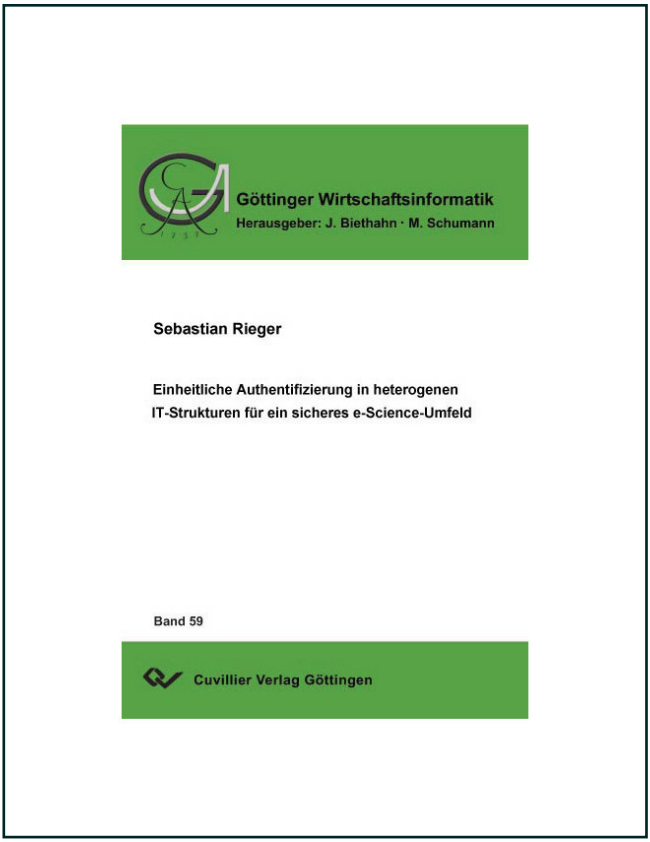
Sebastian Rieger (Autor)

Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science Umfeld



https://cuvillier.de/de/shop/publications/1736

1 Einleitung

In den vergangenen Jahren hat die Dezentralität des Zugriffs auf IT-Anwendungen und Ressourcen nicht zuletzt durch die große Verbreitung des World Wide Web mehr und mehr zugenommen. Web-Shops bieten ihren Kunden unabhängig von Ladenschlusszeiten oder dem Ort, an dem diese sich befinden, Dienstleistungen an.[2] Web-Services bieten darüber hinaus die globale Vernetzung von Applikationen und Geschäftsprozessen und reduzieren gleichzeitig die Komplexität von verteilten Anwendungen.[3] Durch Entwicklungen wie Asynchronous JavaScript and XML (AJAX)[4] und Rich Clients[5] entsteht unter dem Begriff „Web 2.0“ eine neue Generation von Web-Diensten, die teilweise nicht von klassischen Desktop-Applikationen zu unterscheiden sind. Sie tragen dazu bei, dass die Dezentralität der Anwendungen weiter zunimmt und sicherlich auch zukünftig noch steigen wird.

Im wissenschaftlichen Umfeld dienen Grid-Initiativen als Motor für die Dezentralisierung. Leistung von Rechenzentren soll gebündelt, verteilte Anwendungen über ihre Grenzen hinweg verknüpft werden. Treiber sind unter anderem Projekte wie der Large Hadron Collider der European Organisation for Nuclear Research (CERN), für dessen Experimente eine Datenmenge von ca. 15 Petabytes (15 Millionen Gigabytes) pro Jahr erwartet wird.[6] Die Analyse der Daten ist hierbei zentral am CERN aufgrund der großen Datenmenge nicht zu bewerkstelligen. Über schnelle Kommunikationsnetze sollen die Daten daher weltweit an Rechencluster verteilt werden, die deren Auswertung unterstützen. Zusätzlich sollen tausende von Wissenschaftlern Zugriff auf die Daten erhalten. Neben der Hochenergiephysik haben auch andere Wissenschaften wie die Medizin oder auch die Philologie und Linguistik die Bedeutung der vernetzten IT-Ressourcen mittels Grid erkannt.[7] „Ökonomische Chancen bieten sich insbesondere in den Bereichen Digitalisierung der Dienstleistungswirtschaft und Digital Manufacturing / Digital Factory, um neue Dienstleistungen zu ermöglichen, Produktionszyklen zu flexibilisieren und zu beschleunigen und dadurch Wachstumskräfte in diesen Märkten mit dynamischem Wachstumspotenzial anzureizen.“.[8]

---

[2] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 1.

