TECHNISCHE UNIVERSITÄT
ILMENAU

Sicherheitsaspekte in Virtuellen Welten

IT-Sicherheitsanalyse und Anforderungsdefinition unter Berücksichtigung der Faktoren für Unterhaltungserleben

Dissertation zur Erlangung des akademischen Grades

Doktor rerum naturalium (Dr.rer.nat)

Vorgelegt der Fakultät für Mathematik und Naturwissenschaften
der Technischen Universität Ilmenau

von Diplom-Wirtschaftsinformatikerin Anja Beyer

1. Gutachter: Prof. Dr. Andreas Will
2. Gutachter: Prof. Dr. Rüdiger Grimm
3. Gutachter: Prof. Dr. Helmut Reimer

Tag der Einreichung: 20.03.2009
Tag der wissenschaftlichen Aussprache: 25.01.2010

urn:nbn:de:gbv:ilm1-2010000047

Kurzfassung

Virtuelle Welten sind sozio-technische Systeme, also IT-Systeme die in höchstem Maße auf die Anwendung durch Nutzer ausgelegt sind. Die vorgelegte Arbeit führt unter dem Titel „IT-Sicherheitsaspekte in Virtuellen Welten“ eine IT-Sicherheitsanalyse für Virtuelle Welten in einer Client-Server-Architektur durch und gelangt zu einer „Anforderungsdefinition unter Berücksichtigung für Faktoren für Unterhaltungserleben“.

IT-Sicherheit zielt auf den Schutz digitaler Werte vor Gefahren und stellt Maßnahmen zur Verfügung mit denen dieser Schutz erreicht werden kann. Virtuelle Welten in Client-Server-Architekturen werden über das Internet zugänglich gemacht. Da das Internet per se ein unsicheres Netzwerk ist, resultieren eine Reihe von Gefahren, die die Werte in den Virtuellen Welten bedrohen. Um aber geeignete Schutzmechanismen vorzuschlagen, ist es wichtig, dass zunächst eine grundlegende Analyse des Schutzgegenstandes durchgeführt wird.

Virtuelle Welten sind sehr auf einen interaktiven Dialog mit den Nutzern ausgelegt. Die Umsetzung von Sicherheitsmaßnahmen fordert eine uneingeschränkte Akzeptanz der Maßnahmen durch den Nutzer. Daher verfolgt diese Arbeit einen interdisziplinären Blick auf die IT-Sicherheit der modernen Medienanwendung „Virtuelle Welt“.

Im ersten Schritt werden verschiedene Perspektiven auf die Nutzungsmotivation aufgezeigt und die Faktoren für Unterhaltungserleben, wie Bedürfnisbefriedigung, Spielspaß und Flow, herausgearbeitet. Erst durch diese (sozialwissenschaftliche) Betrachtung der Nutzung ist die Analyse der realen Werte aller Akteure innerhalb der Virtuellen Welten möglich.

Anschließend erfolgt die (informatorische) Sicherheitsanalyse. Es wird festgestellt, welche Bedrohungen auf die Werte gerichtet sind (Bedrohungsanalyse) und welche Sicherheitsziele sich für den Schutzgegenstand Virtuelle Welt ergeben. Auf dieser Basis erfolgt eine systematische Ableitung der Anforderungen an die IT-Sicherheit der Virtuellen Welten. Die Autorin definiert ein Schutzprofil nach dem internationalen Standard (ISO/IEC) der Common Criteria for Information Technology Security Evaluation. Die Common Criteria (CC) sind ein erprobtes Instrument zur Bewertung der Sicherheit von IT-Produkten. Mit einem Schutzprofil können Prüfstellen Produkte gleichwertig evaluieren und so die Zusicherung einer Sicherheitsqualität gewährleisten.

Den Abschluss der Arbeit bildet die Empfehlung von konkreten Gestaltungsvorschlägen. Es wird aufgezeigt, wie die technischen Schutzmechanismen umgesetzt werden können, sodass das Unterhaltungserleben der Nutzer nicht gestört wird. So können die Schutzmechanismen zu einer höheren Akzeptanz beim Nutzer führen.

Abstract

Virtual Worlds are socio-technical systems, which means that they are IT-systems that are specifically catered to the users. This PhD thesis provides a systematic IT-Security analysis for Virtual Worlds with a client-server architecture and defines security requirements taking into account the different factors for perceived entertainment.

IT-Security focuses on the protection of digital assets against threats und provides security mechanisms that are able to protect these assets. Virtual Worlds with a client-server architecture are made accessible via the Internet. Due to the Internet being an insecure network by design, a number of threats arise targeting the assets of Virtual Worlds. In order to recommend appropriate protection mechanisms it is however important to conduct a systematic security analysis in a first step.

Virtual Worlds are designed for an interactive dialogue between the user and the system. The installation of security mechanisms requires that these mechanisms are accepted in absolute terms by the user. This dissertation therefore applies an interdisciplinary view on the IT-Security of current/modern media applications, such as Virtual Worlds.

In a first step different perspectives on the motivation for the usage of Virtual Worlds are depicted and the elements for experiencing entertainment such as gratification, fun and flow are identified. By means of the social science perspective regarding user motivation an analysis the actual assets in Virtual Worlds is possible.

The social science perspective is followed by an information technology perspective throughout which an IT-Security analysis is conducted, including the analysis of threats and the definition of security objectives for the specific subject of the protection. On this basis a systematic selection of security requirements is possible. The author defines a Protection Profile according to the Common Criteria for Information Technolgy Evaluation which is an international ISO/IEC standard. The Common Criteria are a well-accepted and approved instrument for the security evaluation of IT products. With a Protection Profile independent and accredited laboratories are able to equally evaluate IT products and offer a certain level of quality assurance.

Finally, recommendations for the design and integration of security mechanisms are provided. Moreover, the author depicts how the technical measures can be integrated into Virtual Worlds so that users are not disturbed during their perception of entertainment which in turn leads to a higher acceptance of the security measures.

Danksagung

Die vorliegende Doktorarbeit ist vorwiegend während meiner Tätigkeit am Fachgebiet „Virtuelle Welten/Digitale Spiele“ an der Fakultät für Mathematik und Naturwissenschaften der Technischen Universität Ilmenau entstanden. Herzlichen Dank an alle, die zum Gelingen der Arbeit beigetragen haben. Ich danke Herrn Prof. Grimm, dem Leiter der Professur IT-Risk-Management der Universität Koblenz-Landau, für seine Betreuung, die wertvollen Anregungen und Hinweise sowie die wohlwollende Begutachtung der Arbeit. Ich danke Herrn Prof. Will, dem Leiter des Fachgebietes Medienmanagement am Institut für Medien und Kommunikationswissenschaft der TU Ilmenau, für seine Unterstützung, das entgegengebrachte Vertrauen, die wertvollen Anregungen sowie die wohlwollende Begutachtung der Arbeit. Ich danke Herrn Prof. Reimer, Herausgeber der Zeitschrift Datenschutz und Datensicherheit und ehemaliger Geschäftsführer der TeleTrusT Deutschland e.V., für seine Unterstützung und das Erstellen des Gutachtens. Meinen ehemaligen Kolleginnen und Kollegen am IfMK, insbesondere Marion Irmer, Gunther Kreuzberger, Imke Hoppe und Marcel Kirchner, danke ich für die fachlichen Anregungen, ihre Unterstützung und das wertvolle Kolloquium. Ein ganz besonderer Dank gilt meinem Lebensgefährten, Sven Peters, für seine Liebe, die mich stark macht und die vielen fachlichen Diskussionen, die mir halfen einige Aspekte klarer zu sehen. Ein weiterer ganz besonderer Dank gilt meinem Vater, Peter Beyer, der mir diesen Weg ermöglicht hat und viele wichtige Denkanstöße sowohl für die Arbeit als auch fürs Leben gibt. Ich danke meiner Alma Mater, der Technischen Universität Ilmenau, für die finanzielle Förderung im Rahmen der Exzellenzinitiative.

„ … und er [der Mensch] ist nur da ganz Mensch, wo er spielt“

Friedrich Schiller, 1793

Inhaltsübersicht

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	**Bedeutung**
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
EAL	Evaluation Assurance Level
EGK	Elektronische Gesundheitskarte
ENISA	European Network and Information Security Agency, deutsch Europäische Agentur für Netz- und Informationssicherheit
EP	Erfahrungspunkte
Etc.	Et cetera
EULA	End User License Agreements, deutsch Endbenutzer-Lizenzvereinbarung
Evaluation	Prüfung
EVG	Evaluierungsgegenstand
CAVE	Cave Automatic Virtual Environment, deutsch: Höhle mit automatisierter Virtueller Umwelt, bezeichnet einen Raum zur Projektion einer dreidimensionalen Virtuellen Welt
CC	Common Criteria for Information Technology Security Evaluation, deutsch Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie
DIN	Deutsches Institut für Normung
DOS	Denial-Of-Service, deutsch Dienstverweigerung, Angriff auf ein System, auch DDOS: Distributed-Denial-Of-Service

GKV	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
IEC	International Electrotechnical Commission, Internationales Normungsgremium
IGE	Internet Gaming Entertainment
IM	Instant Messaging, deutsch Nachrichtensofortversand
ISO	International Organization for Standardization, Normungsorganisation
IT	Informationstechnologie
ITSEC	Information Technology Security Evaluation Criteria, deutsch: Kriterien für die Bewertung der Sicherheit von Informationstechnologie
MMORPG	Massive(ly) Multiplayer Online Role Playing Game, deutsch Massen-Mehrspieler-Online-Rollenspiel
NSA	National Security Agency deutsch Nationale Sicherheitsbehörde, Nachrichtendienst der Vereinigten Staaten
NIST	National Institute of Standards and Technology, Bundesbehörde in den Vereinigten Staaten zuständig für Standardisierungsprozesse
NPC	Non-Player-Character, computersimulierte Spielfigur
OSP	Organizational Security Policy, deutsch Organisatorische Sicherheitsrichtlinien
PP	Protection Profile, vgl. Schutzprofil
RMT	Real Money Trade bezeichnet den Handel virtueller Gegenstände oder Spielwährung mit realem Geld
ST	Security Target, deutsch Sicherheitsvorgaben
TCSEC	Trusted Computer System Evaluation Criteria, deutsch Kriterien für die Bewertung vertrauenswürdiger Computersysteme
TDU	Triadisch Dynamische Unterhaltungstheorie
TSF	TOE Security Funktion, Sicherheitsfunktion des EVG
TOS	Terms of Service, deutsch Nutzungsbestimmungen
Z.B.	Zum Beispiel

Glossar

Begriff	**Bedeutung**
Assets	Werte
Avatar	Spielfigur des Nutzers in der Virtuellen Welt
Evaluation	Prüfung
Cheating	Unfaires Spielen
Flow	Gefühl der Involviertheit, in einer Tätig aufgehen (nach Czikzentmihaly)
Gilde	Zusammenschluss mehrerer Spieler zu einer Gruppe, um gemeinsame Ziele zu erreichen.
Goldfarmer	Professionelle Spieler, die nur zum Erwerb des Goldes in Virtuellen Welten agieren. Sie erspielen Gold oder Gegenstände, um sie in reales Geld zu tauschen (vgl. RMT)
Level	Erfahrungsstufe
Phishing	Kunstwort zusammengesetzt aus Passwort und Fishing, Social Engineering Angriff
Power Leveling	Angebotener Dienst, um einen Avatar auf ein hohes Level zu spielen
Quest	Aufgabe
Social Engineering	Angriff unter Ausübung sozialen Verhaltens
Schutzprofil	enthält eine implementierungsunabhängige Menge von Sicherheitsanforderungen an eine Gruppe oder eine Kategorie von zu untersuchenden IT-Systemen (Evaluierungsgegenstand, kurz EVG)

Kapitel 1

Einführung

Die vorliegende Arbeit widmet sich Aspekten der IT-Sicherheit in Virtuellen Welten. Um dem Leser den Einstieg in die durchaus komplexe Thematik zu erleichtern, erläutert dieses einführende Kapitel die Relevanz, das Ziel und die Herangehensweise an die Arbeit. Wie folgend werden in jedem Kapitel eingangs Fragen formuliert, deren Beantwortung Inhalt des jeweiligen Kapitels ist. Diese Vorgehensweise soll dem Leser übersichtlich darlegen, mit welchen Fragen sich die Autorin in den einzelnen Kapiteln beschäftigt hat und welcher Inhalt den Leser erwartet. Die Fragen, die in diesem ersten Kapitel der Arbeit beantwortet werden, lauten:

- Welche Relevanz hat die Thematik?
- Welches Ziel verfolgt die Arbeit?
- Welche Methodik kommt zum Einsatz?
- Wie ist die Arbeit aufgebaut?

1.1 Relevanz der Arbeit

Werden wir in Zukunft nicht mehr unterscheiden können, ob wir spielen oder arbeiten (vgl. [3Sat 08])? Fakt ist, dass die Berufsgruppen der Ingenieure, Piloten und das Militär

bereits seit Langem Computersimulationen einsetzen um zu arbeiten. Ingenieure konstruieren dreidimensionale Modelle von Fahrzeugen in CAVES (Cave Automatic Virtual Environments), Piloten trainieren für schwierige Manöver und das Militär nutzt Virtuelle Welten um Soldaten auf Einsätze vorzubereiten.

Mit Computerspielen hat sich eine Unterhaltungsindustrie entwickelt, die ihresgleichen sucht. Dass die Unterschiede zwischen Spiel- und Arbeitswelten zunehmend verschwimmen, zeigt die prominente Virtuelle Welt „Second Life“. Unter dem Motto „Verwirkliche dich selbst“ haben die Nutzer die Möglichkeit ihre eigene Wunschrolle in der Virtuellen Welt einzunehmen. In Second Life können die Nutzer spielen und arbeiten. Es gibt Boutiquebesitzer, Künstler, Filmemacher, Musiker, Hostessen und viele andere, die ihre Arbeit in einer Virtuellen Welt verrichten.

Eine besondere Reichweite bei der Vernetzung mit der Realität erzielt Second Life derzeit durch zwei Besonderheiten. Zum einen kann der Spieler selbst Gegenstände herstellen und hält das Urheberrecht an diesen. Zum anderen hat der Spieler die Möglichkeit das gehandelte virtuelle Geld, den Lindendollar, in reale US-Dollar zu tauschen bzw. US-Dollar in Lindendollar. Reale Unternehmen, z.B. IBM, zeigen auch in Second Life Präsenz und nutzen diese Virtuelle Welt als Vertriebsplattform. Durch den erheblichen Aufwand und die eingesetzten finanziellen Mittel steckt ein beträchtlicher Wert in dieser Virtuellen Welt.

Was in vielen Science-Fiction Romanen (wie z.B. Otherland [Williams 05]) als Zukunftsszenario beschrieben wird, ist heute bereits Alltag. Vernetzt über das Internet können viele tausend Nutzer gleichzeitig in einer Virtuellen Welt agieren. Besonderer Beliebtheit erfreuen sich derzeit Onlinespiele. Je nach Genre verfolgen die Spieler dort unterschiedliche Ziele. Die Bandbreite reicht von Shooter-Spielen (z.B. Doom, Quake) über Strategiespiele (z.B. Final Fantasy Reihe) bis hin zu den wohl bekanntesten, den Online-Rollenspielen. Das erfolgreichste MMORPG (Massively Multiplayer Online Role-playing Game), wie diese auch genannt werden, ist World of Warcraft mit weltweit circa zwölf Millionen registrierten Nutzern (Stand Dezember 2008 [Blizzard 08]). Weitere Vertreter dieses Genres sind Guild Wars, Everquest, Ultima Online uvm.

Mit ihrer persönlichen Spielfigur, den so genannten Avataren, bewegen sich die Spieler in der Virtuellen Welt und müssen Quests (Aufgaben) lösen, Gegner bekämpfen, Gegenstände und Gold oder Geld sammeln. Die Onlinespiele zeichnen sich durch ihren hohen Grad an Interaktion aus. Die Spieler können über ein integriertes Nachrichtensystem[1] mit anderen Spielern kommunizieren. Sie haben die Möglichkeit sich in Gilden zusammenzuschließen um gemeinsam Quests zu lösen, was in höheren Leveln auch notwendig ist (vgl. [Schmitz 07], S.23).

Virtuelle Welten haben auch Auswirkungen auf die Realität. Die Nutzer investieren sehr viel Zeit und erarbeiten sich wertvolle Gegenstände. Beim Handel wird reales Geld eingesetzt (Real Money Trade, vgl. Kapitel 2.3), Firmen verlagern teilweise ihr Geschäft in die Virtuelle Welt und es gibt bereits erste Erfolgsgeschichten, die beschreiben, dass Menschen ihren realen Lebensunterhalt in der Virtuellen Welt erarbeiten, indem sie dort ihre Dienste und Produkte anbieten. Virtuelle Welten helfen alltägliche Probleme zu bewältigen, zum Beispiel bei der Informationsbeschaffung, beim Handel von Waren, Bankgeschäften und für die Ausbildung im Sinne von E-Learning. In Virtuellen Welten existieren Werte (zum Beispiel Gegenstände, Geld, etc.), die durch ihre reale Relevanz schützenswert sind.

Insbesondere aufgrund der realen Bedeutung des wertvollen Eigentums (Werte) existieren in den Virtuellen Welten aber auch Risiken. Wie im realen Leben auch, ist wertvolles Eigentum ein beliebtes Ziel für Angriffe. Es existieren Angriffe auf die Werte der Nutzer, die zum Totalverlust oder Wertverlust führen können, z.B. wenn wertvolle Gegenstände von Nutzern unautorisiert gelöscht oder kopiert werden (vgl. Kapitel 4.2). Die Werte der Nutzer erfordern daher Schutz. Das Ziel der IT-Sicherheit ist der Schutz von Werten. Die IT-Branche hat die Notwendigkeit für IT-Sicherheit in Virtuellen Welten erkannt und fordert die Einführung von Sicherheitsstandards für Virtuelle Welten (vgl. [Koll 07]).

[1] Instant Messaging (Nachrichtensofortversand) oder Sprachsysteme

1.2 Ziel und Herangehensweise

Das Ziel der Arbeit ist eine grundlegende Sicherheitsanalyse und die Definition von Anforderungen an die Sicherheit von Virtuellen Welten. Die IT-Sicherheit bietet Mechanismen und Maßnahmen für den Schutz von digitalen Werten. Virtuelle Welten sind IT-Anwendungssysteme, die digitale Werte enthalten. Somit können Mechanismen der IT-Sicherheit eingesetzt werden um diese digitalen Werte geeignet zu schützen.

Für die Definition von Sicherheitsanforderungen an Systeme bzw. Organisationen existieren mehrere Standards bzw. „Best-Practise"-Ansätze, wie die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die ISO/IEC 27001 und ISO/IEC 27002 sowie die Common Criteria for Information Technology Security Evaluation. Während die IT-Grundschutzkataloge und die ISO/IEC 27001 auf die Sicherheit einer Organisation bzw. Unternehmen ausgerichtet sind, fokussiert der ISO/IEC 27002 das IT-Sicherheitsmanagement. Für die Definition von Sicherheitsanforderungen an ein Produkt gibt es neben verschiedenen nationalen Kriterien den international akzeptierten Ansatz der Common Criteria.

Die Common Criteria for Information Technology Security Evaluation [CC 06] stellen ein Rahmenwerk für die Bewertung und Evaluierung der Sicherheit von IT-Anwendungssystemen dar. Anbieter von Systemen (Hardware und Software) haben die Chance nachzuweisen, dass ihre Systeme Funktionalitäten besitzen, die den Sicherheitsanforderungen bestimmter Produktklassen gerecht werden. Die Common Criteria bieten die Möglichkeit für eine solche Evaluierung. Die Sicherheitsanforderungen der Produktklassen werden in so genannten Schutzprofilen beschrieben. Das Ziel der Common Criteria ist die Zusicherung von Vertrauen in ein IT-Produkt auf Basis einer Evaluation. Die Evaluation wird von erfahrenen Experten durchgeführt (vgl. [CCPart3 06], S.15).

Die vorliegende Arbeit entwickelt einen Vorschlag für ein Schutzprofil für die Produktklasse „Virtuelle Welt" nach Common Criteria. Das Schutzprofil ist als Bewertungssystem zu verstehen, nach dem geprüft werden kann, ob ein System die gestellten Anforderungen erfüllt. Der Entwurf dieses Schutzprofils erfordert eine grundlegende Sicherheitsanalyse, das heißt es muss beschrieben werden, welche Akteure mit welchen Werten bei der

Nutzung des Systems beteiligt sind und wie die Werte bedroht werden. Auf dieser Basis können dann Sicherheitsziele und Sicherheitsanforderungen an das Produkt definiert werden.

Die Möglichkeit die Sicherheit eines Systems evaluieren zu lassen, bietet die Chance, das Vertrauen in ein Produkt zu erhöhen. Ein Zertifikat dient als Nachweis für die Evaluation. Das Schutzprofil wird einerseits für die Evaluierung herangezogen, es kann den Entwicklern von Virtuellen Welten aber auch als Empfehlung für die Umsetzung von Sicherheitsmechanismen dienen.

IT-Systeme sind sozio-technische Systeme. Die Erforschung sozio-technischer Systeme reicht in die 1950er Jahre zurück. Bereits 1951 gelangten Trist und Bamforth [Trist 51] zum Verständnis eines Unternehmens als Einheit von Mensch und Technologie. Die soziale und technische Komponente können nicht getrennt werden, sondern funktionieren nur gemeinsam. Dies erfordert, dass die Technik vom Menschen einfach benutzbar ist. Auch Eckert [Eckert 04] hat erkannt, dass IT-Systeme ein Teil sozio-technischer Systeme sind und beschreibt in ihrem Grundlagenwerk zur IT-Sicherheit die Anforderung der Berücksichtigung des Menschen als sozialen Faktor. Sie geht dann leider im gesamten Kompendium nicht weiter darauf ein, sondern konzentriert sich auf die technischen Faktoren der IT-Sicherheit.

Die Akzeptanz und Benutzbarkeit von Systemen ist, neben funktionierender Technik, sehr wichtig. Dennoch werden heute viele IT-Systeme (Software und Hardware) entwickelt, ohne dass sie dieser Anforderung gerecht werden. Es existiert Sicherheitssoft- und -hardware, die von Anwendern jedoch ignoriert wird, weil bei der Entwicklung der Systeme das Nutzerverhalten nicht berücksichtigt wird. Das hat zur Folge, dass Software entweder gar nicht oder falsch bedient wird. Systeme mit schlechter Usability (Benutzbarkeit) stoßen bei Nutzern nicht auf Akzeptanz (vgl. [Whitten 05]).

Virtuelle Welten sind auch Unterhaltungsmedien. Diese Eigenschaft erfordert die Berücksichtigung der Faktoren für Unterhaltungserleben bei der Konzeption von Mechanismen. Es wird untersucht, welche Erfahrungen die Akteure bei der Nutzung von Virtuellen Welten machen und wie sie die Nutzung erleben. Auf Basis einer Literaturrecherche werden verschiedene Perspektiven der Nutzungsmotivation zusammengestellt.

Es ist wichtig, dass die Erkenntnisse der Betrachtung der sozialen Faktoren bei der Umsetzung von Sicherheitsmaßnahmen Berücksichtigung finden. Es werden Vorschläge (Szenarien) erarbeitet, an denen beispielhaft veranschaulicht wird, wie eine Umsetzung aussehen könnte.

Bisherige Arbeiten zur Sicherheit in Virtuellen Welten beziehen sich allein auf Onlinespiele und fokussieren den Aspekt des Cheating (unfaires Spielen) (vgl. [Yan J.J 02, Yee 06, Chen 05]). Andere Arbeiten fokussieren Aspekte der Netzwerksicherheit (vgl. [Köhnlein 05, Banavar 00, Smed 01]).

Die vorliegende Arbeit verfolgt erstmals eine ganzheitliche Betrachtung der Sicherheit in Virtuellen Welten unter Berücksichtigung technischer und sozialer Anforderungen.

1.3 Aufbau der Arbeit

In die Arbeit einleitend, beschreibt Kapitel 2 die Anwendungsdomäne. Es wird erläutert was Virtuelle Welten sind und es werden ausgewählte Beispiele Virtueller Welten vorgestellt (vgl. Abbildung 1.1).

Kapitel 3 betrachtet die sozialen Faktoren der Motivation der Nutzung Virtueller Welten. Es wird aufgezeigt, warum Menschen Virtuelle Welten nutzen, welche Bedürfnisse sie befriedigen und wie Unterhaltung durch den Nutzer erlebt wird.

Virtuelle Welten sind keineswegs nur „virtuell“, sondern haben eine hohe reale Relevanz. Der Begründung dieser Behauptung geht Kapitel 4 nach. Außerdem wird gezeigt, dass IT-Sicherheit einen Beitrag zum Schutz der realen Werte leisten kann. Die Beschreibung der Chancen und der Relevanz Virtueller Welten basiert auf den Erkenntnissen aus den Kapiteln 2 und 3 (vgl. Abbildung 1.1). Außerdem wird erläutert, welchen Beitrag die Evaluierung der IT-Sicherheit leisten kann.

Die Common Criteria sind ein Standard zur Sicherheitsevaluierung und bilden ein Rahmenwerk für die Definition von Anforderungen an die Sicherheit dieser Werte. Der Standard findet in der vorliegenden Arbeit Anwendung und wird in Kapitel 5 vorgestellt.

Das sechste Kapitel widmet sich detailliert der Analyse von Werten und Bedrohungen in Virtuellen Welten. Neben der Problemanalyse geht Kapitel 6 weiterhin darauf ein, eine Sicherheitsstrategie für den Schutz der Werte zu entwerfen. Es werden Annahmen, Richtlinien und Ziele definiert.

Im anschließenden siebten Kapitel werden daraufhin die Anforderungen zum Schutz dieser Werte definiert. Die Anforderungen sind eine begründete Auswahl von Anforderungen aus dem Katalog der Common Criteria.

Die Definition der Sicherheitsstrategie und der Anforderungen verlangt die Verwendung von Abkürzungen für die konkreten Bedrohungen, Annahmen, Richtlinien, Ziele und Anforderungen. Für Leser mit wenig Erfahrung im Bereich Common Criteria wird diese Schreibweise sehr schnell unübersichtlich. Daher wurde im Anhang eine Übersicht mit allen Abkürzungen der Sicherheitsstrategie und der Anforderungsdefinition sowie eine kurze Erläuterung eingefügt. Dieser Teil des Anhangs (Anhang A, S.184) ist ausklappbar und kann so den Leser unterstützen.

Das achte Kapitel fasst die Erkenntnisse aus Kapitel 6 und 7 in einem für Schutzprofile geforderten Format zusammen (vgl. Abbildung 1.1).

Dem Erfordernis einer gemeinsamen Betrachtung von technischen Anforderungen und Nutzungsverhalten widmet sich das neunte Kapitel. In beispielhaften Szenarien werden mögliche Umsetzungen diskutiert. Die Szenarien berücksichtigen Erkenntnisse aus Kapitel 2 (Virtuelle Welten), der Motivation der Nutzung (Kapitel 3), der Sicherheitsanalyse (Kapitel 6) und der Anforderungsdefinition (Kapitel 7) (vgl. Abbildung 1.1).

Kapitel 10 fasst die Arbeit zusammen und gibt einen Ausblick auf weitere Forschungsansätze.

Die Abbildung 1.1 stellt den Aufbau der Arbeit grafisch dar.

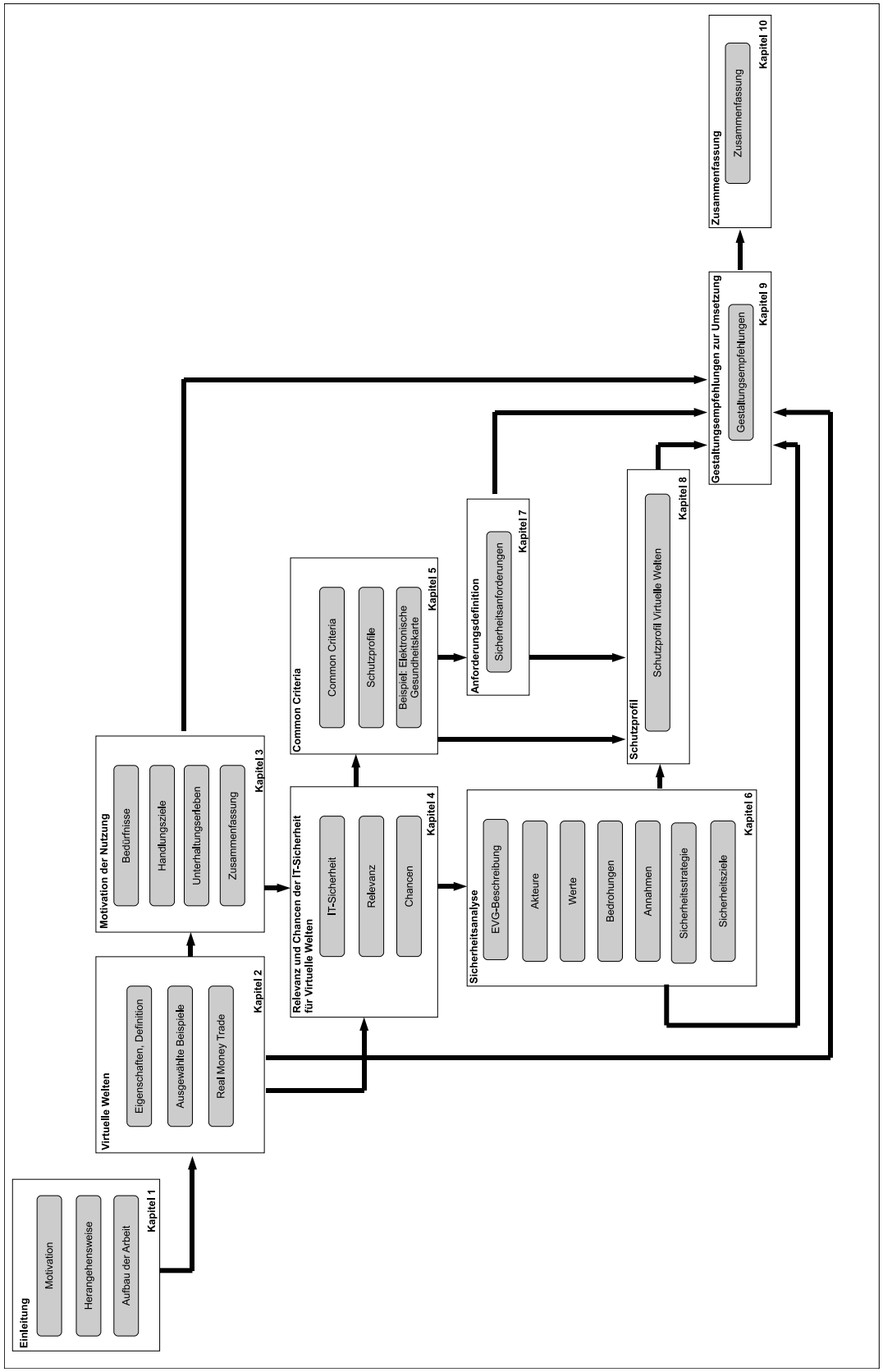


Abbildung 1.1: Aufbau der Arbeit

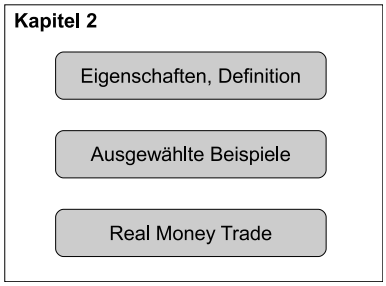
Kapitel 2

Virtuelle Welten

Ein wichtiger Schritt auf dem Weg zur Definition von Sicherheitsanforderungen an Virtuelle Welten ist es, zu verstehen, was Virtuelle Welten sind. Dieser Frage widmet sich das vorliegende zweite Kapitel. Um ein Verständnis zu erzeugen, ist es wichtig die Eigenschaften von Virtuellen Welten genauer zu untersuchen. Dies geschieht im ersten Teil des Kapitels. Durch die Zusammenfassung der Eigenschaften ist es im Anschluss möglich, eine genaue Definition des Begriffs „Virtuelle Welt“ zu erzeugen. Für eine anschauliche Darstellung der Definition sorgt im zweiten Teil des Kapitels die Vorstellung ausgewählter Beispiele von aktuellen Virtuellen Welten. Das Virtuelle Welten durchaus eine reale Relevanz haben, wird dadurch spürbar, dass virtuelle Güter mit realem Geld bezahlt werden. Das Phänomen, das unter dem Begriff „Real Money Trade“ bekannt geworden ist, greift der dritte Teil dieses Kapitels auf.

Zentrale Fragen, die in diesem Kapitel geklärt werden sollen, sind:

- Was sind Virtuelle Welten?
- Welche Eigenschaften haben Virtuelle Welten?
- In welchem Zusammenhang steht die Virtuelle Welt mit der Realität?
- Wie sehen derzeit aktuelle Virtuelle Welten aus?
- Welchen Nutzen/Mehrwert haben Virtuelle Welten?
- Was ist unter Real Money Trade zu verstehen?



2.1 Eigenschaften und Definition

Virtualität

„Virtuell“ wird umgangssprachlich oftmals als „etwas nicht Reales“ bzw. „nur in Gedanken existierend“ verstanden. Die virtuellen Objekte, die eine Virtuelle Welt formen, werden von einer oder mehreren Personen erdacht und entstehen aus der Phantasie der Entwickler. Sie werden durch Grafik, Simulation und visuelle Ausgabegeräte (z.B. Monitor) für alle Beteiligten sichtbar gemacht, so dass alle Partizipierenden dasselbe Bild (bzw. einen Ausschnitt) dieser Welt sehen.

Ein virtuelles Objekt ist aber keineswegs abhängig von einem real existierenden Objekt. Die Entwickler von Virtuellen Welten müssen nicht zwingend nur die Realität abbilden, sondern haben die Freiheit, sich jegliche Fantasieobjekte auszudenken (Fiktion).

Avatare, über die der Nutzer mit der Virtuellen Welt interagiert (siehe Interaktion) können fliegen, ihr Geschlecht binnen 1 Sekunde wechseln, verspüren keinen Hunger oder Durst und benötigen keinen Schlaf.

Obwohl die virtuellen „Sachen“ zwar offensichtlich nicht real existieren, können sie so wirken als ob sie existieren (vgl. [Duden 07a], [Blascovich 02][1], [Birchall 95][2]). Als virtuell wird damit die Eigenschaft einer Sache bezeichnet, die zwar nicht real, aber doch in der Möglichkeit existiert. Virtualität spezifiziert also ein konkretes Objekt über Eigenschaften, die **nicht physisch**, trotzdem ihrer **Leistungsfähigkeit nach vorhanden** sind (vgl. [Scholz 00]). Zur Verdeutlichung dieser Aussage, wird das Beispiel „virtueller Blumenstrauß“ herangezogen. Dieser existiert nicht physisch, das heißt er kann nicht berührt werden und er riecht nicht. Der virtuelle Blumenstrauß kann aber so wirken wie ein realer Blumenstrauß, wenn er Freude erzeugt. Genauso kann virtuelles Geld, wie reales Geld, die Wirkung Gier hervorrufen. Dabei kann das virtuelle Objekt gegenüber seinem realen Abbild einen Nutzenvorteil haben. Der virtuelle Blumenstrauß muss beispielsweise nicht gegossen werden und er verwelkt nicht. Das virtuelle Objekt wird also abstrahiert von den physischen Eigenschaften des realen Objekts.

Computergenerierte Welt

Eine Virtuelle Welt wird durch ein Computerprogramm generiert. Mittels visueller Ausgabegeräte (z.B. Monitore, Leinwände, Datenhelme, etc.) wird sie sichtbar gemacht. Die grafische Präsentation erfolgt in zwei bis drei Dimensionen, wodurch der Eindruck von Räumlichkeit entsteht (vgl. [Castronova 05] S.22).

Interaktion mithilfe eines Avatars

Um in der Welt agieren zu können, treten die Nutzer in einen Aktions-Reaktions-Zyklus mit der Welt. Mit Hilfe von Eingabegeräten lösen die Nutzer eine Aktion auf dem System

[1] „Synthetic sensory information that leads to perceptions of environments and their contents **as if they were not synthetic**“ ([Blascovich 02], S.105).

[2] [Birchall 95] beschreibt virtuell als eine Sache, die zwar „einen **Effekt**, aber **keine physische Bestandsform** hat“.

aus, indem ein Kommando an das System geschickt wird. Nach der Verarbeitung des Kommandos erfolgt eine Reaktion des Systems. Auf diese Weise treten Nutzer und System in einen Dialog, der eine Datenmanipulation zur Folge hat.

Die Interaktion ist als Prozess zu verstehen, der sowohl Veränderungen des Systems als auch Veränderungen beim Nutzer bewirkt und auch als Kommunikationsprozess bezeichnet wird. Beim Nutzer setzt ein Erkenntnisprozess ein, der es ihm erlaubt sich für entsprechende Folgeaktionen zu entscheiden. Dies kann auch als Lernprozess bezeichnet werden. Die Nutzer besitzen die Fähigkeit den Systemstatus durch Datenmanipulationen zu verändern.

Im Gegensatz zu anderen Medien (z.B. Fernsehen) fungiert der Nutzer einer Virtuellen Welt nicht nur als Konsument, sondern gleichzeitig als Produzent. Für die Kombination aus beiden hat sich, im neuen Verständnis des Web 2.0 [3], das Kunstwort „Prosument“ durchgesetzt.

Der Kommunikationsprozess kann bei Virtuellen Welten sowohl zwischen Nutzer und System (Human Computer Interaction) als auch zwischen Nutzern über ein System (Computer Mediated Communication) erfolgen. Bei Virtuellen Welten agieren viele Nutzer gleichzeitig (siehe Multiplayer/Mehrfachkonsumierbarkeit), die über das System in einen Kommunikationsprozess treten, z.B. miteinander chatten. Das Prinzip des Interaktionsprozesses ist vergleichbar mit dem der Human Computer Interaction. Die „Datenmanipulation“ beim Kommunikationspartner kann beispielsweise erreicht werden, wenn es einem Partner gelingt beim anderen einen Denkprozess anzustoßen und von einem Fakt zu überzeugen.

In einer Virtuellen Welt interagieren die Nutzer mit Hilfe eines Avatars. Ein Avatar ist die virtuelle Spielfigur des Spielers und beschreibt eine „grafische Darstellung, Animation, Karikatur o.Ä., mit der sich der Benutzer im Cyberspace eine virtuelle Identität schafft“ [Duden 07a].

[3] Tim O´Reilly prägte 2005 diesen Begriff. Danach existieren sieben Prinzipien der Veränderung des Umgangs mit dem Internet.

Interaktivität

Die Interaktion zwischen Nutzer und System beeinflusst die Interaktivität des Systems. Dies ist die Fähigkeit des Systems den Nutzer zu motivieren am Kommunikationsprozess teilzunehmen bzw. ihn einzubeziehen. Erst eine gute Interaktion zwischen Nutzer und System ermöglicht Interaktivität. Die Interaktivität eines Systems kann durch verschiedene Faktoren beeinflusst werden. Die Gestaltung interaktiver Elemente, wie Bedienelemente, Menüs, Werkzeugleisten und Dialogboxen, aber auch die Gestaltung von Raum und Zeit, der Story, der Benutzerkontrolle beeinflussen die Interaktivität eines Systems. Die Aufgabe der Entwickler ist es eine gute Interaktivität zu ermöglichen. Dazu müssen sie der Frage nachgehen: was passiert wo und zu welchem Zeitpunkt und welche Kontrolle hat der Nutzer zur Beeinflussung des Geschehens? Das Ziel ist eine optimale Aktivierung der Nutzer.

Immersion

Durch eine gute Gestaltung von Interaktion und Interaktivität einer Virtuellen Welt wird Immersion intensiviert. Immersion bezeichnet das „Eintauchen“ in eine Virtuelle Welt, das ein Gefühl das „dort seins“ erzeugt. Dieses Gefühl entsteht durch die Interaktion mit der umgebenden Welt. Werden bei der Interaktion verschiedene Sinne angesprochen (Sehen, Hören, Riechen, Schmecken, Tasten) erhöht dies die Immersion. Die Virtuelle Welt wirkt dann als würde sie physisch existieren. Durch Immersion können sowohl Emotionen transportiert als auch Realitätsverlust entstehen.

Richard Bartle unterscheidet vier Stufen der Immersion, die er mit „player“, „avatar“, „character“ und „persona“ beschreibt (vgl. [Bartle 01]). Die „Player“ sind die Spieler der Realwelt, die vor dem Computer sitzen und mit der Virtuellen Welt verbunden sind. Während „Avatar“ den Repräsentanten des Spielers in der Virtuellen Welt als Puppe bezeichnet, ist hingegen der „Character“ die Erweiterung des Spielers und bezeichnet eine Immersionsebene tiefer. Auf dieser Ebene beginnen die Spieler sich mit dem Spielcharakter zu identifizieren und sprechen in der ersten Person über sie („Ich habe zu wenig Lebensenergie, um diesen Gegner zu besiegen.“). Die tiefste Immersionsebene bezeichnet

Bartle als „Persona“. In dieser Ebene ist die Spielfigur Teil der Identität des Spielers. Nicht die Spielfigur verliert einen Kampf, sondern der Spieler selbst (vgl. [Bartle 01]).

Multiplayer/Mehrfachkonsumierbarkeit

Virtuelle Welten unterstützen den Mehrspielermodus (Multiplayer). Die Welt kann von tausenden Nutzern gleichzeitig genutzt werden (Mehrfachkonsumierbarkeit). Bei Onlinespielen (vgl. Kapitel 2.2) können so mehrere Spieler miteinander oder gegeneinander antreten. Dadurch bilden sich Communities (Gemeinschaften).

Persistenz

Durch die Eigenschaft der Mehrfachkonsumierbarkeit ergibt sich die Notwendigkeit der Persistenz. Sie bezeichnet „das Bestehen bleiben eines Zustands über längere Zeit“ [Duden 07b]. Für Virtuelle Welten bedeutet dies, dass sie dauerhaft zugänglich sind und dass sich das Geschehen weiterentwickelt, auch wenn ein Spieler nicht eingeloggt ist (vgl. [Castronova 05], S.80f.). Objekte, die der Welt zugeordnet werden (z.B. Bäume, Wege) können sich verändern wenn ein Nutzer nicht eingeloggt ist. Die Objekte, die einem Spieler zugeordnet werden, bleiben jedoch unveränderlich.

Zielorientierung

Nutzer haben unterschiedliche Handlungsabsichten bei der Nutzung von Virtuellen Welten, wie Unterhaltung, Handel, Kommunikation, Lernen, etc. Virtuelle Welten werden zielorientiert gestaltet, sodass die Nutzer ihre Handlungsabsichten umsetzen können. Die Zielorientierung der Virtuellen Welten kann unterhaltungsorientiert (z.B. World of Warcraft), handelsorientiert (z.B. Second Life), kommunikationsorientiert (z.B. Lively) und eher lernorientiert (z.B. Whyville) sein (vgl. dazu Kapitel 2.2). Oftmals werden die Virtuellen Welten auf mehrere Ziele ausgerichtet.

Existenz einer Verknüpfung zur Realwelt

Virtuelle Welten sind keine in sich geschlossenen, von der Realwelt getrennten Umgebungen. Vielmehr existiert eine Schnittstelle zur Realität. Castranova bezeichnet die Grenze zwischen den beiden Welten als Membrane. Demnach ist die Grenze keine unüberwindbare Barriere, sondern so „porös“, dass es den Menschen möglich ist sie ständig in beide Richtungen zu überqueren, wobei sie ihre Verhaltensweisen und Einstellungen von der einen Welt mit in die andere hinübernehmen (vgl. [Castronova 05], S. 147). Bei der Gestaltung seines Lebens ist der Mensch gezwungen seine ihm zur Verfügung stehende Zeit entsprechend seiner Bedürfnisse (vgl. Kapitel 3) einzuteilen. Offenbar haben Millionen von Menschen entdeckt, dass sie einen Teil ihrer Bedürfnisse in der Virtuellen Welt befriedigen können. Neben der Bedürfnisbefriedigung haben materielle Werte, wie Gegenstände und Fertigkeiten eine reale Relevanz (vgl. Kapitel 2.3).

