden. Wie gerade dargelegt, kann ein Applikationsfilter auch mit so genannter Proxy-Funktionalität verbunden werden, das bedeutet, häufig angefragte Inhalte werden vom Applikationsfilter/Proxy zwischengespeichert und müssen nicht aus dem externen Netz geladen werden.



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
▶ Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

Verständnisfragen



Verständnisfragen 5

1. Welche Ziele werden mit dem IT-Grundschutz des BSI verfolgt?

Modellierung einer Sicherheitsrichtlinie

Empfehlung von Maßnahmen

Unterstützung der Durchführung von Sicherheits-Audits

Stellt umfangreichen Katalog von Sicherheitswerkzeugen zur Verfügung

2. Welche Komponenten werden für die oben genannten Ziele zur Verfügung gestellt?

Modulbibliotheken

Bausteine

Gefährdungskataloge

Sicherheitssuiten

Maßnahmenkataloge

3. Konkrete organisatorische oder technische Umsetzungsempfehlungen zur Gewährleistung der IT-Sicherheit werden im IT-Grundschutz gegeben in:

Bausteinen

Gefährdungskatalogen

Maßnahmenkatalogen

4. Ein allgemeines Ziel des IT-Grundschutzes des BSI ist:

Ein Hochsicherheitsniveau zu erreichen.

IT-Verantwortliche zu sensibilisieren.

Ein bestimmtes, pauschalisiertes Sicherheitsniveau zu erreichen.

5. Eine inhaltsbasierte Sicherheitsprüfung der durch ein Netzwerk transportierten Daten ist durch den/die folgenden Filter möglich:

Paketfilter

Applikationsfilter

6. Welches sind die grundlegenden Funktionen von Paketfiltern?

Pass

Filter

Scan

Drop

Find

Log

7. Paketfilter entscheiden anhand der folgenden Informationen eines Datenpaketes (Bitte zutreffende Antworten wählen!):

IP-Adresse des Absenders

IP-Adresse des Empfängers

Dateityp (z.B. JPG, TIF, MPG)

Potnummer des Absenders

Portnummer des Empfängers

Uhrzeit der Erstellung der Datei

Protokolle/Typ des Pakets (z.B. TCP, UDP)

Flags im TCP-Header

8. Welche der beiden Firewall-Komponenten kann eine Virusscanner-Funktion enthalten?

Paketfilter

Applikationsfilter



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
Verständnisfragen
► Einsendeaufgaben
Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

Einsendeaufgaben

Aufgabe 5.1 – Sicherheit kryptographischer Verfahren

Worauf sollte die Sicherheit kryptographischer Verfahren ausschließlich beruhen? Begründen Sie Ihre Antwort?

Aufgabe 5.2 – Passwortsicherheit

Warum werden auf sicheren Servern Passwörter nicht als Klartext, sondern nur als nicht-invertierbarer Hash gespeichert?

Aufgabe 5.3 – Salts

Was sind Password-Salts? Wozu dienen sie?

Aufgabe 5.4 – Vergleich symmetrische/asymmetrische Verschlüsselung

Welche Unterschiede bestehen zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren hinsichtlich

- Sicherheit und Geheimhaltung/Schlüsselaustausch
- Nachweisbarkeit/Zuordnung zu Personen/Kommunikationsbeziehungen
- Welche Vor- und Nachteile sehen Sie und wozu wird man symmetrische Verfahren einsetzen, wozu asymmetrische?

Aufgabe 5.5 – Angewandte Kryptographie

- Was ist die Aufgabe von kryptografischen Hashfunktionen? Wozu werden sie benutzt?
- Was ist eine digitale Signatur?

Aufgabe 5.6 – Hybridverfahren

Skizzieren Sie, wie man mit einem asymmetrischen Verfahren eine digitale Signatur unter Einbezug von Hashfunktionen erstellt und wie man sie prüft! Wie und wozu können hierbei Hashfunktionen eingesetzt werden? Verwenden Sie folgende Notation:

- $k_{P,A}$ – öffentlicher Schlüssel von Alice
- $k_{S,A}$ – geheimer Schlüssel von Alice
- m – Nachrichtentext
- c – Chiffre
- H/h – Hashfunktion/Hashwert
- S/s – Signaturfunktion/Signatur
- V – Verifikationsfunktion

Aufgabe 5.7 – Paketfilterung

- a) Welche Vorteile haben Paketfilter?
- b) Welche Nachteile sind zu verzeichnen?

Aufgabe 5.8 – Applikationsfilter

- a) Welche Vorteile haben Applikationsfilter?
- b) Welche Nachteile sind zu verzeichnen?

IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
▶ Abkürzungen und Bezeichner
Referenzen
Stichwortverzeichnis

Abkürzungen und Bezeichner



Abkürzungen und Bezeichner 5

AES - Advanced Encryption Standard
 BSI - Bundesamt für Sicherheit in der Informationstechnik
 c - Geheimtext, Chiffretext (Kryptographie)
 D - Entschlüsselungsfunktion, Decryption (Kryptographie)
 E - Verschlüsselungsfunktion, Encryption (Kryptographie)
 FAT - File Allocation Table
 IP - Internet Protocol
 K - Schlüssel (Kryptographie)
 m - Klartext, Nachricht, Message (Kryptographie)
 NTFS - New Technology File System
 PGP - Pretty Good Privacy
 RSA - asymmetrisches Kryptosystem, benannt nach seinen Entwicklern Ronald L. Rivest, Adi Shamir und Leonard Adleman
 TCP - Transmission Control Protocol
 UDP - User Datagram Protocol



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
5.1 Vorgehen bei Sicherheitskonzepten: BSI-Grundschutzhandbuch
5.2 Ausblick kryptographischer Schutz
5.3 Ausblick Netzsicherheit
Verständnisfragen
Einsendeaufgaben
Abkürzungen und Bezeichner
► Referenzen
Stichwortverzeichnis

Referenzen



Online-Referenzen

An dieser Stelle wird darauf hingewiesen, dass es bei Online-Angeboten immer zu Korrekturen kommen kann, bei denen sich die Adresse bzw. die Verfügbarkeit bestimmter Inhalte kurzfristig ändern kann.

[BSI2008a] BSI Standards, http://www.bsi.de/literat/bsi_standard/index.htm, letzter Aufruf: 09.07.2009

[BSI2008b] IT-Grundschutz-Kataloge, Stand 10. Ergänzungslieferung, <http://www.bsi.de/gshb/deutsch/index.htm>, letzter Aufruf: 09.07.2009

[BSI2009] Startseite Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.de/>, letzter Aufruf: 09.07.2009

[True2009] TrueCrypt – Free Open-Source On-The-Fly Disk Encryption Software for Windows Vista/XP, Mac OS and Linux, <http://www.truecrypt.org>, letzter Aufruf: 12.07.2009



IT Sicherheit
Bearbeitungshinweise
Literaturempfehlungen
1 Einführung und organisatorische Sicherheit
2 Datenschutz und Nicht-technische Datensicherheit
3 Identity Management
4 Angewandte IT Sicherheit
5 Praktische IT Sicherheit
Stichwortverzeichnis

Stichwortverzeichnis

Access Control List
 Access Control Matrix
 Accountability
 Alarm und Anschuldigung
 Alice
 Analyse
 Angreifer
 Angriff
 anonymisierender Proxy
 Anonymisierung
 Anonymität
 Applikationsfilter
 asymmetrische Verschlüsselung
 Attack
 Attacker
 Auftragskontrolle
 Auskunft
 Auslesen
 Auswertung
 Authenticity
 Authentifizierung
 Authentifizierungsobjekt
 Authentizität
 Autorisierung
 Availability
 Baustein
 BDSG
 Bedrohung
 Bell-LaPadula-Modell
 Benutzerauthentifizierung
 Benutzerkontrolle
 Bergung
 Bericht
 Berichtigung
 Beschlagnahme
 Bezeugen
 Biba-Modell
 Biometrie
 Bob
 Boot-Virus
 BSI
 BSI IT-Grundschutz
 Capability List
 Carol
 CC
 Chinese Wall Modell
 Clark Willson-Modell
 CobiT
 Common Criteria
 Computerforensische Werkzeuge
 Computerprogramm
 Confidentiality
 Container

Cookies	
Cross-Site Scripting	
Datenaufnahme	
Datenbank	
Datenpaket	
Datenschutz	
Datenträgerkontrolle	
Dave	
digitale Wasserzeichen	
Discretionary Access Control	
dynamisch	
E-Mail	
Einbettung	
Eingabekontrolle	
Eve	
File-Virus	
Firewall	
Flag	
Gefahr	
Gefährdungskatalog	
geheimer Schlüssel	
geheimes Wissen	
geistiges Eigentum	
Güterabwägung	
Handschrift	
Hash-Funktion	
Hash-Wert	
Hybride Modelle	
hybride Verschlüsselung	
Identifikation	
Identität	
inhaltsbasierte Prüfung	
Integrity	
Integrität	
Internet	
IP	
IP-Adresse	
ISO27001	
IT-Forensik	
IT-Forensiker	
IT-Grundschutz	
IT-Tatort	
ITIL	
Kerberos	
LDAP	
LDSG	
Lightweight Directory Access Protocol	
Löschung	
Makro-Virus	
Mallet	
Mallory	
Mandatory Access Control	
Marvin	
Masterschlüssel	
Maßnahmenkatalog	
Merkmalsextraktion	
Mix	
Multi-Level Access Control	
Multilateral Access Control	
Multimedia-Produktion	
Nachweisbarkeit	
Netzwerk	