[3] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 312.

[4] Vgl. GARRET, J. J.: Ajax: A New Approach To Web Applications, 2005.

[5] Vgl. DAUM, B.: Rich-Client-Entwicklung mit Eclipse 3.2. 2. Aufl., 2006, S. 1 ff.

[6] Vgl. LCG - LHC Computing Grid Project, 2007.

[7] Vgl. MediGRID GRID-Computing für die Medizin und Lebenswissenschaften, 2007; Vgl. TextGrid Modulare Plattform für verteilte und kooperative wissenschaftliche Textdatenverarbeitung - ein Community-Grid für die Geisteswissenschaften, 2007.

[8] Vgl. BMBF-eScience, 2007.

Über die reine Vernetzung der Rechenleistung bzw. Datenverarbeitung sind daher weitere Anwendungen, z.B. in Form von Web-Portalen erforderlich, die die verteilten Anwendungen nutzbar machen und das Potential des Grid ausschöpfen.[9] Wissenstransfer über schnelle, vernetzte Strukturen wie dem Internet und darauf basierendem World Wide Web sollen neue Formen wissenschaftlichen Arbeitens in sich selbst organisierenden Strukturen realisieren.[10] Man spricht in diesem Zusammenhang auch von „enhanced science“ (kurz: e-Science). Dies umfasst auch die Realisierung der erforderlichen IT-Sicherheit, die u.a. den Schutz vertraulicher Daten bei medizinischen Forschungsprojekten gewährleisten soll. Trotz der Vereinfachung des Zugriffs durch die Dezentralisierung soll der Zugriff durch unberechtigte Dritte in jedem Fall ausgeschlossen werden. Dies erfordert nicht zuletzt den Einsatz einer einheitlich über die gesamte IT-Struktur verwendbaren Authentifizierung.

1.1 Problemstellung und Motivation

Die in der Einleitung erläuterte Dezentralität und damit verbundene Vielfalt der Anwendungen z.B. im World Wide Web führt in Bezug auf die Authentifizierung zu einer Vielzahl von Passwörtern bzw. Authentifizierungsmerkmalen, die die Benutzer für ihre Arbeit mit den Anwendungen legitimieren. Die Verwendung und Verwaltung der Authentifizierungsmerkmale, -verfahren und -systeme sorgt dabei sowohl aufseiten der Benutzer als auch seitens der Organisationen bzw. Betreiber für einen erhöhten Aufwand. Gesteigert wird der Aufwand insbesondere aufgrund der bedingt durch die Dezentralisierung gestiegenen Zahl der Benutzer und zugehörigen Benutzerkonten an den einzelnen Standorten. Nicht nur im e-Science Umfeld wird der erhöhte Aufwand zunehmend zu einem Problem. Nahezu alle Internet-Nutzer spüren mittlerweile den erforderlichen Aufwand für die Verwaltung unterschiedlicher Passwörter, so etwa für verschiedene Web-Shops und Internet-Dienste (beispielsweise Amazon, eBay, GMX, usw.). In einer Studie der Fa. SafeNet aus dem Jahr 2004 gaben 29% der befragten 58.000 Benutzer an, sich sieben Passwörter oder mehr allein für die Arbeit merken zu müssen, bei steigender Tendenz. Lediglich 18%, der aus Deutschland, Frankreich, Großbritannien und den USA stammenden Befragten gaben an sich maximal zwei Passwörter merken zu müssen.[11]

Gleichzeitig steigen die Anforderungen an die IT-Sicherheit für die Firmen. Beispielsweise müssen nach der genannten Studie 83% der Benutzer mindestens einmal im Jahr ihr Kennwort ändern. 27%

[9] Vgl. e-Science-Forum, 2007.