Durch die enge Verknüpfung mit der Realwelt entstehen bei den Nutzern auch kognitive und emotionale Wirkungen. Es ist aber auch möglich, dass Nutzer dadurch einen Realitätsverlust erleiden. Durch exzessives Leben in verschiedenen virtuellen Identitäten kann es passieren, dass sich Menschen nicht mehr in der Realität zurechtfinden. Die Betroffenen erleben sich selbst nicht als real und steuerbar (vgl. [te Wildt 07]). Dieser Umstand wird auch als „Alternate World Syndrome“ bezeichnet und beschreibt eine psychologische Störung beim Übergang von der Virtuellen Welt in die reale Welt (vgl. [Heim 98]).

Definition: “Virtuelle Welten“

Virtuelle Welten sind interaktive mehrdimensionale Umgebungen, die durch einen Computer persistent simuliert werden und in denen viele Nutzer gleichzeitig mithilfe ihrer Avatare interagieren um ein Ziel (z.B. Unterhaltung, Information, Handel, Kommunikation, etc.) zu erreichen. Obwohl die Virtuelle Welt nicht physisch existiert, kann sie so wirken als täte sie es (Immersion), wodurch sowohl emotionale und kognitive Wirkungen als auch Realitätsverlust erstehen können. Die Objekte in der Virtuellen Welt können Abbilder aus der realen Welt oder Fiktion sein.

2.2 Ausgewählte Beispiele Virtueller Welten

Die wohl bekanntesten Virtuellen Welten sind die Onlinerollenspiele, auch Massively Multiplayer Online Roleplaying Games (MMORPG) genannt, die auch die erfolgreichsten[4] Onlinespiele sind. Dazu gehören „World of Warcraft“, „Guild Wars“ (vgl. Kapitel 2.2.1), „Everquest“ und „Everquest 2“, „Ultima Online“, „Dofus“, „Star Wars Galaxies“, „Eve Online“ und „Dark Age of Camelot“, „Final Fantasy XI“ und viele weitere.

Die Anfänge der Onlinerollenspiele reichen in die 1970er Jahre zurück zu den so genannten Multi User Dungeons (MUDs). Das erste MUD, dass prägend auch MUD1 hieß, wurde von Roy Trubshaw und Richard Bartle entwickelt (vgl. [Lober 07], S.7).

In Onlinerollenspielen schlüpfen die Nutzer, wie der Name bereits sagt, in eine Rolle. Die Spieler können beispielsweise als Krieger in Schlachten ziehen, als Magier auftreten oder als Bettler oder Prostituierte arbeiten (vgl. [Schmitz 07], S.47).

Mit ihren Avataren bewegen sich die Spieler in der virtuellen Welt und lösen Quests (Aufgaben), kämpfen gegen so genannte NPCs (Non Person Characters), betreiben Handel und sammeln Gegenstände und Gold oder Geld. Dazu gehört auch das „Entdecken von neuen Gebieten“ und „das Erlernen von neuen Fähigkeiten (wofür meist Erfahrung gesammelt werden muss)“ [Lober 07].

Bestimmte Abschnitte im Spiel können nur in Zusammenarbeit mit anderen Spielern absolviert werden. „Diese Elemente zwingen die Spieler zu sozialer Interaktion. Mit Hilfe von integrierten Messenger- oder Voicetools können die Spieler miteinander kommunizieren, wodurch ein hoher Grad an Interaktion entsteht. Darauf gründen sich oft Freundschaften, die teilweise jahrelang halten und fortdauern, wenn die Beteiligten das ursprüngliche Spiel längst verlassen haben“[Lober 07].

Richard Bartle hat herausgefunden, dass die Spieler nicht alle Möglichkeiten gleichermaßen nutzen, sondern verschiedene Präferenzen der Zielerreichung haben. Er unterscheidet in seiner Taxonomie dazu die vier Spielertypen „Achiever“, „Explorer“, „Socialiser“ und „Killer“ [Bartle 96]. „Achiever“ setzen sich selbst spielrelevante Ziele und bewegen sich in der Welt um möglichst viele hochwertige Schätze zu sammeln, schnellstmöglich

[4] 94,1% Marktanteil von Fantasy RPG, [mmogchart.com 08]

ein hohes Level zu erreichen bzw. viele Punkte zu erhalten. „Achiever“ haben Freude an der Beherrschung des Spiels. Sie sind stolz auf ihren Status innerhalb des Spiels und das erreichte Level. „Explorer“ erkunden die Welt. Sie wollen jeden Winkel der Virtuellen Welt kennen. Sie experimentieren mit der Physik des Spiels und finden heraus wie Dinge funktionieren. Dadurch haben sie die Möglichkeit besondere Merkmale und Funktionen oder auch Bugs in der Software zu finden. Explorer sind stolz auf ihr Wissen über die Welt und erhalten Anerkennung, wenn sie zum Beispiel Newcomern mit diesen Informationen weiterhelfen. „Socialiser“ lieben den Kontakt zu anderen Spielern. Sie nutzen alle Möglichkeiten der Kommunikation innerhalb des Spiels (Chat, Gesten, etc.). Sie sympathisieren mit anderen Spielern, machen Witze, unterhalten sich, hören zu und bauen oftmals lang anhaltende Freundschaften auf. „Socialiser“ versuchen andere Spieler genauer kennen zu lernen und sind stolz auf ihre Freundschaften, Kontakte und ihren Einfluss auf sie. „Killer“ verfolgen das Ziel andere Spieler und NPCs zu peinigen. Sie benutzen mit Spaß ihre Waffen. Je größer das Elend der anderen ist, desto größer ist auch ihre eigne Befriedigung. Sie sind stolz auf ihre Reputation und Kampffähigkeiten (vgl. [Bartle 96]).

Die Spielertypen treten nicht in reiner Form auf, sondern jeder Spieler hat Elemente jeden Spieltyps. Spieler deren Hauptausrichtung „Killer“ ist, müssen auch „Achiever“ sein, um genug Punkte und Macht zu haben, um ihre Kämpfe auszuführen. Sie müssen auch in gewissen Maße „Socialiser“ sein, um sich ihre Opfer auszusuchen. „Socialiser“ wiederum sind auch „Explorer“, da sie, wenn sie sich in der Welt bewegen neue Spieler kennen lernen und wenn sie merken, dass einer ihrer Freunde gepeinigt wird, können sie auch selbst zum „Killer“ werden. „Explorer“ sind auch „Killer“, da sie auch diese Funktion im Spiel erkunden müssen, und „Socialiser“, da sie gerne ihr Wissen mit anderen teilen, um Anerkennung zu finden. So hat jeder Spieler seine Hauptausrichtung, die davon abhängt, was ihm die größte Freude, den größten Spaß am Spiel bringt [Bartle 96].

2.2.1 Guild Wars

Neben „World of Warcraft“ gehört „Guild Wars“ zu den erfolgreichsten MMORPGs. Das von Arenanet entwickelte und von NCsoft vertriebene Onlinerollenspiel wurde erstmals im April 2005 veröffentlicht. Später kamen ein Add-on und drei weitere Episoden hinzu,

die sowohl eigenständig als auch in Kombination spielbar sind (vgl. [NCsoft 09]). Die Abbildung 2.1 zeigt eine Szene aus Guild Wars mit vier Spielerfiguren und einem Händler vor seinem Verkaufsstand.

Abbildung 2.1: Szene aus Guild Wars [eigene Abbildung]

Über das integrierte Chat-System können die Spieler miteinander kommunizieren.

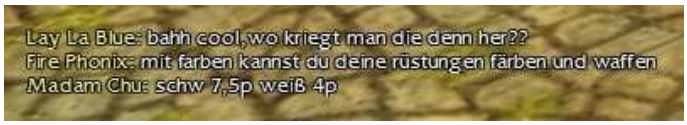


Abbildung 2.2: Chat in Guild Wars [eigene Abbildung]

Abbildung 2.3: Avatar
in Guild Wars
[eigene Abbildung]

Bevor der Spieler die Virtuelle Welt nutzen kann, muss er zunächst einen Avatar erstellen, dem eine Charakterklasse (z.B. Krieger, Mönch, Elementarmagier, Ritualist, etc.) zugewiesen wird. Die Abbildung zeigt die Gestaltung eines Avatars der Klasse Krieger mit angelegter Rüstung.

Abbildung 2.4: Quest
in Guild Wars
[eigene Abbildung]

Die Aufgabe des Spielers besteht darin, die Welt von Tyria vor Angriffen zu schützen. Dazu können sich die Spieler in Gruppen zusammenschließen oder mithilfe von Non-Player-Characters (computergesteuerte Charaktere) Aufgaben (Quests) absolvieren. Die Abbildung 2.5 zeigt die Beschreibung einer Quest, die dem Spieler von einem Non-Player-Character angeboten wird.

Abbildung 2.5: Kampfszene in Guild Wars
[eigene Abbildung]

Bei einem Kampf gegen andere Spieler(-gruppen) oder NPCs kommt es neben den verfügbaren Gegenständen und Fertigkeiten auch auf eine gute Kombination der Charakterklassen an. Die Abbildung 2.5 zeigt einen Avatar während einer Kampfszene mit einer NPC-Kreatur.

Abbildung 2.6: Belohnung in Guild Wars
[eigene Abbildung]

Für das erfolgreiche Töten des „Flussskals“ erhält der Spieler sechs Goldmünzen.

Für erfolgreiches Absolvieren der Quests erhalten die Spieler Gold, Gegenstände sowie Erfahrungspunkte. Die Abbildung 2.7 zeigt die Erfahrung eines Avatars in Guild Wars mit 13665 Erfahrungspunkten und der Erfahrungsstufe 5.

Abbildung 2.7: Übersicht Erfahrungspunkte in Guild Wars [eigene Abbildung]

Das integrierte Handelssystem erlaubt den Kauf und Verkauf der Gegenstände.

Abbildung 2.8: Handel in Guild Wars [eigene Abbildung]

2.2.2 Second Life

Neben den Onlinerollenspielen haben sich Virtuelle Welten als Handelsplattformen etabliert, in denen sich ernsthafte Wirtschaftssysteme (vgl. auch Kapitel 2.3) entwickelt haben. Akademische Forschergruppen widmen sich bereits der Untersuchung der Ökonomie in Virtuellen Welten, auch als „Virtual Economy“ bezeichnet.

Eine durch die Medien sehr bekannt gewordene virtuelle Handelsplattform ist Second Life (Abbildung 2.9). Das von der US Firma Linden Lab 2003 veröffentlichte Second Life erreichte im November 2008 sechzehn Millionen registrierte Nutzer, von denen sich zirka eine Million Nutzer regelmäßig einloggen [SecondLife 07b].

Abbildung 2.9: Szene aus Second Life [eigene Abbildung]

Das „zweite Leben“ bietet den Nutzern die Chance sich mit einer virtuellen Parallel-Identität selbst zu verwirklichen und Träume wahr werden zu lassen.

Die Virtuelle Welt stellt ein Baukastensystem zur Verfügung, mit dem neue Objekte für die Welt erzeugt werden können. Das können Gegenstände, wie Kleidung, Pflanzen, Autos, Waffen, etc. sein. Der Vorstellungskraft der Nutzer sind dabei keine Grenzen gesetzt.

Mit entsprechenden Animationen wird den Objekten „Leben“ eingehaucht. So wird zum Beispiel Wind durch das hin- und herbewegen der Bäume simuliert. Die Nutzer erhalten für alle selbst erstellten Gegenstände das Urheberrecht. Das ist die Grundlage für einen legalen Handel mit den Gegenständen (vgl. Kapitel 2.3).

Eine Möglichkeit Handel zu betreiben, ist der Verkauf von Gegenständen. Viele Bewohner von Second Life haben sich darauf spezialisiert Kleidung herzustellen. Um nicht als „Newbie“ erkannt zu werden bzw. um sich ein individuelles Erscheinungsbild zu geben, nutzen viele Bewohner das Angebot der Boutiquen, die Kleidung anbieten. Aber auch andere virtuelle Güter, wie Haarschnitte, Möbel und Häuser verkaufen sich gut.

Die interne Währung heißt Lindendollar und kann mit einem Kurs von zirka 270:1 mit realen US-Dollar getauscht werden (vgl. [Rymaszewski 07]). Der Lindendollar wird an der offiziellen Second Life Devisenbörse LindeX gehandelt und liegt relativ stabil bei 270 Lindendollar zu einem US-Dollar.

Es gibt außerdem die Möglichkeit virtuelle Grundstücke zu kaufen, wofür zunächst eine Premium-Mitgliedschaft für 9,95 US-Dollar abgeschlossen werden muss. Für zirka 1500 US-Dollar Kaufpreis und 220 US-Dollar Wartungskosten kann ein Grundstück von 65536 Quadratmetern Größe erworben werden. Ein eigenes Grundstück zu kaufen oder zu mieten, ist für das Betreiben eines eigenen Geschäftes in Second Life unabdingbar.

Mit einer kostenlosen Basismitgliedschaft können sich die Nutzer einen Avatar erstellen, der sehr feingranular individuell gestaltet werden kann.

Abbildung 2.10: Gestaltung des Avatars in Second Life [eigene Abbildung]

Viele Firmen der realen Welt, darunter IBM und EnBW, nutzen Second Life für Marketing und Vertrieb ihrer realen Produkte und haben daher ein virtuelles Geschäft eröffnet.

Abbildung 2.11: Präsentation der Firma EnBW in Second Life [eigene Abbildung]

In Second Life kann auch gelernt werden. Die Volkshochschule Goslar bietet viele Kurse (z.B. Sprach- und EDV-Kurse) in der Virtuellen Welt an (vgl. [Vhs 09]).

Abbildung 2.12: Volkshochschule in Second Life [eigene Abbildung]

2.2.3 Whyville

Es existieren Virtuelle Welten als Lernplattformen. Sie sind momentan bei Weitem nicht so bekannt wie die MMORPGs, haben sich aber mit der Vermittlung von Wissen und der Anregung zum Lernen ein hohes Ziel gesteckt.

Eine Virtuelle Welt, die dieses Ziel umsetzt, ist Whyville (vgl. Abbildung 2.13). Das von Numedeon Inc. gegründete Whyville möchte sich die Beliebtheit der Computerspiele bei Kindern und Jugendlichen zu nutze machen, um Wissen auf den Gebieten der Naturwissenschaften, Ökonomie und Sozialkunde zu vermitteln. Dem Ansatz des konstruktivis-

Abbildung 2.13: Whyville [eigene Abbildung]

tischen Lernens folgend, können die Nutzer für die Durchführung von Lernaktivitäten ein virtuelles Gehalt, die so genannten „Clams“ verdienen. Das Geld kann dann für Einkäufe ausgegeben werden. Die Schüler können außerdem ein eigenes Geschäft eröffnen, für eine Zeitung schreiben und sich für den Whyville Senat zur Wahl stellen. Durch die Bildung von Communities werden die Schüler angeregt, sich über verschiedene Themen auszutauschen oder gemeinsam an der Lösung einer Lernaufgabe zu arbeiten. Für die Zukunft ist die Umsetzung einer integrierten Bibliothek geplant, in der die Schüler Zugriff auf Texte sowie Audio- und Videomaterial zu den einzelnen Themen haben.

2.2.4 Google Lively

Die Kommunikation mit anderen Nutzern und die Bildung von Communities ist bei allen Virtuellen Welten ein wichtiger Bestandteil. In den meisten Virtuellen Welten ist die Kommunikation und Interaktion mit Anderen eine wichtige Vorraussetzung für das Erreichen von Zielen, wie der Entwicklung der Rolle bei MMORPG oder den Kontakt mit Kunden bei den virtuellen Handelsplattformen.

Im Juli 2008 hat Google die Virtuelle Welt „Lively“ (vgl. Abbildung 2.14) auf den Markt gebracht, dessen alleinige Zielsetzung die Kommunikation ist. Vergleichbar ist Lively mit Instant Messengern. Während diese eine minimale Oberfläche mit einer Übersicht der Kontakte in Textform bieten, kann der Nutzer von Lively seinen eigenen Raum erstellen und nach seinen Wünschen einrichten und so eine Atmosphäre für Gespräche schaffen.

Abbildung 2.14: Google Lively [eigene Abbildung]

2.3 Real Money Trade

Aus den oben erläuterten Beispielen wird deutlich, dass Handel ein wichtiger Bestandteil in Virtuellen Welten ist. Dieser Handel kann einerseits über das interne Handelssystem

mit Einsatz von „Spielgeld“ erfolgen, andererseits geben Nutzer reales Geld für virtuelle Güter aus. Der Handel virtueller Güter mit Einsatz von realem Geld (US-Dollar, Euro, etc.) wird als Real Money Trade (RMT) bezeichnet. Virtuelle Güter sind Assets, die in Virtuellen Welten gehandelt werden, beispielsweise Charaktere, Gegenstände, und Geld.

Das Urheberrecht ist ein zentraler Aspekt, der beim Handel mit virtuellen Gütern berücksichtigt werden muss. Das Gesetz schützt die wirtschaftlichen Interessen des Urhebers eines Werks. Ist der Anbieter einer Virtuellen Welt der Ersteller des Werks, also der Assets einer Virtuellen Welt, so hat er das Urheberrecht an seiner Kreation. Der Anbieter weist in den End User License Agreements (EULA) und den Terms of Service (TOS) darauf hin. Obwohl dieses Recht besteht, werden die Assets im Internet frei gehandelt. Dafür werden verschiedene Dienste und Plattformen genutzt.

Eine verbreitete Vorgehensweise ist der Handel über die Auktionsplattform Ebay (vgl. Abbildung 2.15). In der Ebay-Kategorie „Onlinespiele“ [Ebay 09] werden Gold, Gegenstände und Charaktere versteigert. Weiterhin haben sich Broker (z.B. Markee Dragon

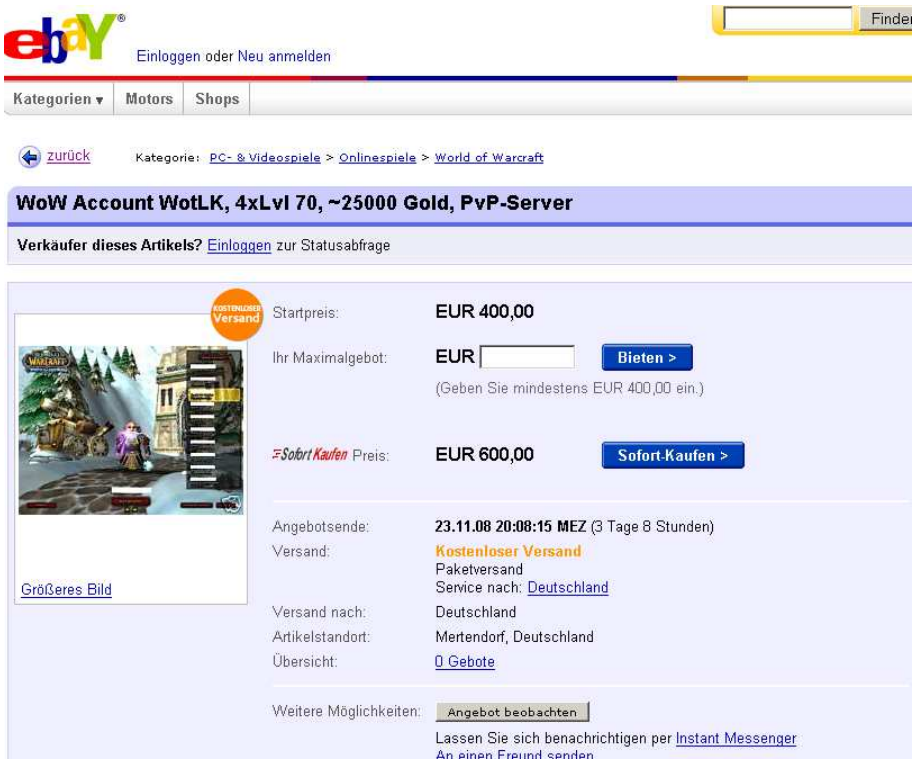


Abbildung 2.15: Verkauf eines World of Warcraft Accounts bei Ebay [eigene Abbildung]

Broker [MDB 08]) etabliert, die sich darauf spezialisiert haben Waren im Spiel billig einzukaufen und für einen höheren Preis wieder zu verkaufen. Dadurch generiert die Firma Umsätze und Gewinne und kann so den Lebensunterhalt einiger Angestellter finanzieren.

Internet Gaming Entertainment [IGE 08] ist eine bekannte Plattform für den Handel virtueller Güter, auf der für verschiedene Virtuelle Welten (Wow, Everquest 2, Eve Online, etc.) vor allem Geld angeboten wird. Dreihundert Stück WoW-Gold werden beispielsweise für 18,45 US-Dollar verkauft (vgl. Abbildung 2.16). Diese professionellen Anbieter akzeptieren Zahlungen per Banküberweisung, Paypal oder Kreditkarte. Da es auch schon vorgekommen ist, dass Käufer ihre Ware nicht erhalten haben, werden Order Tracking Systeme eingesetzt. Außerdem versuchen einige Spieler durch Handel in Virtuellen Wel-

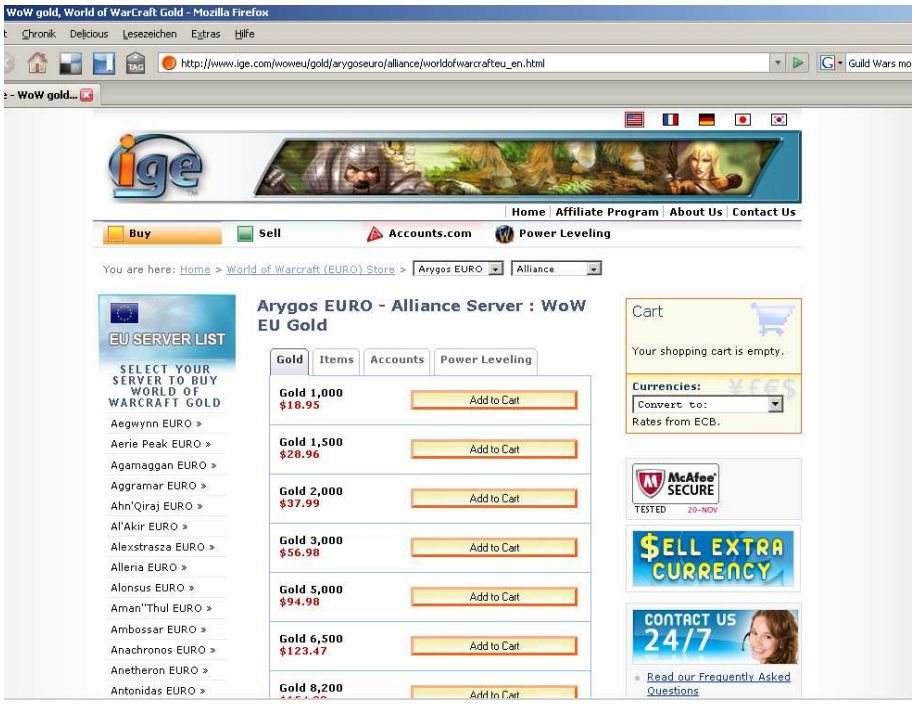


Abbildung 2.16: Verkauf von World of Warcraft Gold bei IGE

ten einen Lebensunterhalt zu verdienen. In einem Experiment in Ultima Online fand der Journalist Julian Dibbell heraus, dass es möglich ist, einen Lebensunterhalt mit dem Handel in Virtuellen Welten zu verdienen. Sein Experiment wurde in seinem Blog regelmäßig beschrieben und später auch in einem Buch veröffentlicht [Dibbell 06].

Eine weitere Verdienstmöglichkeit ist das so genannte „Power Leveling“. Das ist eine Dienstleistung, die darin besteht, Spielern das Spielen abzunehmen. Ein Einsteiger kann so gegen reales Geld seinen Avatar auf ein hohes Level spielen lassen. Er hat dadurch eine Zeitersparnis, da er nicht erst mühsam viele Stunden spielen, viele Quests lösen und viele Monster besiegen muss. Dieses Vorgehen wird in der Community nicht akzeptiert und als Cheating, also unfaires Spielen angesehen.

So genannte „Goldfarmer“ nutzen die Möglichkeiten des Real Money Trade aus, um möglichst viel Geld in kurzer Zeit zu verdienen (vgl. [Heeks 08]). Für eine gleichberechtigte Bereitstellung von Quests für alle Spieler, sind die Onlinespiele so programmiert, dass Herausforderungen ständig angeboten werden. Für das erfolgreiche Lösen von Quests bekommt der Spieler eine Belohnung zum Beispiel in Form von Gold. Eine Quest könnte also lauten, „töte 100 wilde Säbelzahntiger“. Der Spieler tötet also 100 Säbelzahntiger und jeder Tiger lässt, wenn er stirbt, 1 Goldstück fallen. Der Spieler sammelt das Geld ein und beginnt eine andere Quest. Die Spieler die als „Goldfarmer“ arbeiten, nutzen nun die Eigenschaft des „Spawnen“, also das „Wiedererscheinen“ der Charaktere in der Welt. Das bedeutet, dass kurz nachdem 100 Säbelzahntiger getötet wurden, 100 neue auftauchen. Die Goldfarmer tun nichts anderes als ständiges Einsammeln des Goldes. Das Gold wird anschließend für reales Geld extern verkauft und innerhalb der Virtuellen Welt an den Käufer übergeben. Dadurch fließt kein Geld ab und die Menge des Geldes bzw. Goldes erhöht sich ständig. Dadurch erfolgt eine Wertminderung des Geldes (Inflation). Eine rasante Steigerung der Inflation erfährt das Wirtschaftssystem, wenn nicht reale Spieler händisch das Sammeln übernehmen, sondern zusätzliche Softwareprogramme, so genannte Exploits, dies automatisiert tun.

Eine Möglichkeit Geld zu generieren ohne Handel zu betreiben, ist das Ausnutzen von Fehlern in der Programmierung der Software (Bugs). Haben zum Beispiel zwei NPC-Händler unterschiedliche Preise für dasselbe Item, kann ein Spieler bei einem Händler einen Gegenstand billig einkaufen und bei dem anderen teurer wieder verkaufen.

Aufgrund der genannten Probleme mit illegalem Real Money Trade sind einige Anbieter dazu übergegangen RMT zu legalisieren bzw. bewusst zu stimulieren, wie beispielsweise Second Life, Entropia Universe, Habbo Hotel, Everquest 2 und There. In diesen Welten

können die Nutzer offiziell und legal, reales Geld gegen die interne Währung (Lindendollar, PE-Dollar, Habbo Taler, Platinum, Therebucks) tauschen und mit diesem Geld handeln. Der Vorteil dieser Variante liegt im ungestörten Abschluss der Transaktionen ohne das lästige Wechseln auf externe Plattformen.

Drittanbieter, wie Live Gamer [LG 08] haben sich auf die Integration der RMT-Funktionalität in das jeweilige System spezialisiert. Die LiveGamer-Komponente kommt zum Beispiel bei Everquest 2 zum Einsatz.

Neben dem Handel mit Gegenständen hat sich auch das Angebot von Dienstleistungen etabliert. Es werden Leistungen angeboten, die den Handel in der Virtuellen Welt unterstützen. So haben sich, zum Beispiel in Second Life, einige spezialisierte „Berufe“, wie Animateure, Skripter, Builder etc., gebildet, die ihre Dienstleistungen anderen Teilnehmern zur Verfügung stellen.

Um ein fertiges Produkt anbieten zu können, darf es nicht nur eine leere Hülle haben, sondern muss gut aussehen und eine Funktionalität haben. Animateure werden engagiert, um die Bewegungen zu erstellen und Programmierer, füllen das Produkt zusätzlich mit Funktionalitäten. Es haben sich regelrecht Lieferketten von der Produktion der Einzelteile, die Montage und den Vertrieb gebildet. Am Ende der Kette steht der Kunde, der dafür (reales) Geld bezahlt und das Produkt nutzt. Die Wirtschaftssysteme folgen den betriebswirtschaftlichen Prinzipien der Realwelt. Preise gestalten sich nach Angebot und Nachfrage. Ist die Nachfrage groß, das Angebot jedoch klein, ist der Preis hoch. Ist ein großes Angebot vorhanden, die Nachfrage jedoch niedrig, ist auch der Preis niedrig. Die Wirtschaftssysteme einiger Virtueller Welten erreichen ein Bruttoinlandsprodukt, dass vergleichbar ist mit denen einiger europäischer Länder.

Eine weitere Möglichkeit die sich durch Handelssysteme wie Second Life ergeben, ist der Handel mit realen Gütern. Dabei dient die Virtuelle Welt als reine Vertriebsplattform für reale Produkte. Das wohl bekannteste Beispiel hierfür sind die von Adidas, in der Virtuellen Welt von Second Life, verkauften Turnschuhe. Der Nutzer hat die Möglichkeit sich die nachgebildeten Turnschuhe in 3D anzuschauen, indem er sie seinem Avatar anzieht. Es ist möglich direkt eine Transaktion für den Kauf der realen Turnschuhe anzustoßen.

Abbildung 2.17: Potato System der 4FO AG in Second Life [eigene Abbildung]

Auch Technologieanbieter, wie die 4FriendsOnly AG haben Second Life für sich entdeckt und starten erste Probeläufe für den viralen Vertrieb von Musik über Second Life. Im realen Leben stellt die 4FriendsOnly AG unter anderem die Plattform „Potatosystem“ zur Verfügung, dass es Labels und Musikern erlaubt ihre Werke über virales Marketing zu vertreiben.

Abbildung 2.18: IBM Produktpräsentation in Second Life [eigene Abbildung]

Die Firma IBM investiert in Second Life um Konferenzen abzuhalten und Produkte zu präsentieren.

Tabelle 2.1 stellt die oben erläuterten Phänomene des RMT anhand einiger Virtueller Welten gegenüber.

Name Anbieter Webseite (veröffentlicht)	Anzahl Nutzer	Kurzbeschreibung	RMT
World of Warcraft Blizzard/Vivendi www.wow-europe.com (2004/2005)	10 Mio. (Jan. 2008)	In der Welt von Azeroth schlüpfen die Spieler in die Rolle von Kriegern, Elfen, etc. Sie können sich zu Gilden zusammenschließen und gemeinsam Aufgaben (Quests) lösen, die Welt erkunden und Handel betreiben. Die Ingame-Währung Gold, die bei erfolgreichen Quests verdient wird, kann für den Tausch mit Gegenständen eingesetzt werden. Über einen integrierten Chat oder externe VoIP-Tools kommunizieren die Mitglieder untereinander.	RMT wird vom Anbieter verboten und durch EULA und ToS ausgeschlossen, ist aber dennoch sehr verbreitet. WoW-Gold und Accounts werden über externe Plattformen, wie IGE, Ebay, etc. getauscht. Wird RMT durch den Anbieter entdeckt, erfolgt die Schließung des Accounts.
Everquest 2 Verant/Sony IE everquest2.station. sony.com (2004)	270.000	Auf Norrath wählt der Spieler eine Rasse (z.B. Fee, Zwerg, Gnom, Mensch) und eine Charakterklasse (z.B. Kämpfer, Kundschafter, Priester, Magier) und löst allein oder in einer Gruppe Quests, erkundet die Welt, kommuniziert und entwickelt dadurch seinen Charakter weiter.	RMT wird vom Anbieter unterstützt. Platinum und Gold kann sowohl ingame, z.B. über LiveGamer, als auch über externe Plattformen gehandelt werden.
Second Life LindenLab secondlife.com (2003)	15 Mio.	Second Life ist eine virtuelle Handelsplattform, in der Nutzer eigene Gegenstände herstellen und Handel treiben können. Die Währung Linden$ kann gegen reale US$ getauscht werden. Die Besonderheit bei Second Life ist, dass der Anbieter für den nutzergenerierten Content die Urheberrechte den Nutzern explizit einräumt. Viele reale Unternehmen nutzen SL als neuen Absatzkanal ihrer realen Produkte.	RMT ist explizit vorgesehen (270 Linden$ entspricht ca. 1US$).
There Makena Technologies there.com (2003)	k.A.	There ist eine Virtuelle Welt ähnlich Second Life und bietet seinen Nutzern die Möglichkeit zu spielen, zu kommunizieren, eigene Gegenstände zu erstellen und zu handeln. Die interne Währung heißt Therebucks.	
Entropia Universe Mindark entropiauniverse.com (2003)	740.000 (Juli 2008)	Im Entropia Universe können die Nutzer den Planeten Calypso und das Weltall erkunden. Gehandelt wird mit PE-Dollar.	10 PE-Dollar können für einen US-Dollar erworben werden. RMT ist notwendig, um im Spiel vorwärts zu kommen. Mindark verkauft virtuelle Grundstücke an seine Kunden.

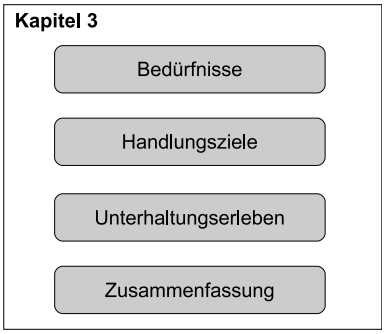
Neopets MTV Networks neopets.com (1999)	162 Mio.	In der Welt von Neopia kümmern sich die Nutzer um virtuelle Haustiere. Durch Spiele gewinnen sie Neopunkte (Währung) mit denen sie Gegenstände kaufen bzw. in Auktionen ersteigern können.	Seit 2007 wird ein externes Einkaufszentrum, NC Center, betrieben. Für reales Geld können die Nutzer Neocash tauschen und Gegenstände kaufen.
Habbo Hotel Sulake Coorp. Oy www.sulake.com (2000)	114 Mio.	In dem, auf Teenager ausgerichteten, Onlinespiel können die Nutzer Räume erstellen und verändern. Die einzelnen Räume sind zu einem Hotel verbunden. Um die Räume einrichten zu können, brauchen die Nutzer virtuelle Möbelstücke, die sie für Habbo Taler (engl. Habbo Credits) kaufen können.	Habbo Taler können per Kreditkarte, Prepaid-Karte, Telefon und Mobiltelefon bezahlt werden (30 Habbo Credits = 5 Euro).
Lively Google Inc. www.lively.com (2008)	k.A.	Lively ist eine auf Kommunikation ausgerichtete Virtuelle Welt, ähnlich einem Instant Messenger. In dem virtuellen 3D-Chat können bis zu 20 Personen gleichzeitig in einem Raum miteinander kommunizieren. Der Text erscheint als Sprechblase über dem jeweiligen Avatar.	Kein RMT
Whyville Numedeon www.whyville.net (1999)	3 Mio. (2008)	Whyville ist eine auf Ausbildung fokussierte Virtuelle Welt, die sich an Schüler zwischen acht und fünfzehn Jahren richtet. Durch Spiele und andere Aktivitäten sollen die Kinder motiviert werden zu lernen. Die Themen reichen von Naturwissenschaften, und Wirtschaft bis Staatsbürgerkunde. Durch die Teilnahme an Ausbildungsaktivitäten verdienen die Nutzer virtuelles Geld. Sie können auch ein eigenes Geschäft eröffnen. Geplant ist der Aufbau einer Virtuellen Bibliothek, der Whybrary (Kunstwort aus Whyville und Library).	Kein RMT

Tabelle 2.1: Real Money Trade in Virtuellen Welten

Der Überblick macht deutlich, dass die Nutzer Werte in der Virtuellen Welt besitzen. Diese Werte müssen vor Angriffen geschützt werden. Welche Werte die Nutzer besitzen und wie diese Werte bedroht werden, wird in Kapitel 6 analysiert. In Kapitel 7 wird erläutert, welche Anforderungen sich daraus an den Schutz der Werte ergeben.

Kapitel 3

Motivation der Nutzung Virtueller Welten



Kapitel 2 ist zu entnehmen, dass Virtuelle Welten IT-Anwendungssysteme sind, die unterschiedliche Ziele erfüllen können. Virtuelle Welten können laut Definition (vgl. Kapitel 2, S.15) genutzt werden um Freizeit zu gestalten, Unterhaltung (z.B. durch Spiel) zu erleben, aber auch um andere Ziele zu erreichen, wie Kommunikation, Information und Arbeit zu verrichten (z.B. Produkte vertreiben). Diese Ziele können jedoch auch mit anderen Medienangeboten (z.B. Fernsehen, Bücher, Zeitschriften, etc.) und anderen Tätigkeiten (z.B. Gespräch, Party, etc.) erreicht werden. Es ist daher zu untersuchen, warum Menschen Virtuelle Welten nutzen. Diese Betrachtung ist auch wichtig, da Virtuelle Welten als sozio-technische Systeme zu betrachten sind. Dieses Kapitel fokussiert die sozialen Faktoren der Nutzung durch Menschen. Bei der Umsetzung von IT-Sicherheitsmaßnahmen in

Virtuellen Welten müssen diese Faktoren berücksichtigt werden. Nur so kann eine Akzeptanz der Maßnahmen bei den Nutzern erreicht werden.

Die Fragen, die im vorliegenden dritten Kapitel daher beantwortet werden, sind:

- Wie lässt sich die Motivation zur Nutzung Virtueller Welten theoretisch erklären? (Warum nutzen Menschen Virtuelle Welten?)
- Inwiefern können Menschen ihre Bedürfnisse in Virtuellen Welten stillen?
- Inwiefern können Menschen ihre Fähigkeiten in Virtuellen Welten entwickeln?

Um auf die Frage nach der Motivation der Nutzung eine Antwort zu finden, stellt die Autorin, auf der Grundlage einer Literaturrecherche, verschiedene Perspektiven auf die Nutzungsmotivation zusammen. Ausgangspunkt bildet die Annahme, dass Menschen Bedürfnisse haben und daher Handlungsziele verfolgen. Im Kontext der Virtuellen Welten und Onlinespiele wird anschließend das Phänomen „Unterhaltungserleben“ genauer untersucht. Eine empirische Überprüfung der verschiedenen Perspektiven ist nicht der Gegenstand dieser Arbeit, sondern muss als Forschungsgegenstand der Sozialwissenschaften verstanden werden.

3.1 Bedürfnisse

Menschen haben Bedürfnisse und streben danach diese zu erfüllen. Sie haben dadurch eine Motivation zur Handlung, denn nur durch Tätigkeiten können die Bedürfnisse gestillt werden. In der Kommunikations- und Medienwissenschaft hat sich der Nutzen-Belohnungs-Ansatz (englisch: Uses-and-Gratifications-Ansatz) für die Erforschung der (Massen-)Mediennutzung etabliert (vgl. [Schweiger 07]). Der Nutzen-Belohnungs-Ansatz stellt sich der Frage, warum Menschen Medien nutzen (vgl. [Schweiger 07], S.60) und geht davon aus, dass sie durch die Nutzung spezifische Bedürfnisse befriedigen (vgl. [Schweiger 07], S.61). Zu den wichtigsten Bedürfnissen, die durch Medien gestillt werden können, zählen Information und Unterhaltung (vgl. [Schweiger 07], S.61). Die Analyse der Bedürfnisse erfolgt in der Regel durch Befragung der Rezipienten und muss

jedoch auf Bedürfnisse beschränkt bleiben, die durch Medien gestillt werden können (vgl. [Schweiger 07], S.62). Der Ansatz geht davon aus, dass der Mensch rational und bewusst handelt und seine Bedürfnisse daher benennen kann (vgl. [Schweiger 07], S.63).

Maslow hingegen behauptet, dass „...eine vernünftige Motivationstheorie das unbewusste Leben nicht vernachlässigen darf“ ([Maslow 77], S.59). Nach Maslow handeln Menschen auch triebgesteuert oder unbewusst und versuchen Bedürfnisse zu stillen, die sie nicht benennen können.

Nach Maslow untergliedern sich die menschlichen Bedürfnisse in einer „Hierarchie der relativen Vormächtigkeit“ in fünf Stufen (vgl. Abbildung 3.1, vgl. [Maslow 77], S. 78). Demnach sind die grundlegenden menschlichen Bedürfnisse die physiologischen, wie Nahrung und Sexualität. Wenn ein Mensch hungrig ist, steht für ihn dieses Bedürfnis im Mittelpunkt und er fokussiert alle Aktivitäten darauf, dieses Bedürfnis zu stillen. „Wenn alle Bedürfnisse unbefriedigt sind und der Organismus damit von den physiologischen Bedürfnissen beherrscht wird, können alle anderen Bedürfnisse einfach aufhören oder sie werden in den Hintergrund gedrängt“ ([Maslow 77], S.76). Wird dieses unterste Bedürfnis gestillt, tauchen sofort neue, höhere Bedürfnisse auf.

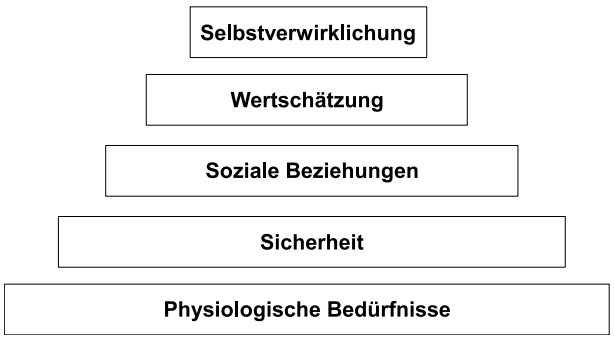


Abbildung 3.1: Maslow's Bedürfnispyramide

Auf der zweiten Ebene steht das Sicherheitsbedürfnis. Dieses Bedürfnis umfasst Stabilität, Ordnung, Gesetz, Grenzen, und Schutzkraft. Wir fühlen uns also in einer ordentlichen, voraussehbaren, gesetzmäßigen Welt wohler als in einer chaotischen unüberschaubaren Welt. Dazu zählen auch Sicherheit des Arbeitsplatzes, finanzielle Si-

cherheit und eine Absicherung, zum Beispiel durch Versicherungen, für den Fall einer Bedrohung (vgl. [Maslow 77], S.79 ff.).

Sobald dieses Bedürfnis befriedigt ist, tauchen Bedürfnisse nach Liebe, Zuneigung und Zugehörigkeit auf. Bedrohungen dieser Bedürfnisse sind Einsamkeit, Ächtung, Zurückweisung, Isolierung und Entwurzelung. Der Mensch hat eine tiefe Neigung zur Gruppenzugehörigkeit (vgl. [Maslow 77], S.85 f.). Hier machen Virtuelle Welten ein Angebot und unterstützen die Bildung von Gemeinschaften (so genannte Communities).

Auf der vierten Ebene steht das Bedürfnis nach Achtung. Das ist der Wunsch nach Wertschätzung der eigenen Person, Selbstachtung und nach Achtung seitens anderer. Wird dieses Bedürfnis frustriert, führt dies zu Gefühlen der Minderwertigkeit, Schwäche und Hilflosigkeit (vgl. [Maslow 77], S.87 f.).

Auf der fünften Ebene der Hierarchie steht die Selbstverwirklichung. „Was ein Mensch sein kann, muss er sein.“ Dieses Bedürfnis beschreibt den Drang des Menschen alle Fähigkeiten, die er hat, auch zu nutzen (vgl. [Maslow 77], S.88 f.).

Maslow macht deutlich, dass die Ebenen nicht starr sind, sondern auch Umkehrungen vorkommen können. Eine hundertprozentige Erfüllung eines Bedürfnisses muss nicht unbedingt gegeben sein um eine höhere Stufe zu erreichen. Die Hierarchie ist so zu verstehen, dass alle Bedürfnisse immer wieder aufs Neue erfüllt werden müssen, dies also einen dynamischen Prozess darstellt.