Nicht-Abstreitbarkeit	
No-read-up	
No-write-down	
Non-Repudiation	
offline	
One-Time-Pad	
online	
Online Analyse	
Organisationskontrolle	
Paketfilter	
Passphrase	
Passwort	
persönlicher Besitz	
physisch	
PIN	
Portnummer	
Post Mortem Analyse	
Privacy	
Privatsphäre	
Protokoll	
Pseudonymität	
public Key	
Reduktion	
Referenz	
Referenzdaten	
Regel	
reguläre Ausdrücke	
RFID	
Risiko	
Risk	
Role-based Access Control	
RStV	
Safety	
Schadenersatz	
Schichtenmodell	
Schlüssel	
Schwachstelle	
Schöpfungshöhe	
secret Key	
Security	
Semantik	
Session Key	
Sicherheit	
Sicherheitsaspekte	
Sicherheitsmodell	
Sicherheitsstandards	
Sicherung	
Signatur	
Sitzungsschlüssel	
Smart Card	
Speicherkontrolle	
Sperrung	
SQL Injection	
Staatsvertrag für Rundfunk und Telemedien	
statisch	
Steganographie	
symmetrische Verschlüsselung	
Tatortsicherung	
TCP	
technische Dokumentation	
Telefax	
Telefon	

Telekommunikationsgesetz
Telekommunikationsüberwachung
Telemediengesetz
Threat
Ticket
TKG
TMG
Transportkontrolle
Trojanisches Pferd
UDP
Unbeobachtbarkeit
Unverkettbarkeit
Urheberrecht
Verbindlichkeit
Verfügbarkeit
verhaltensbasiert
Verifikation
verschlüsseltes Dateisystem
Vertraulichkeit
Virus
Vorgehensmodell nach Casey
Vorratsdatenspeicherung
VPN-Anonymisierer
Vulnerability
Widerspruch
Wurm
XSS
Zugangskontrolle
Zugriffskontrolle
öffentlicher Schlüssel
Übermittlungskontrolle

öffentlicher Schlüssel Vertraulichkeit

Lightweight Directory Access Protocol Schöpfungshöhe
Baustein statisch Nicht-Abstreitbarkeit RStV Signatur

Internet Post Mortem Analyse Access Control List

Kerberos Beschlagnahme VPN-Anonymisierer

Unverkettbarkeit PIN Session Key Marvin Analyse Boot-

Virus Berichtigung Pseudonymität Hybride Modelle

Applikationsfilter Benutzerkontrolle IP-Adresse

Referenz **Integrität** Vorratsdatenspeicherung

Confidentiality Referenzdaten Alice Threat

Transportkontrolle Gefährdungskatalog Access Control

Matrix **Multilateral Access Control**

verschlüsseltes Dateisystem Mallory Cookies IT-

Grundschutz physisch Online Analyse **Identifikation**

geheimer Schlüssel LDAP Sicherheitsaspekte

Regel One-Time-Pad Availability **Hash-**

Funktion XSS Sitzungsschlüssel SQL

Injection Mallet Authentifizierung Semantik RFID

Angreifer Bell-LaPadula-Modell

Steganographie Privatsphäre Autorisierung Gefahr

Netzwerk LDSG Capability List Datenpaket TKG Risk

Datenaufnahme BSI IT-Grundschutz File-Virus technische

Dokumentation Risiko Dave dynamisch offline

Datenträgerkontrolle Auswertung Unbeobachtbarkeit

Merkmalsextraktion Schadenersatz Zugriffskontrolle

symmetrische

Verschlüsselung Authentizität

Eingabekontrolle Portnummer Masterschlüssel
verhaltensbasiert Bob Protokoll Multimedia-Produktion

Biba-Modell Widerspruch Übermittlungskontrolle

Discretionary Access Control Telefon

Benutzerauthentifizierung Zugangskontrolle

Telekommunikationsüberwachung

Auskunft **reguläre Ausdrücke** Cross-Site

Scripting Ticket Privacy

Authentifizierungsobjekt

Sicherung Auftragskontrolle Safety TMG geheimes Wissen

Security Computerforensische Werkzeuge **public Key**

Alarm und Anschuldigung Telemediengesetz E-Mail

Anonymisierung Verbindlichkeit Schwachstelle Schlüssel

Schichtenmodell BSI anonymisierender Proxy Sperrung

Datenbank CC Auslesen Eve Wurm **Angriff** Non-

Repudiation Vorgehensmodell nach Casey Trojanisches

Pferd Urheberrecht Löschung Multi-Level Access Control

Speicherkontrolle **asymmetrische**

Verschlüsselung Hash-Wert

Staatsvertrag für Rundfunk und Telemedien Bedrohung

Telekommunikationsgesetz ITIL Firewall Nachweisbarkeit

Clark Willson-Modell geistiges Eigentum Virus

Flag Passphrase **secret Key** Datenschutz

Paketfilter Container Verfügbarkeit Accountability Mix

Attack Telefax Makro-Virus digitale Wasserzeichen

Bezeugen ISO27001 Organisationskontrolle Common

Criteria Passwort Einbettung Attacker IT-Forensiker online

Carol Tatortsicherung Identität **Verifikation**

Handschrift **IT-Forensik** Role-based Access Control

IP **hybride Verschlüsselung** Vulnerability

Sicherheitsstandards

Güterabwägung Maßnahmenkatalog Sicherheit Bergung

persönlicher Besitz Biometrie CobiT inhaltsbasierte Prüfung

Computerprogramm IT-Tatort TCP UDP Sicherheitsmodell

Bericht Integrity Smart Card No-read-up **Chinesische**

Wall Modell Mandatory Access Control Authenticity

Anonymität Reduktion BDSG No-write-down