[10] Vgl. BMBF-eScience, 2007.

[11] Vgl. SAFENET: Annual Password Survey Results, 2004, S 1. ff.

dürfen bei der Passwort-Änderung kein altes Passwort erneut verwenden, 30% müssen Zahlen und Sonderzeichen neben Buchstaben in ihrem Passwort vergeben. Um sich ihr Passwort merken zu können, schreiben es allerdings 50% auf, 35% teilen ihr Passwort außerdem Kollegen mit. Die erzielte Sicherheit ist somit trotz der Komplexitätsanforderungen sowie unterbundenen Wiederverwendbarkeit der Passwörter eingeschränkt. Zusätzlich bestätigt die Studie nicht nur die verbundene Minderung der Benutzbarkeit (Usability) durch den Aufwand für die Benutzer, sondern auch die steigenden Kosten für die Organisationen. 9% der Angestellten müssen sich drei- bis viermal im Jahr ihr Passwort zurücksetzen lassen. Insgesamt 47% der Befragten benötigen mindestens einmal pro Jahr eine Rücksetzung. Dabei werden in der Studie Kosten zwischen $30 und $50 für das Rücksetzen angenommen. Einen guten Überblick über ähnliche Statistiken zu dem Aufwand und der erzielten Sicherheit durch Passwörter liefert PasswordResearch.[12] Der zunehmende Aufwand sowie die eingeschränkte Sicherheit durch die anwachsende Diversität bilden die Problemstellung der vorliegenden Arbeit.

Die einheitliche Authentifizierung ermöglicht durch die Reduzierung des Aufwands und die Gewährleistung der erzielten Sicherheit eine Optimierung von heterogenen IT-Strukturen. Dies stellt die Motivation dieser Arbeit dar. Die einheitliche Authentifizierung bildet eine Grundlage für ein sicheres e-Science Umfeld sowie IT-Strukturen im Allgemeinen. Aufgrund dieses Potenzials bieten viele Hersteller Soft- und Hardware-Lösungen für die skizzierte Optimierung an. Häufig weisen diese jedoch Einschränkungen auf. Insbesondere lassen sich die Lösungen nicht für alle Anwendungen in einer heterogenen IT-Struktur einsetzen, ohne hohe Kosten oder Einschränkungen in Kauf zu nehmen. Das Potenzial sowie externe Anforderungen an die IT-Sicherheit sorgen jedoch seit einigen Jahren für einen anhaltenden Hype um das Thema Identity Management und „Single Sign-On“. Diese Arbeit befasst sich im Gegensatz hierzu mit den theoretischen Grundlagen für die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen und stellt ein geeignetes Modell vor. Sie baut dabei auf bestehenden Bewertungsmodellen zum Aufwand der IT-Sicherheit und Authentifizierung sowie der erzielten Sicherheit als Nutzen auf. Existierende Lösungen für die Realisierung der einheitlichen Authentifizierung werden bewertet sowie Möglichkeiten und Herausforderungen für zukünftige Lösungen definiert. Zusätzlich werden anhand von Fallstudien Ergebnisse der Anwendung in der Praxis beschrieben.

[12] Vgl. Password Research Institute, 2005.