Bei der Betrachtung der Theorie in Bezug auf Virtuelle Welten wird klar, wo die Motivation zur Nutzung von Virtuellen Welten herrühren kann. Die Welten bieten die Möglichkeit der Befriedigung der Bedürfnisse der oberen vier Ebenen. Mit ihrer Besonderheit der sozialen Interaktion und der Möglichkeit der Zugehörigkeit zu einer oder mehreren Gruppen kann das Bedürfnis nach Zugehörigkeit und Liebe befriedigt werden. Auch Maslow ist der Meinung, dass die Mobilität, das Fehlen der Vertrautheit der Familien und der zunehmenden Urbanisierung der heutigen Gesellschaft zunehmend zur Frustration dieses Bedürfnisses führt (vgl. [Maslow 77], S.86).

Es kann vermutet werden, dass Menschen in Virtuellen Welten eine Möglichkeit finden, dieses Gefühl wieder zu erleben. Eng damit verbunden kann der Wunsch nach Wertschätzung und Achtung bei entsprechendem Verhalten in der Virtuellen Welt erfüllt

werden. Insbesondere die letzte Stufe der Selbstverwirklichung ist in der realen Welt oftmals schwierig. In der Virtuellen Welt ist dieses Ziel viel leichter zu erreichen, wobei die Befriedigung dieses Bedürfnisses nicht virtuell sondern real stattfindet. Virtuelle Welten wie Second Life sprechen genau dieses Bedürfnis der Selbstverwirklichung an, indem sie den Nutzern die Möglichkeit und die Freiheit geben die Welt selbst mitzugestalten und sich so selbst zu verwirklichen. Virtuelle Welten wie Second Life haben durch ihre Möglichkeiten eine enorme Gestaltungsfreiheit für die Nutzer und erlauben ihnen in verschiedene Rollen zu schlüpfen. So kann der Nutzer sich selbst ausprobieren und herausfinden was er „sein kann“. Außerdem sind die Nutzer Virtueller Welten sehr viel unabhängiger von äußeren Einflüssen, wie örtliche und persönliche Gegebenheiten.

Zu beachten ist, dass die Bedürfnisse, wie Selbstverwirklichung nicht nur in der Virtuellen Welt gelten, sondern für die Nutzer auch in der Realität relevant sind. Der Wert, der aus einem Leben in der Virtuellen Welt gewonnen wird, könnte ebenso in die Realwelt transferiert werden, denn durch die Möglichkeit der Selbstverwirklichung könnte sich beim Nutzer real ein Gefühl der Zufriedenheit einstellen, dass unabhängig ist vom Ort der Erfüllung. Zur Verdeutlichung dieses Sachverhaltes trägt das folgende Beispiel bei.

Beispiel: Angenommen es gibt eine kreative Künstlerin, nennen wir sie Kitty Kreativ, die ihre Selbstverwirklichung darin sieht ihre Gedanken in Bildern auszudrücken. Sie möchte mit ihren Bildern die Menschen erreichen, sie zum Nachdenken anregen. Gelingt es ihr mit ihren Gemälden die Menschen zum gegenseitigen Gedankenaustausch anzuregen ist das für Kitty die höchste Stufe der Erfüllung. Damit Kitty ihre Stufe der Selbstverwirklichung erreichen kann, muss sie (nach Maslow) auch die anderen Stufen der Bedürfnisse durchlaufen. Das bedeutet, sie muss sich einen Lebensunterhalt verdienen, der ihr finanzielle Sicherheit (Stufe 2) gibt und ihre Existenz sichert (Stufe 1). Kapitel 2 macht deutlich, dass es durchaus möglich ist, einen Lebensunterhalt in der Virtuellen Welt zu verdienen. Kitty muss schon in der realen Welt essen, trinken und schlafen, aber die zweite Stufe der Bedürfnispyramide, die finanzielle Sicherheit zur Existenzsicherung, kann bereits in der Virtuellen Welt erreicht werden. Für Kitty macht es keinen Unterschied, ob sie ihre Kunstwerke auf einem, mit Leinen bespannten, Keilrahmen in ihrem Atelier in der Realwelt erzeugt oder auf ihrem Rechner als digitales dreidimensionales Objekt. Kitty sieht

ihre Möglichkeit zur Selbstverwirklichung darin, ihre Kunstwerke in einer Virtuellen Galerie in Second Life zu platzieren. Andere Nutzer in Second Life, die sich für Kunst und den Gedankenaustausch darüber interessieren, treffen sich dort. Sie können vor Ort mit der Künstlerin in Kontakt treten und Kitty hat die Möglichkeit die Kunstinteressierten zum Nachdenken und zum Austausch anzuregen. Des Weiteren haben die Nutzer die Gelegenheit die Gemälde zu kaufen, um damit ihre virtuellen Wohnzimmer zu dekorieren. Durch diese Chance verdient sich Kitty ihren Lebensunterhalt, bekommt die Anerkennung und Wertschätzung aus der Community und hat zu diesem Zeitpunkt das Gefühl sich selbst verwirklicht zu haben. Maslow beschreibt jedoch, dass die Bedürfnisbefriedigung kein statischer Zustand ist, sondern ein Prozess. Auch für Kitty ist der Prozess nicht abgeschlossen, sondern für sie entstehen neue Herausforderungen, denen sie mit ihren erworbenen Fähigkeiten begegnen kann.

3.2 Verfolgung von Handlungszielen

Aus der Notwendigkeit der Bedürfnisbefriedigung heraus, ergibt sich für die Menschen eine Motivation zur Handlung. Um die Bedürfnisse stillen zu können, verfolgen sie verschiedene Handlungsziele, zum Beispiel Unterhaltung, Kommunikation, Information und Arbeit. Prinzipiell haben Virtuelle Welten die Chance so gestaltet zu werden, dass diese Handlungsziele erreicht und Bedürfnisse gestillt werden können. Es existieren bereits tatsächlich solche Virtuelle Welten, wie am obigen Beispiel erläutert wurde.

An dieser Stelle muss die Frage gestellt werden, warum dann nicht alle Menschen Virtuelle Welten nutzen, um die Handlungsziele zu erreichen. Mit anderen Medienangeboten, wie Fernsehen, Büchern und Zeitschriften, etc. lassen sich die genannten Handlungsziele genauso umsetzen. Um diese Frage zu beantworten, lohnt ein Blick in die triadisch-dynamische Unterhaltungstheorie nach Früh (vgl. [Früh 03]). Nicht jedes Medienangebot eignet sich gleichermaßen zum Erreichen der Handlungsziele. Früh führt in seiner Triadisch-Dynamischen Unterhaltungstheorie (TDU) den Begriff des „Triadischen Fitting“ ein. Demnach kommt es bei der Nutzung von Medienangeboten auf die optimale Passung der drei Faktoren:

- Person,
- Situation und
- Medienangebot

an (vgl. [Früh 03], [Wünsch 06]).

Jede Person mit ihren individuellen Eigenschaften und Vorlieben, entscheidet sich in Abhängigkeit von der jeweiligen Situation, in der sie sich gerade befindet, für ein Medienangebot. Das kann in der einen Situation das eine Medienangebot sein und in einer späteren Situation das andere. Das bedeutet also, dass nicht prinzipiell jeder Mensch sich in jeder Situation zur Verfolgung eines Handlungsziels für die Virtuelle Welt entscheidet. Eine Person fühlt sich in der einen Situation (zum Beispiel in geselliger Runde mit Freunden am Abend) beim Spiel in einer Virtuellen Welt unterhalten. Dies muss in einer anderen Situation (zum Beispiel am Nachmittag allein zu Hause) schon nicht mehr zutreffen.

Menschen, die mit Virtuellen Welten noch nie konfrontiert waren, werden eher eine große Hürde haben, Virtuelle Welten zu nutzen. Sie müssen den Umgang erst erlernen. Ältere Menschen dürften dem Medium eher skeptischer gegenüber stehen als jüngere Menschen. Das könnte daran liegen, dass ältere Generationen im Laufe ihres Lebens anders sozialisiert wurden, da sie auf das zur jeweiligen Zeit verfügbare Medium (z.B. Radio, Fernsehen) beschränkt waren. Die heute junge Generation erlernt den Umgang mit neuen Medien bereits in der Schule und im Kontakt mit Freunden. Das bedeutet, dass es durchaus Personen gibt, die sich in einer bestimmten Situation für Virtuelle Welten entscheiden, um die Zielverfolgung aufzunehmen.

Die Zielverfolgung stellt für die Nutzer eine Herausforderung dar. Um diesen begegnen zu können, setzen sie ihre Fähigkeiten ein, die sie durch die Erziehung ihrer Eltern, die Ausbildung (z.B. in der Schule, dem Studium oder der Lehre) und bisherige Erfahrungen und Handlungen gelernt haben.

Virtuelle Welten können so gestaltet werden, dass sie den Nutzer möglichst gut motivieren Handlungsziele zu erreichen. Die beste Motivation wird nach Csikszentmihalyi [Csikszentmihalyi 91] genau dann erreicht, wenn die Fähigkeiten und die Herausforderun-

gen in einer Balance stehen. Ein Zustand, der von Csikszentmihalyi als „Flow“ bezeichnet wird (vgl. [Csikszentmihalyi 91], [Csikszentmihalyi 00]).

Flow „is the holistic sensation that people feel when they act with total involvement“ [Csikszentmihalyi 91]. Flow ist also die ganzheitliche Sensation, die Menschen fühlen, wenn sie mit voller Beteiligung agieren. Das kommt immer dann vor, wenn jemand mit Spaß bei einer Sache ist, zum Beispiel auch beim Lesen eines Buches. Csikzentmihaly's Untersuchungen haben gezeigt, dass Menschen Flow erleben, wenn sie eine Spannung zwischen der Herausforderung und ihren Fähigkeiten spüren. Das bedeutet, dass Tätigkeiten als langweilig empfunden werden, die keine Herausforderung darstellen oder unterhalb der Fähigkeiten liegen. Andererseits reichen die Fähigkeiten nicht aus bzw. ist die Herausforderung zu schwierig, wird dies als Angst oder Ärger wahrgenommen (vgl. Abbildung 3.2). Die große Chance Menschen zu motivieren, liegt darin die Balance zwischen einer Herausforderung und den Fähigkeiten zu finden. Den Menschen wird dadurch das Gefühl von Kontrolle gegeben [Csikszentmihalyi 00]. Csikzentmihaly beschreibt Flow auch als „au-

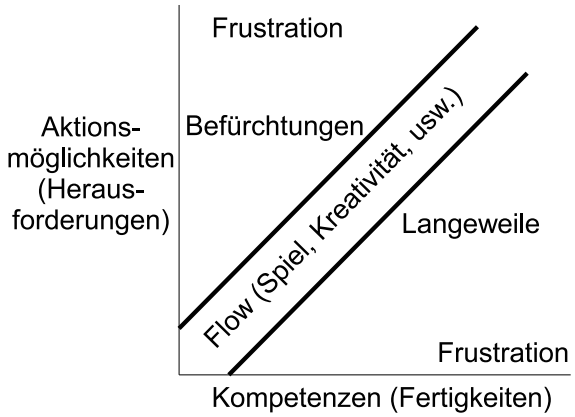


Abbildung 3.2: Modell des Flow-Zustands (vgl.[Csikszentmihalyi 00], Original englisch)

totelic experience“ ([Csikszentmihalyi 00], S.36), wobei *autotelic* aus dem Griechischen für *auto = selbst* und *telic = Ziel* übersetzt werden kann. Eine Flow-Erfahrung hat ihre Begründung in sich selbst und erfordert keine extrinsische Motivation[1]. Die Belohnung liegt in der Sache selbst, es muss keine extrinsische Belohnung geben, obwohl diese einer

[1]Die extrinsische Motivation ist die Summe der Beweggründe, die nicht aus einem inneren Anlass erfolgt sondern aufgrund äußerer Zwänge, z.B. einer Strafe (vgl. [Duden 07a]).

intrinsischen Belohung nicht im Weg steht. Das heißt, wenn eine Tätigkeit intrinsisch motiviert[2] ist, erhält der Mensch bereits eine Belohnung aus der Tätigkeit selbst. Wird die Tätigkeit zusätzlich extrinsisch motiviert, zum Beispiel durch Bezahlung, steht das dem Flow-Erlebnis nicht im Weg.

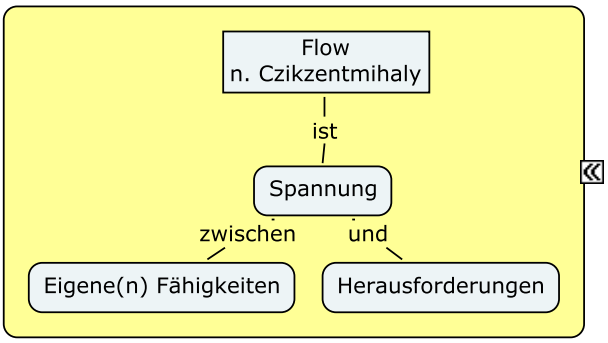


Abbildung 3.3: Flow als Spannung zwischen Herausforderung und eigenen Fähigkeiten [eigene Abbildung]

Virtuelle Welten sind so ausgelegt, dass der Nutzer die Chance hat, diese Balance bzw. Spannung zwischen Herausforderungen und seinen Fähigkeiten zu spüren (vgl. Abbildung 3.3). Virtuelle Welten, insbesondere die Spiele, sind so aufgebaut, dass der Einstieg sehr einfach ist. Dem Nutzer wird zu Beginn die Möglichkeit gegeben sich zurechtzufinden und seine Fähigkeiten zu entwickeln. Oft sind in Virtuellen Welten und Onlinespielen kleine Übungen vorhanden, die dem Nutzer Handlungsanleitungen für seine ersten Schritte bieten. Mit steigender Befähigung würde beim Nutzer bald Langeweile entstehen und er würde die Nutzung aufgeben. Daher wird die Schwierigkeit stufenweise weiter gesteigert (vgl. [Schmitz 07], S.22).

Wie kann erkannt werden, dass die Handlungsziele erreicht wurden? Diese Aussage lässt sich für die Ziele Arbeit, Information und Kommunikation leicht treffen, da eine Zielerreichung überprüfbar ist. Das Handlungsziel Arbeit ist genau dann erreicht, wenn die definierte Arbeit verrichtet ist. Ein Handlungsziel Information ist genau dann erreicht, wenn die Information vorliegt. Auch die Erreichung eines Kommunikationsziels kann überprüft werden, z.B. wenn während des Kommunikationsprozesses ein neuer Gedanke, eine neue

[2]Intrinsische Motivation: „durch die von einer Aufgabe ausgehenden Anreize bedingte Motivation“ [Duden 07b].

Idee entstanden ist oder der Kommunikationspartner vom eigenen Standpunkt überzeugt wurde. Schwieriger ist die Aussage bei dem Handlungsziel Unterhaltung. Die für diese Arbeit relevante Form des Unterhaltungserlebens durch Spiel wird im folgenden Unterkapitel daher genauer untersucht.

3.3 Unterhaltungserleben durch Spiel

Bereits Friedrich Schiller schrieb 1795 in seinen Briefen über die ästhetische Erziehung des Menschen „Denn, um es endlich auf einmal herauszusagen, der Mensch spielt nur, wo er in voller Bedeutung des Worts Mensch ist, und er ist nur da ganz Mensch, wo er spielt.“ ([Schiller 00] S.62, im Jahr 2000 aufgelegte Sammlung der Briefe über die ästhetische Erziehung des Menschen, Zitat aus dem 15. Brief)
Diese frühe Aussage zum Spiel von Friedrich Schiller macht bereits die Wichtigkeit des Spielens für den Menschen deutlich. Demnach kann der Mensch seine Fähigkeiten spielend entfalten, denn dabei „wird das Leben frei vom Ernst einer bedrückenden Wirklichkeit, 'von den Fesseln jedes Zwecks, jeder Pflicht, jeder Sorge' ([Schiller 00], S.263).
Bevor Spiel aber sein „ungebundenes Vermögen“[Schiller 00] entwickeln kann, müssen die Bedürfnisse der Wirklichkeit (Zwang, Mangel, Not) bereits gestillt sein (vgl., [Schiller 00], S.108, im Jahr 2000 aufgelegte Sammlung der Briefe über die ästhetische Erziehung des Menschen, Zitat aus dem 26. Brief, [Maslow 77]).

Huizinga [3] beschreibt: „Spiel ist eine freiwillige Handlung oder Beschäftigung, die innerhalb gewisser festgesetzter Grenzen von Zeit und Raum nach freiwillig angenommenen, aber unbedingt bindenden Regeln verrichtet wird, ihr Ziel in sich selber hat und begleitet wird von einem Gefühl der Spannung und Freude und einem Bewusstsein des 'Andersseins' als das 'gewöhnliche Leben'“ ([Huizinga 06], S.37). Huizinga formte den Begriff des *homo ludens* (lat. der spielende Mensch). Auch er vertritt, wie Schiller, die Ansicht, dass der Mensch seine Fähigkeiten über das Spiel entwickeln kann (vgl. Abbildung 3.4).

[3] Johan Huizinga war von 1915 bis 1942 Professor für allgemeine Geschichte an der Universität Leiden/Niederlande und rückte das Spiel erstmals ins akademische Rampenlicht. Er prägte 1938 den kulturanthropologischen Spielbegriff (Verhältnis des Menschen zur Kultur).

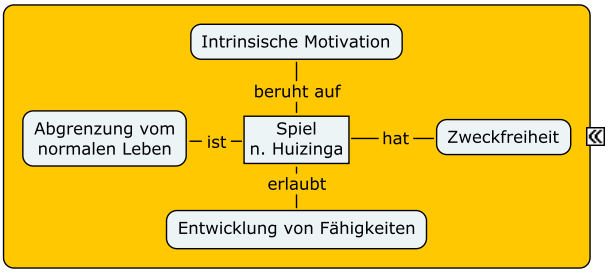


Abbildung 3.4: Spiel nach Huizinga [eigene Abbildung]

Arbeit nimmt einen großen Anteil der für die Menschen zur Verfügung stehenden Zeit ein. In ihrer Freizeit versuchen sie daher einen Ausgleich zum Arbeitsalltag zu finden und Kompensation bzw. Abwechslung (vgl. [Früh 03]) zu erleben. Das Zustandekommen von Unterhaltungserleben hängt von verschiedenen Faktoren, wie Selbstbestimmtheit, Unbestimmtheit, Fähigkeiten, Herausforderungen, Souveränität der Kontrolle und Rahmung ab (vgl. Abbildung 3.5). Selbstbestimmtheit ist fokussiert auf das Gefühl persönlicher Frei-

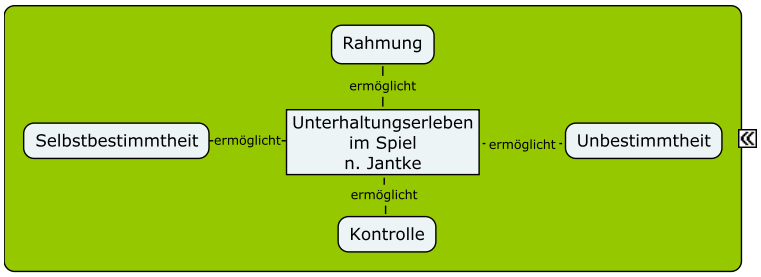


Abbildung 3.5: Faktoren des Unterhaltungserlebens (vgl. [Jantke 06] in Anlehnung an [Fritz 04])

heit (vgl. [Jantke 06]) und ist gegeben, wenn der Rezipient eines Mediums Handlungs- und Entscheidungsfreiheiten hat (vgl. [Früh 03]). Andererseits werden von außen bestimmte Handlungen vorgegeben oder eingeschränkt, eine Eigenschaft die auch als Unbestimmtheit bezeichnet wird. Die Unbestimmtheit macht gewisse Reaktionen des Rezipienten notwendig. Die Handlungen können durch bestimmte zufällige Ereignisse und die Spielmechanik eingeschränkt werden. Es sind nur Handlungen möglich, die der Programmierer vorgesehen hat. Beispielsweise kann der Spieler den Wunsch haben auf möglichst kurzem Weg einen Ort zu erreichen und er möchte den Berg zwischen ihm und dem Ort überqueren. Wenn

dieser Weg vom Programmierer nicht vorgesehen war, wird der Spieler den weiteren Weg um den Berg herum nehmen müssen. Weiterhin können mögliche notwendige Reaktionen auf eine Handlung eines Gegners oder Mitspielers sein. Wird der Spieler beispielsweise von einem Gegner angegriffen, muss er sich zunächst verteidigen, bevor er seinen inneren Wünschen folgen kann, zumindest wenn er nicht in Kauf nehmen will, das Spiel zu verlieren. Gerade diese Ungewissheit kann aber Auslöser für Spannung und Aufregung sein. Steht der Spieler allerdings ständig unter dieser Belastung der Spannung wird er auch relativ schnell den Spaß am Spiel verlieren. Es kommt also auf ein gut ausgewogenes Verhältnis selbstbestimmten und unbestimmten Handelns an. (vgl. [Jantke 06]).

Die Reaktionsfähigkeiten des Nutzers hängen von seinen Fähigkeiten ab. Durch die von außen bestimmten Handlungen entstehen für ihn Herausforderungen. Ein intensives Unterhaltungserleben entsteht aber erst dann, wenn zwischen Selbstbestimmtheit und Unbestimmtheit und somit zwischen den gegebenen Herausforderungen und den eigenen Fähigkeiten eine Spannung entsteht. Unter Rahmung wird die Abgrenzung vom alltäglichen Leben und das Eintauchen verstanden (vgl.[Jantke 06], [Huizinga 06]). Die Handlungen finden demnach in einem fiktiven Rahmen einer neu geschaffenen und unverbindlichen Realität statt (vgl.[Wünsch 06]). Souveränität der Kontrolle bezieht sich auf die Beherrschbarkeit und Überschaubarkeit der Konsequenzen der Rezeption (vgl. [Wünsch 06]). Dabei kommt es weniger auf die vorgegebene Kontrolle an, sondern vielmehr auf die, die der Rezipient empfindet. Dadurch wird deutlich, dass Unterhaltung ein subjektives Erleben darstellt (vgl. [Wünsch 06], S.98). Das souveräne Aufgeben der Kontrolle (kontrollierter Kontrollverlust) und deren Wiedererlangung durch Kompetenz führen zu einem positiven Gefühl des Erfolgs und somit zu Unterhaltung (vgl. [Wünsch 06], S.101).

Was ist das Wichtigste an einem Spiel? Wird ein Spieler oder ein Spieleentwickler gefragt, ist die Antwort „Spielspaß“ (vgl. [Waldo 08], [Koster 05]). Denn letztendlich ist es der Spielspaß, der die Spiele vergnüglich macht. Koster [Koster 05] beschreibt „fun...is the feedback the brain gives us when we are absorbing patterns for learning purposes“ and „fun is primarily about practising and learning not about excercicing mastery“ [Koster 05]. In seiner „Theory of fun“ beschreibt Koster, dass beim Spielen das menschliche Gehirn

versucht Muster zu erkennen. Dadurch wird das Gehirn trainiert und es findet ein Lernprozess statt (vgl. Abbildung 3.6). Wenn das Muster einmal erkannt wurde, stellt es keine Herausforderung mehr dar und Langeweile setzt ein. Es kann dann davon ausgegangen werden, dass etwas gelernt wurde, denn ein einmal erkanntes Muster kann bei neuen Fragestellungen wieder angewendet werden. Die reine Anwendung des Musters verursacht keinen Spaß mehr.

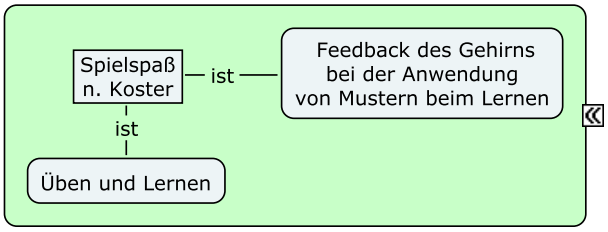


Abbildung 3.6: Spielspaß nach Koster [eigene Abbildung]

3.4 Zusammenfassung

Die verschiedenen untersuchten Perspektiven auf die Nutzungsmotivation werden in dem Schaubild in Abbildung 3.7 grafisch dargestellt und im Folgenden zusammengefasst.

Menschen haben Bedürfnisse, die sie versuchen zu befriedigen. Sie haben dadurch eine Motivation zur Handlung, denn nur durch Tätigkeiten können die Bedürfnisse gestillt werden. Um die Bedürfnisse stillen zu können, verfolgen sie verschiedene Handlungsziele, zum Beispiel Unterhaltung, Kommunikation, Information und Arbeit. Virtuelle Welten bieten den Menschen die Möglichkeit viele Bedürfnisse zu befriedigen, angefangen auf Maslow's Stufe 2 der Sozialen Sicherheit (Lebensunterhalt), über Stufe 3 (soziale Beziehungen) und 4 (Wertschätzung, Anerkennung) bis hin zur Stufe 5 (Selbstverwirklichung), wenn eine optimale Passung der drei Faktoren Person, Situation und Medienangebot (triadisches Fitting) eintritt. Die Nutzer haben Fähigkeiten und begegnen ständig Herausforderungen. Virtuelle Welten können durch ihre Gestaltung eine Spannung zwischen Fähigkeiten und Herausforderungen, also ein Gefühl von Flow entstehen lassen. Dadurch wird die Motivation der Nutzer zur Bedürfnisbefriedigung in Virtuellen Welten gesteigert.

Die Nutzer können in den Virtuellen Welten verschiedene Handlungsziele verfolgen und ihre Fähigkeiten entwickeln. Bei der Gestaltung von Virtuellen Welten ist der Entstehung von Unterhaltungserleben besondere Aufmerksamkeit zu schenken, da so die Motivation der Nutzung gesteigert wird. Dabei kommt es neben der Schaffung eines fiktiven Rahmens (Rahmung) auch auf ein ausgewogenes Verhältnis zwischen Selbstbestimmtheit und Unbestimmtheit, die Schaffung einer Spannung zwischen Herausforderungen und Fähigkeiten (Flow) an. Dadurch entsteht beim Nutzer das Gefühl der Kontrolle. Durch das positive Gefühl des Erfolgs entsteht Unterhaltung.

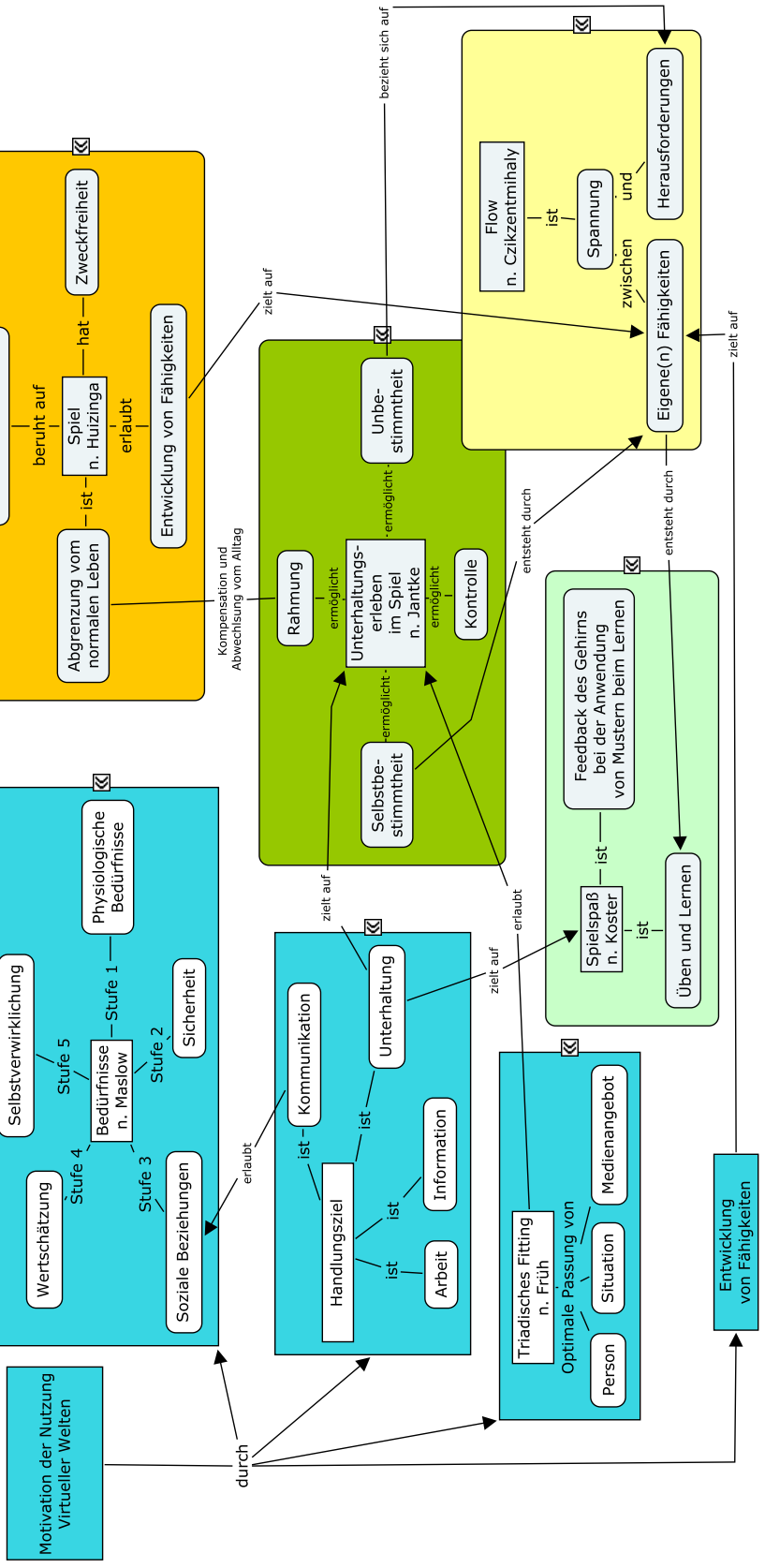


Abbildung 3.7: Verschiedene Perspektiven auf die Nutzungsmotivation [eigene Abbildung]

Kapitel 4

Relevanz und Chancen der IT Sicherheit für Virtuelle Welten

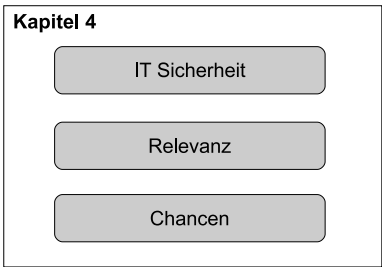
Die Motivation der Nutzung Virtueller Welten erwächst aus realen Bedürfnissen und Handlungszielen der Nutzer (vgl. Kapitel 3). Außerdem begründet sich die reale Relevanz aus den, für reales Geld gehandelten, virtuellen Gütern (vgl. Kapitel 2). Aus dieser realen Relevanz heraus entstehen aber auch Gefahren. Denn dort wo es Werte gibt, tauchen auch Betrüger und Angreifer auf, die auf die realen Werte abzielen. Eine Studie der ENISA[1] [Enisa 08] zeigt, dass diese Gefahren nicht nur theoretisch existieren, sondern tatsächlich Nutzer von solchen Fällen berichten. Der Studie zufolge haben bereits 30% der befragten Nutzer den Verlust eines Wertes in einer Virtuellen Welt erlebt [Enisa 08].

Virtuelle Welten sind IT-Systeme, in denen reale Werte existieren und bedroht werden. Schutz gegen diese Bedrohungen können Mechanismen der IT-Sicherheit bieten. Dieses Kapitel widmet sich daher der Frage nach der Relevanz und den Chancen der IT-Sicherheit für Virtuelle Welten. Zuvor wird erläutert, was unter dem Begriff IT-Sicherheit verstanden wird.

[1] European Network and Information Security Agency (deutsch: Europäische Agentur für Netz- und Informationssicherheit)

Fragen, die in diesem Kapitel beantwortet werden, lauten:

- Was wird unter IT-Sicherheit verstanden?
- Welche Relevanz hat IT-Sicherheit für Virtuelle Welten?
- Welchen Beitrag kann IT-Sicherheit für Virtuelle Welten leisten?



4.1 IT-Sicherheit

Sicherheit ist eine Eigenschaft eines Systems, die dadurch gekennzeichnet ist, dass die als bedeutsam angesehenen Bedrohungen, die sich gegen die schützenswerten Güter richten, durch besondere Maßnahmen so weit ausgeschlossen sind, dass das verbleibende Risiko akzeptiert wird (vgl. [Amann 92]). Um IT-Sicherheit zu gewährleisten, ist es notwendig, wertvolle Güter vor Bedrohungen zu schützen. Schützenswerte Güter (auch Assets, Werte) sind beispielsweise Daten, Informationen und Dokumente. Bedrohungen ergeben sich durch den Verlust von Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Abstreitbarkeit und des Datenschutzes (Schutzziele).

Wann ist ein System sicher? IT-Sicherheit ist dann gegeben, wenn die Schutzziele gewährleistet werden.

Vertraulichkeit liegt genau dann vor, wenn Unautorisierte keinen Zugang zu Daten und Informationen erlangen. Die Kommunikation zwischen zwei Parteien soll geheim verlaufen und kein unberechtigter Dritter darf Zugang zu diesen Informationen erhalten.

Integrität ist gegeben, wenn Daten und Informationen nicht unberechtigt verändert werden können. Die Informationen müssen korrekt und unverändert vorliegen. Das be-

deutet, dass nur berechtigte Personen die richtigen Änderungen vornehmen dürfen und dass ungewollte oder unberechtigte Veränderungen sichtbar sind.

Verfügbarkeit liegt vor, wenn der Zugriff auf ein System oder einen Dienst gewährleistet ist und keine unberechtigte Störung möglich ist. Die Nutzer sind in der Lage die gesamte Funktionalität des Systems oder des Dienstes zu nutzen.

Nicht-Abstreitbarkeit ist gegeben, wenn eine Menge von Aktionen einem Subjekt zugeordnet werden kann, das heißt es ist nicht möglich die Durchführung im Nachhinein abzustreiten.

Ein weiteres wichtiges Ziel ist der **Datenschutz**, der die informationelle Selbstbestimmung umsetzt. Jede Person hat das Recht, selbst festzulegen, was mit den eigenen personenbezogenen Daten passieren darf oder soll. Durch die EU Directive 95/46/EC [Parlament 95] wurde die Basis für eine Vereinheitlichung der Gesetze in Europa geschaffen.

Wo es Werte gibt, tauchen Angreifer auf, die es auf diese Werte abgesehen haben. Die Motivation der Angreifer ist vielschichtig und reicht von Zerstörungswut und Selbstprofilierung über die Verschaffung von Vorteilen bis hin zur Unwissenheit. Angriffe auf Werte sind nicht immer vorsätzlich und zielgerichtet. Sie können auch unbeabsichtigt geschehen, wenn zum Beispiel administratives Personal Daten in einer Datenbank unabsichtlich löscht. Die IT-Sicherheit versucht geeignete Maßnahmen bereitzustellen, um solchen Bedrohungen entgegenzuwirken bzw. Schwachstellen zu beseitigen.

Die Abbildung 4.1 stellt diesen Zusammenhang übersichtlich dar. Schwachstellen in Systemen führen dazu, dass das Risiko für das Eintreten einer Bedrohung steigt. Nutzen Angreifer diese Schwachstelle aus, können Werte verletzt werden. Um die Werte zu schützen, werden Gegenmaßnahmen umgesetzt. Durch Sicherheitstechniken wird das Risiko für Bedrohungen und Angriffe reduziert, indem der potenzielle Schaden reduziert, verhindert oder eliminiert wird. Um einschätzen zu können welche Gegenmaßnahmen am besten vor den Bedrohungen schützen, müssen zunächst Sicherheitsanforderungen definiert werden. Sicherheitsanforderungen beschreiben, was das System vom Design her können muss und stellen sicher, dass das System seine Schutzziele erreichen kann.

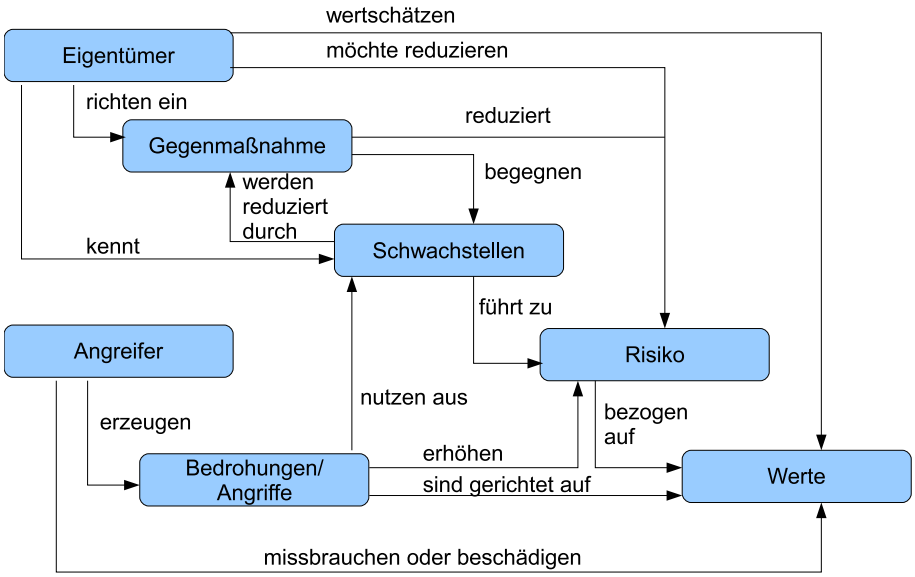


Abbildung 4.1: Zusammenhang IT-Sicherheit (vgl. [Merkow 05], Orig. engl.)

Die Konzepte „Angriff“ und „Bedrohung“ müssen unterschieden werden. Sowohl ein Angriff als auch eine Bedrohung sind auf die Sicherheit eines Systems fokussiert. Während ein Angriff die konkrete Ausführung einer Methode beschreibt, zum Beispiel Denial-Of-Service-Angriff, beschreibt die Bedrohung die Auswirkung eines potenziellen Angriffs. An dieser Stelle wird im Folgenden ein klassisches Beispiel aus der IT-Sicherheitspraxis herangezogen. Der Denial-of-Service[2]-Angriff ist ein Angriff und keine Bedrohung, da er beschreibt, wie etwas ausgeführt wird (Methode). Die zugehörige Bedrohung ist der Verlust der Verfügbarkeit (z.B. eines Servers). Tabelle 4.1 stellt den klassischen Bedrohungen der IT-Sicherheit konkrete Angriffsbeispiele gegenüber, um diesen Aspekt zu verdeutlichen. Angriffe können sehr vielfältig gestaltet und trotzdem auf dieselbe Bedrohung gerichtet sein. Für die Analyse der Sicherheit von Systemen muss grundlegend die Bedrohung betrachtet werden, um zu definieren was gefährdet ist. Geht es dann um die Umsetzung von Mechanismen ist ein Verständnis der Angriffe wichtig, um geeignete Gegenmaßnahmen zu ergreifen.

[2]Deutsch: Dienstverweigerung

Bedrohung	Mögliche Angriffe
Verlust der Vertraulichkeit	- Mittels Man-in-the-Middle-Angriff wird die Kommunikation zwischen zwei Personen belauscht. - Spionage-Software[3] gelangt unberechtigt an Informationen. - Bei Phishing geben die Opfer in gutem Glauben selbst die Informationen an den Angreifer.
Verlust der Integrität	- Malware[4] verletzt die Integrität eines Rechners. - Datenmanipulation: Daten werden unberechtigt verändert, z.B. Bildmanipulationen erzeugen neue inhaltliche Zusammenhänge. - E-Mail Fälschung - Wahlfälschung
Verlust der Verfügbarkeit	- Denial-Of-Service-Angriffe führen dazu, dass Server nicht mehr erreichbar sind. - Spam
Verlust der Nicht-Abstreitbarkeit	- Der Empfänger einer Nachricht behauptet, diese nicht erhalten zu haben.
Verletzung des Datenschutzes	- Ein Bankmitarbeiter gibt vertrauliche Daten der Kunden an Dritte weiter.

Tabelle 4.1: Bedrohungen und Angriffe

Ein anderer Angriff ist zum Beispiel *Phishing*[5], bei dem die Angreifer unter Angabe einer falschen Identität E-Mails verschicken und die Adressaten auffordern Kontodaten des eigenen Kontos preiszugeben. Die Angreifer bitten um die Eingabe der Kontonummer, PIN

[3]Englisch Spyware

[4]Kunstwort für Malicious Software, deutsch Schadsoftware

[5]Kunstwort zusammengesetzt aus Passwort und Fishing

und mehrerer TANs. Diese wertvollen Daten werden auch als Assets bzw. Werte bezeichnet. Mit diesen Informationen ist der Angreifer in der Lage Geldtransfers auszuführen. Sie nutzen die Gutgläubigkeit bzw. Unwissenheit der Menschen aus, um ihren Angriff durchzuführen. Bedroht wird in diesem Fall das Schutzziel Vertraulichkeit. Gegenmaßnahmen können von potenziellen Opfern einfach ergriffen werden, indem sie ihre geheimen Daten vertraulich behandeln. Die Herausforderung für den Schutz vor Phishing-Angriffen ist die Sensibilisierung der Menschen, sich solcher Gefahren bewusst zu werden. Banken wollen ein Bewusstsein[6] schaffen und bieten für ihre Kunden Schulungen an.

Hundertprozentige Sicherheit kann niemand garantieren. Das Ziel von Sicherheitsfunktionen kann lediglich sein, das Level der Sicherheit zu erhöhen und es potenziellen Angreifern möglichst schwer zu machen. Um geeignete Maßnahmen zum Schutz vor Angriffen einzusetzen, ist es notwendig, die Einsatzbereiche genau zu untersuchen und eine Sicherheitsanalyse durchzuführen. Bei einer Sicherheitsanalyse werden die Werte aller Akteure identifiziert. Es wird untersucht, welche Bedrohungen sich gegen diese Werte richten. Anschließend werden Anforderungen an die Sicherheit des Systems gestellt und geeignete Maßnahmen zum Schutz definiert.

4.2 Relevanz der IT-Sicherheit für Virtuelle Welten

Wie in Kapitel 3 bereits erläutert wurde, ist die Motivation der Nutzung Virtueller Welten vielschichtig und reicht von der Möglichkeit der Bedürfnisbefriedigung über die Erfüllung von Handlungszielen bis hin zur Entwicklung von Fähigkeiten. Das Unterhaltungserleben ist den Nutzern genauso wichtig, wie die Gelegenheit zur Kommunikation und Information und die Verrichtung von Arbeit. Für die Nutzung investieren die Anwender reale Werte, wie Zeit und Geld. Das Erwerben von Fähigkeiten und eines Status erfordert viel Geschick und vor allem Zeit.

Viele Unternehmen der Realwelt schaffen sich eine virtuelle Präsenz. Einige nutzen die Möglichkeit für eine Zusammenarbeit in virtuellen Teams, organisieren ihre Meetings und Tagungen in der Virtuellen Welt oder vertreiben ihre Produkte.

[6] oftmals wird auch der englische Begriff „Awareness“ verwendet

Ihre jeweiligen Ziele können Nutzer nur erreichen, wenn sie ständig auf die Virtuelle Welt zugreifen können. Sie sind auf die Verfügbarkeit des Dienstes angewiesen. Die Verfügbarkeit wird durch unberechtigte Störungen verletzt. Einige World of Warcraft Nutzer mussten einen solchen Vorfall erleben. Linux-Nutzer verwenden Software wie Cedega[7], um das Spiel unter dem Betriebssystem Linux spielen zu können. Nach einer Aktualisierung hat das in World of Warcraft integrierte Anti-Cheating-System[8] jedoch Cedega als Cheating-Software erkannt. Daraufhin wurde diesen Nutzern das Konto gesperrt und sie konnten nicht auf den bereits bezahlten Dienst zugreifen (vgl. [Klaß 06b]).

Es existieren Gefahren, die die Integrität der Werte betreffen. In Second Life erstellen Nutzer Gegenstände und besitzen das Urheberrecht an diesen. Wenn sie die Gegenstände verkaufen, erhält der Käufer gegen Bezahlung ebenfalls den Gegenstand, praktisch eine Kopie. Im Jahr 2006 tauchte ein Programm namens CopyBot in Second Life auf, mit dessen Hilfe unberechtigte Kopien von Gegenständen angefertigt werden konnten. Die Hersteller erlitten einen Wertverlust ihrer Gegenstände, da diese einfach kopiert werden konnten ohne dafür zu bezahlen (vgl. [Porteck 06]).

Die virtuellen Gegenstände dürfen nicht verloren gehen (Verfügbarkeit der Werte). In einigen virtuellen Welten, wie zum Beispiel Second Life, haben die Spieler die Möglichkeit selbst Gegenstände zu erzeugen und besitzen das Urheberrecht an diesen. Die Integrität und Verfügbarkeit der Gegenstände muss gewährleistet sein.

Ein Social Engineering[9] Angriff auf Habbo Hotel[10] Nutzer führte zum Verlust der Vertraulichkeit der Nutzerdaten. Die Angreifer erlangten die Zugangsdaten ihrer Opfer und haben so Zugriff auf deren Nutzerkonten und deren Werte. Sie konnten sich die Möbel der Opfer in ihr eigenes Habbo Hotel Zimmer transferieren (vgl. [BBCNews 07]).

Viele Nutzer identifizieren sich mit ihrer virtuellen Identität. Dabei ist der Schutz dieser virtuellen Identität genauso wichtig, wie die Möglichkeit die reale Identität des Nutzers anonym zu halten.

[7] Windows-kompatible Laufzeitumgebung

[8] überprüft, ob Nutzer unfair spielen, indem sie zusätzliche Software verwenden, zum Beispiel „Bots“, um Tätigkeiten automatisiert durchzuführen

[9] Vorspiegelung falscher Tatsachen

[10] die Nutzer kaufen virtuelle Möbel, um sich ihre eigenen virtuellen Hotelzimmer einzurichten

Außerdem besteht eine Gefahr, dass die Kommunikation zwischen zwei Partnern belauscht wird, wenn sich zum Beispiel ein gegnerischer Spieler einen Vorteil verschaffen will (Verlust der Vertraulichkeit).

Zu einer Verletzung des Datenschutzes kam es 2006 bei LindenLab, dem Betreiber von Second Life, als Dritte unberechtigt Zugriff auf Nutzerdaten bekamen. In der Folge forderte LindenLab alle Nutzer auf ihre Passwörter zu ändern [Klaß 06a].

Es wird deutlich, dass in Virtuellen Welten Werte existieren. Bedrohungen zielen darauf ab, die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, den Datenschutz und die Nicht-Abstreitbarkeit zu verletzen. Um die Bedrohungen abzuwehren, eignen sich Maßnahmen der IT-Sicherheit, beispielsweise Verschlüsselung der Kommunikation. Die Teilnehmer von Virtuellen Welten müssen diese Maßnahmen einfordern und die Anbieter müssen sie umsetzen.

In ihrem Positionspapier beschreibt die European Network and Information Security Agency (ENISA) mögliche Angriffe, die auf genau diese Schutzzielverletzungen wirken [Hogben 08].

4.3 Chancen

IT-Sicherheit beschäftigt sich mit dem Schutz von Werten in IT-Systemen. Um einen möglichst guten Schutz der Werte zu erreichen, muss zunächst eine systematische Sicherheitsanalyse durchgeführt werden. Im Rahmen der systematischen Methodik der Sicherheitsanalyse wird zunächst eine Inventarliste der Sicherheitswerte (Assets) aufgestellt, auf dessen Basis eine Bedrohungsanalyse durchgeführt werden kann. Um die Werte vor den Bedrohungen zu schützen, müssen geeignete Gegenmaßnahmen getroffen werden. Sicherheitsmechanismen sind beispielsweise elektronische Signaturen, Hashfunktionen und Verschlüsselung. Diese basieren auf kryptografischen Verfahren wie beispielsweise RSA, einem asymmetrischen Kryptosystem, das nach den Erfindern Rivest, Shamir und Adleman benannt ist.

Um herauszufinden, welche Sicherheitsmechanismen ein System benötigt, wird im Anschluss an die Analyse ein Sicherheitskonzept aufgestellt. In diesem Konzept werden auf

Basis der Bedrohungsanalyse Anforderungen an das System definiert. Es existieren Kataloge (z.B. ITSEC[11], Common Criteria) mit Anforderungen, aus denen die notwendigen Anforderungen für das entsprechende System ausgewählt werden können. Damit wird Entwicklern eine Hilfestellung beim Systementwurf gegeben. Für die Überprüfung der eingesetzten Mechanismen bietet sich eine Evaluierung der Systeme an. Die Evaluierung wird von einer unabhängigen Instanz (eine zertifizierte Prüfstelle) durchgeführt. Bei einer positiven Evaluierung kann eine Zertifizierung vorgenommen werden. Das Zertifikat ist „ein amtlich bestätigter Nachweis der Sicherheitsleistungen eines Produkts“ [Eckert 04]. Mit einem Zertifikat kann beim Kunden das Vertrauen in das Produkt gesteigert werden.

Die Wahl des Zertifizierungsverfahrens hängt vom Einsatzgebiet des Produktes ab. Im internationalen Einsatz hat sich die Evaluierung unter Einsatz der Common Criteria for Information Technology Security Evaluation durchgesetzt. Die Common Criteria sind ein relativ neuer Standard, der die in Europa und Amerika eingesetzten Standards ITSEC und TCSEC ablöst. Es sind bereits eine Vielzahl von Produkten erfolgreich zertifiziert worden, z.B. die deutsche elektronische Gesundheitskarte, Chipkartenlesegeräte und der ePass [Ochel 05]. Eine Zertifizierung nach Common Criteria muss nur einmalig in einem Land vorgenommen werden und wird von allen anderen Ländern anerkannt. Dadurch kann sich eine Firma die Zertifizierung nach verschiedenen nationalen Standards ersparen.

Virtuelle Welten zielen auf eine internationale Nutzerbasis ab. Aus diesem Grund ist nur ein internationaler Ansatz zur Evaluierung und Zertifizierung sinnvoll. Zurzeit bieten allein die Common Criteria die Möglichkeit der internationalen Anerkennung.

Im Weiteren wird die Sicherheitsanalyse nach Common Criteria für Virtuelle Welten durchgeführt (vgl. Kapitel 6) und ein Protection Profile (Schutzprofil) entwickelt (vgl. Kapitel 8). Um ein genaueres Verständnis der Vorgehensweise der Sicherheitsanalyse zu gewinnen, wird im folgenden Kapitel 5 der Ansatz der Common Criteria vorgestellt.

[11] Europäischer Standard für die Bewertung und Zertifizierung von Soft- und Hardwareprodukten (Information Technology Security Evaluation Criteria)

Kapitel 5

Common Criteria for Information Technology Security Evaluation

Die Common Criteria for Information Technology Security Evaluation[1] sind ein internationaler Standard und definieren Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik. Die Kriterien bieten einen Vorteil durch die Anwendung einer einheitlichen Methodik. Die internationale Anerkennung ermöglicht ein einheitliches Vorgehen bei der Evaluation von Software und Hardware und schafft dadurch eine Erleichterung einer weltweiten Akzeptanz der Evaluierung. Die Common Criteria sind eine Weiterentwicklung verschiedener nationaler Kriterien, wie ITSEC[2] in Europa, TCSEC[3] der USA und der kanadischen CTCPEC[4] und lösen diese ab.

Der erste Teil dieses Kapitel beschreibt die grundlegenden Prinzipien und Ziele der Common Criteria. Die Zielsetzung der Arbeit umfasst das Erstellen eines Schutzprofils im Rahmen der Definition von Anforderungen an die Sicherheit Virtueller Welten. Was ein Schutzprofil (Protection Profile) ist und wie es aufgebaut ist, wird im zweiten Teil dieses

[1] Deutsch: Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie

[2] Information Technology Security Evaluation Criteria (deutsch: Kriterien für die Bewertung der Sicherheit von Informationstechnologie), europäischer Standard

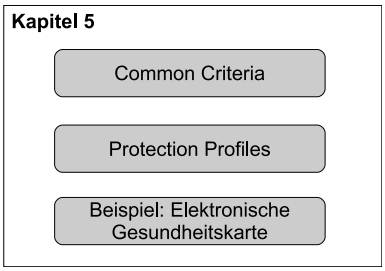
[3] Trusted Computer System Evaluation Criteria (deutsch: Kriterien für die Bewertung vertrauenswürdiger Computersysteme), US-amerikanischer Standard

[4] Canadian Trusted Computer Product Evaluation Criteria (deutsch: Kanadische Kriterien für die Bewertung vertrauenswürdiger Computerprodukte), kanadischer Standard

Kapitels erläutert. Zur Veranschaulichung des Aufbaus und des Inhaltes eines Schutzprofils dient das Beispiel der deutschen elektronischen Gesundheitskarte.

Die Fragen, die im vorliegenden fünften Kapitel beantwortet werden, lauten:

- Was sind die Common Criteria?
- Welche Ziele verfolgen die Common Criteria?
- Was ist ein Schutzprofil (Protection Profile)?
- Wie ist ein Schutzprofil aufgebaut?



5.1 Ziele, Begriffe und Schlüsselkonzepte

„Das Ziel einer Common Criteria-Evaluierung ist die Bestätigung, dass die vom Hersteller behauptete Sicherheitsfunktionalität wirksam ist“ [BSI 09c]. Die Common Criteria definieren eine Reihe von Sicherheitsanforderungen an Systeme, mit dem Ziel eine Basis für Vertrauen in die Sicherheit der Systeme zu schaffen ([Merkow 05], S.34). Das können Hardwaresysteme, Softwaresysteme und hybride Systeme sein. Sie unterstützen den Entwicklungsprozess der Systeme, indem sie Entwicklern von Systemen eine Hilfestellung beim Entwurf und bei der Entwicklung bieten. Andererseits ist es möglich, die Systeme evaluieren zu lassen um damit einen Beweis zu schaffen, dass die Systeme „sicher“ sind. Bei einer Evaluierung wird geprüft, ob die Systeme den (in Protection Profiles, Security Targets bzw. Requirements Packages) definierten Anforderungen entsprechen. Mit einem Zertifikat wird diese Entsprechung „ausgezeichnet“. Es ist zu beachten, dass die Überprüfung der Einhaltung der Anforderungen nur innerhalb eines gewissen Rahmens

zugesichert werden kann. Das Level der Zusicherung wird mittels so genannter Evaluation Assurance Levels (EALs) festgelegt. EALs werden in den Stufen 1 bis 7 unterschieden, wobei die höhere Stufe eine größere Zusicherung bedeutet. Mit steigendem Level steigen auch die Anforderungen an die Überprüfung und damit auch die Kosten.

Die Common Criteria (CC) verwenden einige kennzeichnende Begriffe, die hier erläutert werden sollen.

Der **Evaluationsgegenstand (EVG)**[5] ist das zu evaluierende Objekt. Das können Produkte wie Firewalls oder Datenbanken sein.

Ein **Schutzprofil**[6] ist ein Dokument, das Sicherheitsanforderungen für eine bestimmte Produktklasse definiert. Es existiert bereits eine Vielzahl verschiedener Schutzprofile für Firewalls, Wahlcomputer, die virtuelle Poststelle des Bundes usw. Ein Schutzprofil fasst jeweils ein Set von Anforderungen (sowohl funktionale als auch Anforderungen an die Zusicherung) zusammen. Die Anforderungen können entweder aus dem CC Katalog stammen oder selbst definierte Anforderungen sein. Wichtig ist, dass die Anforderungen an eine Produktklasse, nicht an ein konkretes Produkt definiert werden. Die Anforderungen müssen daher implementationsunabhängig definiert werden. Jedes Schutzprofil legt ein Evaluation Assurance Level (Level an Zusicherung) fest.

Ein **Security Target (ST)** bildet die Basis für eine vollständige Systemevaluation und kann sich auf mehrere Schutzprofile beziehen. Im Gegensatz zum Schutzprofil richtet sich das Security Target an ein konkretes Produkt.

Schutzprofile und Security Targets (Sicherheitsvorgaben) müssen auch evaluiert werden.

5.2 Common Criteria Rahmenwerk

Die Common Criteria stellen ein Rahmenwerk für eine Analyse der Anforderungen vor. Das Rahmenwerk stellt kein Vorgehensmodell für die Entwicklung eines Systems dar,

[5] Englisch: TOE, Target of Evaluation

[6] Englisch: Protection Profile (PP)

sondern soll vielmehr als Orientierungsleitfaden für Entwickler von Schutzprofilen und Security Targets dienen.

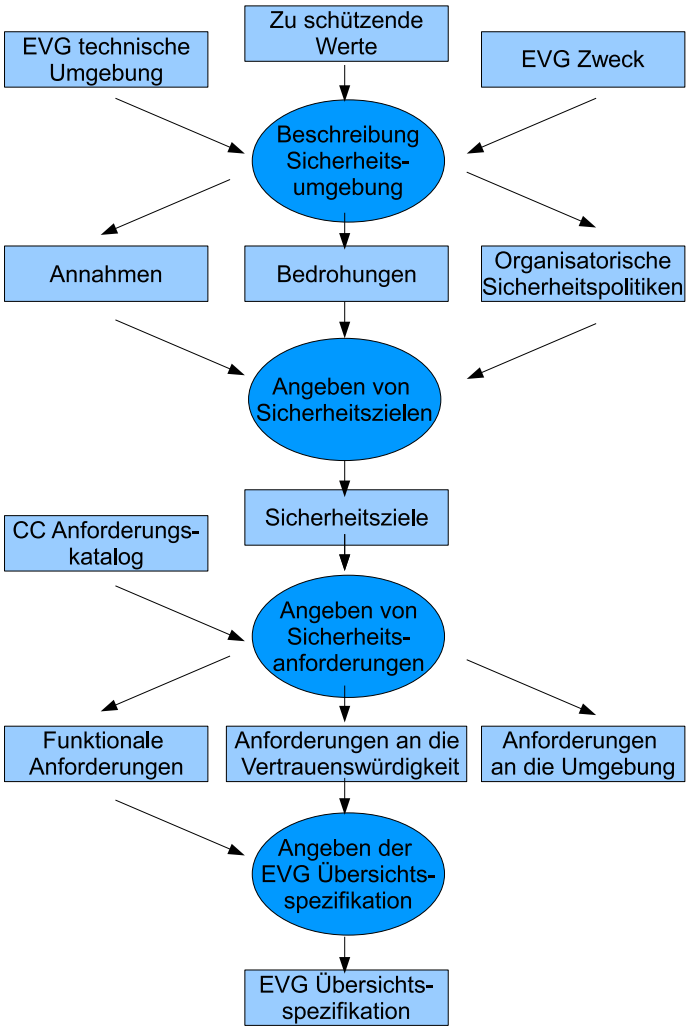


Abbildung 5.1: Common Criteria Rahmenwerk [Merkow 05]

Zunächst werden die Werte (Assets) identifiziert, die geschützt werden sollen. Im Schutzprofil und in den Sicherheitsvorgaben (ST) muss des Weiteren genau spezifiziert werden, welchen Zweck der EVG erfüllen soll. Außerdem wird die Umgebung des zu evaluierenden Systems beschrieben. Für die Betrachtung der Sicherheit eines Systems ist es wichtig, die systemumgebende Umwelt zu betrachten. Gesetze, organisatorische Regeln usw. können für die Sicherheit eines Systems ausschlaggebend sein.

Im zweiten Schritt werden alle relevanten Bedrohungen gegen die Assets des EVG und dessen Umgebung identifiziert. Es muss genau spezifiziert werden, welche Annahmen für

den Einsatz des EVG in seiner Umgebung gelten. Außerdem wird geprüft, welche organisatorischen Sicherheitsrichtlinien die Umgebung des EVG vorgibt. Daraus ergeben sich die Sicherheitsziele für den EVG. Anhand des CC Anforderungskatalogs und selbst definierter Anforderungen werden alle Anforderungen an den EVG und seine Umwelt definiert. Dabei wird unterschieden zwischen Funktionalen Anforderungen (Functional Requirements) und Anforderungen an die Zusicherung (Assurance Requirements). Zusammengefasst ergeben die funktionalen Anforderungen und die Anforderungen an die Zusicherung die Spezifikation der Sicherheit des EVG (EVG Security Specifications).

5.3 Entwicklung eines Schutzprofils

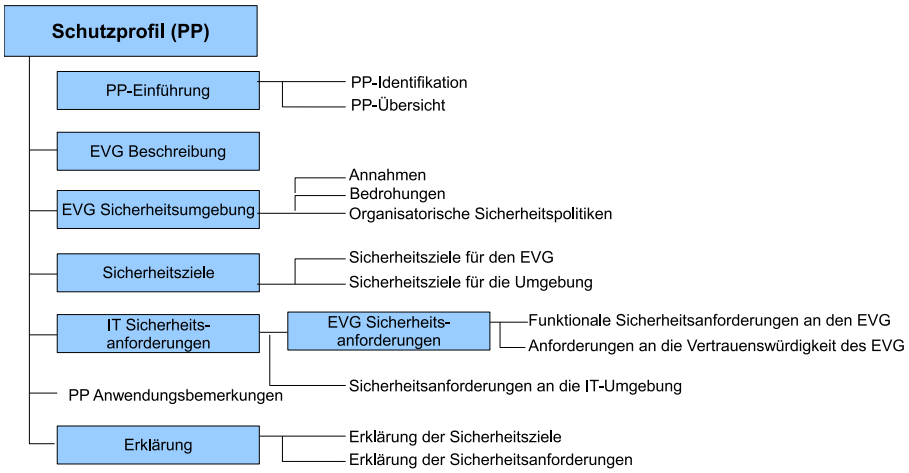


Abbildung 5.2: Aufbau eines Schutzprofils [Merkow 05]

5.3.1 Funktionale Sicherheitsanforderungen (Security Functional Requirements)

Die funktionalen Anforderungen werden in einer hierarchischen Strukturierung bestehend aus Klassen, Familien, Komponenten und Elementen dargestellt, die zur leichteren Lesbarkeit Abkürzungen verwenden. Ein Beispiel für eine funktionale Anforderung ist FAU_GEN.2.1. Die Abkürzung setzt sich folgendermaßen zusammen:

- *FAU* beschreibt die Klasse *Security Audit* (F steht für eine funktionale Anforderung)
- *GEN* beschreibt die Familie, *hier:* Generation of Audit Data *(Generierung von Auditdaten)*
- *.2* beschreibt die zweite Komponente der Familie GEN, *hier:* User Identity Association *(Zuordnung der Benutzeridentität)*
- *.1* beschreibt das erste Element der Komponente, *hier:* Es muss möglich sein, zu jedem prüffähigen Event die Benutzeridentität zuzuordnen.

Die Common Criteria Teil 2 [CCPart2 06] enthalten einen Katalog mit Anforderungen und deren genauer Beschreibung. Ein grober Überblick über die Anforderungen wird in Tabelle 5.1 dargestellt. Darüber hinaus ist es den Erstellern von Schutzprofilen und Sicherheitsvorgaben (ST) möglich eigene Anforderungen zu definieren.

Name	Erläuterung
Audit (FAU_)	Security Audit: Erkennen, Aufzeichnen, Speichern und Analysieren von Daten, Ergebnis: Audit Records, die für Review und Analyse zur Verfügung stehen
Communications (FCO_)	Anforderungen für die Nicht-Abstreitbarkeit zwischen zwei Kommunikationspartnern, d.h. weder der Sender noch der Empfänger kann bestreiten, an der Kommunikation teilgenommen zu haben.
Cryptographic Support (FCS_)	Aspekte des Managements und der Verwendung kryptografischer Schlüssel
User Data Protection (FDP_)	Schutz der Benutzerdaten während Import, Speicherung und Export
Identification and Authentification (FIA_)	Eindeutige Identifikation und Authentifizierung der Nutzer, Festlegung und Verifikation der Nutzeridentität und Zugangsrechte
Security Management (FMT_)	Sicherheitsattribute, EVG Daten und Funktionalität der Sicherheitsfunktionen

Privacy (FPR_)	Schutz der Identität des Nutzers gegen Enthüllung und Missbrauch
Protection of the Trusted Functions (FPT_)	Schutz der EVG-Sicherheitsfunktionen
Resource Utilization (FRU_)	Verfügbarkeit kritischer und notwendiger Ressourcen
TOE Access (FTA_)	Kontrolle (Limitierung) der Einrichtung einer Nutzersitzung
Trusted Path/Channel (FTP_)	Anforderungen für einen vertrauenswürdigen Kanal zwischen Nutzern und den EVG-Sicherheitsfunktionen bzw. innerhalb der Funktionen

Tabelle 5.1: Funktionale Sicherheitsanforderungen (vgl.[Merkow 05])

5.3.2 Anforderungen an die Vertrauenswürdigkeit (Security Assurance Requirements)

Die Sicherung des Vertrauens in ein IT-Produkt oder -System basiert auf einer strengen Evaluierung des EVG. Dabei prüfen IT-Experten das IT-Produkt und dessen Dokumentation auf Validität.

Die Anforderungen an die Vertrauenswürdigkeit sind wie bei den Sicherheitsanforderungen an die Funktionalität mittels Klassen, Familien und Komponenten strukturiert. Das sinnvolle und abgestimmte Zusammenfügen von Vertrauenswürdigkeitskomponenten ergibt eine Evaluationsstufe für Vertrauenswürdigkeit (Evaluation Assurance Level, EAL) (vgl. [CCPart3 06]).

5.3.3 Stufe der Vertrauenswürdigkeit (Evaluation Assurance Level)

Das Vertrauen in eine Sicherheitsleistung wird in den Common Criteria nach sieben Stufen unterschieden (vgl. Tabelle 5.2). Jede Stufe hat genaue Anforderungen an die Prüfung der IT-Sicherheit. Je höher die Stufe der Vertrauenswürdigkeit, desto größer ist auch der Prüfaufwand. Eine niedrigere EAL-Stufe wird mit geringerer Prüftiefe und mit anderen Prüfmethoden untersucht als eine höhere Stufe. Ein zentrales Prüfziel aller Stufen ist die Analyse von Schwachstellen, die von Angreifern ausgenutzt werden könnten (vgl. [BSI 09c]).

EAL	**Bedeutung**
EAL1	funktionell getestet
EAL2	strukturell getestet
EAL3	methodisch getestet und überprüft
EAL4	methodisch entwickelt, getestet und durchgesehen
EAL5	semiformal entworfen und getestet
EAL6	semiformal verifizierter Entwurf und getestet
EAL7	formal verifizierter Entwurf und getestet

Tabelle 5.2: Sieben Stufen der Vertrauenswürdigkeit (vgl. [CCPart3 06])

5.4 Exkurs: Schutzprofil am Beispiel der elektronischen Gesundheitskarte

Um ein besseres Verständnis für die Zusammenhänge der Common Criteria zu erreichen, soll an dieser Stelle ein kurzes Beispiel erläutert werden. Dieser Exkurs enthält nicht die vollständigen Angaben des Schutzprofils der elektronischen Gesundheitskarte. Die hier genannten Beispiele sollen lediglich einem besseren Verständnis des Aufbaus, der Namenskonventionen und der Methodik der Common Criteria dienen.

Durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung vom November 2003 [GMG 03] wird die Einführung einer elektronischen Gesundheitskarte vorgeschrieben. Die Einführung der Karte für alle Versicherten war bereits für die zweite Jahreshälfte 2007 geplant und befindet sich zurzeit (Stand: März 2009) im Rollout in Testregionen [BMG 09a]. Die Karte soll aufgrund digitaler Datenverarbeitung und -übermittlung Kosten senken und Prozessschritte verkürzen. Das Ziel ist, alle relevanten Informationen auf einer Karte zu speichern (z.B. Röntgen-, Ultraschallbilder, Befunde, etc.). Die Einführung erfolgt in mehreren Phasen, wobei in einer ersten Phase zunächst freiwillig Informationen zu Arzneimitteln und Notfalldaten gespeichert werden können. Der Ausbau der Funktionalität erfolgt stufenweise. Dadurch ergibt sich die Möglichkeit einer medienbruchfreien Verwendung gesundheitsrelevanter Informationen und Dokumente. Der Arzt wird in der Lage sein, neben einem Befund, dem Arztbrief und Untersuchungsergebnissen auch ein elektronisches Rezept, eine Überweisung und die Patientenakte abzulegen. Der Patient kann damit das Rezept in der Apotheke einlösen, Ansprüche bei der Krankenkasse geltend machen oder einen weiterbehandelnden Arzt aufsuchen, der schnell und einfach auf alle Daten zugreifen kann. Basis ist dabei die Einwilligung des Patienten. Das Ziel der elektronischen Gesundheitskarte ist die effizientere Versorgung der Patienten und eine Kosteneinsparung bei den Leistungserbringern [BMG 09b].

Um Akzeptanz bei allen Beteiligten (Leistungserbringer im Gesundheitswesen, IT-Zulieferer) zu erreichen, ist es notwendig eine einheitliche Telematikinfrastruktur zu schaffen und eine verbindliche Rahmenarchitektur zu definieren. Ein Beitrag zur Schaffung von Akzeptanz kann auch die Verwendung von Standards sein. Für alle sicherheitsrelevanten

Bereiche der Gesundheitskarte wurden die Common Criteria eingesetzt und Schutzprofile entwickelt, die beim Bundesamt für Sicherheit in der Informationstechnik (BSI) hinterlegt sind.

Es ist offensichtlich, dass eine solche Anwendung sicherheitskritische Merkmale besitzt und diverse Schutzziele eingehalten werden müssen, wie z.B.:

- Verfügbarkeit: ein Technikausfall in Praxen oder Apotheken würde zu einem nicht akzeptablen Stillstand führen
- Authentifizierung und Autorisierung: Personen, die auf die Daten zugreifen wollen, müssen berechtigt sein
- Vertraulichkeit: nur berechtigte Personen sollen Zugriff auf die Daten haben, Sozialdaten müssen unabhängig von medizinischen Daten gespeichert werden
- Nicht-Abstreitbarkeit: Protokollierung der Zusammenführung von Sozialdaten und medizinischen Daten

Die Aufzählung ist keinesfalls abschließend, sondern soll der Veranschaulichung dienen. Genauere Informationen sind dem Bericht [Krüger 07] zu entnehmen.

Folgend werden einige wichtige Aspekte aus dem Common Criteria Schutzprofil „electronic Health Card (eHC) - elektronische Gesundheitskarte (EGK)“ [Krüger 07] zur Veranschaulichung des Standards vorgestellt.

Definition des Evaluationsgegenstandes (TOE Description)

Der EVG ist eine Smartcard (die elektronische Gesundheitskarte), die dem ISO Standard 7810 entspricht. Der EVG und seine Umgebung entsprechen den gesetzlichen Bestimmungen des GKV (Gesetz zur Modernisierung der gesetzlichen Krankenversicherung), dem Sozialgesetzbuch und dem Datenschutzgesetz des Bundes und der Länder in Deutschland. Die Karte besteht aus folgenden drei Teilen:

- „TOE_IC“: Integrated Circuit (integrierte Halbleiterschaltung)
- „TOE_ES“: IC embedded Software (Betriebssystem)

- „TOE_APP“: EGK-Anwendungen (Datenstrukturen und -inhalte)

Die Karte wird von den Besitzern benutzt, wenn sie Dienste der Gesundheitsversorgung in Anspruch nehmen. Die Karte enthält Daten zur Identifikation des Besitzers, Kontakt- und Finanzdaten, medizinische Daten und Rezepte. Die Karte muss verschiedene Sicherheitsdienste bereitstellen, wie zum Beispiel gegenseitige Authentisierung unter Verwendung asymmetrischer Verfahren.

Beschreibung des Sicherheitsproblems (Security Problem Definition)

Die **Assets**, die vom EVG geschützt werden sollen, sind neben den medizinischen und personenbezogenen Daten auch eine Reihe privater und öffentlicher Schlüssel, z.B. für die Authentisierung. Subjekte, die mit dem EVG interagieren, sind neben dem Besitzer auch Mediziner, Arzthelfer, die Krankenkasse, die Hersteller der Karte, verschiedene Service-Anbieter und Hardware, wie die zu benutzenden Terminals [Krüger 07].

Im Schutzprofil werden eine Reihe **organisatorischer Sicherheitsrichtlinien** (Organizational Security Policy, OSP) beschrieben, die bei der Herstellung und Implementierung der Karte zu beachten sind, z.B.:

- OSP.eHC_Spec: Die Spezifikation der Gesundheitskarte muss eingehalten werden.
- OSP.Electronic_Presecriptions: Der Zugang zu elektronischen Rezepten darf nur nach erfolgreicher Authentifizierung erfolgen.
- OSP.User_Information: Der Karteninhaber muss über die sichere Benutzung der Karte aufgeklärt werden.

Bedrohungen gegen die Werte sind beispielhaft wie folgt identifiziert worden:

- T.Compromise_Internal_Data: Ein Angreifer versucht vertrauliche Daten auf der Karte zu kompromittieren (z.B. durch Löschen, Verändern oder Kopieren).
- T.Intercept: Einem Angreifer gelingt es, die Kommuniktion zwischen dem EVG und dem Terminal zu belauschen und so vertrauliche Daten zu lesen, zu verändern oder zu löschen.

Annahmen, die gemacht werden, sind z.B.:

- A.Users: Eine adäquate Benutzung des EVG innerhalb seiner Umgebung wird vorausgesetzt, d.h. der Inhaber hält die PINs geheim
- A.Perso: Sichere Handhabung der Daten, d.h. Daten, die während der Personalisierungsphase verwendet werden, sind korrekt bezüglich Integrität und Vertraulichkeit.

Sicherheitsziele (Security Objectives)

Security Objectives beschreiben die Schutzziele für den EVG, die alle Aspekte der identifizierten Bedrohungen abdecken, beispielsweise:

- OT.Access_rights: Zugangskontrollrichtlinien für die Daten des EVG
- OT.Services: definiert, welche Dienste vom EVG bereitgestellt werden müssen (z.B. Logging, gegenseitige Authentifizierung, Datenentschlüsselung)
- OT.Cryptography: Implementierung kryptografischer Verfahren (z.B. RSA für Karte-zu-Karte Authentisierung)

Funktionale Sicherheitsanforderungen (Security Functional Requirements)

- FCS_CKM.1.1/SM: Cryptographic Key Generation - Secure Messaging Keys: Die TSF[7] sollten Kryptoschlüssel in Übereinstimmung spezifizierter Algorithmen und Schlüssellänge von 112 Bit verwenden verwenden
- FCS_COP.1.1/SHA Cryptographic Operation Hash Algorithm: Die TSF für Hashfunktionen sollte SHA-1[8] sein
- FIA_AFL.1.1/PIN Authentication Failure Handling: Die TSF müssen misslungene Authentifizierungsversuche entdecken
- FIA_UID.1.2: Die TSF müssen durchsetzen, dass jeder Nutzer vor Zugriff auf Funktionalitäten des EVG erfolgreich identifiziert wurde

[7] TOE Security Functions, deutsch: Sicherheitsfunktionalität des Evaluationsgegenstandes
[8] Secure Hash Algorithm, englisch für sicherer Hash-Algorithmus

- FDP_SDI.2.2: Stored Data Integrity: Wenn ein Datenintegritätsfehler entdeckt wird, muss die Verwendung der Daten verboten werden und die verbundene Entität (Benutzer) informiert werden

Anforderungen an die Vertrauenswürdigkeit (Security Assurance Requirements)

Für die Evaluierung anhand des Schutzprofils wird Evaluation Assurance Level EAL-4 verlangt.

Kapitel 6

Problemanalyse und Strategiedefinition der IT-Sicherheit in Virtuellen Welten

Im zweiten Kapitel wurde erläutert, was Virtuelle Welten sind und welche Eigenschaften sie haben. Es wurde gezeigt, dass es unterschiedliche Arten von Virtuellen Welten gibt, die verschiedene Handlungsziele (Unterhaltung, Kommunikation, Handel, etc.) unterstützen. Die in diesem Kapitel angestrebte Analyse der IT-Sicherheit Virtueller Welten entsprechend der Common Criteria erfordert die genaue Beschreibung eines Evaluationsgegenstandes (EVG) (vgl. Kapitel 5). Der EVG ist aber kein konkretes Produkt, sondern eine Produktklasse. Daher müssen zunächst die Eigenschaften des EVG, für den die Sicherheitsanalyse durchgeführt wird, festgeschrieben werden. Auf dieser Basis können anschließend die beteiligten Akteure beschrieben und die zu schützenden Werte in Virtuellen Welten identifiziert werden.

In Kapitel 4 wurde bereits der IT-Sicherheitszusammenhang ausführlich erläutert. Er zeigt, dass Angreifer versuchen Schwachstellen auszunutzen um die Werte zu missbrauchen oder zu schädigen. In diesem Kapitel wird verdeutlicht, welchen Bedrohungen und Angriffen die Werte ausgesetzt sind.

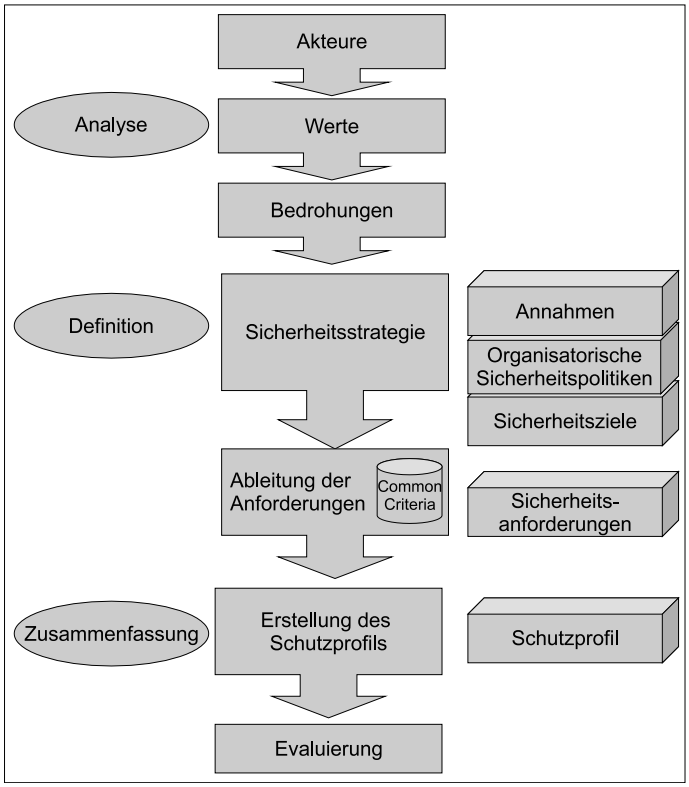
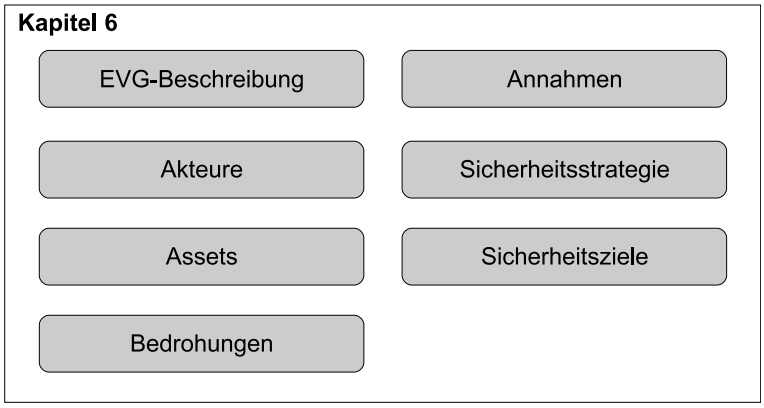


Abbildung 6.1: Vorgehensweise bei der Sicherheitsanalyse und Anforderungsdefinition

Das Ziel der IT-Sicherheit ist der Schutz von bedrohten Werten. Daher wird im Anschluss an die grundlegende (Problem-) Analyse eine Sicherheitsstrategie definiert, die den Schutz der Werte umsetzen kann. Das Ergebnis der Definition der Sicherheitsstrategie ist eine Aufstellung der Annahmen, der organisatorischen Sicherheitspolitiken und der Sicherheitsziele für den EVG und dessen Umgebung (vgl. Abbildung 6.1). Aus dieser Definition der Sicherheitsstrategie können anschließend die Sicherheitsanforderungen abgeleitet (Kapitel 7) und das Schutzprofil (Kapitel 8) aufgestellt werden. Vorarbeiten zu dieser Problemanalyse wurden von der Autorin bereits in [Beyer 06], [Beyer 07a], [Beyer 07b] und [Beyer 09] veröffentlicht.

In diesem Kapitel werden folgende Fragen beantwortet.

- Für welchen Evaluationsgegenstand wird die Sicherheitsanalyse durchgeführt?
- Welche Akteure nehmen am Prozess teil?
- Welche Werte besitzen die Akteure?
- Welche Bedrohungen sind gegen diese Werte gerichtet?
- Welche Annahmen müssen für den EVG getroffen werden?
- Welche organisatorischen Sicherheitspolitiken müssen berücksichtigt werden?
- Welche Sicherheitsziele gelten für den EVG und welche für die Umgebung?



6.1 Beschreibung des Evaluationsgegenstandes

Der Evaluationsgegenstand ist ein Softwareprogramm, dass aus einer Client- und einer Serveranwendung besteht und der Generierung, Darstellung und Speicherung Virtueller Welten dient. Innerhalb dieser Welten haben die Benutzer verschiedene Möglichkeiten der Handlung. Nach dem Start der Clientanwendung loggt sich der Benutzer mit seinen Accountdaten auf dem Server ein. Bei der ersten Verwendung muss der Benutzer einen Avatar erstellen und gestalten, d.h. Kleidung auswählen und ein Erscheinungsbild festlegen (z.B. Augenform und -farbe, Körperproportionen, etc). Anschließend steht dem Benutzer die Virtuelle Welt zur Erkundung offen.

Im Folgenden werden einige mögliche Aktionen exemplarisch erläutert, die vom EVG bereitgestellt werden können. Auf den Streifzügen durch die Welt erhält der Benutzer die Möglichkeit bestimmte Herausforderungen in Form von Aufgaben und Herausforderungen (so genannte Quests) anzunehmen. Gelingt es ihm die Aufgabe zu lösen, erhält der Benutzer eine Belohnung in Form von Erfahrungspunkten, Gegenständen oder finanzielle Mittel, wie Geld oder Gold. Der Benutzer kann Gegenstände auch selbst herstellen. Der Avatar kann verschiedene Fertigkeiten (schmieden, fischen, zaubern, etc.) erlangen. Mit den Gegenständen kann Handel betrieben werden. In der Welt stehen Marktplätze zur Verfügung, auf denen die Gegenstände ge- und verkauft werden können. Die Benutzer können sich mit anderen Benutzern oder Non-Person-Characters[1] (NPCs) in Kämpfen messen. Derjenige, der die besseren Waffen und Fertigkeiten besitzt, hat im Kampf klare Vorteile. Außerdem kann sich der Benutzer mit anderen Benutzern zu einer Gruppe zusammenschließen. Solche Partner- bzw. Freundschaften erleichtern das Leben in der Virtuellen Welt. Zum Beispiel erhält man Unterstützung im Kampf oder kann auf Erfahrung der Freunde zurückgreifen.

Der Aufbau des EVG verfolgt den Client-Server-Ansatz. Ein Server bzw. Serververbund stellt die Funktionalität zur Verfügung. Die Clientsoftware, ein Softwareprogramm, das auf dem Rechner des Benutzers installiert wird, dient der Darstellung der Welt und der Kommunikation mit dem Server. Für die Interaktion mit anderen Benutzern stellt der EVG einen Kommunikationskanal zur Verfügung. Aus technischer Sicht bedeutet dies, dass keine direkte Kommunikation zwischen zwei Benutzern möglich ist, sondern über einen zentralen Server abläuft.

Oftmals verwenden Anwender externe Software zur Kommunikation (z.B. Skype) oder zur Abwicklung von Bezahlvorgängen (Zahlungsserver). Diese externen Anwendungen entziehen sich der Kontrolle sowie der Verantwortlichkeit des Anbieters und liegen daher nicht im Machtbereich der Sicherheitsfunktionalitäten des EVG. Sie müssen vom EVG abgegrenzt werden und sind daher nicht Gegenstand des EVG. Für sie kann kein Schutz seitens des EVG erfolgen. Weiterhin wird keine Hardware auf Client- und Serverseite von

[1]Nicht-Spieler-Charaktere sind Figuren in der Virtuellen Welt, die nicht von Spielern geführt werden. Sie sind Elemente der Virtuellen Welt

den EVG-Sicherheitsfunktionen abgedeckt. Folgende Komponenten werden vom EVG eingeschlossen (vgl. Abbildung 6.2):

- Serversoftware
- Clientsoftware
- Kommunikationskanal (Netzwerk) zwischen diesen.

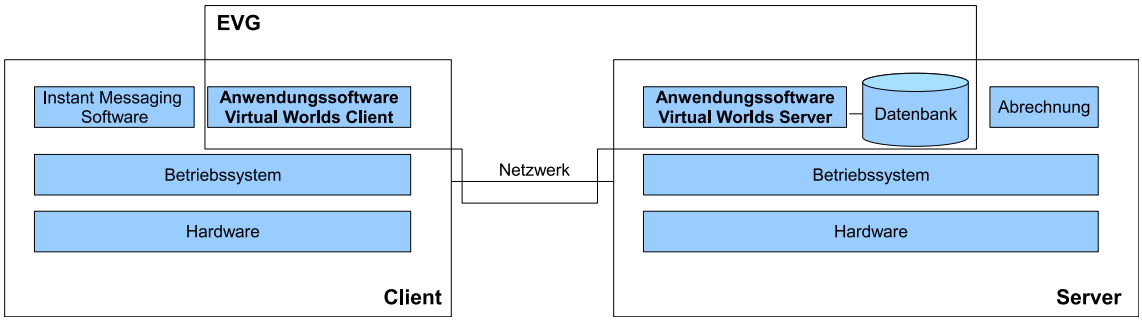


Abbildung 6.2: Aufbau des EVG [eigene Abbildung]

Folgende Funktionen werden durch den EVG unterstützt:

- Darstellung einer 3D-Welt
- Kommunikation der Benutzer über integriertes Chat-System
- Sammeln von Erfahrungspunkten
- Speichern von nutzerbezogenen Daten
- Speichern von handlungsbezogenen Daten

Diese Werte werden auf Serverseite in einer Datenbank gespeichert.

Der auf Nutzerseite zu installierende Softwareclient dient lediglich zur Darstellung der einzelnen Werte und enthält die folgenden grundlegenden Funktionselemente:

- Inventar (zur Darstellung der Gegenstände)
- Chat (zur Darstellung der Kommunikation mit anderen Nutzern)

- Kontaktliste (zur Darstellung der Kontakte/Freunde)
- Teleport (zur Navigation innerhalb der Welt)
- Suche (zum Finden von anderen Nutzern und Gebieten)
- Karte (zur Darstellung der Welt)

6.2 Akteure

Folgende Subjekte sind am Nutzungsprozess beteiligt:

- Nutzer: Über den Softwareclient ist der Nutzer in der Lage in der Virtuellen Welt zu agieren. Er kann die Spielwelt erkunden, Quests lösen, gegen andere Nutzer oder NPCs kämpfen und sich mit anderen Nutzern in Interessengruppen zusammenschließen und zusammenarbeiten.
- Interessengruppen: Eine Interessengruppe stellt den Zusammenschluss mehrerer Nutzer mit gleichen Interessen über einen längeren Zeitraum dar. Das können etwa Gilden, Allianzen oder Berufe sein. Die Zusammenfassung aller Nutzer eines Spiels heißt Community.
- Anbieter: Der Anbieter eines Spiels stellt die Funktionalität des Spiels und die notwendige Software zur Verfügung. Der Anbieter handelt mit einem marktwirtschaftlichen Interesse. Sein Ziel stellt die Gewinnmaximierung dar. Mit dem Spiel verdient der Anbieter Geld. Es gibt dabei verschiedene Geschäftsmodelle (Abonnementgebühren, Werbung, Zusatzdienste, etc.). Sein Interesse ist daher die stabile Verfügbarkeit des Service, da sonst die Zahlungen der Kunden ausbleiben.