1.2 Zielsetzung

Ziel dieser Arbeit ist die Minimierung des Aufwands für die Authentifizierung in heterogenen IT-Strukturen bei gleichzeitiger Gewährleistung der durch sie erzielten IT-Sicherheit. Hierfür werden bestehende Ansätze für die Quantifizierung von Aufwand und Sicherheit erweitert und auf ein theoretisches Modell für die einheitliche Authentifizierung in heterogenen IT-Strukturen abgebildet. Dadurch ergeben sich für die Bewertung von Kosten und Nutzen der IT-Sicherheit neue Beiträge.[13] Zusätzlich wird der Einfluss der einheitlichen Authentifizierung auf die Optimierung von IT-Strukturen in Bezug auf den Aufwand bei der Verwendung und Verwaltung bereitgestellter Dienste sowie der erzielten IT-Sicherheit bewertet. Durchgeführte Fallstudien, die die Anwendung des Modells in der Praxis verdeutlichen, liefern zudem Ergebnisse, die für die Vereinheitlichung der Authentifizierung in anderen wissenschaftlichen und betrieblichen heterogenen IT-Strukturen verwendet werden können. Anhand des Modells werden darüber hinaus Probleme identifiziert, die durch bestehende Lösungen für die Realisierung einer einheitlichen Authentifizierung nicht adressiert werden. In dieser Arbeit werden Anforderungen an neue Authentifizierungsverfahren genannt, die diese Probleme adressieren, und prototypische Lösungen diskutiert. Sie dienen dabei als Erweiterung der bestehenden Verfahren für Identity Management[14] sowie in der Entwicklung befindlicher benutzerzentrierter Lösungen.[15]

1.3 Methodik und Aufbau der Arbeit

Zunächst werden in Kapitel 2 die Grundlagen für das Verständnis der zur Authentifizierung zählenden Begriffe und Funktionen erläutert. Kapitel 3 beschreibt die Gründe für den in Abschnitt 1.1 beschriebenen erhöhten Aufwand der Authentifizierung in heterogenen IT-Strukturen. Für die Reduzierung des Aufwands existieren bereits Hard- und Software-Lösungen unterschiedlicher Hersteller, die in Abschnitt 3.2 beschrieben und in Bezug auf ihre Eignung für heterogene IT-Strukturen bewertet werden. Probleme der Lösungen werden abschließend zusammengefasst und in

---

[13] Beispiele für bestehende Bewertungen für Kosten der IT-Sicherheit finden sich in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006; GORDON, L. A.; LOEB, M. P.: Managing Cyber-Security Resources - A cost-benefit analysis, 2005; Economics and Security Resource Page, 2007.

[14] Vgl. KUPPINGER, M.: Trends im Identity Management, Vortrag: IdM Day, 2006.

[15] Beispiele für aktuelle Entwicklungen sind MICROSOFT: Introducing Windows CardSpace, 2007; SXIP identity, 2007; COMMUNICATIONS-ELECTRONICS SECURITY GROUP: ID-PKC: a new approach to Public Key Cryptography, 2007.

Abschnitt 3.3 auf Anforderungen für die optimale Gestaltung von IT-Strukturen durch den Einsatz einheitlicher Authentifizierung abgebildet.

Kapitel 4 benennt die Anforderungen und Ziele für eine einheitliche Authentifizierung in heterogenen IT-Strukturen. Für eine einheitliche Authentifizierung werden in Kapitel 4 sowohl Anforderungen aus wissenschaftlichen als auch aus betrieblichen IT-Strukturen betrachtet, die aufgrund ihrer verschiedenen Charakteristika unterschiedlich von der Vereinheitlichung der Authentifizierung profitieren. Da sich die Authentifizierung in den Aufgabenbereich der IT-Sicherheit einbettet[16], werden in Abschnitt 4.3 Schnittstellen zu nachgelagerten Verfahren, wie der Autorisierung und Abrechnung, genannt.

Kapitel 5 und 6 beinhalten den methodischen Kern der vorliegenden Arbeit. In Kapitel 5 wird das in Abschnitt 2.4.2 eingeführte erweiterte Authentifizierungsmodell für heterogene IT-Strukturen auf ein graphentheoretisches Modell abgebildet, dessen Kantengewichte den erforderlichen Aufwand sowie die durch die Authentifizierung erzielte Sicherheit bilden. Im Folgenden beschreiben die Abschnitte des Kapitel 5 die Faktoren für die Optimierung dieses Graphen hinsichtlich der Anzahl seiner Knoten und Summe der Kantengewichte. Hierfür werden mögliche Vereinheitlichungen definiert und, soweit verfügbar, mit bestehenden Lösungen für eine einheitliche Authentifizierung aus Abschnitt 3.2 in Beziehung gesetzt.