6.3 Zu schützende Werte/Assets

IT-Sicherheit ist verbunden mit dem Schutz von Werten. Werte sind dabei Einheiten, die für jemanden von wert sind. Folgende Assets können für den EVG identifiziert werden.

Avatar: Der Avatar repräsentiert den Nutzer in der Virtuellen Welt. Die Gestaltung des Avatars ist abhängig von den Vorgaben des Anbieters und der Erfahrung des Nutzers. Der Avatar kann sehr individuell gestaltet werden, wodurch eine Identifizierung des Nutzers mit dem Avatar und damit der Virtuellen Welt erreicht wird.

Gegenstände: Während des Spiels bzw. dem Aufenthalt in der Virtuellen Welt erhält der Nutzer Gegenstände wie Kleidung für den Avatar, Waffen, Autos, Elixiere, etc. Jeder Gegenstand, der in Besitz des Nutzers gelangt, muss geschützt werden. In einigen Virtuellen Welten hat der Nutzer die Möglichkeit selbst Gegenstände zu erzeugen und nach seinen Wünschen zu gestalten. Gegenstände können gehandelt werden. Besonders seltene oder nützliche Gegenstände sind wertvoll und können daher für einen hohen Preis verkauft werden.

Zahlungsmittel: Jede Virtuelle Welt hat eine interne Währung. Das können Geld, Gold oder andere finanzielle Mittel sein. Der Nutzer kann sich während der Nutzung durch verschiedene Aktionen Geld verdienen, wie Handel mit Gegenständen oder Anbieten von Dienstleistungen.

Fertigkeiten: Der Avatar lernt während der Nutzung bestimmte Fertigkeiten, wie Fischen, Zaubertränke herstellen, Waffen reparieren etc.

Erfahrungsstufen (Level)/Erfahrungspunkte (EP): Für erfolgreiche Aktionen (z.B. das Lösen von Quests) erhält der Nutzer Erfahrungspunkte und steigt in den Erfahrungsstufen (Leveln) auf. Die Punkte und Erfahrungsstufen, die Nutzer erreichen, liefern eine Aussage darüber, wie erfolgreich er ist.

Welt: Die Welt ist der Platz, wo sich die Avatare während der Nutzung aufhalten. Der Aufbau und die Gestaltung dieser virtuellen 3D-Welt sind abhängig von der jeweiligen Virtuellen Welt. Jeder Gegenstand, der nicht einem Avatar zugeordnet werden kann, wird der Welt zugeordnet. Je nach Geschäftsmodell kann die Welt vom Anbieter oder von der Community entwickelt werden.

(Verhaltens-)Regeln: Der Anbieter legt Verhaltensregeln fest, um Fairness für alle Beteiligten zu gewährleisten. Kein Nutzer sollte einen unfairen Vorteil gegenüber einem anderen haben. Wenn sich alle Nutzer nach den Regeln verhalten, ist Fairness sichergestellt.

Kommunikationsdaten: Während des Kommunikationsprozesses tauschen die Beteiligten sensible Informationen aus, die vertraulich behandelt werden müssen. Zum Beispiel tauschen die Mitglieder einer Gilde vertrauliche Informationen aus, wenn Sie sich eine Strategie für den Kampf gegen eine andere Gilde überlegen. Der Kommunikationsinhalt könnte auch personenbezogene Daten enthalten, auf die unautorisierte Personen keinen Zugriff haben dürfen.

Transaktionsdaten: Beim Auslösen einer Transaktion entstehen Daten, die deren Durchführung betreffen. Dazu gehören unter anderem der Name des Käufers und des Verkäufers, eindeutige Bezeichner der Ware(n), der Betrag des Geldes, Datum, Uhrzeit, Status, etc.

Zugangsdaten: Um Zugang zur Virtuellen Welt zu erlangen, benötigt der Nutzer Zugangsdaten (z.B. Benutzername und Passwort) um sich gegenüber dem System zu identifizieren.

Kontaktdaten: Die Virtuellen Welten sind auf Kommunikation bzw. Interaktion der Avatare untereinander ausgelegt. Die Nutzer knüpfen soziale Kontakte zu anderen Beteiligten und bilden Netzwerke mit Gleichgesinnten.

Kontodaten: Beim Erstellen der Benutzerkonten werden personenbezogene Daten erfasst und gespeichert. Dazu zählen Informationen wie Name, Adresse, Geburtstag, etc.

Reputation: Reputation ist eine soziale Ressource und bildet die Basis für den Aufbau von Vertrauensverhältnissen. Die Reputation ist der Ruf einer Person, die sie innerhalb einer Gemeinschaft genießt. Ein guter Ruf bzw. eine gute Reputation erhöht die Glaubwürdigkeit einer Person. Die Reputation kann nach Bourdieu [Bourdieu 92] auch als das kulturelle Kapital einer Person bezeichnet werden. Die Reputation eines Nutzers in der Virtuellen Welt wird über vergangene Aktionen wahrgenommen. Über die Reputation eines Nutzers, die auf seinem Verhalten in der Vergangenheit beruht, kann auf zukünftige Aktionen geschlossen werden. Wenn ein Nutzer zum Beispiel bei Handelstransaktionen in der Vergangenheit zuverlässig war, wird vermutet, dass er auch bei zukünftigen Handelstransaktionen zuverlässig handelt[2].

[2]Bei der Auktionsplattform Ebay wird das Reputationsmanagement zum Beispiel über das Bewertungssystem veranschaulicht.

6.4 Analyse der Bedrohungen

Um erfolgreich Bedrohungen eines Systems zu identifizieren, ist ein systematisches Vorgehen zur Analyse notwendig. Leider mangelt es in der Literatur für IT-Sicherheit an guten Vorschlägen für ein solches Vorgehen. Zur systematischen Analyse komplexer Zusammenhänge haben sich Kreativitätstechniken, wie z.B. der morphologische Kasten, gut etabliert. Der morphologische Kasten ist eine mehrdimensionale Matrix, in der bestimmte Merkmale und mögliche Ausprägungen der Merkmale gegenübergestellt werden. In der Matrix werden senkrecht die Merkmale aufgetragen und waagerecht die möglichen Ausprägungen der Merkmale. In den Zellen steht die Beschreibung der Merkmalsausprägung (vgl. Abbildung 6.3). Der morphologische Kasten ist Vorbild für die Entwicklung eines

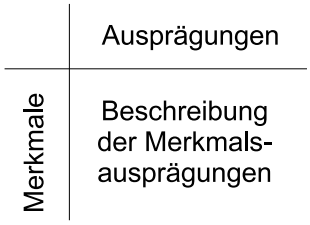


Abbildung 6.3: Morphologischer Kasten

Rasters zur systematischen Bedrohungsanalyse, das wie folgt definiert wurde. Senkrecht werden die Werte aufgestellt, gegen die Bedrohungen gerichtet sein können. Waagerecht aufgetragen werden die Kriterien für die Sicherheit eines Systems in Form der Schutzziele. Die Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität, Verfügbarkeit, Datenschutz und Nichtabstreitbarkeit (vgl. Kapitel 4). Durch dieses Raster kann für jeden Wert untersucht werden, wie eine Verletzung der Schutzziele aussieht. Die Verletzung der Schutzziele jedes Wertes stellt eine konkrete Bedrohung gegen die Sicherheit der Virtuellen Welt dar. Das Raster wird in Tabelle 6.1 visualisiert.

Diese Bedrohungen können durch Angreifer ausgelöst werden. Angreifer sind diejenigen Subjekte, die bewusst oder unbewusst, absichtlich oder versehentlich, aktiv oder passiv diese Bedrohungen durch Angriffe erwirken. Dazu gehören neben Netzwerkangreifern auch unfaire Nutzer und administratives Personal des Anbieters.

Tabelle 6.1: Systematische Bedrohungsanalyse

	Verlust/Verletzung der/des:				
Wert	Vertraulichkeit	Integrität	Verfügbarkeit	Datenschutzes	Nichtabstreitbarkeit
Avatar	Unbefugtes Lesen von Avatareigenschaften (1)	Unbefugte(s) Modifikation/Löschen des Avatars (2)	Nichtverfügbarkeit des Avatars (3)	Über den Avatar werden personenbezogene Daten preisgegeben (4)	Eine Aktion kann einem Avatar nicht zugeordnet werden (5)
Gegenstände	Unbefugtes Lesen von Gegenstandseigenschaften (6)	Unbefugte(s) Modifikation/Löschen der Gegenstände (7)	Nichtverfügbarkeit der Gegenstände (8)	Über selbst erstellte Gegenstände werden personenbezogene Daten preisgegeben (9)	Der Empfänger einer Ware bestreitet die Ware erhalten zu haben (10)
Zahlungsmittel	Unbefugtes Lesen der verfügbaren Zahlungsmittel eines Nutzers (11)	Unbefugte(s) Modifikation/Löschen der Zahlungsmittel (12)	Nichtverfügbarkeit der Zahlungsmittel (13)	--[3]	Der Verkäufer bestreitet das Geld erhalten zu haben (14)
Fertigkeiten	Unbefugtes Lesen von Fertigkeiten eines Avatars (15)	Unbefugte(s) Modifikation/Löschen der Fertigkeiten (16)	Nichtverfügbarkeit der Fertigkeiten (17)	--	--

[3]Der EVG schließt Zahlungsverkehr außerhalb der Welt aus. Reale Konten und Bezahldienste werden vom EVG abgegrenzt. Der interne Zahlungsverkehr ist unabhängig von der Identität des Nutzers.

Tabelle 6.1: Systematische Bedrohungsanalyse

Fortsetzung

	Verlust/Verletzung der/des:				
Wert	Vertraulichkeit	Integrität	Verfügbarkeit	Datenschutzes	Nichtabstreitbarkeit
Level/EP	--[4]	Unbefugte(s) Modifikation/Löschen der Level/EP (18)	Nichtverfügbarkeit der Level/EP (19)	--	--
Welt	Unbefugtes Lesen der Eigenschaften der Welt (20)	Unbefugte(s) Modifikation/Löschen der Welt (21)	Nichtverfügbarkeit der Welt (22)	--	--
Regeln	--[5]	Unbefugte(s) Modifikation/Löschen der Regeln (23)	Die Nutzer haben nicht die Möglichkeit bzw. Gelegenheit die Regeln einzusehen (24)	--	Nutzer verhalten sich nicht entsprechend der Regeln (Verletzung der Fairness), Nutzer behaupten die Regeln nicht zu kennen (25)

[4]Informationen zu Level/EP sind öffentliche Daten.

[5]Regeln sind keine vertraulichen Daten sondern müssen zugänglich sein.

Tabelle 6.1: Systematische Bedrohungsanalyse

Fortsetzung

	Verlust/Verletzung der/des:				
Wert	Vertraulichkeit	Integrität	Verfügbarkeit	Datenschutzes	Nichtabstreitbarkeit
Kommunikationsdaten	Unbefugtes Lesen von Kommunikationsdaten (26)	Unbefugte(s) Modifikation/Löschen der Kommunikationsdaten (27)	Nichtverfügbarkeit der Kommunikationsdaten (28)	Kommunikationsdaten werden in einer Weise verwendet, der ein Nutzer nicht zugestimmt hat(29)	Ein Nutzer bestreitet die Kommunikation bzw. den Inhalt einer Kommunikation (30)
Transaktionsdaten	Dritte erlangen Kenntnis über den Inhalt einer Transaktion (31)	Unbefugte(s) Modifikation/Löschen der Transaktionsdaten (32)	Transaktionsdaten gehen verloren (33)	Transaktionsdaten werden in einer Weise verwendet, der ein Nutzer nicht zugestimmt hat (34)	Der Inhalt einer Transaktion wird bestritten (35)
Logindaten	Unbefugtes Lesen von Logindaten (36)	Unbefugte Modifikation von Logindaten (37)	Dem Nutzer ist mit korrekten Logindaten kein Zugang zur Welt möglich (Nichtverfügbarkeit Logindaten auf Serverseite) (38)	Die Logindaten lassen auf die reale Identität des Nutzers schließen (39)	--

Tabelle 6.1: Systematische Bedrohungsanalyse

Fortsetzung

	Verlust/Verletzung der/des:				
Wert	Vertraulichkeit	Integrität	Verfügbarkeit	Datenschutzes	Nichtabstreitbarkeit
Kontaktdaten	Unbefugtes Lesen von Kontaktdaten (40)	Unbefugte(s) Modifikation/Löschen der Kontaktdaten (41)	Nichtverfügbarkeit der Kontaktdaten (42)	Personenbezogene Daten werden in einer Weise verwendet, der ein Nutzer nicht zugestimmt hat (43)	Ein Nutzer bestreitet eine Aktion in Bezug auf seine Kontaktdaten durchgeführt zu haben (44)
Kontodaten	Unbefugtes Lesen von Kontodaten (45)	Unbefugte(s) Modifikation/Löschen der Kontodaten (46)	Nichtverfügbarkeit der Kontodaten (47)	Kontodaten werden in einer Weise verwendet, der ein Nutzer nicht zugestimmt hat (48)	Eine Person bestreitet ein Konto angelegt zu haben (49)
Reputation	--[6]	Unberechtigte Manipulation der Reputation eines Nutzers (50)	--	Über das Reputationsmanagement werden personenbezogene Daten preisgegeben (51)	--[7]

[6]Die Reputation ist nicht vertraulich sondern öffentlich.

[7]Die Reputation ist immer einer Person zugeordnet, auch wenn unberechtigte Informationen (vgl. Integrität) verbreitet werden.

Die Werte (mit Ausnahme der Reputation) existieren in Form von Daten, die in Bewegungs- und Bestandsdaten unterschieden werden können. Bewegungsdaten sind die Daten, die über das Netzwerk zwischen Client und Server transportiert werden. Bestandsdaten sind Daten, die in einer Datenbank gespeichert vorliegen und über Funktionalitäten der Software verändert werden. Zu den Bewegungsdaten zählen Transaktionsdaten, Kommunikationsdaten und Logindaten. Bestandsdaten sind Daten von Avatar, Gegenständen, Zahlungsmitteln, Fertigkeiten, Level/Erfahrungspunkte, Welt, Regeln, Kontaktdaten und Kontodaten.

Die Bedrohungen ergeben sich aus der Verletzung der Schutzziele und haben Auswirkungen auf das Unterhaltungserleben innerhalb der Welt. Welche Auswirkungen das sein können, wird in den folgenden Abschnitten für jeden Wert erläutert.

6.4.1 Auswirkungen der Bedrohungen auf den Avatar

Wie bereits in Kapitel 6.3 beschrieben, ist der Avatar von besonderer Bedeutung für den Nutzer, da er über ihn in der Virtuellen Welt repräsentiert wird.

Der Avatar hat Eigenschaften, die für andere Nutzer sichtbar sind (z.B. Größe, Haarfarbe, Gruppenzugehörigkeit, etc.) und andere Eigenschaften, die nur der Nutzer kennt. Gelingt es anderen Nutzern (z.B. gegnerischen Spielern) die Eigenschaften des Avatars eines Nutzers zu lesen, kann das zu einem Nachteil für den Nutzer sein, da der Gegner in einer Wettbewerbssituation einen unberechtigten Wissensvorteil hat.

Kommt es zu einer unbefugten Modifikation des Avatars durch das Personal des Anbieters oder einen externen Angreifer, kann damit der Ruf des Nutzers in der Welt geschädigt werden.

Beispielszenario: Alice ist Universitätsdozentin und hält in der Virtuellen Welt Vorlesungen und Seminare. Dort muss sie sich durch ihren Avatar repräsentieren lassen. Während Sie auf einem virtuellen Podium Inhalte präsentiert, sitzen die Studenten bzw. ihre Avatare in den Rängen und hören zu. Findet während einer Sitzung ein Angriff auf die Datenbank statt, kann dies beispielsweise zu einer Veränderung der Gestalt des Avatars führen. Dadurch kann die Unterrichtseinheit gestört werden, da die Studenten durch

den Vorfall abgelenkt sind und dem Vortrag der Dozentin keine Aufmerksamkeit mehr schenken.

Die Nichtverfügbarkeit des Avatars (z.B. durch Account-Diebstahl) bedeutet für den Nutzer, dass er nicht mehr in der Welt agieren kann, die Welt wird dadurch nutzlos für ihn.
Über den Avatar kann der Nutzer persönliche Daten preisgeben, z.B. indem er bei der Namensvergabe für den Avatar seinen realen Namen verwendet.
Kritische Aktionen, bei denen es zur Verletzung der Nichtabstreitbarkeit kommt, wenn sie dem Avatar nicht zugeordnet werden können, sind Transaktionen und Kommunikation. Bei diesen beiden Prozessen muss klar sein, von welchem Avatar die Aktionen ausgelöst werden.

6.4.2 Auswirkungen der Bedrohungen auf die Gegenstände

Gegenstände erhält bzw. erstellt der Nutzer während seines Aufenthaltes in der Virtuellen Welt.

Das unbefugte Lesen von Gegenstandseigenschaften kann zu Wettbewerbsnachteilen führen, wenn z.B. in einer Kampfsituation der Gegner Informationen zum Status der Waffentauglichkeit erhalten kann. Waffen können in Onlinerollenspielen so gestaltet werden, dass sie im Laufe ihrer Lebensdauer an Qualität verlieren. Je öfter ein Schwert benutzt wird, umso stumpfer wird es. So könnten sich Spieler nur solche Gegner aussuchen, bei denen sie wissen, dass sie nur schwache Waffen besitzen.

Eine unbefugte Modifikation eines Gegenstandes kann zu einem enormen Wertverlust führen.
Beispielszenario: Alice entwirft virtuelle Modeaccessoires und stellt diese her. Für interessierte Kundinnen und Kunden in der Virtuellen Welt bietet sie eine Demoversion (Probeartikel) des Accessoires an, damit es ausprobiert werden kann. Die Demoversionen sind immer mit einem Zusatzelement versehen, auf dem in großer Schrift „Demo“ geschrieben steht. Die Verkaufsversionen enthalten dieses Element nicht. Um das Modeaccessoire sinnvoll einsetzen zu können, müssen die Kundinnen den Gegenstand kaufen. Gelingt es

einem unfairen Nutzer die Demoversion so zu verändern, dass das Zusatzelement mit der Aufschrift „Demo“ verschwindet, braucht er kein Geld auszugeben und Alice verliert Umsatz. Diese Bedrohung kann auch (versehentlich) vom administrativen Personal des Anbieters ausgehen, zum Beispiel durch Software-Updates.

Wird ein Gegenstand unberechtigt gelöscht, führt dies zur Nichtverfügbarkeit des Gegenstandes. Der Nutzer kann den Gegenstand dann nicht mehr nutzen, was für ihn eine Einschränkung im Nutzungserleben darstellen kann.

Über die Produktion eigener Gegenstände können Nutzer personenbezogene Daten von sich preisgeben, z.B. indem sie T-Shirts entwerfen, auf denen ihre reale Adresse steht. So gibt der Nutzer selbst zu viele Informationen über seine reale Identität preis.

Der Handel eines Gegenstands ist eine Transaktion und umfasst die drei Phasen:

- Einigung,
- Zahlung des Geldes und
- Übergabe der Ware.

Zunächst müssen sich Käufer und Verkäufer einigen, das heißt der Verkäufer bietet einen Gegenstand zum Kauf an und nennt einen Preis. Der Käufer muss den Kaufpreis akzeptieren und seine Absichtserklärung über den Kauf abgeben. In der zweiten Phase bezahlt der Käufer den Kaufpreis und in der dritten Phase übergibt der Verkäufer die Ware. Die Phasen zwei und drei können auch in vertauschter Reihenfolge stattfinden. Wichtig für eine konsistente Transaktion ist, dass sie entweder vollständig oder gar nicht ausgeführt wird. Es darf also nicht passieren, dass der Käufer zwar das Geld zahlt, aber die Ware nicht bekommt. Genauso wenig darf es passieren, dass der Verkäufer die Ware übergibt aber das Geld nicht erhält. Bei einer vollständigen Transaktion muss beim Käufer das Geld abgebucht und dem Verkäufer gutgeschrieben werden. Die Ware muss vom Verkäufer zum Käufer übergehen.

Bei der Betrachtung der Nichtabstreitbarkeit wird davon ausgegangen, dass eine Transaktion zwar vollständig und konsistent ausgeführt wurde, eine der beiden Parteien dies aber bestreitet. In Bezug auf den Gegenstand liegt die Bedrohung darin, dass der

Verkäufer die Ware übergeben hat, der Empfänger aber abstreitet die Ware erhalten zu haben.

6.4.3 Auswirkungen der Bedrohungen auf die Zahlungsmittel

Zahlungsmittel wie Geld, Gold, Silber oder Platin können zum Tausch mit Waren oder Dienstleistungen eingesetzt werden. Welche Währung in einer Virtuellen Welt als Tauschmittel akzeptiert wird, wird vom Anbieter durch die Programmierung der Welt vorgegeben.

Die Höhe der verfügbaren Zahlungsmittel eines Nutzers sind nur ihm selbst bekannt und für andere Nutzer nicht sichtbar. Ein unbefugtes Lesen der verfügbaren Zahlungsmittel stellt eine Verletzung der Vertraulichkeit dar.

Wird ein Datenbankeintrag unberechtigt verändert oder gelöscht, führt dies zum Wertverlust bzw. Totalverlust des Zahlungsmittels für den Nutzer.
Beispielszenario: Alice besitzt in einer Virtuellen Welt 100 Goldstücke. Ein Administrator verändert unbefugt den entsprechenden Datenbankeintrag auf 10. Dies hat zur Folge, dass Alice nur noch 10 Goldstücke besitzt, ohne dass sie eines ausgegeben hat. Dies führt zur Nichtverfügbarkeit der Differenz von 90 Goldstücken.

Die Bedrohung der Abstreitung einer Handlung in Bezug auf Zahlungsmittel liegt vor, wenn der Käufer das Geld zwar übergeben hat, der Verkäufer aber dessen Erhalt abstreitet.

6.4.4 Auswirkungen der Bedrohungen auf die Fertigkeiten

Mit zunehmender Nutzungsdauer einer Virtuellen Welt steigern sich die Fertigkeiten, die ein Nutzer dort hat.

Beispielszenario: In einem Onlinerollenspiel übernimmt ein Spieler die Rolle des Magiers. Um im Spiel voranzukommen, muss er verschiedene Fertigkeiten erlernen, die für einen Magier typisch sind, beispielsweise verzaubern oder Zauberelixiere herstellen. Bei gemeinsamen Kämpfen mit anderen Spielern kann er diese Fertigkeiten einsetzen, um

die Gruppe zu unterstützen.
Ist es durch einen Angriff möglich, die Fertigkeiten des Magiers zu verändern oder zu löschen, beeinträchtigt ihn das in seinem Fortkommen im Spiel. Kann der Nutzer seine Fertigkeiten aufgrund nicht vorhandener Verfügbarkeit nicht nutzen, kann er der Gruppe nicht helfen und verliert dadurch an Anerkennung innerhalb der Gruppe. Gelingt es Angreifern, die Fertigkeiten eines Avatars zu lesen, entsteht dem Nutzer ein Nachteil, da gegnerische Spieler einen Wettbewerbsvorteil erlangen können.

6.4.5 Auswirkungen der Bedrohungen auf die Erfahrungsstufen (Level)/die Erfahrungspunkte (EP)

Für erfolgreiche Aktionen innerhalb der Welt erhält der Nutzer Erfahrungspunkte und steigt in seinen Erfahrungsstufen (Level). Das Level und die Punkte eines Nutzers drücken aus, welche Erfahrung er in der Virtuellen Welt bereits gesammelt hat. Die Anzahl der Punkte und das aktuelle Level eines Nutzers werden auch in einer Datenbank gespeichert. Manipulationen an der Datenbank können auch Auswirkungen auf diese Werte haben. Je höher das Level eines Nutzers ist, desto mehr Erfahrung hat er in der Welt. Oftmals werden bestimmte Gebiete der Welt für einen Nutzer erst zugänglich, wenn er ein gewisses Level erreicht hat.

Werden diese Daten manipuliert, kann das zweierlei Folgen haben, je nach Modifikation. Werden die Werte so verändert, dass der Nutzer in ein niedrigeres Level gestuft wird, führt das dazu, dass ihm eventuell nicht alle Gebiete zugänglich sind. Sein Arbeitseinsatz der vergangenen Spielzeit ist verloren und er muss sie erneut erarbeiten. Auch das Ansehen des Nutzers, welches mit steigender Erfahrung wächst, nimmt Schaden durch so eine Veränderung.

Werden diese Werte so manipuliert, dass größere Werte entstehen, wird der Nutzer in ein Level gestuft, dass er noch nicht erarbeitet hat. Dies kann natürlich einen positiven Effekt haben, indem der Nutzer Zeit spart, ihm zusätzliche Gebiete zugänglich sind, ohne dass er einen Aufwand dafür erbringen musste. Genauso kann der Effekt aber auch negative Auswirkungen haben, da der Nutzer überfordert werden kann. Ihm fehlt die ent-

sprechende Erfahrung aus den Leveln dazwischen, die ihn auf bestimmte Situationen, wie Kämpfe mit starken Gegnern, vorbereitet hätte. Das kann dazu führen, dass er demotiviert wird, da er nicht die entsprechenden Fähigkeiten für die gestellten Herausforderungen hat (möglicher Verlust des Flow-Erlebnisses, vgl. Kapitel 3).

Das Löschen der Erfahrungspunkte führt zu deren Nichtverfügbarkeit. Diese Bedrohung führt dazu, dass einem Nutzer seine bisherige Erfahrung nicht zugeordnet werden kann. Es ist nicht klar, welche Gebiete und Handlungsmöglichkeiten dem Nutzer zugänglich sind. Die Bedrohung kann außerdem zum Verlust des Ansehens innerhalb der Community führen.

6.4.6 Auswirkungen der Bedrohungen auf die Welt

Die Welt bezeichnet die Gebiete (Kontinente, Inseln, Plätze, etc.) einer Virtuellen Welt, in denen sich die Avatare der Nutzer aufhalten können.

Durch unbefugtes Lesen der Eigenschaften der Welt können Nutzer einen unberechtigten Vorteil erlangen, da sie Informationen haben, die andere Nutzer nicht haben. Veränderungen der Welt können zu ungleichen Bedingungen für verschiedene Nutzergruppen (z.B. Klassen) führen und somit zu einem unausgewogenen Spiel (unbalanced game) beitragen, wodurch die Fairness verletzt wird.

Beispielszenario: Alice spielt ein Onlinerollenspiel, in dem es zwei verschiedene Gruppen gibt, die Nachtschattenelfen und die Fleischfressergefährten. Beide Gruppen sind verfeindet und kämpfen gegeneinander. Jede der beiden Gruppen besitzt einen eigenen Kontinent, auf dem sie sich unbescholten bewegen können. Nur in speziellen Arenen können sich die beiden Gruppen treffen, um sich zu messen. Die Arenen sind in den Grenzgebieten der jeweiligen Kontinente, sodass die Anreise zu den Arenen für beide Gruppen gleich weit ist. Alice gehört den Nachtschattenelfen an. Bei einem Angriff auf die Datenbank können die Fleischfressergefährten die Welt so verändern, dass die auf ihrem Kontinent vorkommenden Hindernisse (Bäume, Häuser, Flüsse etc.) verschwinden und sie somit einen viel kürzeren Weg zu den Arenen haben. Während die Nachtschattenelfen sich mühevoll um die Hindernisse bewegen müssen, haben die Fleischfressergefährten

einen Vorteil erlangt, da sie dies nicht tun müssen. Bei einem Kampf (so genannte Battle) in einer Arena können von den Fleischfressergefährten viel schneller viele Krieger anreisen, um die Gruppe zu unterstützen, während die Nachtschattenelfen noch ihre Hindernisse überqueren müssen. Der Kontinent wurde also so verändert, dass eine Gruppe einen Vorteil erlangt und die Fairness verletzt wurde.

Wenn Teile der Welt unbefugt gelöscht werden und nicht mehr verfügbar sind, hat das genauso Auswirkungen auf die Fairness. Im Extremfall, beispielsweise einem Totalausfall der Server, ist die Welt (vorübergehend) gar nicht mehr verfügbar, was dazu führt, dass kein Nutzer die Welt betreten kann.

6.4.7 Auswirkungen der Bedrohungen auf die Regeln

Um Fairness in den Virtuellen Welten zu ermöglichen, legen die Anbieter bestimmte Verhaltensregeln fest, an die sich alle Nutzer halten müssen. Damit ein Nutzer weiß, wie er sich richtig verhält, müssen ihm die Regeln bekannt und zugänglich sein. Diese Bedingung kann nicht erfüllt werden, wenn es durch Angriffe zu Veränderungen der Regeln kommt bzw. die Regeln gelöscht werden.

Beispielszenario: Eine Regel in einem Rollenspiel könnte lauten, dass bei Begräbnissen nicht über den offenen Chat gesprochen werden darf, um den Anstand vor den Trauernden zu wahren. Um diese Regel zu kennen, muss ein Nutzer sie gelesen oder anderweitig registriert (z.B. gehört) haben. Ihm muss Gelegenheit dazu gegeben werden, zum Beispiel indem eine Benachrichtigung erfolgt sobald die Regel eingeführt wird oder er den Regeln beim Einloggen zustimmen muss. Mit der Zustimmung zu den Regeln erklären die Nutzer ihr Einverständnis. Verhalten sich die Nutzer nicht entsprechend der Regeln oder streitet ein Nutzer die Zustimmung zu den Regeln ab, wird die Fairness verletzt.

Das unberechtigte Verändern oder Löschen der Regeln führt zum Verlust der Grundlage für die Fairness.

6.4.8 Auswirkungen der Bedrohungen auf die Kommunikationsdaten

Kommunikationsdaten sind Daten, die während einer Kommunikation entstehen. Unter Kommunikation wird an dieser Stelle der Austausch von Informationen zwischen mehreren Personen verstanden. Durch unbefugtes Lesen der Kommunikationsdaten werden diese Informationen unberechtigten Dritten bekannt. Durch Veränderung der Daten kann eine Veränderung der Information erreicht werden. Das Löschen der Daten hat zur Folge, dass Informationen entweder nicht mehr verfügbar sind oder gar nicht erst wahrgenommen werden. Sind es personenbezogene Daten und erlangt ein unberechtigter Dritter Zugang zu diesen, kann er diese auch weitergeben. Dies führt zu einer Nutzung der Daten, der der Eigentümer nicht zugestimmt hat und so zur Verletzung des Datenschutzes.

Beispielszenario: In einem Onlinerollenspiel gibt es zwei rivalisierende Gilden, die sich in einer Schlacht (Battle) gegenseitig bekämpfen, um die besseren Kampffähigkeiten zu beweisen. Bei so einem Kampf spielt die gewählte Strategie eine Rolle, die die Gildenmitglieder über den Gildenchat entwickeln. Gelingt es der gegnerischen Gilde diese Informationen abzufangen und zu lesen, haben sie dadurch im Kampf einen Vorteil durch unberechtigte Kenntnis der Informationen.

Ein häufiges Problem in großen Gemeinschaften ist Mobbing. Wie in der realen Welt, versuchen Nutzer in der virtuellen Welt andere Nutzer anzugreifen, indem sie sie bedrängen, beschimpfen oder falsche Tatsachen verbreiten. Um der Bedrohung des Mobbing zu begegnen, müssen Inhalte von Kommunikation nachverfolgbar und insbesondere den Nutzern zuordenbar sein. Ist dies nicht möglich, können die Angreifer ihre Handlungen abstreiten. Zur Wahrung der Fairness innerhalb der Gemeinschaft müssen Kommunikationsdaten einem Nutzer zugeordnet werden können.

6.4.9 Auswirkungen der Bedrohungen auf die Transaktionsdaten

Transaktionsdaten sind die Daten die bei einer Transaktion entstehen. Sie sind äußerst sicherheitskritisch, in Bezug auf die Vertraulichkeit, Integrität, Verfügbarkeit, den Daten-

schutz und die Nichtabstreitbarkeit. Beim Auslösen einer Transaktion entstehen Daten wie Namen und Preise etc., die von Unberechtigten gelesen, verändert oder gelöscht werden können. Gehen Transaktionsdaten verloren, z.B. durch Löschen der Daten, kommt keine Transaktion zustande.

Im Geschäftsleben stellt Spionage ein Problem dar. Für Spionageangriffe sind Transaktionsdaten wertvolle Informationen, da etwa eine Konkurrenzfirma erfahren kann, mit wem Transaktionen durchgeführt werden, welche und wie viele Produkte verkauft werden und zu welchem Preis (Verletzung der Vertraulichkeit). Handelt es sich bei den Daten um personenbezogene Daten, wird der Datenschutz verletzt.

Gelingt es einem Angreifer Transaktionsdaten, wie den Preis einer Ware oder die bestellte Anzahl zu verändern, würde dies zu finanziellen Verlusten führen. In diesem Zusammenhang muss auch das Problem der Nichtabstreitbarkeit betrachtet werden. Der Transaktionsinitiator kann nicht beweisen, dass die veränderten Daten nicht von ihm eingegeben wurden.

6.4.10 Auswirkungen der Bedrohungen auf die Logindaten

Ein Nutzer verwendet die Logindaten, wie Benutzername und Passwort, um sich gegenüber dem System zu identifizieren.

Gelingt es einem Angreifer die Zugangsdaten zu lesen, kann er sich unberechtigt Zugriff zur Virtuellen Welt verschaffen. Dadurch ist es ihm zum Beispiel möglich die Logindaten zu ändern was zur Folge hat, dass der berechtigte Nutzer keinen Zugriff mehr hat.

Manipulationen am Server können dazu führen, dass sich ein berechtigter Nutzer nicht am System anmelden kann, obwohl er im Besitz korrekter Authentifikationsmerkmale ist. Dadurch kann der Nutzer den Dienst nicht in Anspruch nehmen.

Die Kontakte eines Nutzers sind nur ihm zugänglich. Gelingt es einem Angreifer die Daten über die Kontakte auszulesen, kann er diese Informationen für Mobbing-Angriffe nutzen (z.B. indem er den Betroffenen bei seinen Freunden diffamiert). Gibt der Angreifer personenbezogene Daten der Kontakte an Dritte weiter wird außerdem der Datenschutz verletzt.

Die Bedrohung der Nichtabstreitbarkeit in Bezug auf Kontaktdaten wird möglich, wenn einem Nutzer eine Aktion nicht zugeordnet werden kann. So könnte ein Nutzer seine Kontaktdaten löschen, behauptet aber gegenüber dem Anbieter sie seien verloren gegangen. Aktionen können im Fall einer Beschwerde nicht nachvollzogen werden.

6.4.11 Auswirkungen der Bedrohungen auf die Kontaktdaten

Kontaktdaten sind Daten über die sozialen Kontakte eines Nutzers in der Virtuellen Welt. Jeder Nutzer kann über die Client-Software die Liste seiner Kontakte (Freundesliste) einsehen, die Namen und Kontaktdetails enthält. Kann der Nutzer auf diese Daten nicht mehr zugreifen, da sie verändert oder gelöscht wurden, kann er seine Freunde und Bekannte nicht mehr erreichen. Sein Unterhaltungserleben wird gestört.

6.4.12 Auswirkungen der Bedrohungen auf die Kontodaten

Die Kontodaten umfassen die Informationen über den Inhaber eines Accounts. Dazu können unter anderem sein realer Name, Anschrift, E-Mail-Adressen und Zahlungsinformationen zählen.

Durch verschiedene Angriffe kann die Vertraulichkeit, die Integrität, die Verfügbarkeit und der Datenschutz gefährdet werden, indem Daten gelesen, verändert, gelöscht oder weitergegeben werden.

Personen können behaupten, ein Konto nicht angelegt zu haben. Der Anbieter muss überprüfen ob die Eröffnung eines Kontos wirklich von der behaupteten Identität in Auftrag gegeben wurde.

6.4.13 Auswirkungen der Bedrohungen auf die Reputation

Die eigene Reputation ist für die Nutzer sehr wichtig, um in der Virtuellen Welt agieren zu können. Nur wer eine gute Reputation genießt, wird von der Gemeinschaft und als Handelspartner akzeptiert.

Angriffe auf die Reputation können durch unberechtigte Manipulationsversuche Dritter durchgeführt werden, indem zum Beispiel falsche Informationen über einen Nutzer verbreitet werden. Um sich in der Virtuellen Welt positiv darzustellen, betreiben Nutzer Reputationsmanagement, d.h. sie versuchen möglichst gute Informationen über sich zu streuen. Ein übertriebenes Reputationsmanagement könnte dazu führen, dass die Nutzer zu viele private Daten über sich preisgeben und so selbst ihren Datenschutz verletzen.

6.5 Bedrohungen und Angriffe

In den vorangegangen Kapiteln wurden die Auswirkungen der Schutzzielverletzungen für die einzelnen Werte beschrieben. Es hat sich gezeigt, dass die Auswirkungen für die Werte ähnlich sind. Daher lassen sich die Bedrohungen zu den folgenden sechs Grundbedrohungen zusammenfassen. Die Bedrohungen erhalten eindeutige Bezeichner (T.*). Das T steht für engl. „Threat“, also Bedrohung. Diese Bezeichner werden im Schutzprofil verwendet (vgl. Kapitel 8).

- **T.UnbefugtesLesen**: Unbefugten gelingt es Daten auf dem Übertragungsweg zwischen Client und Server oder in der Datenbank zu lesen (vgl. Kapitel 8.3.2, S.142).
- **T.UnbefugteModifikation**: Unbefugten gelingt es Daten auf dem Übertragungsweg zwischen Client und Server oder in der Datenbank zu verändern (vgl. Kapitel 8.3.2, S.142).
- **T.UnbefugtesLöschen**: Unbefugten gelingt es Daten auf dem Übertragungsweg zwischen Client und Server oder in der Datenbank zu löschen (vgl. Kapitel 8.3.2, S.143).
- **T.VerlustVerfügbarkeit**: Angreifern gelingt es die Verfügbarkeit des Servers oder der Datenbank zu beeinträchtigen (vgl. Kapitel 8.3.2, S.144).
- **T.VerletzungDatenschutz**: Unberechtigte erlangen Zugriff auf personenbezogene Daten (vgl. Kapitel 8.3.2, S.145).

- **T.AbstreitungHandlung**: Einem Nutzer kann eine Aktion nicht zugeordnet werden (vgl. Kapitel 8.3.2, S.145).

Tabelle 6.2 zeigt, wie die Grundbedrohungen die in Tabelle 6.1 identifizierten Bedrohungen abdecken.

Name der Bedrohung	Abdeckung des Rasters (Tabelle 6.1)
T.UnbefugtesLesen	(1), (6), (11), (15), (20), (26), (31), (36), (40), (45)
T.UnbefugteModifikation	(2), (7), (12), (16), (18), (21), (23), (27), (32), (37), (42), (46), (50)
T.UnbefugtesLöschen	(2), (7), (12), (16), (18), (21), (23), (27), (32), (42), (46)
T.VerlustVerfügbarkeit	(3), (8), (13), (17), (19), (22), (24), (28), (33), (38), (42), (47)
T.VerletzungDatenschutz	(4), (9), (29), (34), (39), (43), (48), (51)
T.AbstreitungHandlung	(5), (10), (14), (25), (30), (35), (44), (49)

Tabelle 6.2: Abdeckung des Rasters

Eine Bedrohung T.VerletzungIntegrität wird nicht gebildet, sondern die Bedrohungen T.UnbefugtesLöschen und T.UnbefugteModifikation werden aufgeführt, da die Bedrohungen (37) und (50) (vgl. Tabelle 6.1, S.80) das Löschen nicht betrifft.

Angriffe

In Kapitel 4 wurde erläutert, dass Bedrohungen eher allgemein auf die Verletzung der Schutzziele gerichtet sind und Angriffe eine konkrete Methode darstellen die Bedrohungen zu erreichen. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) hat in einem Positionspapier solche Angriffe vorgestellt (vgl. [Hogben 08]). Im folgenden Abschnitt wird detailliert gegenübergestellt, welche Angriffe auf welche Bedrohungen zielen. Die konkrete Bedrohung „Verlust der Vertraulichkeit der Logindaten (26)“ wirkt direkt auf die Verfügbarkeit aller Werte. Hat ein Angreifer diese vertraulichen Informationen für sich zugänglich gemacht (T.UnbefugtesLesen), ist er in der Lage den Eigentümer des Kontos auszusperren (indem er die Logindaten ändert) und Transaktionen durchzuführen.

Erreicht wird dies durch Accountdiebstahl. Angriffe, die dem Zweck des Diebstahls von Logindaten (z.B. Benutzername, Passwort) dienen, sind zum Beispiel so genannte IFrame-Schwachstellen[8] (vgl. [Sophos 07]), Trojaner (vgl. [Symantec 06], [Register 06]) oder Keylogger (vgl. [Hogben 08], S.29). Abgesehen von diesen technischen Angriffsmöglichkeiten gibt es auch Angriffe des Social Engineering, zum Beispiel Phishing (vgl. [Hogben 08], S.29). Dabei geben die Opfer diese Informationen selbst an die Angreifer, die durch Vortäuschen falscher Identitäten das Vertrauen der Opfer ausnutzen.

Die Bedrohung „Verlust der Integrität“ kann durch unbefugte Modifikation (T.UnbefugteModifikation) und unbefugtes Löschen (T.UnbefugtesLöschen) erreicht werden. Ein Angriff auf die unbefugte Modifikation der Transaktionsdaten (22) tritt auf, wenn es zu einer Automatisierung der Transaktionen kommt. Die Automatisierung wird von so genannten Bots ausgeführt, die z.B. Finanztransaktionen ausführen oder Gegenstände kopieren (vgl. Second Life Copybot [Linden 06]). Die unbefugte Modifikation von Gegenständen (3) gelingt beispielsweise mithilfe so genannter Duping-Angriffe. Dabei werden Fehler in der Programmierung des Spiels (engl. bugs) ausgenutzt, um wertvolle Objekte zu duplizieren (vgl. [ZDNet 05], [Hogben 08]). Die Folge ist ein Wertverlust der Objekte für die Besitzer (vgl. [Castronova 07], [Hogben 08]).

Werte wie Gegenstände und Konten können gelöscht werden. Gelingt einem Angreifer das unberechtigte Löschen von Werten, liegt eine Verletzung der Integrität vor. Die Bedrohung des unbefugten Löschens muss dabei nicht zwangsläufig von externen Angreifern vorsätzlich geschehen, sondern kann auch unbewusst durch Mitarbeiter des Anbieters ausgeführt werden, wenn er Zugriff auf die Datenbank erlangt und versehentlich Daten löscht.

Der Verlust der Verfügbarkeit (T.VerlustVerfügbarkeit) von Werten kann z.B. durch Distributed-Denial-of-Service (DDoS)-Angriffe erreicht werden. Das Ziel bei einem DDoS-Angriff ist eine Überlastung des Servers. Meist geschieht dies durch einen gleichzeitigen Zugriff vieler Clients. Die Automatisierung der gleichzeitigen Zugriffe erfolgt mithilfe von Bot-Software[9], die sich auf vernetzten Rechnern eingeschleust haben.

[8] HTML-Dateien, die versuchen schädliche Dateien auszuführen

[9] Bot ist die Kurzform für Robot und bezeichnet die automatische Ausführung von Befehlen, d.h. es gibt keinen Eingriff vom Nutzer.

Die Verletzung des Datenschutzes (T.VerletzungDatenschutz) ist gegeben, wenn Daten in einer Weise verwendet werden, der der Eigentümer der Daten nicht zugestimmt hat. Oftmals geht diese Bedrohung mit sorglosem Umgang mit Daten einher. Insbesondere in sozialen Netzwerken und Communities in Virtuellen Welten geben die Nutzer viele Daten von sich preis (vgl. [Beyer 08], [Hogben 08]). Bei jeder Aktion, Transaktion und bei Kommunikation werden digitale Fußspuren und Daten hinterlassen (engl. footprinting). Diese Daten können für Marketing-Zwecke ausgewertet und zu Nutzerprofilen zusammengefasst werden. Die Anwendung „ContextAds“ [ContextAds 09] in Second Life verwendet z.B. den Inhalt der Kommunikation zwischen den Benutzern, um ihnen personalisierte Werbung zu präsentieren[10].