Kapitel 6 überträgt das skizzierte theoretische Modell auf Anforderungen aus der Realität wissenschaftlicher und betrieblicher IT-Strukturen und zeigt eine exemplarische Realisierung einer geeigneten einheitlichen Authentifizierung auf. Basierend darauf wird in Abschnitt 6.2 eine Methodik für die Optimierung des Modells bestimmt. Für die Optimierung werden die anhand des Bewertungsmodells aus Kapitel 5 quantifizierten Werte auf ein Fuzzy-Logic Modell übertragen, um die Unschärfe der Begriffe Aufwand und Sicherheit im Modell abzubilden. Die Anwendung der in Abschnitt 6.3 genannten Lösungen in einem Referenzmodell für die durchgeführten Fallstudien in Abschnitt 6.4 führt schließlich zur Bewertung der Ergebnisse in Abschnitt 6.5. Kern des Referenzmodells für die Implementierung der einheitlichen Authentifizierung stellen dabei die Abgrenzung der Vereinheitlichung in den einzelnen Bereichen des in Abschnitt 6.3.3 eingeführten Ebenenmodells sowie eine stufenweise Integrations- und Migrationsstrategie in Abschnitt 6.3.4 dar.

Kapitel 7 fasst die Ergebnisse zusammen und gibt einen Ausblick auf zukünftige Arbeiten.

[16] Die Authentifizierung sichert die Authentizität, deren Bedeutung in Abschnitt 2.2.5 definiert wird.

2 Grundlagen der Authentifizierung in IT-Strukturen

Die folgenden Abschnitte stellen die Grundlagen, die für eine Authentifizierung in IT-Strukturen benötigt werden, vor. Es wird vorrangig die Authentifizierung von Benutzern bzw. Personen gegenüber einem System oder einer Organisation beschrieben. Für die Gewährleistung der IT-Sicherheit ist insbesondere die gegenseitige Authentifizierung zwischen Systemen, Organisationen und Benutzern erforderlich. Beispielsweise sollen in der Regel nur dann geheime Daten für die Authentifizierung des Benutzers an ein System übermittelt werden, wenn dieses vom Benutzer eindeutig identifiziert und als vertrauenswürdig ermittelt wurde. Ohne eine Authentifizierung des Systems vor der Übermittlung der geheimen Informationen, wie z.B. eines Passwortes, könnten diese Informationen an unberechtigte Dritte gesendet werden, die sie dann ihrerseits für eine erfolgreiche Authentifizierung am eigentlichen System verwenden.

Die hierbei beteiligten Informationen, Verfahren und zugehörigen Begriffe erläutert der nachfolgende Abschnitt.

2.1 Begriffsdefinitionen

Die nachfolgenden Abschnitte definieren die in Bezug auf die Authentifizierung in dieser Arbeit verwendeten Begriffe. Größtenteils finden sich die aufgeführten Begriffe auch in der Fachliteratur zur Authentifizierung bzw. IT-Sicherheit wieder.[17]

2.1.1 Benutzer

Um die Authentizität bzw. die eindeutige Identität einer natürlichen oder juristischen Person oder eines Systems überprüfen zu können, wird diesen ein Kennzeichen als digitale Identität zugewiesen. Dieses Kennzeichen kann ein Benutzername sein. Der Begriff der Identität umfasst hierbei sowohl Personen als auch Systeme oder Endgeräte, die an einer Authentifizierung teilnehmen.[18] Im Folgenden wird aus diesem Grund der Begriff Identität gleichermaßen für Personen und Systeme verwendet. Personen, die Zugriff auf eine Ressource in der IT-Struktur nehmen, werden als Benutzer bezeichnet.

Eine Person oder ein System kann mehrere digitale Identitäten besitzen, die z.B. für unterschiedliche Funktionen oder Zugehörigkeiten genutzt werden. Die Zuordnung erfolgt jedoch in jedem Fall

---

[17] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 437 ff. oder SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002.

[18] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 4 f.

eindeutig. Eine digitale Identität ist genau einer Person oder System zugeordnet, während eine Person oder ein System unterschiedliche digitale Identitäten besitzen kann.