Bei der Nutzung von Virtuellen Welten müssen Regeln eingehalten werden, um einen fairen Umgang miteinander zu gewährleisten. Kommt es aber zu Zwischenfällen, bei denen ein Verstoß gegen eine Regel vorliegt, muss dies von einer unabhängigen Stelle geklärt werden. Virtuelle Welten setzen dafür so genannte Dispute-Resolution-Systeme (deutsch Beschwerdestelle) ein.
Ein unabhängiger Gamemaster (deutsch Spielmeister) muss mit den Beteiligten den Streit beilegen und versucht den Fall zu untersuchen. Liegen keine eindeutigen Beweise gegen den Urheber des Regelverstoßes vor, kann er regelwidrige Aktionen, wie z.B. Beleidigungen im Chat, einfach abstreiten (T.AbstreitungHandlung).

Tabelle 6.3 stellt Beispiele für Angriffe auf die Werte in Virtuellen Welten den Bedrohungen gegenüber.

[10] „A ContextAds board listens to the conversations of those avatars around it, displaying advertisements when certain keywords are mentioned“ [ContextAds 09].

Bedrohungen	Angriffe
T.UnbefugtesLesen	IFrame-Schwachstellen, Trojaner, Keylogger, Phishing
T.UnbefugteModifikation	Copybot, Duping, Automatisierung
T.UnbefugtesLöschen	Unbefugte Mitarbeiter löschen versehentlich Daten
T.VerlustVerfügbarkeit	DDoS
T.VerletzungDatenschutz	Sorgloser Umgang mit eigenen Daten, Footprinting, Profile
T.AbstreitungHandlung	Abstreitung eines Regelverstoßes, z.B. Mobbing

Tabelle 6.3: Mögliche Angriffe auf Werte in Virtuellen Welten

6.6 Definition der Sicherheitsstrategie

Die Definition der Sicherheitsstrategie umfasst:

- die Festlegung der Annahmen (A.*),
- die Definition der Organisatorischen Sicherheitspolitiken (P.*),
- die Definition der Sicherheitsziele für den EVG (O.*) und
- die Ableitung der Sicherheitsziele für die Betriebsumgebung des EVG (OE.*) aus den Annahmen.

Die Abbildung 6.4 stellt den Zusammenhang zwischen den einzelnen Komponenten der Sicherheitsstrategie dar. Die Beziehungen sagen Folgendes aus.

- Jedes Sicherheitsziel (O.* und OE.*) verfolgt mindestens eine Bedrohung (T.*), Politik (P.*) oder Annahme (A.*). Das stellt sicher, dass es keine unberechtigten Sicherheitsziele gibt (vgl. [CCPart1 06], S.57).
- Jede Bedrohung, Politik und Annahme wird durch mindestens ein Sicherheitsziel (O.* oder OE.*) abgedeckt. Das stellt sicher, dass dem Sicherheitsproblem angemessen begegnet wird (vgl. [CCPart1 06], S.57).
- Die Annahmen beziehen sich immer auf die Betriebsumgebung des EVG, daher zielen keine Sicherheitsziele des EVG (O.*) auf die Annahmen. Diese werden al-

lein durch die Sicherheitsziele der Umgebung (OE.*) abgedeckt (vgl. [CCPart1 06], S.57).

- Mehrere Sicherheitsziele können auf eine Bedrohung oder Politik abzielen. Das sagt aus, dass eine Kombination mehrerer Sicherheitsziele einer Bedrohung entgegenwirkt (vgl. [CCPart1 06], S.57).

Die Einhaltung der Forderung wird im Zwischenfazit (vgl. Kapitel 6.7, S.107) und im Schutzprofil (vgl. Kapitel 8.4.3, S.154) bewiesen.

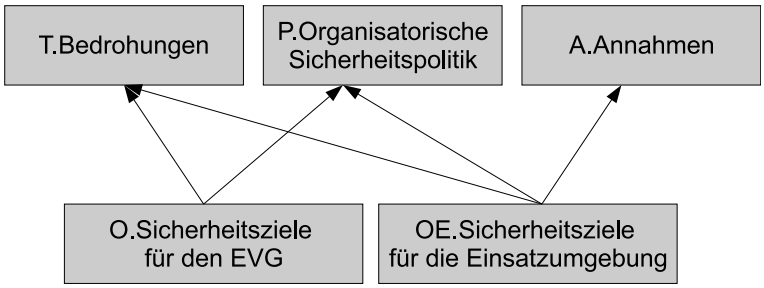


Abbildung 6.4: Beziehungen zwischen Bedrohungen, Richtlinien, Annahmen und Sicherheitszielen [in Anlehnung an [CCPart1 06], S.57]

6.6.1 Annahmen (Assumptions)

Um die IT-Sicherheit Virtueller Welten zu erhöhen sind einerseits Sicherheitsfunktionen für das System zu installieren, andererseits müssen gewisse technische und personelle Aspekte vorausgesetzt werden. Diese werden als Annahmen definiert. Die Annahmen betreffen Sicherheitsauflagen an die Umgebung des Systems, die zur Sicherheit beitragen aber nicht vom EVG selbst erwartet werden können und somit auch nicht Bestandteil der Evaluierung sein können. Die Annahmen erhalten eindeutige Bezeichner (A.*). Das A steht für engl. „Assumption“, also Annahme. Diese Bezeichner werden im Schutzprofil verwendet.

Annahmen über technische Aspekte der Betriebsumgebung

Als grundlegende Voraussetzung für eine ordnungsgemäße Funktion der Sicherheitsfunktionen des EVG ist eine ordnungsgemäße Installation und Initialisierung des EVG sowohl auf Client- als auch auf Serverseite (**A.Installation**). Dazu gehört auch die ordnungsgemäße Installation des Betriebssystems (**A.Betriebssystem**) und ein Schutz vor Schadsoftware (z.B. Viren, Würmer, Trojaner, etc.) durch eine Firewall und einen Virenscanner. Bei der Evaluation des EVG kann nicht untersucht werden, ob Schadsoftware bzw. Cheatingsoftware auf dem Client- bzw. Serverrechner installiert ist. Dies muss als Annahme für die Umgebung definiert werden und kann zur Durchsetzung der Interessen vom Anbieter in die Regeln für den fairen Umgang (vgl. P.Verhaltensregeln) aufgenommen werden. Vorausgesetzt werden muss außerdem, dass das Betriebssystem und die Schutzsoftware regelmäßig durch die Installation von Updates auf den neuesten Stand gebracht werden.

Da auf dem Server-EVG alle Werte-relevanten Daten gespeichert werden, ist dort insbesondere zu beachten, dass ein ausreichender physischer Schutz des Servers gewährleistet wird (**A.PhysSchutz**). Der physische Schutz muss durch angemessene Gestaltung der Räumlichkeiten gewährleistet werden. Dazu gehören feuerfeste Wände, Einbruchs- und Diebstahlsicherung, Klimaanlage, Zugangsbeschränkung, etc.

Wenn es vorkommt, dass sich Nutzer nicht entsprechend der Regeln (vgl. P.Verhaltensregeln) verhalten, muss es Möglichkeiten geben Sanktionen durchzusetzen (**A.Sanktionen**). Da Sanktionen von verantwortlichen Mitarbeitern des Anbieters durchgeführt werden, kann dieses Erfordernis nicht von den EVG-Funktionen verlangt werden, sondern muss als Annahme formuliert werden.

Es wird davon ausgegangen, dass der Anbieter geeignete Maßnahmen ergreift, um die Servicequalität und die Verfügbarkeit des Dienstes zu gewährleisten (**A.Verfügbarkeit**).

Annahmen über personelle Aspekte der Betriebsumgebung

Für die Identifikation der Nutzer und deren Authentifizierung am EVG erhalten die Nutzer so genannte Identifikations- und Authentifizierungsmittel, umgangssprachlich auch als Logindaten bezeichnet. Es muss vorausgesetzt werden, dass die Nutzer verant-

wortungsvoll mit diesen Daten umgehen und insbesondere nicht an Dritte weitergeben (**A.AuthDaten**). Dies muss als Annahme definiert werden, da dies nicht zuverlässig vom EVG überprüft werden kann.

Administratoren des Clientrechners dürfen keine Manipulationen durchführen, um etwa eine Veränderung der EVG-Funktionalität zu erreichen (**A.Admin.1**). Dies spielt insbesondere eine Rolle beim Schutz gegen unfaires Spielen (so genanntes Cheating).

Die Administratoren des Anbieters spielen eine besondere Rolle, da sie Zugang zu hoch sicherheitsrelevanten Daten haben. Es ist daher notwendig, dass Administratoren vertrauenswürdige Personen sind (**A.Admin.2**). Dies beinhaltet, dass sie nicht absichtlich versuchen die Sicherheitspolitiken des EVG zu verletzen, zum Beispiel indem sie sich unberechtigt Zugang zu Informationen verschaffen. Die Vertrauenswürdigkeit kann der Anbieter bei Mitarbeitereinstellung überprüfen, indem er beispielsweise ein polizeiliches Führungszeugnis verlangt und regelmäßig Überprüfungen durchführt.

Zur Sicherstellung der Fairness ist es wichtig, dass alle Nutzer die Verhaltensregeln kennen (vgl. Kapitel 6.6.3, O.Regeln) und sich den Regeln entsprechend verhalten. Da die funktionalen Sicherheitsmechanismen keinen Einfluss auf das Nutzerverhalten haben, muss als Annahme festgehalten werden, dass die Nutzer sich fair verhalten, das heißt entsprechend der Verhaltensregeln agieren (**A.Regeln**).

Der Nutzer der Virtuellen Welt hat ein Recht auf informationelle Selbstbestimmung seiner Daten. Das bedeutet, dass er darüber bestimmen darf, wer welche personenbezogenen Daten von ihm erhält. Es muss vorausgesetzt werden, dass sich der Anbieter an diese Vorgaben hält und Daten über seine Kunden nicht an Dritte weitergibt (**A.Datenschutz**).

Der EVG enthält Sicherheitsfunktionen, die vor technischen Angriffen (z.B. Denial-of-Service-Angiffe, Schadsoftware, etc.) schützen. Bei eher sozialen Angriffen auf die Nutzer (z.B. Phishing) ist das schwieriger. Daher ist es wichtig, dass sich Nutzer solcher Gefahren bewusst sind und kompetent auf soziale Angriffe reagieren können. Es ist wichtig, dass der Anbieter seine Nutzer über solche Gefahren aufklärt (**A.Awareness**). Der EVG kann diese Awareness-Maßnahmen des Anbieters unterstützen, indem er relevante Informationen benutzerfreundlich anzeigt.

6.6.2 Sicherheitsrichtlinien (Security Policies)

Die organisatorische Sicherheitspolitik umfasst Richtlinien (englisch policies), organisatorische Vorgaben, Leitfäden und (gesetzliche) Regeln, mit denen der EVG übereinstimmen muss. Die geltenden Sicherheitspolitiken werden später in Sicherheitsziele überführt. Für den EVG werden die folgenden Sicherheitspolitiken festgehalten. Die Politiken erhalten eindeutige Bezeichner (P.*). Das P steht für engl. „Policy“, also Richtlinie. Diese Bezeichner werden im Schutzprofil verwendet.

Bei der Umsetzung von Sicherheitsfunktionen in Virtuellen Welten kommen für verschiedene Funktionen kryptografische Algorithmen zum Einsatz, zum Beispiel bei der Verschlüsselung der Kommunikation zwischen Client und Server oder der Erzeugung von digitalen Signaturen und Hashwerten[11]. Um aktuellen Anforderungen entsprechen zu können, ist es notwendig, dass die kryptografischen Verfahren den aktuellen Standards entsprechen (**P.Crypt**). Entsprechende Empfehlungen werden beispielsweise von der Bundesnetzagentur [BNetzA 09], dem Bundesamt für Sicherheit in der Informationstechnik (BSI) [BSI 09a] und dem National Institute of Standards and Technology (NIST) [NIST 09] veröffentlicht.

Wie bereits oben erwähnt, sollten für die Erhaltung der Fairness unter den Nutzern bestimmte Verhaltensregeln vom Anbieter definiert werden. Um sich fair verhalten zu können, ist es wichtig, dass alle Nutzer wissen, wie die Regeln lauten. Daher wird als Sicherheitspolitik definiert, dass jeder Nutzer Zugang zu den Regeln haben muss und ihnen zustimmen muss (**P.Verhaltensregeln**). Der EVG muss dies entsprechend unterstützen. Sollte es dennoch zu Verhaltensverstößen kommen, müssen die Nutzer die Möglichkeit haben dies dem Anbieter mitzuteilen, damit er entsprechende Maßnahmen zur Durchsetzung der Regeln vornehmen kann. Für diesen Fall soll ein Beschwerdekanal eingerichtet werden (**P.Beschwerdekanal**).

Serversysteme, wie die zur Verwaltung Virtueller Welten, erfordern regelmäßige Wartungsarbeiten um einen guten Service anbieten zu können. Wartungsarbeiten können während des laufenden Betriebs stattfinden. Ist dies aber zum Beispiel durch umfangreichere Wartungsmaßnahmen nicht möglich, muss der Server vorübergehend vom Netz

[11] eindeutige Kennzeichnung einer Datenmenge, auch Fingerprint genannt

genommen werden. Dies führt zu einer vorübergehenden Nichtverfügbarkeit des Dienstes für den Nutzer. Um die Unannehmlichkeiten dieser Nichtverfügbarkeit im Rahmen zu halten, müssen die Arbeiten rechtzeitig angekündigt werden. Informationen über die voraussichtliche Dauer der Wartungsarbeiten müssen den Nutzern mitgeteilt werden. Wenn die Wartungsarbeiten regelmäßig stattfinden müssen, sollten sie zu einem feststehenden regelmäßigen Termin durchgeführt werden. Der EVG muss sicherstellen, dass die Hinweise über die Wartungsarbeiten und die vorübergehende Nichtverfügbarkeit zugänglich sind. Aus diesem Grund wurde die organisatorische Sicherheitspolitik **P.HinweisWartung** definiert.

Die Betrachtung des Datenschutzes ist ein wichtiger Aspekt innerhalb der IT-Sicherheit. Virtuelle Welten sind auf eine internationale Zielgruppe ausgerichtet, daher kann in den Organisatorischen Sicherheitspolitiken nicht auf ein nationales Datenschutzgesetz verwiesen werden. Vielmehr ist es erforderlich, dass der Anbieter eine Datenschutzrichtlinie erstellt, an die er sich halten muss (**P.Datenschutzrichtlinie**). Darin muss der Anbieter festlegen, wie mit personenbezogenen Daten umgegangen wird.

6.6.3 Sicherheitsziele für den Evaluationsgegenstand (Security Objectives)

In Kapitel 6.4 wurde das Sicherheitsproblem beschrieben, d.h. welche Bedrohungen für eine Virtuelle Welt entstehen können. Damit das System auf die Bedrohungen geeignet reagieren kann, muss es entsprechende Sicherheitsfunktionen enthalten, die eine Absicherung des Systems bewirken. Um zu analysieren, welche Sicherheitsfunktionen benötigt werden, muss zunächst definiert werden, welches Ziel damit verfolgt wird. In den nächsten Abschnitten werden daher Ziele an das System beschrieben, die Voraussetzung für die Wirksamkeit der Sicherheitsfunktionen sind. Wie die hier definierten Sicherheitsziele zur Abwehr der Bedrohungen beitragen, wird in Kapitel 6.7.2 erläutert. Die Ziele erhalten eindeutige Bezeichner (O.*). Das O steht für engl. „Objective“, also Ziel. Diese Bezeichner werden im Schutzprofil verwendet.

Zunächst muss der EVG sicherstellen, dass sich alle Nutzer identifizieren und authentifizieren, bevor sie Zugang zum EVG erhalten (**O.AuthNutzer**). Auch wenn der Anbieter die realen Nutzerdaten seiner Kunden erhebt, muss das System sicherstellen können, dass der Nutzer unter einem Pseudonym auftreten kann (**O.Pseudonym**), um seine reale Identität zu schützen.

In der Datenbank werden alle Daten über die Werte der Nutzer gespeichert. Das System muss sicherstellen, dass nur berechtigte Personen Zugriff auf die entsprechenden Bereiche erlangen. Eine Zugriffskontrollpolitik legt Zugriffsrechte fest.
Daher müssen Lese-/Schreibzugriffsrechte (Zugriffskontrollliste) vom System unterstützt werden (**O.ZugriffDB**).

Da es sich bei den betrachteten Virtuellen Welten um Client-Server-Anwendungen handelt, ist offensichtlich, dass zwischen der Clientanwendung und der Serveranwendung Daten übertragen werden müssen. Um den oben erläuterten Bedrohungen entgegenzuwirken, ist es wichtig, dass der Datenaustausch zwischen Client und Server (Nachrichten) vertraulich stattfindet (**O.GeheimeNachricht**) und dass die Daten nicht unberechtigt verändert werden können (**O.IntegritätNachricht**).

Um manipulierte Daten in der Datenbank zu vermeiden, ist es notwendig, dass bevor Daten in die Datenbank geschrieben werden, eine Plausibilitätsprüfung durchgeführt wird (**O.DBCheck**).

Des Weiteren sind vom System Funktionen vorzusehen, die das Ziel der Fairness unterstützen. Dazu zählt, dass die Nutzer die Regeln kennen und dass sie diesen zustimmen (**O.Regeln**). Die Überprüfung der Einhaltung der Regeln kann aber vom System nicht erwartet werden. Dennoch kann es vorkommen, dass sich einige Nutzer unfair verhalten und gegen die Regeln verstoßen. Daher ist es wichtig, dass das System eine Funktionalität hat, die es erlaubt Beschwerden einzureichen, um Regelverstöße zu melden (**O.EinreichenBeschwerde**). Das allein reicht aber nicht aus. Vielmehr muss auch sichergestellt werden, dass diesen Beschwerden nachgegangen wird. Deshalb muss sichergestellt sein, dass die Verantwortlichen über die Beschwerde Kenntnis erlangen (**O.KenntnisBeschwerde**).

Virtuelle Welten sind unter anderem darauf ausgerichtet Handel zu betreiben. Handelsaktionen und Besitzübergänge sollten im System als Transaktionen erfolgen. Da unvollständig ausgeführte Transaktionen zur Benachteiligung eines Handelspartners und zu inkonsistenten Daten führen können, muss das System die vollständige Durchführung von Transaktionen unterstützen (**O.VollständigkeitTR**). Sollte eine Transaktion abgebrochen werden, muss es möglich sein, den Zustand vor der Transaktion wieder herzustellen.

Die erfolgreiche Durchführung einer Transaktion umfasst außerdem den Schutz vor Abstreitung der Transaktionshandlung (**O.NichtabstreitbarkeitTR**). Nach einer erfolgreichen Transaktion darf kein Beteiligter die Handlung abstreiten können. Das System muss eine Funktionalität zur Verfügung stellen, mit der nachgewiesen werden kann, dass beide Handelspartner in die Transaktion eingewilligt haben.

Für einen fairen Umgang der Nutzer innerhalb der Community ist es wichtig, dass der EVG eine Funktionalität zum Nachweis einer Kommunikation enthält (**O.NichtabstreitbarkeitKommunikation**). Es ist wichtig dass der Inhalt einer Kommunikation bei Bedarf einem Nutzer zugeordnet werden kann. Nur wenn einem Nutzer nachgewiesen werden kann, welche Äußerungen er im Chat gemacht hat, kann er für regelwidriges Verhalten (z.B. Mobbing) zur Verantwortung gezogen werden. Des Weiteren ist vorstellbar, dass die Nutzer den Chat für Verhandlungen zum Abschluss von Verträgen nutzen. Erachten es die Beteiligten für wichtig, die Vereinbarungen festzuhalten, sind Nachweise erforderlich. In diesem Zusammenhang muss dem Nutzer mittels Awareness-Maßnahmen (vgl. OE.Awareness) vermittelt werden, dass er für seine Äußerungen (Kommunikationsinhalt) in der Virtuellen Welt verantwortlich ist.

Insbesondere für die Durchführung von Transaktionen und zur Beweissicherung müssen die Zeitpunkte von Aktionen erfasst und gespeichert werden. Daher muss das System auf verlässliche Zeitstempel zurückgreifen können, die ihm vom EVG bereitzustellen sind (**O.Zeitstempel**).

6.6.4 Sicherheitsziele für die Umgebung des EVG (Security Objectives Environment)

Für den EVG wurden bereits Annahmen getroffen, die die Einsatzumgebung des EVG betreffen. Die Sicherheitsziele für die Umgebung des EVG spezifizieren die materiellen, verfahrens- und verwaltungsmäßigen Maßnahmen, die zur Sicherheit des EVG beitragen, vom EVG selbst aber nicht verlangt werden können. Sie beschreiben also Sicherheitsmechanismen außerhalb des EVG. Die Ziele für die Umgebung erhalten eindeutige Bezeichner (OE.*). Das OE steht für engl. „Objective Environment“, also Ziel der Umgebung. Diese Bezeichner werden im Schutzprofil (vgl. Kapitel 8) verwendet.

Eine Maßnahme, auf die sich der EVG verlassen muss, ist die ordnungsgemäße Installation der Anwendungssoftware (**OE.Installation**). Dies ist vom Nutzer sicherzustellen, der EVG hat darauf keinen Einfluss. Weiterhin müssen vom Anwender Maßnahmen zur Absicherung des Client-PC gegen Schadsoftware getroffen werden (**OE.Betriebssystem**), etwa durch Installation von Antivirensoftware und einer Firewall. Diese Schutzprogramme sind vom Nutzer durch Installation von Updates ständig auf den neuesten Stand zu bringen.

Serverseitig sind Maßnahmen zu treffen, sodass der Server-EVG physisch geschützt ist (**OE.PhysSchutz**). Dazu zählen Zugriffskontrollmechanismen, die sicherstellen, dass nur berechtigte Personen Zugriff auf den Server-EVG haben.

Um die Robustheit, Servicequalität und Verfügbarkeit des Dienstes zu gewährleisten, ergreift der Anbieter Maßnahmen zum Schutz der Server und des Netzwerks und gewährleistet im Falle von Ausfällen die schnelle Wiederherstellung des Dienstes (**OE.Verfügbarkeit**).

Bei der Gewährung des Zugriffs auf den EVG wird davon ausgegangen, dass es sich um berechtigte Nutzer handelt. Daher wird von den Anwendern des EVG erwartet, dass sie ihre Identifikations- und Authentifikationsmerkmale geheim halten und daher nur berechtigte Nutzer im Besitz von korrekten Identifikations- und Authentisierungsmerkmalen sind (**OE.AuthDaten**).

Ein Ziel der Umgebung betrifft die Integrität des Client-EVG. Der Nutzer muss sicherstellen, dass die Administratoren des Client-EVGs keine unberechtigte Veränderung der Client-Funktionalität vornehmen (**OE.Admin.1**).

Ein weiteres Sicherheitsziel, das für die Umgebung definiert werden muss, ist die Schulung der Administratoren und die Feststellung der Vertrauenswürdigkeit der Personen, die als Administratoren eingestellt werden (**OE.Admin.2**).

Die Systemumgebung muss sicherstellen, dass es unberechtigten Personen nicht gelingt, die personenbezogenen Daten der Nutzer auszulesen. Zusätzlich verpflichtet sich der Anbieter, personenbezogene Daten nicht an Dritte weiterzugeben (**OE.Datenschutz**).

Ein weiteres Umgebungsziel betrifft personelle Aspekte und richtet sich an das Verhalten der Nutzer. Es wird vorausgesetzt, dass sich Nutzer entsprechend der Regeln verhalten (**OE.Regeln**). Sollte der Fall eintreten, dass ein Nutzer die Regeln verletzt und andere Nutzer die Fairness bedroht sehen, können sie einen Beschwerdekanal nutzen (vgl. O.EinreichenBeschwerde). Halten es die Verantwortlichen für notwendig einen unfairen Nutzer zu bestrafen, muss das System die Durchsetzung von Sanktionen erlauben (**OE.Sanktionen**).

Da sich einige Ziele der Umgebung auf personelle Aspekte beziehen, die ein angemessenes Verhalten der Nutzer voraussetzen, ist es nützlich und sinnvoll, dass der Anbieter regelmäßig Awareness-Maßnahmen durchführt (**OE.Awarenesss**). Diese Maßnahmen richten sich darauf bei den Nutzern einen Prozess der Bewusstseinsbildung gegenüber Gefahren anzustoßen. So können die Nutzer lernen, wie sie sich richtig und kompetent in der Virtuellen Welt verhalten.

6.7 Zwischenfazit

Die in diesem Kapitel erzielten Ergebnisse sind die Analyse des Sicherheitsproblems (Akteure, Werte, Bedrohungen) und die Definition einer Sicherheitsstrategie. Es wird im Folgenden geprüft, ob die Sicherheitsstrategie zur Lösung des identifizierten Sicherheitsproblems beiträgt.

Aus den tabellarischen Übersichten ist ersichtlich, dass jede Bedrohung, jede Sicherheitspolitik und jede Annahme von mindestens einem Sicherheitsziel adressiert wird und jedes Sicherheitsziel mindestens eine Bedrohung, Sicherheitspolitik oder eine Annahme adressiert.

6.7.1 Abdeckung der Annahmen

Die Annahmen (A.*) definieren Maßnahmen, die zur Sicherheit beitragen aber vom System nicht erfüllt werden können. Sie werden erneut in der Definition der Sicherheitsziele für die Umgebung (OE.*) dargelegt. Daher muss jede getroffene Annahme (A.*) durch ein Sicherheitsziel der Umgebung (OE.*) abgedeckt sein (vgl. Tabelle 6.4).

	OE.Installation	OE.Betriebssystem	OE.PhysSchutz	OE.Sanktionen	OE.Verfügbarkeit	OE.AuthDaten	OE.Admin.1	OE.Admin.2	OE.Regeln	OE.Datenschutz	OE.Awareness
A.Installation	x										
A.Betriebssystem		x									
A.PhysSchutz			x								
A.Sanktionen				x							
A.Verfügbarkeit					x						
A.AuthDaten						x					
A.Admin.1							x				
A.Admin.2								x			
A.Regeln									x		
A.Datenschutz										x	
A.Awareness											x

Tabelle 6.4: Abdeckung der Annahmen

6.7.2 Abwehr der Bedrohungen durch den EVG

Die Lösung des Sicherheitsproblems ist gewährleistet, wenn die Sicherheitsziele des EVG und die Sicherheitsziele der Umgebung zur Abwehr der Bedrohungen beitragen. Tabelle 6.5 zeigt die Abwehr der Bedrohungen. Der Zusammenhang wird im Folgenden erläutert.

T.UnbefugteModifikation

Die Bedrohung wird durch folgende Ziele abgewehrt:

- O.AuthNutzer (da nur berechtigte Personen Zugang zum System erlangen),
- O.ZugriffDB (da für alle Zugriffe auf die Datenbank geprüft wird, ob entsprechende Zugriffsrechte vorliegen),
- O.IntegritätNachricht (da ein geschützter Kommunikationspfad zwischen Client und Server die Modifikation von Daten verhindert).

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Installation (da eine ordnungsgemäße Installation der Client- und Serversoftware sicherstellt, dass durch keine Schadsoftware und keine falsche Konfiguration eine unbefugte Modifikation möglich ist),
- OE.Betriebssystem (da eine ordnungsgemäße Installation des Betriebssystems und aktuelle Schutzsoftware einen weiteren Schutz vor unautorisierter Modifikation gewährleistet),
- OE.PhysSchutz (da die Umgebung des EVG so geschützt ist, dass keine unberechtigten Personen Zugriff auf den EVG haben)
- OE.AuthDaten (da davon ausgegangen wird, dass nur berechtigte Personen im Besitz gültiger Identifikations- und Authentifikationsmerkmale sind),
- OE.Awareness (da durch Awareness-Maßnahmen des Anbieters die Nutzer kompetent mit ihren Authentifikationsdaten umgehen und so nicht in die Hände Unbefugter gelangen).

T.UnbefugtesLöschen

Die Bedrohung wird durch folgende Ziele abgewehrt:

- O.AuthNutzer (da nur berechtigte Personen Zugang zum System erlangen),
- O.ZugriffDB (da für alle Zugriffe auf die Datenbank geprüft wird, ob entsprechende Zugriffsrechte vorliegen),
- O.IntegritätNachricht (da ein geschützter Kommunikationspfad zwischen Client und Server das Löschen von Daten verhindert).

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Installation (da eine ordnungsgemäße Installation der Client- und Serversoftware sicherstellt, dass durch keine Schadsoftware und keine falsche Konfiguration unbefugtes Löschen von Daten möglich ist),
- OE.Betriebssystem (da eine ordnungsgemäße Installation des Betriebssystems und aktuelle Schutzsoftware einen weiteren Schutz vor unautorisiertem Löschen gewährleistet),
- OE.PhysSchutz (da die Umgebung des EVG so geschützt ist, dass keine unberechtigten Personen Zugriff auf den EVG haben),
- OE.AuthDaten (da davon ausgegangen wird, dass nur berechtigte Personen im Besitz gültiger Identifikations- und Authentifikationsmerkmale sind),
- OE.Awareness (da durch Awareness-Maßnahmen des Anbieters die Nutzer kompetent mit ihren Authentifikationsdaten umgehen und so nicht in die Hände Unbefugter gelangen).

T.UnbefugtesLesen

Die Bedrohung wird durch folgende Ziele abgewehrt:

- O.AuthNutzer (da nur berechtigte Personen Zugang zum System erlangen),

- O.ZugriffDB (da für alle Zugriffe auf die Datenbank geprüft wird, ob entsprechende Zugriffsrechte vorliegen),
- O.GeheimeNachricht (da durch einen verschlüsselten Datenaustausch gewährleistet werden kann, dass unautorisierte Personen die Daten nicht lesen können).

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Installation (da eine ordnungsgemäße Installation der Client- und Serversoftware sicherstellt, dass keine Schadsoftware und keine falsche Konfiguration Zugriff auf vertrauliche Daten erlaubt),
- OE.Betriebssystem (da eine ordnungsgemäße Installation des Betriebssystems und aktuelle Schutzsoftware einen weiteren Schutz vor unberechtigtem Lesen von vertraulichen Daten bietet),
- OE.PhysSchutz (da die Umgebung des EVG so geschützt ist, dass keine unberechtigten Personen Zugriff auf den EVG haben),
- OE.AuthDaten (da davon ausgegangen wird, dass nur berechtigte Personen im Besitz gültiger Identifikations- und Authentifikationsmerkmale sind),
- OE.Awareness (da durch Awareness-Maßnahmen des Anbieters die Nutzer kompetent mit ihren Authentifikationsdaten umgehen und so nicht in die Hände Unbefugter gelangen).

T.VerlustVerfügbarkeit

Die Bedrohung wird durch folgende Ziele abgewehrt:

- O.DBCheck (da eine Plausibilitätsprüfung durchgeführt wird, bevor Daten in die Datenbank gespeichert werden. Das stellt sicher, dass auf korrekte Werte zugegriffen werden kann.),
- O.VollständigkeitTR (da sichergestellt wird, dass nur vollständig ausgeführte Transaktionen wirksam werden).

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Installation (da eine ordnungsgemäße Installation der Client- und Serversoftware erst sicherstellt, dass dem Nutzer der Dienst zur Verfügung steht),
- OE.PhysSchutz (da die Umgebung des EVG so geschützt ist, dass keine unberechtigten Personen Zugriff auf den EVG haben),
- OE.Verfügbarkeit (da Maßnahmen zur Sicherung der Robustheit und Servicequalität des Dienstes gewährleistet werden. Im Falle von Störungen werden adäquate Maßnahmen zur Wiederherstellung der Verfügbarkeit durchgeführt),
- OE.Admin.2 (da nur vertrauenswürdige Personen als Administratoren eingestellt werden, kann sichergestellt werden, dass diese nicht versuchen absichtlich Manipulationen am Server durchführen. Da Administratoren geschult sind, wissen sie wie in Störungsfällen vorzugehen ist).

T.VerletzungDatenschutz

Die Bedrohung wird durch folgende Ziele abgewehrt:

- O.GeheimeNachricht (durch die Verwendung einer verschlüsselten Kommunikation können unberechtigte Dritte keinen Zugang zu persönlichen Daten erlangen),
- O.AuthNutzer (da nur berechtigte Personen Zugang zu den Daten erlangen),
- O.ZugriffDB (da für alle Zugriffe auf die Datenbank geprüft wird, ob entsprechende Zugriffsrechte vorliegen),
- O.Pseudonym (die Möglichkeit der Verwendung von Pseudonymen erlaubt, dass die Nutzer nicht mit ihrer realen Identität bei der Nutzung des Dienstes auftreten).

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Datenschutz (der Anbieter verpflichtet sich personenbezogene Daten nicht an unberechtigte Dritte weiterzugeben),

- OE.Awareness (durch Awareness-Maßnahmen werden die Nutzer für einen vorsichtigen Umgang mit den eigenen Daten sensibilisiert).

T.AbstreitungHandlung

Die Bedrohung wird durch folgende Ziele abgewehrt:

- O.AuthNutzer (da sich die Nutzer vor Inanspruchnahme des Dienstes identifizieren und authentifizieren kann gewährleistet werden, dass die Identität der Beteiligten festgestellt werden kann),
- O.IntegritätNachricht (durch die Sicherstellung der Integrität der (Kommunikations)-Daten, kann gewährleistet werden, dass kein Beteiligter behaupten kann, dass die Daten auf dem Transportweg verändert wurden),
- O.VollständigkeitTR (die Sicherstellung der Vollständigkeit der Transaktionen gewährleistet, dass kein Beteiligter behaupten kann eine Leistung nicht erhalten zu haben).
- O.Zeitstempel (die Verwendung von verlässlichen Zeitstempeln erlaubt den Nachweis eines Zeitpunktes einer Aktion),
- O.NichtabstreitbarkeitTR (da die Erzeugung von Nachweisen sicherstellt, dass eine Transaktion nicht abgestritten werden kann),
- O.NichtabstreitbarkeitKommunikation (da Nachweise von Kommunikationsinhalten erzeugt werden).

	T.UnbefugteModifikation	T.UnbefugtesLöschen	T.UnbefugtesLesen	T.VerlustVerfügbarkeit	T.VerletzungDatenschutz	T.AbstreitungHandlung
O.AuthNutzer	x	x	x		x	x
O.ZugriffDB	x	x	x		x	
O.GeheimeNachricht			x		x	
O.IntegritätNachricht	x	x				x
O.DBCheck				x		
O.Regeln						
O.EinreichenBeschwerde						
O.KenntnisBeschwerde						
O.NichtabstreitbarkeitTR						x
O.VollständigkeitTR				x		x
O.NichtabstreitbarkeitKommunikation						x
O.Pseudonym					x	
O.Zeitstempel						x
OE.Installation	x	x	x	x		
OE.Betriebssystem	x	x	x			
OE.PhysSchutz	x	x	x	x		
OE.Sanktionen						
OE.Verfügbarkeit				x		
OE.AuthDaten	x	x	x			
OE.Admin.1						
OE.Admin.2				x		
OE.Regeln						
OE.Datenschutz					x	
OE.Awareness	x	x	x		x	

Tabelle 6.5: Abwehr der Bedrohungen

6.7.3 Durchsetzung der organisatorischen Sicherheitspolitik durch den EVG

Die Sicherheitsziele (des EVG und der Umgebung) müssen die Durchsetzung der organisatorischen Sicherheitspolitiken erlauben. Tabelle 6.6 stellt die Durchsetzung der organisatorischen Sicherheitspolitik dar.

P.Crypt

Die Politik wird von folgenden Zielen durchgesetzt:

- O.AuthNutzer (die verwendeten Authentisierungsmerkmale entsprechen den aktuellen Anforderungen an kryptografische Verfahren),
- O.GeheimeNachricht (die Mechanismen zur Verschlüsselung von Daten entsprechen den aktuellen Anforderungen an kryptografische Verfahren, z.B. bei der Generierung von Schlüsseln),
- O.IntegritätNachricht (die Mechanismen zur Erzeugung von digitalen Signaturen entsprechen den aktuellen Anforderungen an kryptografische Verfahren, z.B. bei der Generierung von Hashwerten),
- O.NichtabstreitbarkeitTR (die Mechanismen zur Erzeugung von Nachweisen entsprechen den aktuellen Anforderungen an kryptografische Verfahren, z.B. bei der Generierung von digitalen Signaturen),
- O.Zeitstempel (für die Generierung von Nachweisen werden digitale Signaturen eingesetzt. Zur Bescheinigung des Ausstellungsdatums werden Zeitstempel verwendet).

P.Beschwerdekanal

Die Politik wird von folgenden Zielen durchgesetzt:

- O.EinreichenBeschwerde (da Beschwerden nur eingereicht werden können, wenn es einen (Beschwerde-)Kanal gibt),

- O.KenntnisBeschwerde (da Beschwerden nur erkannt werden können, wenn es einen (Beschwerde-)Kanal gibt),

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Sanktionen (da Sanktionen nur umgesetzt werden können, wenn die Beschwerden nachvollziehbar sind).

P.Verhaltensregeln

Die Politik wird von folgenden Zielen durchgesetzt:

- O.Regeln (die Zustimmung bzw. Akzeptanz der Verhaltensregeln kann nur erfolgen, wenn diese Regeln festgeschrieben und bekannt sind).

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Regeln (dem Nutzer können die Regeln nur bekannt sein, wenn sie festgeschrieben wurden und einsehbar sind).

P.HinweisWartung

Die Politik wird von folgenden Zielen der IT-Umgebung unterstützt:

- OE.Verfügbarkeit (die Verfügbarkeit wird durch regelmäßige Wartung des Systems unterstützt, durch Hinweise auf Wartungsarbeiten wird der Nutzer rechtzeitig auf die Einschränkung des Dienstes hingewiesen).

P.Datenschutzrichtlinie

Die Politik wird von folgenden Zielen durchgesetzt:

- O.Pseudonym (durch die Verwendung von Pseudonymen können personenbezogene Daten einer realen Identität nicht zugeordnet werden.)

Hierbei werden sie durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Datenschutz (da keine personenbezogene Daten durch den Anbieter an Dritte weitergegeben werden),
- OE.Awareness (wenn die Nutzer mithilfe von Awareness-Maßnahmen sensibilisiert werden, und nur mit einer bewussten Entscheidung persönliche Daten von sich preisgeben).

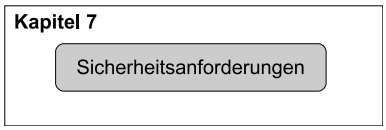
	P.Crypt	P.Beschwerdekanal	P.Verhaltensregeln	P.HinweisWartung	P.Datenschutzrichtlinie
O.AuthNutzer	x				
O.ZugriffDB					
O.GeheimeNachricht	x				
O.IntegritätNachricht	x				
O.DBCheck					
O.Regeln			x		
O.EinreichenBeschwerde		x			
O.KenntnisBeschwerde		x			
O.NichtabstreitbarkeitTR	x				
O.VollständigkeitTR					
O.NichtabstreitbarkeitKommunikation					
O.Pseudonym					x
O.Zeitstempel	x				
OE.Installation					
OE.Betriebssystem					
OE.PhysSchutz					
OE.Sanktionen		x			
OE.Verfügbarkeit				x	
OE.AuthDaten					
OE.Admin.1					
OE.Admin.2					
OE.Regeln			x		
OE.Datenschutz					x
OE.Awareness					x

Tabelle 6.6: Durchsetzung der Sicherheitspolitiken

Kapitel 7

Auswahl und Beschreibung der Anforderungen an die Sicherheit in Virtuellen Welten

Auf der Grundlage der Analyse des Sicherheitsproblems und der Definition der Sicherheitsstrategie (vgl. Kapitel 6) können nun Anforderungen an das System abgeleitet werden. Dabei wird nach funktionalen Anforderungen und Anforderungen an die Vertrauenswürdigkeit des EVG unterschieden. Die funktionalen Anforderungen beschreiben, was das System vom Design her können muss. Die Anforderungen an die Vertrauenswürdigkeit des EVG beschreiben, wie die funktionalen Anforderungen des Systems implementiert sein sollen und wie diese getestet werden sollen.



Folgende Fragen werden im vorliegenden siebten Kapitel beantwortet:

- Welche funktionalen Sicherheitsanforderungen ergeben sich aus der Definition der Sicherheitsstrategie für den EVG?

- Welche Anforderungen an die Vertrauenswürdigkeit des EVG müssen definiert werden?

7.1 Funktionale EVG-Sicherheitsanforderungen

Die Common Criteria Teil 2 enthalten einen Katalog mit Anforderungen, aus denen die für den konkreten EVG relevanten Anforderungen herausgegriffen werden. Die Sicherheitsanforderungen stellen im Falle ihrer Erfüllung sicher, dass der EVG seine Sicherheitsziele (O.*) erfüllen kann. In der Tabelle 7.1 erfolgt die Auswahl der Anforderungen. Anschließend wird diese Auswahl begründet.

Auswahl	Bezeichnung	Beschreibung
FAU: Sicherheitsprotokollierung/Audit		
X	FAU_ARP	Automatische Reaktion der Sicherheitsprotokollierung
X	FAU_GEN	Generierung der Sicherheitsprotokolldaten
X	FAU_SAA	Analyse der Sicherheitsprotokollierung
X	FAU_SAR	Durchsicht der Sicherheitsprotokollierung
	FAU_SEL	Ereignisauswahl für die Sicherheitsprotokollierung
	FAU_STG	Ereignisspeicherung der Sicherheitsprotokollierung
FCO: Kommunikation		
X	FCO_NRO	Nichtabstreitbarkeit der Urheberschaft
X	FCO_NRR	Nichtabstreitbarkeit des Empfangs
FCS: Kryptografische Unterstützung		
	FCS_CKM	Kryptographisches Schlüsselmanagement
X	FCS_COP	Kryptographischer Betrieb
FDP: Schutz der Benutzerdaten		
X	FDP_ACC	Zugriffskontrollpolitik
X	FDP_ACF	Zugriffskontrollfunktionen
	FDP_DAU	Datenauthentisierung
	FDP_ETC	Export nach außerhalb der TSF-Kontrolle
	FDP_IFC	Politik der Informationsflußkontrolle
	FDP_IFF	Funktionen der Informationsflußkontrolle
	FDP_ITC	Import von außerhalb der TSF-Kontrolle
X	FDP_ITT	EVG-interner Transfer
	FDP_RIP	Schutz bei erhalten gebliebenen Informationen

X	FDP_ROL	Rückgängig
X	FDP_SDI	Integrität der gespeicherten Daten
	FDP_UCT	Schutz der Benutzerdatenvertraulichkeit bei Inter-TSF-Transfer
	FDP_UIT	Schutz der Benutzerdatenintegrität bei Inter-TSF-Transfer

FIA: Identifikation und Authentifizierung

X	FIA_AFL	Authentisierungsfehler
	FIA_ATD	Definition der Benutzerattribute
	FIA_SOS	Spezifikation der Geheimnisse
X	FIA_UAU	Benutzerauthentisierung
X	FIA_UID	Benutzeridentifikation
	FIA_USB	Benutzer-Subjekt-Bindung

FMT: Sicherheits-Management

	FMT_MOF	Management der TSF-Funktionen
X	FMT_MSA	Management der Sicherheitsattribute
	FMT_MTD	Management der TSF-Daten
	FMT_REV	Widerruf
	FMT_SAE	Verfall der Sicherheitsattribute
X	FMT_SMR	Rollen im Sicherheitsmanagement

FPR: Datenschutz/Privacy

	FPR_ANO	Anonymität
X	FPR_PSE	Pseudonymität
	FPR_UNL	Unverkettbarkeit
	FPR_UNO	Unbeobachtbarkeit

FPT: Schutz der EVG Sicherheitsfunktionen

	FPT_AMT	Test der zugrundeliegenden abstrakten Maschine
	FPT_FLS	Sicherer Fehlerzustand
	FPT_ITA	Verfügbarkeit von exportierten TSF-Daten
	FPT_ITC	Vertraulichkeit von exportierten TSF-Daten
	FPT_ITI	Integrität von exportierten TSF-Daten
	FPT_ITT	EVG-interner TSF-Datentransfer
	FPT_PHP	Materieller TSF-Schutz
	FPT_RCV	Vertrauenswürdige Wiederherstellung
	FPT_RPL	Erkennen von Wiedereinspielung
	FPT_RVM	Referenzverbindung
	FPT_SEP	Bereichsseparierung

	FPT_SSP	Protokoll zur Zustandssynchronisierung
X	FPT_STM	Zeitstempel
	FPT_TDC	Inter-TSF TSF-Datenkonsistenz
	FPT_TRC	TSF-Datenkonsistenz bei EVG-interner Datenreproduktion
	FPT_TST	TSF-Selbsttest
FRU: Betriebsmittelnutzung		
	FRU_FLT	Fehlertoleranz
	FRU_PRS	Priorität der Dienste
	FRU_RSA	Betriebsmittelzuteilung
FTA: EVG Zugriff/Access		
	FTA_LSA	Begrenzung des Anwendungsbereiches der auswählbaren Attribute
	FTA_MCS	Begrenzung bei mehreren gleichzeitigen Sitzungen
	FTA_SSL	Sperren der Sitzung
X	FTA_TAB	EVG-Zugriffswarnmeldung
	FTA_TAH	EVG-Zugriffshistorie
X	FTA_TSE	EVG-Sitzungseinrichtung
FTP: Vertrauenswürdiger Pfad/Kanal		
	FTP_ITC	Inter-TSF Vertrauenswürdiger Kanal
	FTP_TRP	Vertrauenswürdiger Pfad

Tabelle 7.1: Auswahl der für den EVG relevanten Anforderungen

Die folgenden Abschnitte erläutern diese Auswahl der Anforderungen an Virtuelle Welten im Detail. Dabei wird für jedes Sicherheitsziel beschrieben, welche Anforderungen zur Erfüllung relevant sind.