Im Englischen spricht man während der Authentifizierung in Bezug auf die Person häufig von einem Principal (deutsch: Vorsteher oder Auftraggeber), der den Auftrag zu seiner Authentifizierung erteilt.[19] Die Identität wird vom Benutzer in der Regel zusammen mit einem Authentifizierungsmerkmal als Auftrag an das authentifizierende System zur Prüfung übermittelt. Auch der Begriff Supplicant (deutsch: Supplikant oder Bittsteller) ist hierbei gebräuchlich.[20]

2.1.2 Betreiber

Als Betreiber werden im Folgenden Personen bzw. Organisationen bezeichnet, die ein System unterhalten, das eine Authentifizierung erfordert.[21] Dies bezieht auch Administratoren, die Authentifizierungskonten, -merkmale sowie Identitäten betreuen, mit ein. Betreiber können Authentifizierungssysteme für unterschiedliche Gruppen von Identitäten oder verschiedene Organisationen betreiben.

Betreiber sind für die Gewährleistung der IT-Sicherheit gegenüber ihren Benutzern zuständig. Dies bezieht neben der vertraulichen Speicherung der Authentifizierungsmerkmale auch die sorgsame Auswahl und Wartung von Authentifizierungsverfahren mit ein.

2.1.3 Ressource

Eine erfolgreiche Authentifizierung ermöglicht den Zugriff auf eine von dem Benutzer gewünschte Ressource. Unter dem Begriff Ressourcen werden im Folgenden Dienste, Anwendungen und Geräte zusammengefasst, die in einer IT-Struktur bereitgestellt werden (z.B. E-Mail-Konto, Netzwerkfreigaben und -zugänge usw.). Man spricht hierbei auch davon, dass sich der Benutzer für den Zugriff auf diese konkrete Ressource authentifiziert hat. Betreiber setzen eine Authentifizierung für die von Ihnen angebotenen Ressourcen voraus, um so den Zugriff durch unberechtigte Dritte zu unterbinden oder sie allgemein vor Missbrauch zu schützen.

---

[19] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 17.

[20] Vgl. IEEE: 802.1X Port-Based Network Access Control, 2004, S. 7.

[21] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 73.

2.1.4 Authentifizierung

Die Überprüfung einer Identität[22] anhand eines Authentifizierungsmerkmals durch einen Dritten bezeichnet man aus Sicht des Überprüfenden als Authentifizierung.[23] Im Gegenzug wird der Vorgang aus Sicht des Überprüften im deutschen Sprachgebrauch Authentisierung genannt[24], die englische Bezeichnung „Authentication“ die Sichten beider Beteiligten gleichermaßen umfasst. In den folgenden Abschnitten wird im Regelfall die Sicht der Betreiber eines Dienstes, die Identitäten überprüfen, dargestellt und daher der Begriff der Authentifizierung verwendet. In der deutschen Literatur wird hierfür teilweise synonym der Begriff Authentifikation gebraucht, der jedoch im allgemeinen Sprachgebrauch der IT eine geringere Verbreitung besitzt.[25]

Eine Authentifizierung hat in jedem Fall ein eindeutiges Ergebnis. Sie lässt sich anhand einer zweiwertigen Aussagenlogik beschreiben und führt daher zu genau zwei möglichen Ergebnissen. Entweder ist die Authentifizierung erfolgreich oder nicht erfolgreich.[26]

Im Allgemeinen wird eine Authentifizierung zu Beginn einer Sitzung bzw. eines Vorgangs an IT-Systemen durchgeführt und ist dann bis zu deren Beendigung gültig. Zugriffskontrollen (Autorisierung) und etwaige Abrechnung (Accounting) setzen auf die durch eine erfolgreiche Authentifizierung gesicherte Vertrauensbasis auf. Die Authentifizierung ist nicht nur die Grundlage für nachfolgende Prozesse wie die Prüfung von Berechtigungen; sie ermöglicht etwa durch den Austausch von Schlüsseln beim Authentifizieren auch die Gewährleistung der Vertraulichkeit der übertragenen Informationen während einer Sitzung. Dies unterstreicht nicht zuletzt die hohe Bedeutung der Authentifizierung für die IT-Sicherheit.[27]

2.1.5 Authentifizierungsmerkmal

Die Angabe der Identität eines Benutzers gegenüber einem System reicht nicht aus, um eine Person oder ein System eindeutig identifizieren zu können. Auch ein unberechtigter Dritter, der diese Be-

---

[22] Vgl. Abschnitt 2.1.1.