7.1.1 Anforderungen zur Erfüllung des Ziels O.AuthNutzer

Bevor Nutzer Aktionen in der Virtuellen Welt durchführen können, müssen sie sich gegenüber dem System authentifizieren. Der Prozess wird umgangssprachlich oft als „Anmelden“ oder „Login“ bezeichnet. Das System muss dazu Sicherheitsfunktionen zur Identifizierung und Authentifizierung der Nutzer (vgl. Kapitel 6 Sicherheitsziel O.AuthNutzer) bieten.

Authentifikation und Authentisierung beschreiben denselben Prozess aus unterschiedlichen Sichtweisen. Die Authentisierung beschreibt die Nutzersicht und besteht aus den zwei Teilschritten Identifikation und Autorisierung. Der Benutzer authentisiert sich am System, indem er eine Identität (z.B. durch Benutzernamen) behauptet (Identifikation) und ein Zugriffsrecht nachweist (Autorisierung). Der Nachweis wird erbracht, indem er etwas weiß (Authentisierung anhand von Wissen, z.B. Passwort), etwas besitzt (Authentisierung anhand von Besitz, z.B. Smartcard) oder bestimmte Eigenschaften hat (Authentisierung anhand von biometrischen Merkmalen, z.B. Fingerabdruck). Für eine Authentifizierung aus Systemsicht werden die Nutzer mit bestimmten Sicherheitsattributen (z.B. Benutzername und Passwort) verbunden, mit denen sie eindeutig vom System erkannt werden.

Die Einrichtung und Verifizierung von Benutzeridentitäten wird in den Common Criteria Teil 2 in der Klasse FIA (Identifikation und Authentisierung) geregelt (vgl.[CCPart2 06] S.99ff). In FIA_UID.2.1 (Benutzeridentifikation, vgl. Kapitel 8.5.1, S.163) wird der Zeitpunkt der Identifikation festgelegt. Aktionen in der Virtuellen Welt machen nur Sinn, wenn sie dem Avatar des Benutzers zugeordnet werden können. Das System kann einen Avatar seinem Benutzer erst nach dessen Identifikation zuordnen. Deshalb ist es notwendig, dass der Zeitpunkt der Identifikation vor jeglichen anderen Aktionen liegt.

Das gleiche Verfahren wird in FIA_UAU.2.1 (vgl. Kapitel 8.5.1, S.163) für die Authentisierung verlangt (vgl.[CCPart2 06] S.94ff).

Für die Unterstützung der Authentisierung müssen die Sicherheitsfunktionen des EVG auf kryptografische Verfahren zurückgreifen können. Dies erfordert die Einbeziehung der Anforderung FCS_COP (Kryptografischer Betrieb, vgl. Kapitel 8.5.1, S.160).

Um den Account eines Nutzers vor möglichen Denial-of-Service-Angriffen zu schützen, wird es von der Autorin als wichtig erachtet, dass die Login-Versuche mengenmäßig begrenzt sind, d.h. dass der Prozess der Sitzungseinrichtung nach einer spezifizierten Anzahl von misslungenen Benutzerauthentisierungsversuchen abgebrochen wird. Diese Anforderung wird in FIA_AFL.1.2 (Authentisierungsfehler, vgl. Kapitel 8.5.1, S.163) beschrieben [vgl.[CCPart2 06] S.89ff, S.243ff].

7.1.2 Anforderungen zur Erfüllung des Ziels O.ZugriffDB

Die Identifikation und Authentifizierung ist auch notwendig um unberechtigen Zugriff auf die Datenbank und die darin enthaltenen Werte sicherzustellen (vgl. Kapitel 6 Sicherheitsziel O.ZugriffDB). So können unberechtigte Nutzer keine Daten lesen, löschen oder modifizieren. Eine unberechtigte Modifikation und unberechtigtes Löschen durch autorisierte Nutzer kann jedoch damit noch nicht unterbunden werden.

Zusätzlich notwendig ist daher eine Zugriffskontrollpolitik. Zugriffskontrollen werden nur für zu schützende Einheiten (Objekte) durchgeführt (vgl. [Eckert 04]). Zu schützende Einheiten sind in diesem Fall die Tabellen mit den Daten über die Werte (Assets) in der Datenbank. Zum Beispiel sollte ein Nutzer nur auf seinen Avatar lesend und schreibend zugreifen dürfen, nicht aber auf die Avatare anderer Nutzer. Für die Durchsetzung der Zugriffskontrollen existieren Zugriffskontrollmodelle (z.B. Zugriffsmatrix-Modell, Rollenbasierte Modelle). Für die Rechtezuweisung können Zugriffssteuerungslisten (ACL) verwendet werden.

Die Anforderung der Einrichtung einer Zugriffskontrollpolitik wird in den Common Criteria in der Klasse FDP (Schutz der Benutzerdaten) festgelegt. In das Schutzprofil muss daher die Familie FDP_ACC (Zugriffskontrollpolitik, vgl. Kapitel 8.5.1, S.161ff.) aufgenommen werden. Die Einrichtung einer funktionalen Sicherheitspolitik erfordert die Festlegung eines eindeutigen Namens (z.B. „Datenbank-Nutzer SFP“), die festlegt wie sich die Zugriffskontrollpolitik gestaltet. Die Zugriffskontrollpolitik erfordert die Definition von Subjekten, Objekten und Operationen (vgl.[CCPart2 06] S.57ff). Beispielsweise darf jeder Nutzer (Subjekt) nur auf seinen Datensatz (Objekte, bspw. Daten über den Avatar) lesend und schreibend (Operation) zugreifen. Um gemeinsamen Zugriff auf Objekte zu gewährleisten (z.B. die Welt), können Subjektgruppen (Benutzergruppen) definiert werden.

In FDP_ACF (Zugriffskontrollfunktionen, vgl. Kapitel 8.5.1, S.161ff.) werden dann die Attribute (Ort, Zeit, Zugriffsrechte) festgelegt. Beispielsweise können die Attribute in einer Zugriffskontrollliste (ACL) festgelegt werden (vgl.[CCPart2 06] S.59ff). In FDP_ACC werden die Sicherheitspolitiken und Attribute deklariert und in FDP_ACF werden sie definiert.

Die Attribute müssen verwaltet werden, weshalb die Familie FMT_MSA (Management der Sicherheitsattribute, vgl. Kapitel 8.5.1, S.164f.) der Klasse FMT (Sicherheitsmanagement) hinzugezogen wird. In FMT_MSA werden die Gruppen bzw. Rollen für die Sicherheitsattribute (z.B. die ACL) definiert. Die Sicherheitsfunktionen des EVG müssen durchsetzen, dass die Zugriffskontrollpolitik „Datenbank-Nutzer SFP“ eingehalten wird. Es wird durchgesetzt, dass nur berechtigte Personen Sicherheitsattribute modifizieren, löschen, etc. dürfen. Die Komponente FMT_MSA.3 (Initialisierung statischer Attribute) der Familie FMT_MSA spezifiziert vorgegebene Standardwerte von Sicherheitsattributen (vgl.[CCPart2 06] S.106ff).

Die Zuweisung der Rollen zu den Nutzern wird über die Familie FMT_SMR (Rollen im Sicherheitsmanagement, vgl. Kapitel 8.5.1, S.164f.) definiert. Es wird festgelegt, welche Rollen es gibt (FMT_SMR.1.1) und dass Benutzer mit Rollen verknüpft werden können (FMT_SMR.1.2) (vgl.[CCPart2 06] S.115ff).

7.1.3 Anforderungen zur Erfüllung des Ziels O.DBCheck

Werden Operationen auf den Daten (der Datenbank) ausgeführt, ist es notwendig, dass die Daten auf Integrität geprüft werden können (vgl. Kapitel 6 Sicherheitsziel O.DBCheck). In FDP_ITT.1 (Einfacher Schutz des EVG-internen Transfers, vgl. Kapitel 8.5.1, S.161ff.) wird gefordert, dass die funktionale Sicherheitspolitik die Daten vor Preisgabe oder Modifikation schützen muss, wenn Daten zwischen internen Teilen des EVG (bspw. zwischen Datenbank und Anwendungssoftware des Servers) übertragen werden (vgl.[CCPart2 06] S.74ff).

Tritt ein Integritätsfehler bei den gespeicherten Daten auf (z.B. aufgrund eines Hardwarefehlers), muss dies angezeigt werden. Diese Forderung wird in FDP_SDI (Integrität der gespeicherten Daten, vgl. Kapitel 8.5.1, S.161ff.) beschrieben (vgl.[CCPart2 06] S.81ff).

7.1.4 Anforderungen zur Erfüllung des Ziels O.GeheimeNachricht

Das Sicherheitsziel O.GeheimeNachricht (vgl. Kapitel 6) zielt auf eine geheime Übertragung von Daten zwischen Client und Server ab. Die Anforderung der Vertraulichkeit der Benutzerdaten auf einem internen Kanal des EVG wird in den Common Criteria in der Familie FDP_ITT (Einfacher Schutz des EVG-internen Transfers, vgl. Kapitel 8.5.1, S.161) der Klasse FDP (Schutz der Benutzerdaten) definiert (vgl.[CCPart2 06] S.74ff). Die Sicherheitsfunktionen des EVG müssen gewährleisten, dass Objekte bei der Übertragung vor nicht autorisierter Preisgabe geschützt sind (FDP_ITT.1.1, vgl. Kapitel 8.5.1, S.161f).

7.1.5 Anforderungen zur Erfüllung des Ziels O.IntegritätNachricht

Das Sicherheitsziel O.IntegritätNachricht (vgl. Kapitel 6) stellt ähnliche Anforderungen an die Sicherheitsfunktionen des EVG, wie das Ziel O.GeheimeNachricht (siehe oben). Der Schutz der Benutzerdatenintegrität auf einem internen Kanal des EVG wird in den Common Criteria in der Klasse FDP_ITT (Einfacher Schutz des EVG-internen Transfers, vgl. Kapitel 8.5.1, S.161) definiert. Die Sicherheitsfunktionen des EVG müssen gewährleisten, dass Objekte bei der Übertragung vor nicht autorisierter Modifikation geschützt sind (FDP_ITT.1.1, vgl. Kapitel 8.5.1, S.161f).

7.1.6 Anforderungen zur Erfüllung des Ziels O.Regeln

In Virtuellen Welten bilden sich aufgrund des starken sozialen Charakters Gemeinschaften. Wenn Menschen in Gemeinschaften leben, muss es Regeln für den gegenseitigen Umgang geben. Nur wenn sich die Mitglieder der Gemeinschaft an die Regeln halten, kann ein faires Miteinander gewährleistet werden. Für die Sicherstellung der Fairness innerhalb der sozialen Gemeinschaft, wurde das Sicherheitsziel O.Regeln (vgl. Kapitel 6) eingeführt.

Zur Umsetzung dieses Ziels muss vom System gefordert werden, dass es eine Funktionalität bereitstellt, die garantiert, dass die Mitglieder die Möglichkeit haben, die Regeln zu

kennen. Dies wird mithilfe der Anforderung FTA_TAB (Vorgegebene EVG-Zugriffswarnmeldung, vgl. Kapitel 8.5.1, S.166f) umgesetzt. In dieser Familie werden Anforderungen aufgelistet, die die Anzeige konfigurierbarer Warnmeldungen über die korrekte Benutzung des EVG auf dem Bildschirm ermöglichen. Dies kann dazu genutzt werden, dem Nutzer einer Virtuellen Welt die Regeln anzuzeigen (vgl.[CCPart2 06] S.165ff).

Bevor der Zugang zur Virtuellen Welt (Sitzungseinrichtung) gewährt wird, muss der Nutzer den Regeln zustimmen. Eine während der Nutzung stattfindende Zustimmung würde das Unterhaltungserleben stören und ein mögliches Immersions- oder Flowerlebnis unterbrechen. Daher wird im Schutzprofil verlangt, dass eine Sitzungseinrichtung nicht gestattet wird, wenn der Nutzer den Regeln nicht zustimmt. Diese Anforderung wird in FTA_TSE (EVG-Sitzungseinrichtung, vgl. Kapitel 8.5.1, S.166) definiert. Nutzern, die den Regeln nicht zustimmen, kann kein Zugang zur Welt gestattet werden. Mit FTA_TSE.1.1 kann erreicht werden, dass dem Nutzer die Erlaubnis des Zutritts verwehrt bleibt (vgl.[CCPart2 06] S.167ff). In Kapitel 9 (S.174) wird ein Szenario für die konkrete Umsetzung dieser Forderungen vorgestellt.

7.1.7 Anforderungen zur Erfüllung des Ziels O.EinreichenBeschwerde

Es muss davon ausgegangen werden, dass trotz einer Zustimmung zu den Verhaltensregeln gegen sie verstoßen wird, was zur Fairnessverletzung führt. Daher muss es Möglichkeiten geben, in einem solchen Fall Fairness nachträglich herzustellen, indem die Regelverletzung sanktioniert wird.

Dies erfordert die Möglichkeit des Einreichens einer Beschwerde (vgl. Kapitel 6 Sicherheitsziel O.EinreichenBeschwerde) und der Durchführung von Sanktionen seitens einer dafür zuständigen Stelle. Dies kann der Anbieter sein oder ein von der Nutzer-Community gewähltes Gremium.

Damit die zuständige Stelle den Fall beurteilen kann, muss die Aufzeichnung von Auditdaten gefordert werden. Diese Anforderung wird in den Common Criteria in der Klasse FAU_GEN (Generierung von Sicherheitsprotokolldaten, vgl. Kapitel 8.5.1, S.156) definiert

(vgl.[CCPart2 06] S.31f). Die Generierung von Protokolldaten erfordert laut Common Criteria auch die Bereitstellung verlässlicher Zeitstempel (FPT_STM) durch das System.

Die Protokolldaten müssen Aussagen über die beteiligten Personen und den Zeitpunkt der Einreichung treffen können. Dies macht den Einbezug der Anforderungen FIA_UID (Benutzeridentifikation, siehe oben) und FPT_STM (Zeitstempel, vgl. Kapitel 8.5.1, S.165) unabdingbar. Die EVG-Funktionen müssen einen verlässlichen Zeitstempel zur Verfügung stellen (FPT_STM.1.1).

7.1.8 Anforderungen zur Erfüllung des Ziels O.KenntnisBeschwerde

Damit die für Beschwerden zuständige Stelle Hinweisen der Fairnessverletzung nachgehen kann, muss sie zunächst Kenntnis von der Beschwerde erlangen (vgl. Kapitel 6 Sicherheitsziel O.KenntnisBeschwerde).

Vom System muss verlangt werden können, dass es eine Funktionalität enthält, die bei Eintreten des Ereignisses „Beschwerde eingereicht“ einen Alarm auslöst, also die zuständige Stelle benachrichtigt wird. Diese Anforderung kann mit FAU_ARP (Automatische Reaktion der Sicherheitsprotokollierung, vgl. Kapitel 8.5.1, S.156ff.) umgesetzt werden (vgl.[CCPart2 06] S.30). Der Alarm könnte so gestaltet sein, dass die befugte Stelle eine Meldung „neue Beschwerde eingegangen“ erhält.

Außerdem muss vom System verlangt werden, dass die zuständige Stelle bei der Analyse der Protokolldaten zu den Beschwerdefällen geeignet unterstützt wird. Die Sicherheitsfunktionen des EVG müssen daher die Anforderung FAU_SAR (Durchsicht der Sicherheitsprotokollierung, vgl. Kapitel 8.5.1, S.156ff.) unterstützen. In FAU_SAR.1.1 muss definiert werden, wer Zugang zu welchen Protokolldaten hat. In FAU_SAR.1.2 wird verlangt, dass die Auditdaten so dargestellt werden, dass sie einfach von den Berechtigten gelesen und interpretiert werden können (vgl.[CCPart2 06] S.37f).

Des Weiteren muss vom System verlangt werden, dass es eine automatische Analyse der Protokolldaten (Monitoring) unterstützt. Daher wird die Anforderung FAU_SAA (Analyse der Sicherheitsprotokollierung, vgl. Kapitel 8.5.1, S.156ff.) ins Schutzprofil auf-

genommen. In FAU_SAA.2 können Profile zum Filtern der Auditdaten definiert werden (vgl.[CCPart2 06] S.33ff). So könnten beispielsweise die Beschwerden vorgefiltert werden, in denen es um Beleidigungen geht, zum Beispiel weil in den Fällen bekannte Schimpfwörter enthalten sind.

7.1.9 Anforderungen zur Erfüllung des Ziels O.NichtabstreitbarkeitTR

Ein weiteres Sicherheitsziel, das die Generierung von Protokolldaten (FAU_GEN, siehe oben) verlangt, betrifft die Sicherheit der Transaktionen (vgl. Kapitel 6 Sicherheitsziel O.NichtabstreitbarkeitTR). Für jede Transaktion müssen Protokolldaten angelegt werden, um diese auch im Nachhinein nachvollziehen zu können.

Es werden die Identität der Beteiligten (FIA_UID) und der Zeitpunkt der Transaktion (FPT_STM) protokolliert. Diese Daten müssen für eine Durchsicht unterstützt werden (FAU_SAR). Dazu muss das System einen Nachweis des Ursprungs von Informationen erzeugen und die Identität des Urhebers mit den Informationen verbinden können. Daher wird die Anforderung FCO_NRO (Nichtabstreitbarkeit der Urheberschaft, vgl. Kapitel 8.5.1, S.159ff.) ins Schutzprofil aufgenommen. Die Anforderung FCO_NRO.1 (Selektiver Urheberschaftsbeweis) stellt sicher, dass Benutzer Urheberschaftsnachweise generieren können (vgl.[CCPart2 06] S.44f).

In gleicher Weise müssen Nachweise über den Erhalt der Daten erzeugt werden. Diese Anforderung wird in FCO_NRR (Nichtabstreitbarkeit des Empfangs, vgl. Kapitel 8.5.1, S.159) beschrieben. Die Anforderung FCO_NRR.1 (Selektiver Empfangsbeweis) stellt sicher, dass Benutzer Empfangsnachweise generieren können (vgl.[CCPart2 06] S.46f).

Für die Erzeugung der Nachweise bedarf es der Unterstützung krypotografischer Verfahren, zum Beispiel zur Erzeugung von Hashwerten. Die Anforderung FCS_COP (Kryptografischer Betrieb, vgl. Kapitel 8.5.1, S.160) wird daher in das Schutzprofil aufgenommen (vgl.[CCPart2 06] S.52f). Die Sicherheitsfunktionen des EVG müssen kryptografische Operationen durchführen können (FCS_COP.1).

7.1.10 Anforderungen zur Erfüllung des Ziels O.Vollständigkeit-TR

Sollte eine Transaktion nicht vollständig ausgeführt werden können, muss ein konsistenter Zustand (Zustand vor der Transaktion) wieder herstellbar sein (vgl. Kapitel 6 Sicherheitsziel O.VollständigkeitTR). Die Umsetzung dieser Forderung verlangt, dass unvollständig ausgeführte Transaktionen zurück abgewickelt werden können. Daher wird die Einbindung der Anforderung FDP_ROL.1 (Einfaches Rückgängig, vgl. Kapitel 8.5.1, S.161) in das Schutzprofil gefordert. Die Sicherheitsfunktionen des EVG müssen unterstützen, dass bei einem Fehler ein wohl definierter Zustand hergestellt werden kann, nämlich der Zustand vor der Transaktion (vgl. [CCPart2 06], S.79f).

7.1.11 Anforderungen zur Erfüllung des Ziels O.NichtabstreitbarkeitKommunikation

Das Sicherheitsziel O.NichtabstreitbarkeitKommunikation fordert Nachweise für den Inhalt von Kommunikation (vgl. Kapitel 6 Sicherheitsziel O.NichtabstreitbarkeitKommunikation). Diese Forderung verlangt die Generierung von Protokolldaten (FAU_GEN, siehe oben). Neben den Kommunikationsdaten müssen die Identität der Beteiligten (FIA_UID) und der Zeitpunkt der Kommunikation (FPT_STM) protokolliert werden.

7.1.12 Anforderungen zur Erfüllung des Ziels O.Pseudonym

Den Nutzern soll die Möglichkeit der Verwendung von Pseudonymen in der Virtuellen Welt gegeben werden (vgl. Kapitel 6 Sicherheitsziel O.Pseudonym). Daraus ergibt sich die Anforderung FPR_PSE (Pseudonymität, vgl. Kapitel 8.5.1, S.165), die das System erfüllen muss. Die Sicherheitsfunktionen des EVG müssen sicherstellen, dass Benutzer die Virtuelle Welt benutzen können, ohne ihre reale Identität preiszugeben aber dennoch für ihre Handlungen verantwortlich gemacht werden können (vgl.[CCPart2 06] S.120f), z.B. bei der Durchführung von Transaktionen.

7.1.13 Anforderungen zur Erfüllung des Ziels O.Zeitstempel

Die Sicherheitsfunktionen des EVG müssen für die Erfüllung von Anforderungen auf verlässliche Zeitstempel zurückgreifen können. Deshalb wird die Anforderung FPT_STM (Zeitstempel, vgl. Kapitel 8.5.1, S.165) in das Schutzprofil aufgenommen (vgl. [CCPart2 06], S.146).

7.2 Abdeckung der Sicherheitsziele

Nachdem eine Auswahl der Sicherheitsanforderungen getroffen wurde, muss untersucht werden, ob die Sicherheitsziele durch die Anforderungen abgedeckt werden. Die Abbildung 7.1 zeigt, dass nur die Sicherheitsziele des EVG durch die Sicherheitsanforderungen abgedeckt werden. Zusätzlich werden Anforderungen an die Vertrauenswürdigkeit definiert (vgl. Kapitel 7.3).

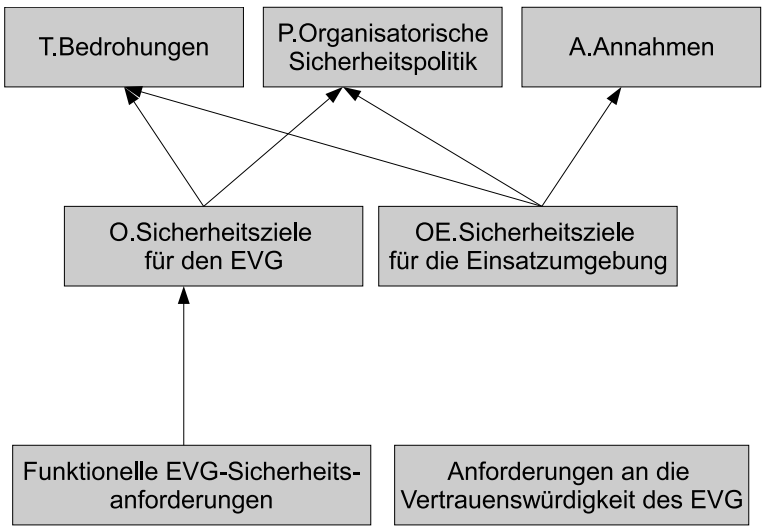


Abbildung 7.1: Abdeckung der Sicherheitsziele [in Anlehnung an [CCPart1 06], S.62]

In der Tabelle 7.2 wird die Abdeckung für die oben definierten Sicherheitsziele visualisiert.

	O.AuthNutzer	O.ZugriffDB	O.GeheimeNachricht	O.IntegritätNachricht	O.DBCheck	O.Regeln	O.EinreichenBeschwerde	O.KenntnissBeschwerde	O.NichtabstreitbarkeitTR	O.VollständigkeitTR	O.Pseudonym	O.Zeitstempel	O.NichtabstreitbarkeitKommunikation
FAU_ARP								x					
FAU_GEN							x		x				x
FAU_SAA								x					
FAU_SAR								x	x				
FCO_NRO									x				
FCO_NRR									x				
FCS_COP	x		x	x					x				
FDP_ACC		x	x	x									
FDP_ACF		x	x	x									
FDP_ITT			x	x	x								
FDP_ROL					x					x			
FDP_SDI					x								
FIA_AFL	x												
FIA_UAU	x												x
FIA_UID	x						x		x				x
FMT_MSA		x	x	x									
FMT_SMR		x	x	x									
FPR_PSE											x		
FPT_STM							x		x			x	x
FTA_TAB						x							
FTA_TSE						x							

Tabelle 7.2: Abdeckung der Sicherheitsziele

7.3 Anforderungen an die Vertrauenswürdigkeit des EVG

Die Assurance Requirements (deutsch: Anforderungen an die Zusicherung von Vertrauen) sind die Basis für Vertrauen, dass ein IT Produkt seine Sicherheitsziele erfüllt. Die sieben Stufen der Zusicherung (Evaluation Assurance Levels) stellen unterschiedliche Anforderungen an die Prüfung der IT-Sicherheit. Details zur Prüftiefe der sieben Stufen werden in den Common Criteria Teil 3 beschrieben.

Für das Schutzprofil wird EAL-Stufe 2 empfohlen (vgl. Kapitel 8, S.168). Die Bedrohungen der IT-Sicherheit des Systems sind aufgrund der Relevanz der Werte (vgl. Kapitel 4) als ernst einzustufen, weshalb Stufe 1 zu niedrig gewählt wäre. Die Evaluierung muss aber mit einer geschäftlichen Praxis noch vereinbar sein, weshalb Stufe 2[1] angemessen erscheint.

Die Tabelle 7.3 zeigt die Anforderungen der EAL-Stufe 2.

Klasse	Bezeichnung	Beschreibung
ADV: Entwicklung	ADV_ARC.1	Beschreibung der Sicherheitsarchitektur
	ADV_FSP.2	Sicherheitsdurchsetzende Funktions-Spezifikation
	ADV_TDS.2	Basis Design
AGD: Handbücher	AGD_ADM.1	Systemverwalterhandbuch
	AGD_OPE.1	Benutzerhandbuch
	AGD_PRE.1	Vorbereitende Vorgänge
ALC:Lebenszyklus-Unterstützung	ALC_CMC.2	Verwendung eines CM Systems
	ALC_CMS.2	Teile der EVG CM Abdeckung
	ALC_DEL.1	Vorgang der Auslieferung
ASE: Security Target[2]	ASE_CCL.1	Postulate zur Übereinstimmung

[1] „EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort [...] than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time“ [CCPart3 06], S.34.

[2] Sicherheitsvorgaben

	ASE_ECD.1	Definition erweiterter Komponenten
	ASE_INT.1	ST Einführung
	ASE_OBJ.2	Sicherheitsziele
	ASE_REQ.2	Abgeleitete Sicherheitsanforderungen
	ASE_SPD.1	Definition des Sicherheitsproblems
	ASE_TSS.1	EVG-Definition Zusammenfassung
ATE: Tests	ATE_COV.1	Analyse der Testabdeckung
	ATE_FUN.1	Funktionales Testen
	ATE_IND.2	Unabhängiges Testen - Stichprobenartig
AVA: Schwachstellen- bewertung	AVA_VAN.2	Schwachstellenanalyse

Tabelle 7.3: EAL 2 [CCPart3 06]

Kapitel 8

Schutzprofil für Anwendungssoftware Virtueller Welten

In Kapitel 5 wurde der Aufbau eines Schutzprofils nach Common Criteria beschrieben. Im Kapitel 6 wurde eine Sicherheitsanalyse für Virtuelle Welten durchgeführt und in Kapitel 7 wurde die Auswahl der relevanten Anforderungen aus dem Katalog der Common Criteria begründet. Dieses Kapitel umfasst das eigenständige Schutzprofil für Anwendungssoftware Virtueller Welten, das aus der Arbeit herauslösbar ist. In dem Schutzprofil wird auf die Erkenntnisse der Kapitel 6 und 7 zurückgegriffen. Die Bedrohungen, Annahmen, Sicherheitspolitiken, Sicherheitsziele werden nur erwähnt und nicht begründet.

8.1 EVG Beschreibung

8.1.1 Kurzbeschreibung und Aufbau

Bei dem EVG handelt es sich um eine Software zur Nutzung und Bereitstellung Virtueller Welten. Der Zugang zur Virtuellen Welt erfolgt über die Clientsoftware, die auf einem beliebigen Clientgerät (bspw. PC, Handy, PDA) installiert ist. Die Clientsoftware übernimmt hierbei nur die Darstellung der mehrdimensionalen Welt. Alle Bestandsdaten (vgl. Kapitel 6, S.84) werden auf einem zentralen Server gespeichert.

Der EVG bezieht sich ausschließlich auf die Client-Server-Architektur. Andere Architekturen, wie beispielsweise Peer-To-Peer, erfordern möglicherweise andere/weitere Sicherheitsanforderungen, die gesondert analysiert und festgelegt werden müssen. Die von dieser Beschreibung abweichenden Eigenschaften eines Systems zur Nutzung Virtueller Welten sind gesondert zu untersuchen.

Es handelt sich bei dem EVG um ein Anwendungsprogramm, dass in seinen Sicherheitsfunktionen von der Systemkonfiguration des Clientgeräts und des Betriebssystems abhängig ist.

Die Abbildung 8.1 zeigt, wie der EVG in seine Umwelt eingebettet ist. Bestandteile des EVGs sind die Client-Anwendungssoftware, die Server-Anwendungssoftware, der Kommunikationskanal über den Nachrichten zwischen Client und Server ausgetauscht werden (Netzwerk) und die Datenbank, in der alle für die Virtuelle Welt relevanten Daten gespeichert werden. Nicht Bestandteil des EVGs sind die Hardware und das Betriebssystem des Client- und des Serversystems. Ein möglicherweise angegliederter Abrechnungsserver, der die Zahlungstransaktionen und -informationen verwaltet, ist nicht Teil des EVG, da diese sich dem Kontroll- und Verantwortlichkeitsbereich des Anbieters entziehen können.

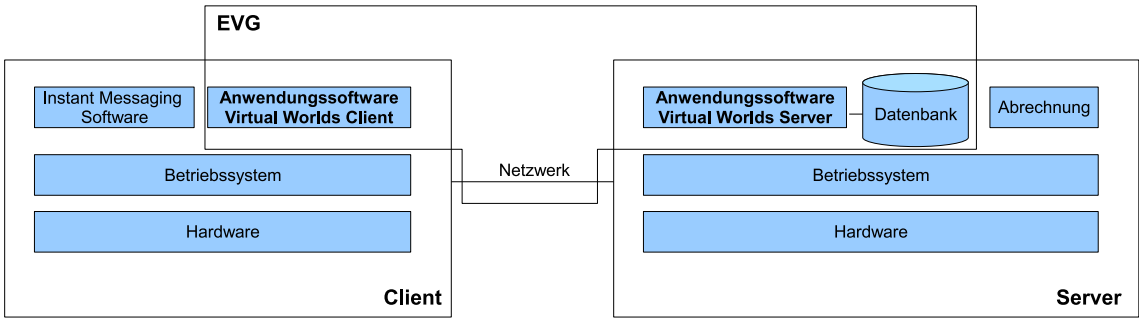


Abbildung 8.1: Aufbau des EVG [eigene Abbildung]

8.1.2 Aufgabenstellung und Prozessbeschreibung

Über den EVG haben die Benutzer Zugang zur Virtuellen Welt und können verschiedene Aktionen ausführen, wie beispielsweise Transaktionen auslösen oder mit anderen Nutzern in Kontakt treten.

Der EVG stellt Funktionalitäten zu Verfügung, um die nachfolgenden Aufgaben zu ermöglichen.

Virtuelle Welten sind soziale Netzwerke, in denen Nutzer eine Vielzahl an Handlungsmöglichkeiten haben. Möchte eine Person das Netzwerk nutzen, muss er/sie ein Nutzerkonto, unter Angabe des Namens und evtl. weiterer personenbezogener Daten, eröffnen. Das Konto erlaubt die Zuordnung von Werten zu einem Nutzer. Mit der Eröffnung des Accounts ist die Erstellung eines Avatars vorgegeben. Der Avatar repräsentiert den Nutzer in der Virtuellen Welt. Angaben, die bei der Erstellung eines Avatars gemacht werden müssen, sind:

- ein eindeutiger Bezeichner (z.B. Vorname, Name)
- das gewünschte Erscheinungsbild wie Größe, Hautfarbe, Kleidung, etc. (der Avatar hat eine initiale Standardeinstellung (z.B. weißes T-Shirt, blaue Jeans), die der Nutzer beibehalten kann).

Sobald der Nutzer einen Avatar besitzt, stehen ihm alle Funktionalitäten der Virtuellen Welt zur Verfügung, die er beliebig nutzen kann.

Funktionalitäten, die die Welt bereitstellt sind:

Navigation

Über Eingabegeräte (z.B. Tastatur, Maus) kann sich der Nutzer mit Hilfe seines Avatars in der Virtuellen Welt bewegen.

Kommunikation/Socialising/ soziale Kontakte pflegen

Die Client-Anwendungssoftware verfügt über eine Instant Messaging-Funktion, mit der sich Nutzer kontaktieren und unterhalten können (Nachrichtenaustausch). Das Socialising ist ein wichtiger Teil eines soziales Netzwerkes, da oftmals Freundschaften geknüpft oder Interessengruppen gegründet werden, die für die Nutzer auch in der Realwelt wichtig sind.

Gruppenbildung/sich einer Gruppe anschließen

Ganz eng verbunden mit dem Socialising ist die Möglichkeit eine Interessengruppe zu gründen bzw. sich einer Gruppe anzuschließen. Dies ermöglicht den Nutzern:

1. Zugang zu Informationen,
2. Unterstützung durch die Gruppe (z.B. beim Lösen von Aufgaben),
3. das Gefühl der Zusammengehörigkeit.

Aufgaben/Quests lösen

Nutzer von Virtuellen Welten suchen die Herausforderung und finden Spaß daran Rätsel zu lösen und Aufgaben zu erledigen, beispielsweise eine Vorlesung halten, Begleitservice, Suche nach Gegenständen etc.

Wettbewerb/Kampf

Eine weitere Herausforderung für die Nutzer stellt sich darin, sich mit Anderen im Wettbewerb zu messen. Dafür benutzt der Avatar Fertigkeiten, die er im Laufe der Zeit erlangt. Solche Fertigkeiten der Avatare sind Funktionalitäten der Software, nicht die physischen oder kombinatorischen Fähigkeiten des Nutzers. Beispiele für Fähigkeiten sind zaubern, heilen, Todesfluch, fliegen, etc. Darunter zählen auch Gesten, wie zum Beispiel Gähnen oder applaudieren.

Eine mögliche Form des Wettbewerbs ist der Kampf. Es treten Einzelspieler oder Gruppen gegeneinander oder gegen NPC's an. Innerhalb einer Gruppe erfordert dies die Entwicklung taktischer Strategien um sich zu behaupten. Für eine erfolgreiche Durchführung von Wettbewerben oder bei der Lösung beziehungsweise Erledigung von Fragen oder Aufgaben werden die Nutzer mit zusätzlichen Punkten oder einem Levelupgrade belohnt.

Gegenstände erstellen

Der EVG stellt dem Nutzer eine Funktionalität zu Verfügung um Gegenstände (3D-Objekte) zu erstellen. Die Gegenstände können so programmiert werden, dass sie eine Funktionalität haben.

Handel treiben

Der EVG verfügt über einen Marktplatz, auf dem Gegenstände und Dienste angeboten und gekauft werden können. Bezahlt werden Güter und Dienstleistungen mit einem Zahlungsmittel, beispielsweise Geld oder Gold. Die Zahlungsmittel können für reales Geld gekauft werden (RMT).

Land kaufen/mieten

Der EVG stellt eine Funktion zur Verfügung, die es dem Nutzer erlaubt Land zu kaufen oder zu mieten. Auf dem Land hat der Nutzer das Recht Gegenstände (z.B. Häuser, Bäume) zu erbauen und dieses Verhalten zu programmieren (Bäume bewegen sich im Wind).

8.1.3 Zusätzlich notwendige Hardware/Software/Firmware

Der clientseitige EVG befindet sich auf dem Endgerät des Nutzers. Über das Internet ist der Client mit dem serverseitigen EVG verbunden. Zur IT-Umgebung des clientseitigen EVG zählen die Teile des Endgerätes, die zur Verwendung des EVGs notwendig sind, wie beispielsweise die Hardware, das Betriebssystem und das Netzwerk in einer PC-Umgebung. Der serverseitige EVG wird auf dem Server des Anbieters betrieben. Zur IT-Umgebung des serverseitigen EVGs zählt neben der Hardware auch das das Betriebssystem des Servers und das Netzwerk in einer Rechenzentrumsumgebung. Das Netzwerk wird als nicht vertrauenswürdige Komponente angesehen. Dadurch entstehende Bedrohungen werden von den Anforderungen an den EVG vollständig abgedeckt.

8.2 Postulate zur Übereinstimmung

Das Schutzprofil postuliert Übereinstimmung mit Common Criteria Version 3.1 Release 1.

Das Schutzprofil stimmt mit Common Criteria Part 2 überein.

Das Schutzprofil stimmt mit Common Criteria Part 3 überein.

Das Schutzprofil unterstützt EAL-Stufe 2.

8.3 Definition des Sicherheitsproblems

Die Darlegung des Sicherheitsproblems umfasst die Sicherheitsaspekte der Umgebung, in der der EVG eingesetzt werden soll und beschreibt die erwartete Art des Gebrauchs. Sie umfasst all die organisatorischen Sicherheitspolitiken, die als relevant gelten. Zur Definition des Sicherheitsproblems gehören insbesondere die Bedrohungen der Sicherheit, die in der Umgebung vorhanden sind beziehungsweise von deren Vorhandensein ausgegangen wird.

Bei der Definition des Sicherheitsproblems wurde Folgendes berücksichtigt:

- die materielle Umgebung des EVG, die alle für die Sicherheit relevanten Aspekte der EVG-Einsatzumgebung angibt, einschließlich bekannter materieller und personeller Sicherheitsvorkehrungen
- die Werte, die Schutz durch die Bestandteile des EVG benötigen, für die die Sicherheitsanforderungen oder -politiken gelten werden.

8.3.1 Zu schützende Werte

- Avatar
- Gegenstände
- Zahlungsmittel
- Fertigkeiten
- Level/Erfahrungspunkte

- Welt
- Regeln
- Kommunikationsdaten
- Transaktionsdaten
- Logindaten
- Kontaktdaten
- Kontodaten
- Reputation

Subjekte

Folgende Subjekte sind in den EVG Prozess einbezogen:

- Nutzer
- Interessengruppen
- Anbieter
- Administratives Personal des Anbieters

Die folgenden Subjekte sind Angreifer, also Personen, die den ordnungsgemäßen Ablauf der EVG-Aufgabenstellungen zu stören, zu manipulieren oder zu verhindern versuchen.

- Netzwerkangreifer
- Nutzer
- Administratives Personal des Anbieters

8.3.2 Definition von Bedrohungen

Hier werden alle Bedrohungen gegen die zu schützenden Werte betrachtet, die bei der Bedrohungsanalyse als für den EVG relevant ermittelt werden. Die Common Criteria charakterisieren eine Bedrohung anhand ihrer Urheber, der Angriffe und der angegriffenen Werte. Urheber von Bedrohungen werden beschrieben, indem auf Aspekte wie Fachkenntnisse,

verfügbare Betriebsmittel und Motivation eingegangen wird. Angriffe werden beschrieben, indem Aspekte wie Angriffsmethode, Gelegenheiten und ausgenutzte Schwachstellen angesprochen werden.

Definitionen – Methode, Gelegenheit, Fachkenntnis

Methode – Ein Angriff wird als direkt bezeichnet, wenn der Angreifer durch dessen erfolgreiche Ausführung sein endgültiges Ziel (z.B. das Löschen von Datenbankeinträgen) direkt erreicht.

Gelegenheit – Ein Angriff wird als aktiv bezeichnet, wenn der Angriffszeitpunkt durch den Angreifer bestimmt werden kann, indem er aktiv ins Geschehen eingreift, beispielsweise durch Erzeugen, Löschen oder Verändern von Nachrichten auf dem Übertragungsweg. Das reine Mitlesen von Nachrichten zählt zu den passiven Angriffen.

Fachkenntnis und Verfügbare Betriebsmittel des Angreifers

1. Netzwerkangreifer

   Fachkenntnis: Profi

   Verfügbare Betriebsmittel: Betriebsmittel, die leicht zu beschaffen sind.

   Es wird von einem Angriffspotential ausgegangen, das nach Common Criteria Profiwissen voraussetzt, aber mit üblichem Equipment auskommt und auf die Fähigkeit zur Durchführung von Netzwerkangriffen (z.B. Man-in-the-Middle Angriffe) beschränkt ist.

   Ein Netzwerkangreifer ist ein Angreifer, der Daten auf dem Übertragungsweg mitliest, löscht, hinzufügt oder verändert. Der Netzwerkangreifer hat keinen physikalischen Zugang zum Endgerät des Nutzers.

2. Nutzer

   Fachkenntnis: Laie

   Verfügbare Betriebsmittel: clientseitiger EVG

3. Anbieter

   Fachkenntnis: Profi

   Verfügbare Betriebsmittel: serverseitiger EVG

T.UnbefugtesLesen

1. Ein Unbefugter [Zuweisung: Nutzer, Netzwerkangreifer] greift direkt in das Netzwerk ein, um vertrauliche Daten auf dem Übertragungsweg mitzulesen.
2. Einem Unbefugten gelingt es Datenbankeinträge zu lesen.

- Motivation:
  - Ein Nutzer möchte sich einen unberechtigten Vorteil verschaffen.
  - Ein Netzwerkangreifer möchte sich unberechtigt Informationen beschaffen (z.B. Sabotage, Spionage).
- Angriffsmethode: direkt
- Gelegenheit: passiv
- Ausgenutzte Schwachstelle: Kommunikationsnetz, Menschliches Verhalten, Authentisierungsverfahren
- Angegriffene Werte: Avatar, Gegenstände, Zahlungsmittel, Fertigkeiten, Welt, Kommunikationsdaten, Transaktionsdaten, Logindaten, Kontaktdaten, Kontodaten

T.UnbefugteModifikation

1. Ein Unbefugter [Zuweisung: Nutzer, Netzwerkangreifer] greift direkt in das Netzwerk ein, um Daten auf dem Übertragungsweg unbemerkt zu verändern.
2. Einem Unbefugten [Zuweisung: Nutzer, Netzwerkangreifer] gelingt es Datenbankeinträge zu manipulieren.