[23] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 179.

[24] Vgl. DUDEN: Das Fremdwörterbuch, 7. Aufl., 2001, S. 106.

[25] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 187; DUDEN: Das Fremdwörterbuch, 7. Aufl., 2001, S. 106.

[26] Eine detaillierte Betrachtung zweiwertiger Aussagelogik lässt sich in DÖRFLER, W.; PESCHEK, W.: Einführung in die Mathematik für Informatiker, 1988, S. 83 nachlesen.

[27] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 7, wobei Authentizität als erstes Schutzziel der IT-Sicherheit genannt wird.

zeichnung (z.B. den Benutzernamen) einer Person kennt, kann diese direkt an das System übermitteln und den rechtmäßigen Inhaber der Identität impersonieren. Daher ist für die Gewährleistung der Authentizität[28] ein zusätzliches, eindeutiges Authentifizierungsmerkmal notwendig.[29] Dieses Authentifizierungsmerkmal kann auf einer geheimen Information wie einem Passwort basieren, die nur der berechtigten Person bekannt ist, oder einer Eigenschaft, die die Person eindeutig identifiziert. Somit kann durch die Verwendung oder Überprüfung des geheimen Authentifizierungsmerkmals die Identität der Person gesichert überprüft werden.

Authentifizierungsmerkmale müssen vor dem Zugriff durch unberechtigte Dritte geschützt werden. Erlangt ein unberechtigter Dritter Zugriff auf das Authentifizierungsmerkmal, so kann er die Identität des Inhabers vortäuschen oder übernehmen. Authentizität und Verbindlichkeit der zum Authentifizierungsmerkmal gehörigen Identität wären somit nicht mehr gewährleistet.[30] Authentifizierungsmerkmale werden genau einer Identität zugeordnet.

2.1.6 Authentifizierungsfaktor

Erfordert die erfolgreiche Überprüfung einer Identität eines Benutzers mehrere Authentifizierungsmerkmale (z.B. den Besitz eines Tokens und die Kenntnis eines zugehörigen Passwortes), so spricht man in Bezug auf die Merkmale auch von Authentifizierungsfaktoren.[31] Der Benutzer muss in diesem Fall alle Faktoren eindeutig nachweisen, um seine Identität glaubhaft zu bestätigen. Man spricht in diesem Zusammenhang auch von einer Multi-Faktor-Authentifizierung. Häufig werden für die einzelnen Faktoren unterschiedliche technische Verfahren verwendet. Diese Verfahren basieren in der Regel auf der Kenntnis (etwa einer eine Information, die die Identität kennt), dem Besitz (z.B. ein Gegenstand, den sie besitzt) oder einer eindeutigen Eigenschaft (z.B. ein persönliches bzw. biometrisches Kennzeichen).

2.1.7 Authentifizierungskonto

Um die Authentifizierung durchführen zu können, benötigt die überprüfende Instanz die Bezeichnung der Identität sowie eine Kopie des Authentifizierungsmerkmals. Identität und Authentifizie-

---

[28] Der Begriff der Authentizität wird im folgenden Abschnitt als Grundwert der IT-Sicherheit definiert.

[29] Vgl. „distinguishing characteristic“ in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 3 f.

[30] Die Identität des Benutzers kann nicht verbindlich nachgewiesen werden. Somit ist die Zuordnung zur realen Person, bzw. die Authentizität nicht gewährleistet. Verbindlichkeit und Authentizität werden im folgenden Abschnitt als Grundwerte der IT-Sicherheit beschrieben.

[31] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 28 ff.