3. Administratives Personal nimmt unberechtigt Änderungen an Datenbankeinträgen vor.

4. Ein Nutzer verbreitet falsche Informationen in der Gemeinschaft.

- Motivation:
  - Ein Nutzer möchte sich einen unberechtigten Vorteil verschaffen oder einem anderen Nutzer schaden.
  - Ein Netzwerkangreifer möchte dem Anbieter schaden.
  - Administratives Personal nutzt die Position aus, um sich einen persönlichen Vorteil zu verschaffen.
- Angriffsmethode: direkt
- Gelegenheit: aktiv
- Ausgenutzte Schwachstelle: Netzwerk, Datenbank-Zugriffsberechtigung, Menschliches Verhalten, Authentisierungsverfahren
- Angegriffene Werte: Avatar, Gegenstände, Zahlungsmittel, Fertigkeiten, Level/EP, Welt, Regeln, Kommunikationsdaten, Transaktionsdaten, Logindaten, Kontaktdaten, Kontodaten, Reputation

T.UnbefugtesLöschen

1. Ein Unbefugter [Zuweisung: Nutzer, Netzwerkangreifer] greift direkt in das Netzwerk ein, um Daten auf dem Übertragungsweg unbemerkt zu löschen.

2. Einem Unbefugten [Zuweisung: Nutzer, Netzwerkangreifer] gelingt es Datenbankeinträge zu löschen.

3. Administratives Personal löscht unberechtigt Datenbankeinträge.

- Motivation:
  - Ein Nutzer möchte sich einen unberechtigten Vorteil verschaffen oder einem anderen Nutzer schaden.
  - Ein Netzwerkangreifer möchte Schaden anrichten.
  - Administratives Personal nutzt die Position aus, um sich einen persönlichen Vorteil zu verschaffen.
- Angriffsmethode: direkt
- Gelegenheit: aktiv
- Ausgenutzte Schwachstelle: Netzwerk, Datenbank-Zugriffsberechtigung, Menschliches Verhalten, Authentisierungsverfahren
- Angegriffene Werte: Avatar, Gegenstände, Zahlungsmittel, Fertigkeiten, Level/EP, Welt, Regeln, Kommunikationsdaten, Transaktionsdaten, Kontaktdaten, Kontodaten

T.VerlustVerfügbarkeit

Netzwerkangreifer führen zu viele Anfragen auf den Server aus oder lassen dies automatisiert durchführen.

- Motivation: Der Netzwerkangreifer möchte Schaden anrichten.
- Angriffsmethode: direkt
- Gelegenheit: aktiv
- Ausgenutzte Schwachstelle: Server
- Angegriffene Werte: Avatar, Gegenstände, Zahlungsmittel, Fertigkeiten, Level/EP, Welt, Regeln, Kommunikationsdaten, Transaktionsdaten, Logindaten, Kontaktdaten, Kontodaten

T.VerletzungDatenschutz

Unberechtigte erlangen Informationen über personenbezogene Daten.

- Motivation:
  - Der Anbieter gibt die Daten an unberechtigte Dritte weiter.
  - Die Nutzer sind zu freizügig mit ihren persönlichen Daten.
- Angriffsmethode: direkt
- Gelegenheit: aktiv
- Ausgenutzte Schwachstelle: Menschliches Verhalten, Machtposition
- Angegriffene Werte: Avatar, Gegenstände, Kommunikationsdaten, Transaktionsdaten, Logindaten, Kontaktdaten, Kontodaten, Reputation

T.AbstreitungHandlung

Einem Nutzer kann eine Aktion nicht zugeordnet werden (Transaktion, Kommunikation).

- Motivation: Ein Nutzer möchte sich einen Vorteil verschaffen.
- Angriffsmethode: indirekt
- Gelegenheit: passiv
- Ausgenutzte Schwachstelle: Fehlende Zuordenbarkeit von Aktionen
- Angegriffene Werte: Avatar, Gegenstände, Zahlungsmittel, Regeln, Kommunikationsdaten, Transaktionsdaten, Kontaktdaten, Kontodaten

8.3.3 Organisatorische Sicherheitspolitik

Die Organisatorische Sicherheitspolitik beinhaltet Aussagen über Regeln, Praktiken oder Richtlinien, welche vom EVG und seiner Umgebung befolgt werden müssen. Sie werden von der Organisation festgelegt, in der sich der EVG und seine Umgebung befinden.

Schutzprofilkonforme EVG müssen die organisatorischen Sicherheitspolitiken, welche im Folgenden beschrieben werden erfüllen:

P.Crypt

Alle verwendeten kryptografischen Verfahren müssen den aktuellen Anforderungen und Sicherheitsstandards entsprechen (z.B. Bundesnetzagentur/NIST anerkannte Algorithmen).

P.Beschwerdekanal

Den Nutzern muss eine Möglichkeit gegeben werden, Hinweise und Beschwerden an den Anbieter senden zu können. Es muss ein Beschwerdekanal eingerichtet werden.

P.Verhaltensregeln

Der Anbieter definiert Verhaltensregeln um einen fairen Umgang der Nutzer untereinander zu gewährleisten. Der Nutzer muss der Einhaltung der Regeln zustimmen. Der EVG muss die Voraussetzung für die Zustimmung schaffen. Der EVG muss sicherstellen, dass diese Regeln für alle Nutzer verständlich und wahrnehmbar sind.

P.Datenschutzrichtlinie

Der Anbieter definiert Datenschutzrichtlinien, die klarstellen, wie mit personenbezogenen Daten der Nutzer umgegangen wird. Der Anbieter verpflichtet sich zur Einhaltung der Richtlinien und insbesondere die Daten nicht an Dritte weiterzugeben.

P.HinweisWartung

Um einen guten Service anbieten zu können, müssen Wartungsarbeiten am Serversystem durchgeführt werden. Der Anbieter muss den Nutzer darüber informieren, dass es in regelmäßigen Abständen zu Wartungsarbeiten kommen kann. Der Nutzer muss über die ungefähre Dauer der Wartungsarbeiten informiert werden. Der EVG muss sicherstellen, dass diese Regeln für alle Nutzer verständlich und wahrnehmbar sind.

8.3.4 Annahmen

Dieser Teil beschreibt Annahmen, welche diesem Schutzprofil zugrunde liegen. Diese Annahmen decken die Sicherheitsaspekte der physischen und personellen Sicherheit ab.

Annahmen über technische Aspekte der Betriebsumgebung

A. Installation

Es wird angenommen, dass die Anwendungssoftware ordnungsgemäß installiert und initialisiert ist. Der Anbieter stellt für die Installation der Clientsoftware eine Installationsroutine zur Verfügung. Es wird vorausgesetzt, dass an der Software keine Manipulationen stattfinden.

A.Betriebssystem

Das dem EVG zugrunde liegende Betriebssystem bietet grundlegenden Schutz vor Softwarebedrohungen, für den EVG und das ganze System, durch eine integrierte/zusätzlich installierte Firewall sowie einen Virenscanner.

A.PhysSchutz

Es wird angenommen, dass der physische Schutz des Servers entsprechend des Wertes und der beinhalteten Daten ausgewählt wird.

A.Sanktionen

Für die Durchsetzung von fairem Verhalten bei den Nutzern setzt der Anbieter bei Regelverstößen Sanktionen ein. Es wird angenommen, dass die Sanktionen durchgesetzt werden können.

A.Verfügbarkeit

Die Robustheit, die Servicequalität und die Verfügbarkeit des Netzwerkes und des Servers sind gegeben.

Annahmen über personelle Aspekte der Betriebsumgebung

A.AuthDaten

Der Nutzer weiß, wie er mit seinem Identifikations- und seinem Authentisierungsmittel umzugehen hat und hält sich daran, d.h. er gibt diese insbesondere nicht an Dritte weiter.

A.Admin.1

Lokale Administratoren des Client-EVG versuchen nicht absichtlich die EVG Sicherheitspolitik, welche für die korrekte Funktionalität des EVG notwendig ist, zu verletzen.

A.Admin.2

Es wird angenommen, dass Administratoren vertrauenswürdige Personen sind. Der Anbieter unternimmt Aktionen, um die Vertrauenswürdigkeit der Administratoren zu prüfen. Dies muss zunächst beim Eintreten in das Unternehmen aber auch in regelmäßigen Abständen erfolgen.

A.Regeln

Es wird angenommen, dass sich die Nutzer den Regeln entsprechend verhalten.

A.Datenschutz

Es muss sichergestellt werden, dass personenbezogene Daten vertraulich behandelt werden und insbesondere nicht an Dritte weitergegeben werden. Der Anbieter verpflichtet sich, geltende Datenschutzrichtlinien durchzusetzen.

A.Awareness

Der Anbieter muss die Nutzer über mögliche Gefahren innerhalb der Virtuellen Welt (z.B. Phishing Angriffe) aufklären. Der Anbieter führt daher in regelmäßigen Abständen Awareness-Maßnahmen in geeigneter Art und Weise durch. Der EVG kann diese Maßnahme unterstützen, indem er die relevanten Informationen deutlich wahrnehmbar anzeigt.

8.4 Sicherheitsziele

Dieses Kapitel beschreibt die Sicherheitsziele des EVG und die der Einsatzumgebung des EVG. Die Sicherheitsziele werden geteilt in EVG-Sicherheitsziele (Sicherheitsziele, welche direkt an den EVG gestellt werden) und Sicherheitsziele für die Einsatzumgebung des EVG (Sicherheitsziele, welche an das IT-Umfeld oder an nicht-technische oder ablauforientierte Belange gerichtet sind).

8.4.1 Sicherheitsziele für den EVG

O.AuthNutzer

Der EVG soll sicherstellen, dass sich alle Nutzer identifizieren und authentisieren, bevor sie Zugang zum EVG erhalten.

O.ZugriffDB

Der EVG soll sicherstellen, dass der Zugriff zur Datenbank beschränkt wird. Der EVG stellt die Durchsetzung einer Zugriffskontrollpolitik sicher, indem er Zugriffsrechte unterstützt.

O.GeheimeNachricht

Der EVG soll sicherstellen, dass die Daten, die zwischen Client und Server übertragen werden, vertraulich bleiben. Unter Verwendung eines geschützten Kommunikationspfades stellt der EVG sicher, dass unberechtigt keine Daten gelesen werden können.

O.IntegritätNachricht

Der EVG soll sicherstellen, dass Daten, die zwischen Client und Server übertragen werden, nicht unberechtigt verändert werden können. Der EVG verwendet einen geschützten Kommunikationspfad, sodass Daten zwischen Client und Server nicht unberechtigt verändert oder gelöscht werden können.

O.DBCheck

Der EVG soll sicherstellen, dass eine Plausibilitätsprüfung durchgeführt wird bevor Daten endgültig in die Datenbank geschrieben werden.

O.Regeln

Der EVG soll sicherstellen, dass der Anbieter vom Nutzer eine Zustimmung zu den geltenden (Verhaltens-)Regeln verlangen kann. Eine Zustimmung zu den Regeln setzt voraus, dass den Nutzern die Regeln zugänglich und bekannt sind. Der EVG muss Mechanismen enthalten, die eine Bekanntmachung der Regeln und eine Zustimmung der Nutzer zu den Regeln unterstützten.

O.EinreichenBeschwerde

Zur Sicherstellung eines fairen Umgangs in der Virtuellen Welt, soll der EVG sicherstellen, dass Beschwerden eingereicht werden können.

O.KenntnisBeschwerde

Der EVG soll sicherstellen, dass eine verantwortliche Stelle Kenntnis über eine Beschwerde erlangen kann, um den Beschwerden nachgehen zu können.

O.NichtabstreitbarkeitTR

Der EVG soll sicherstellen, dass Transaktionen nicht abstreitbar sind. Dazu stellt der EVG eine Funktionalität zur Verfügung mithilfe derer Nachweise für die Durchführung einer Transaktion (auf Anfrage) erzeugt werden können.

O.VollständigkeitTR

Der EVG soll sicherstellen, dass für Transaktionen nur konsistente Datenzustände erzeugt werden. Der EVG stellt sicher, dass Transaktionen nur vollständig durchgeführt werden. Bei Störungen stellt der EVG den konsistenten Zustand vor Durchführung der Transaktion wieder her.

O.NichtabstreitbarkeitKommunikation

Der EVG soll sicherstellen, dass der Inhalt einer Kommunikation nichtabstreitbar ist. Dazu stellt der EVG eine Funktionalität zur Verfügung mithilfe derer Nachweise für die Kommunikation (auf Anfrage) erzeugt werden können.

O.Pseudonym

Der EVG stellt sicher, dass der Nutzer unter einem Pseudonym auftreten kann.

O.Zeitstempel

Der serverseitige EVG stellt verlässliche Zeitstempel zur Verfügung. Die Zeitstempel müssen gewährleisten, dass die tatsächliche Reihenfolge von Aktionen und der Zeitpunkt von Aktionen ausreichend genau festgestellt werden kann.

8.4.2 Sicherheitsziele für die Einsatzumgebung

OE.Installation

Der Nutzer stellt sicher, dass die Anwendungssoftware ordnungsgemäß installiert ist.

OE.Betriebssystem

Das Betriebssystem bietet Schutzmöglichkeiten vor Schadsoftware.

OE.PhysSchutz

Die Umgebung bietet physischen Schutz und Zugriffskontrollmechanismen, sodass es nur autorisierten Personen gestattet ist, auf den Server-EVG zuzugreifen.

OE.Sanktionen

Eine zuständige Stelle (Teil der Systemumgebung) stellt sicher, dass bei Regelverstößen Sanktionen gegen Nutzer durchgesetzt werden können.

OE.Verfügbarkeit

Die Robustheit, Servicequalität und Verfügbarkeit des Netzwerks und des Anbieterservers müssen ausreichend hoch sein, um einen reibungslosen Service zu ermöglichen. Die Wahl des Netzwerks liegt in der Verantwortung des Anbieters. Der Anbieter sorgt dafür, dass die Verfügbarkeit des Servers und seiner Netzwerkanbindung bei Störungen und Ausfällen mit angemessenem Service Level wiederhergestellt wird. Der Anbieter legt fest, wie das Netzwerk und der Server überwacht und Störungen oder Ausfälle feststellt, und mit welchen Maßnahmen den Störungen oder Ausfällen begegnet werden soll. Für Probleme mit der Robustheit, Servicequalität und Verfügbarkeit des Netzwerks oder des Servers, die nicht in angemessener Zeit behoben werden können, definiert der Anbieter geeignete Notfallszenarios.

OE.AuthDaten

Nur berechtigte Nutzer sind im Besitz der notwendigen Identifikations- und Authentifikationsmerkmale.

OE.Admin.1

Der Nutzer stellt sicher, dass lokale Administratoren des Client-EVG keine Veränderung an der EVG-Funktionalität vornehmen.

OE.Admin.2

Der Anbieter sorgt dafür, dass nur vertrauenswürdige Personen als Administratoren eingestellt werden und dass sie ausreichend geschult sind.

OE.Regeln

Der Nutzer stellt sicher, dass ihm die Regeln bekannt sind und sein Verhalten richtet sich nach den Regeln.

OE.Datenschutz

Der Anbieter sorgt dafür, dass personenbezogene Daten nicht weitergegeben werden. Der Anbieter hält sich an die Datenschutzrichtlinien.

OE.Awareness

Der Anbieter führt Awareness-Maßnahmen durch.

8.4.3 Erklärung der Sicherheitsziele

Abdeckung der Annahmen

	OE.Installation	OE.Betriebssystem	OE.PhysSchutz	OE.Sanktionen	OE.Verfügbarkeit	OE.AuthDaten	OE.Admin.1	OE.Admin.2	OE.Regeln	OE.Datenschutz	OE.Awareness
A.Installation	x										
A.Betriebssystem		x									
A.PhysSchutz			x								
A.Sanktionen				x							
A.Verfügbarkeit					x						
A.AuthDaten						x					
A.Admin.1							x				
A.Admin.2								x			
A.Regeln									x		
A.Datenschutz										x	
A.Awareness											x

Tabelle 8.1: Abdeckung der Annahmen

Abwehr der Bedrohungen

	T.UnbefugteModifikation	T.UnbefugtesLöschen	T.UnbefugtesLesen	T.VerlustVerfügbarkeit	T.VerletzungDatenschutz	T.AbstreitungHandlung
O.AuthNutzer	x	x	x		x	x
O.ZugriffDB	x	x	x		x	
O.GeheimeNachricht			x		x	
O.IntegritätNachricht	x	x				x
O.DBCheck				x		
O.Regeln						
O.EinreichenBeschwerde						
O.KenntnissBeschwerde						
O.NichtabstreitbarkeitTR						x
O.VollständigkeitTR				x		x
O.NichtabstreitbarkeitKommunikation						x
O.Pseudonym					x	
O.Zeitstempel						x
OE.Installation	x	x	x	x		
OE.Betriebssystem	x	x	x			
OE.PhysSchutz	x	x	x	x		
OE.Sanktionen						
OE.Verfügbarkeit				x		
OE.AuthDaten	x	x	x			
OE.Admin.1						
OE.Admin.2				x		
OE.Regeln						
OE.Datenschutz					x	
OE.Awareness	x	x	x		x	

Tabelle 8.2: Abwehr der Bedrohungen

8.5 IT Sicherheitsanforderungen

Die IT-Sicherheitsanforderungen sind die Verfeinerung der Sicherheitsziele in eine Menge von Sicherheitsanforderungen an den EVG, die im Falle ihrer Erfüllung sicherstellen, dass der EVG seine Sicherheitsziele erfüllen kann. Die Sicherheitsanforderungen enthalten sowohl Anforderungen an das Vorhandensein des gewünschten Verhaltens als auch Anforderungen an die Abwesenheit des unerwünschten Verhaltens.

8.5.1 Funktionale EVG-Sicherheitsanforderungen

Die funktionalen Sicherheitsanforderungen des EVG enthalten die folgenden Komponenten aus Teil 2 der Common Criteria.

FAU: Sicherheitsprotokollierung

FAU_GEN.1 Generierung der Protokolldaten
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

FAU_GEN.1.1 Die TSF[1] müssen in der Lage sein, für folgende protokollierbare Ereignisse eine Protokollaufzeichnung zu generieren:
a) Starten und Beenden der Protokollierungsfunktionen;
b) Alle protokollierbaren Ereignisse für den Protokollierungsgrad

$$Auswahl : Minimal, Einfach, Detailliert, nichtangegeben$$

und
c) [Zuweisung: sonstige speziell festgelegte protokollierbare Ereignisse].

FAU_GEN.1.2 Die TSF müssen innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:

[1] TOE Security Functions, deutsch: EVG-Sicherheitsfunktionen

a) Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjekts und das Ergebnis (Erfolg oder Misserfolg) des Ereignisses; und
b) basierend auf den Definitionen der in PP/ST eingebundenen protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen [Zuweisung: sonstige protokollierungsrelevante Information].

FAU_GEN.2 Verknüpfung der Benutzeridentität
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten, FIA_UID.1 Zeitpunkt der Identifikation

FAU_GEN.2.1 Die TSF müssen in der Lage sein, jedes protokollierbare Ereignis mit der Identität desjenigen Benutzers zu verknüpfen, der dieses Ereignis verursacht hat.

FAU_ARP.1 Sicherheitsalarme
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FAU_SAA.1 Analyse von möglichen Verletzungen

FAU_ARP.1.1 Die TSF müssen [Zuweisung: Liste der am wenigsten störenden Aktionen] bei Erkennen einer potentiellen Sicherheitsverletzung ausführen.

FAU_SAA.1 Analyse von möglichen Verletzungen
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

FAU_SAA.1.1 Die TSF müssen in der Lage sein, beim Überwachen der protokollierten Ereignisse eine Menge von Regeln anzuwenden und auf Grundlage dieser Regeln eine potentielle Verletzung der TSP anzuzeigen.

FAU_SAA.2 Profilbasierende Erkennung von Anomalien
Ist hierarchisch zu: FAU_SAA.1 Störfallanalyse

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FAU_SAA.2.2 Die TSF müssen in der Lage sein, für jeden Benutzer, dessen Aktivitäten in einem Profil aufgezeichnet werden, einen Verdachtswert zu erhalten. Dieser Verdachtswert stellt dar, inwieweit die augenblickliche Aktivität des Benutzers inkonsistent zu den ermittelten, im Profil dargestellten Nutzungsmustern ist.

FAU_SAR.1 Durchsicht der Protokollierung
Ist hierarchisch zu: Keinen anderen Komponenten.
Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

FAU_SAR.1.1 Die TSF müssen für [Zuweisung: autorisierte Benutzer] die Fähigkeit bereitstellen, [Zuweisung: Liste der Protokollinformationen] aus den Protokollaufzeichnungen zu lesen.
FAU_SAR.1.2 Die TSF müssen die Protokollaufzeichnungen in einer für die Interpretation der Informationen durch den Benutzer geeigneten Art und Weise bereitstellen.

FCO: Kommunikation/Nichtabstreitbarkeit

FCO_NRO.1 Selektiver Urheberschaftsbeweis

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FCO_NRO.1.1 Die TSF müssen auf Anforderung des [Auswahl: Urhebers, Empfängers, [Zuweisung: Liste Dritter]] für übertragene [Zuweisung: Liste der Informationsarten] Urheberschaftsnachweise generieren können.

FCO_NRO.2 Erzwungener Urheberschaftsbeweis

Ist hierarchisch zu: FCO_NRO.1

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FCO_NRO.2.1 Die TSF müssen für übertragene [Zuweisung: Liste der Informationsarten] die Generierung des Urheberschaftsnachweises zu jeder Zeit erzwingen.

FCO_NRR.1 Selektiver Empfangsbeweis

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FCO_NRR.1.1 Die TSF müssen auf Anforderung des [Auswahl: Urhebers, Empfängers, [Zuweisung: Liste Dritter]] für empfangene [Zuweisung: Liste der Informationsarten] Empfangsnachweise generieren können.

FCS: Kryptografische Unterstützung

FCS_COP.1 Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute

oder

FCS_CKM.1 Kryptographische Schlüsselgenerierung]

FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

FMT_MSA.2 Sichere Sicherheitsattribute

FCS_COP.1.1 Die TSF müssen [Zuweisung: Liste der kryptographischen Operationen] gemäß eines spezifizierten kryptographischen Algorithmus [Zuweisung: kryptographischer Algorithmus] und kryptographischer Schlüssellängen [Zuweisung: kryptographische Schlüssellänge], die den folgenden [Zuweisung: Liste der Normen] entsprechen, durchführen.

FDP: Schutz der Benutzerdaten

FDP_ACC.1 Teilweise Zugriffskontrolle

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

FCO_ACC.1.1 Die TSF müssen die [Zuweisung: SFP für Zugriffskontrolle] für [Zuweisung: Liste der Subjekte, Objekte und der durch die SFP abgedeckten Operationen zwischen Subjekten und Objekten] durchsetzen.

FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FDP_ACC.1 Teilweise Zugriffskontrolle, FMT_MSA.3 Initialisierung statischer Attribute

FCO_ACF.1.1 Die TSF müssen die [Zuweisung: SFP für Zugriffskontrolle] für Objekte, die auf [Zuweisung: Sicherheitsattribute, genannte Gruppen von Sicherheitsattributen] basieren, durchsetzen.

FDP_ITT.1 Einfacher Schutz des internen Transfers

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

FDP_ITT.1.1 Die TSF müssen die [Zuweisung: für SFPs für Zugriffskontrolle und/oder SFPs für Informationsflusskontrolle] durchsetzen, um [Auswahl: Preisgabe, Modifizierung, Zugangsverlust] von Benutzerdaten zu verhindern, wenn diese zwischen materiell getrennten Teilen des EVG übertragen werden.

FDP_ROL.1 Einfaches Rückgängig

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

FDP_ROL.1.1 Die TSF müssen die [Zuweisung: SFPs für Zugriffskontrolle und/oder SFPs für Informationsflusskontrolle] für das Erlauben von Rückgängigmachen der [Zuweisung: Liste der Operationen] für [Zuweisung: Liste der Objekte] durchsetzen. FDP_ROL.1.2 Die TSF müssen das Rückgängigmachen von Operationen innerhalb [Zuweisung: Grenze für das Rückgängigmachen] erlauben.

FDP_SDI.2 Überwachung der Integrität der gespeicherten Daten und Reaktionen

Ist hierarchisch zu: FDP_SDI.1

Abhängigkeiten: Keine Abhängigkeiten.

FDP_SDI.2.1 Die TSF müssen die innerhalb des TSC[2] gespeicherten Benutzerdaten auf [Zuweisung: Integritätsfehler] bei allen Objekten auf Basis folgender Attribute: [Zuweisung: Benutzerdaten- Attribute] überwachen.

FDP_SDI.2.2 Bei Erkennen eines Datenintegritätsfehlers müssen die TSF [Zuweisung: auszuführende Aktion].

[2]TSF Scope of Control — Anwendungsbereich der TSF-Kontrolle

FIA: Identifikation und Authentifizierung

FIA_AFL.1 Handhabung von Authentisierungsfehlern

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FIA_UAU.1 Zeitpunkt der Authentisierung

FIA_AFL.1.1 Die TSF müssen erkennen, wenn [Zuweisung: Anzahl] misslungene Authentisierungsversuche auftreten, die in Bezug zu [Zuweisung: Liste der Authentisierungsereignisse] stehen.

FIA_AFL.1.2 Wenn die definierte Anzahl von fehlgeschlagenen Authentisierungsversuchen erreicht oder überschritten wird, müssen die TSF [Zuweisung: Liste der Aktionen].

FIA_UAU.2 Benutzerauthentisierung vor jeglicher Aktion

Ist hierarchisch zu: FIA_UAU.1 Zeitpunkt der Authentisierung.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FIA_UAU.2.1 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

Ist hierarchisch zu: FIA_UID.1 Zeitpunkt der Identifikation.

Abhängigkeiten: Keine Abhängigkeiten.

FIA_UID.2.1 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

FMT: Security Management

FMT_MSA.1 Management der Sicherheitsattribute

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

FMT_SMR.1 Sicherheitsrollen

FMT_MSA.1.1 Die TSF müssen die [Zuweisung: SFP für Zugriffskontrolle, SFP für Informationsflusskontrolle] zur Beschränkung der Fähigkeit zum [Auswahl: Standardvorgabe ändern, Abfragen, Modifizieren, Löschen, [Zuweisung: andere Operationen]] der Sicherheitsattribute [Zuweisung: Liste der Sicherheitsattribute] auf [Zuweisung: die autorisierten identifizierten Rollen] durchsetzen.

FMT_MSA.3 Initialisierung statischer Attribute

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FMT_MSA.1 Management der Sicherheitsattribute, FMT_SMR.1 Sicherheitsrollen

FMT_MSA.3.1 Die TSF müssen die [Zuweisung: SFP für Zugriffskontrolle, SFP für Informationsflusskontrolle] zur Bereitstellung von vorgegebenen Standardwerten mit [Auswahl: einschränkenden, freizügigen, anderen Eigenschaften] für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

FMT_SMR.1 Sicherheitsrollen

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FMT_SMR.1.1 Die TSF müssen die Rollen [Zuweisung: die autorisierten identifizierten Rollen] erhalten.

FMT_SMR.1.2 Die TSF müssen Benutzer mit Rollen verknüpfen können.

FMT_SMR.2 Einschränkungen der Sicherheitsrollen

Ist hierarchisch zu: FMT_SMR.1

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FMT_SMR.2.3 Die TSF müssen sicherstellen, dass die Bedingungen [Zuweisung: Limitierung der Login-Versuche für alle Rollen] erfüllt werden.

FPR: Privacy

FPR_PSE.1 Pseudonymität

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: Keine Abhängigkeiten

FPR_PSE.1.1 Die TSF müssen sicherstellen, dass [Zuweisung: Benutzer- und/oder Subjektmenge] nicht in der Lage sind, den mit [Zuweisung: Liste der Subjekte und/oder Operationen und/oder Objekte] verbundenen tatsächlichen Benutzernamen festzustellen.

FPT: Schutz der EVG Sicherheitsfunktionen

FPT_STM.1 Verlässliche Zeitstempel

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: Keine Abhängigkeiten

FPT_STM.1.1 Die TSF sollen einen verlässlichen Zeitstempel für den Eigengebrauch bereitstellen.

FTA: EVG Zugriff

FTA_TAB.1 Vorgegebene EVG-Zugriffswarnmeldung

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: Keine Abhängigkeiten

FTA_TAB.1.1 Vor Einrichtung einer Benutzersitzung müssen die TSF einen beratenden Warnhinweis für den nicht autorisierten Gebrauch des TOE (EVG) anzeigen.

FTA_TSE.1 EVG-Sitzungseinrichtung

Ist hierarchisch zu: Keinen anderen Komponenten.

Abhängigkeiten: Keine Abhängigkeiten

FTA_TSE.1.1 Die TSF müssen in der Lage sein, basierend auf [Zuweisung: Attribute] eine Sitzungseinrichtung zu verweigern.

Abdeckung der Sicherheitsziele des EVG

	O.AuthNutzer	O.ZugriffDB	O.GeheimeNachricht	O.IntegritätNachricht	O.DBCheck	O.Regeln	O.EinreichenBeschwerde	O.KenntnissBeschwerde	O.NichtabstreitbarkeitTR	O.VollständigkeitTR	O.Pseudonym	O.Zeitstempel	O.NichtabstreitbarkeitKommunikation
FAU_ARP								x					
FAU_GEN							x		x				x
FAU_SAA								x					
FAU_SAR								x	x				
FCO_NRO									x				
FCO_NRR									x				
FCS_COP	x		x	x					x				
FDP_ACC		x	x	x									
FDP_ACF		x	x	x									
FDP_ITT			x	x	x								
FDP_ROL					x					x			
FDP_SDI					x								
FIA_AFL	x												
FIA_UAU	x												x
FIA_UID	x						x		x				x
FMT_MSA		x	x	x									
FMT_SMR		x	x	x									
FPR_PSE											x		
FPT_STM							x		x			x	x
FTA_TAB						x							
FTA_TSE						x							

Tabelle 8.3: Abdeckung der Sicherheitziele

8.5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in Tabelle 8.4 aufgeführt. Sie enthalten die Komponenten der Vertrauenswürdigkeitsstufe EAL2 aus Teil3 der Common Criteria.

Klasse	Bezeichnung	Beschreibung
ADV: Entwicklung	ADV_ARC.1	Beschreibung der Sicherheitsarchitektur
	ADV_FSP.2	Sicherheitsdurchsetzende Funktions-Spezifikation
	ADV_TDS.2	Basis Design
AGD: Handbücher	AGD_ADM.1	Systemverwalterhandbuch
	AGD_OPE.1	Benutzerhandbuch
	AGD_PRE.1	Vorbereitende Vorgänge
ALC:Lebenszyklus-Unterstützung	ALC_CMC.2	Verwendung eines CM[3] System
	ALC_CMS.2	Teile der EVG CM Abdeckung
	ALC_DEL.1	Vorgang der Auslieferung
ASE: Security Target[4]	ASE_CCL.1	Postulate zur Übereinstimmung
	ASE_ECD.1	Definition erweiterter Komponenten
	ASE_INT.1	ST Einführung
	ASE_OBJ.2	Sicherheitsziele
	ASE_REQ.2	Abgeleitete Sicherheitsanforderungen
	ASE_SPD.1	Definition des Sicherheitsproblems
	ASE_TSS.1	EVG-Definition Zusammenfassung
ATE: Tests	ATE_COV.1	Analyse der Testabdeckung
	ATE_FUN.1	Funktionales Testen
	ATE_IND.2	Unabhängiges Testen - Stichprobenartig
AVA: Schwachstellen- bewertung	AVA_VAN.2	Schwachstellenanalyse

Tabelle 8.4: EAL 2 [CCPart3 06]

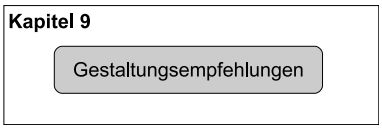
[3]Configuration Management

[4]Sicherheitsvorgaben

Kapitel 9

Empfehlungen für die Gestaltung von Sicherheitsmaßnahmen in Virtuellen Welten

Nach den Ausführungen der vorangehenden Kapitel stellt sich die Frage: wie können Sicherheitsanforderungen so umgesetzt werden, dass sie die Faktoren für Unterhaltungserleben berücksichtigen? Im vorliegenden neunten Kapitel werden Empfehlungen für die



Gestaltung von Sicherheitsmaßnahmen in Virtuellen Welten gegeben. In die Formulierung der Empfehlungen gehen Erkenntnisse aus den vorangegangenen Kapiteln ein, die im Folgenden kurz zusammengefasst werden.

9.1 Ausgangssituation

Im zweiten Kapitel wurde erläutert, was Virtuelle Welten sind und Beispiele existierender Welten wurden vorgestellt. Es wurde verdeutlicht, dass es verschiedene Arten von Virtuellen Welten gibt, z.B. Onlinerollenspiele wie World of Warcraft, Virtuelle Welten zur

Kommunikation wie Google Lively und primär handelsorientierte Welten wie Second Life. In allen Welten existieren reale Werte.

Das dritte Kapitel widmete sich der Erläuterung sozialer Faktoren. Es geht darauf ein, was Menschen motiviert Virtuelle Welten zu nutzen. Da Virtuelle Welten sozio-technische Systeme sind, ist es dringend erforderlich, bei der Umsetzung von technischen Sicherheitsmaßnahmen die Nutzerperspektive zu berücksichtigen. Das Verständnis sozialer Aspekte, insbesondere des Nutzerverhaltens, ist wichtig für die Akzeptanz der Sicherheitsfunktionen beim Nutzer. Nur so sind Sicherheitsexperten in der Lage geeignete Maßnahmen einzusetzen, die beim Nutzer Akzeptanz und Anwendung finden und so zum Schutz bedrohter Werte beitragen können.

Das sechste Kapitel umfasst die Analyse des Sicherheitsproblems Virtueller Welten und die Definition einer Sicherheitsstrategie. Es wurde gezeigt, welche Werte die Nutzer von Virtuellen Welten haben und wie diese bedroht werden können. Es gibt Maßnahmen, die zwar die Sicherheit des Systems erhöhen, bei einer Evaluation der Sicherheitsfunktionen aber nicht überprüft werden können (z.B. dass Benutzer ihre Zugangsdaten geheim halten). Die Sicherheitsstrategie legt fest, welche Annahmen daher bei der Umsetzung von Sicherheitsmaßnahmen getroffen werden müssen. Die Annahmen müssen als Sicherheitsziele für die Umgebung des Systems definiert werden. Außerdem müssen bei der Gestaltung von Sicherheitsmaßnahmen organisatorische oder gesetzliche Regelungen beachtet werden (Politiken). Auf Basis der Bedrohungsanalyse konnte festgelegt werden, welche Sicherheitsziele an das System formuliert werden müssen.

Um diese Ziele zu erfüllen, muss das System den Anforderungen gerecht werden. Die Sicherheitsanforderungen, die für Virtuelle Welten gelten müssen, sind aus dem Katalog der Common Criteria ausgewählt und im Kapitel 7 dargestellt worden.

Kapitel 8 fasst die Sicherheitsanalyse, die Definition der Sicherheitsstrategie und die Sicherheitsanforderungen entsprechend der Vorgaben der Common Criteria in einem Schutzprofil zusammen.

Die Empfehlungen für die Gestaltung von Sicherheitsmaßnahmen beruhen auf diesen Erkenntnissen. Sie beziehen sich auf die konkrete Umsetzung einiger ausgewählter Anforderungen (Kapitel 7), deren Basis die Definition der Sicherheitsstrategie ist. Die konkrete

Umsetzung muss aber immer die Faktoren für Unterhaltungserleben (vgl. Kapitel 3, Nutzerperspektive) berücksichtigen.

Die Empfehlungen für die Gestaltung der Sicherheitsmaßnahmen in Virtuellen Welten werden im Weiteren anhand einiger Szenarien für ausgewählte Anforderungen erläutert. Die folgenden Szenarien greifen exemplarisch Anforderungen heraus und zeigen, wie die Gestaltung von Sicherheitsmaßnahmen unter Berücksichtigung der Nutzerperspektive aussehen kann.

Es ist nicht allein ausreichend die technischen Sicherheitsfunktionen ordnungsgemäß umzusetzen. Mindestens ebenso wichtig ist die Anforderung, dass die Funktionen für den Benutzer handhabbar sind. Das betrifft die Funktionen, die Kontakt zum Benutzer erfordern.

9.2 Vorüberlegungen

Die Faktoren für Unterhaltungserleben wurden im theoretischen Erklärungsmodell zur Motivation der Nutzung hergeleitet. Die technischen Sicherheitsfunktionen des Systems müssen auf den Benutzer und sein Nutzungsverhalten angepasst umgesetzt werden. Dies führt zu einer höheren Akzeptanz der Sicherheitsfunktionen beim Nutzer und zu einer leichteren Benutzbarkeit der Systeme. Die Sicherheitsmechanismen sollten so umgesetzt werden, dass sie:

A. das Flow-Erlebnis nicht stören,

B. der Spielspaß nicht verloren geht,

C. dem Nutzer das Gefühl der Kontrolle gegeben wird,

D. nicht erfordern, dass der Spieler die Rahmung verlassen muss,

E. Lerneinheiten verwenden, um deren Anwendung zu vermitteln.

Punkt A.: Gelingt es dem Nutzer einer Virtuellen Welt Flow zu erleben, erreicht er eine Spannung zwischen den eigenen Fähigkeiten und vorgegebenen Herausforderungen.

Die Motivation der Nutzung ergibt sich hierbei aus der Tätigkeit selbst (intrinsisch) ohne einem Anreiz von außen (vgl. Kapitel 3). Dieses Erlebnis darf die Verwendung von Sicherheitsmaßnahmen nicht zerstören. Können Sicherheitsmechanismen so gestaltet werden, dass deren Anwendung intrinsisch motiviert ist - also aus der Tätigkeit selbst heraus - steigert dies das Flow-Erlebnis. Demzufolge wird der Nutzer durch die Anwendung von Sicherheitsmaßnahmen belohnt und akzeptiert diese.

Punkt B.: Spielspaß entsteht nach Koster bei der Anwendung von Mustern beim Lernen. Die Sicherheitsmaßnahmen können den Spielspaß unterstützen, wenn sie die Verwendung von Mustern einbeziehen. Instanzen von Mustern können so umgesetzt werden, dass Prozessschritte immer nach dem gleichen Schema ablaufen und ein vorausschaubares, gesetzmäßiges Design bei der Gestaltung des Prozesses berücksichtigt wird.

Punkt C.: Ein positives Unterhaltungserleben wird außerdem unterstützt, wenn dem Nutzer das Gefühl der Kontrolle gegeben wird. Dazu gehört eine Stabilität des Handlungsablaufes, auf die sich der Nutzer verlassen kann. Insbesondere bei der Beschreibung von Regeln für den gegenseitigen Umgang fördert eine Stabilität das positive Unterhaltungserleben. Wenn klar ist, welche Konsequenzen die Verletzung von Regeln hat, wird der Nutzer die Sanktionen eher akzeptieren.

Punkt D.: Wenn sich der Spieler in die Rahmung begibt - also ins Spiel eintaucht - darf er durch Sicherheitsmechanismen nicht herausgerissen werden. Ein Beispiel für eine schlechte Umsetzung wäre, dass der Spieler aus dem Spiel heraus auf eine externe Webseite umgeleitet wird, um beispielsweise eine Nutzerregistrierung oder Autorisierung vorzunehmen. Die Maßnahmen sollten vielmehr in den Handlungsablauf in der Virtuellen Welt eingebettet sein.

Punkt E.: Durch üben und lernen entwickeln die Nutzer Fähigkeiten. Die Anwendung von Sicherheitsmechanismen ist eine Fähigkeit, die der Nutzer eines Systems erlernen kann. Es ist wichtig die Sicherheitsfunktionen darauf auszulegen, dass der Nutzer deren Anwendung leicht erlernen kann.

9.3 Szenario: Vertrauliche Kommunikation

In den Anforderungen an das System (vgl. Kapitel 7) wurde festgelegt, dass es eine Funktionalität bereitstellen soll, die eine vertrauliche Kommunikation zwischen Client und Server gewährleistet, um eine unautorisierte Preisgabe vertraulicher Daten zu verhindern. Würde das System jedoch sämtlichen Datenverkehr zwischen Client und Server verschlüsseln, würde dies zu einer hohen Inanspruchnahme von Hardwareressourcen führen.

Um einen verzögerungsarmen Datentransfer zu gewährleisten, der für ein Immersionserlebnis wichtig ist, wird empfohlen eine vertrauliche Kommunikationssitzung bei Bedarf einzurichten. Daher soll eine Verschlüsselung von Daten nur dann erfolgen, wenn der Nutzer eine vertrauliche Kommunikation für erforderlich hält. Es ist wichtig, dass diese Funktion möglichst gut in die Virtuelle Welt eingebettet ist.

Um Nutzern den Prozess der Verschlüsselung zu verdeutlichen (vgl. Punkt E.), müssen die Verschlüsselungsfunktionen transparent und handhabbar gestaltet werden. Dies wäre der Fall, wenn entsprechende Symbole (wie z.B. Schloss, Schlüssel, Briefumschlag, etc.) der realweltlichen Analogie verwendet werden.

Es wird empfohlen eine Lerneinheit zu integrieren, mit der der Prozess der Verschlüsselung zunächst erlernt und erprobt werden kann und der Nutzer die Funktion im Bedarfsfall bereits kennt. Dies könnte zum Beispiel als Tutorial oder in Form einer Quest umgesetzt werden. Es ist wichtig, den Nutzer nicht zu überfordern aber auch nicht zu unterfordern (Spannung zwischen Herausforderung und Fähigkeiten, vgl. Kapitel 3). Eine Anpassung an die bereits vorhandene Erfahrung ist sinnvoll.

Virtuelle Welten haben die Chance IT-Sicherheit spielerisch zu verpacken. Die Nutzer können die Anwendung von Sicherheitsmaßnahmen spielerisch erlernen und später auch in anderen Anwendungen selbstverständlich nutzen.

9.4 Szenario: Identifikation und Authentisierung

Die Anforderungen in Kapitel 7 beschreiben die Notwendigkeit des Einsatzes von Maßnahmen zur Identifikation und Authentisierung. Derzeit sind dazu Benutzernamen und

Passwörter sehr verbreitet. Denkbar wären aber auch biometrische Merkmale (z.B. Fingerabdrücke, Iris, etc.) oder Chipkarten.

Eine Einbettung des Prozesses der Identifikation und Authentisierung in die Funktionen der Virtuellen Welt (z.B. den Spielablauf) kann dazu beitragen das Immersionserlebnis des Nutzers zu erhöhen.

Beispiel: Wünscht ein Nutzer eines Onlinespiels Zugang zur Virtuellen Welt, könnte er zunächst vor einer Burg stehen und um Einlass bitten. Die Wachen der Burg sind computergesteuerte Charaktere (NPCs) und fragen den Benutzer nach seinem Namen und einem Geheimcode. Wenn der Nutzer die Fragen der Wachen richtig beantwortet, wird ihm der Zugang zur Burg und zur Spielwelt gewährt. Die Rahmung (vgl. Punkt D.), d.h. der Login-Prozess, wird Teil des Spiels und kann beim Nutzer Spielspaß erzeugen.

9.5 Szenario: Fairness

Zur Gewährleistung von Fairness im Umgang der Teilnehmer untereinander legt der Anbieter Regeln fest, an die sich die Teilnehmer halten müssen. Die Regeln können nur wirksam werden, wenn die Nutzer die Regeln beachten. Um die Regeln anwenden zu können, müssen die Benutzer sie kennen und verstehen. Die Anforderungen legen fest, dass die Benutzer Zugang zu den Regeln haben müssen und ihnen zustimmen müssen (vgl. O.Regeln, Kapitel 6).

Eine benutzerfreundliche Umsetzung dieser Anforderung ist nur dann möglich, wenn die Nutzer die Informationen aufnehmen können ohne lange Texte lesen zu müssen. Die Hinweise müssen daher so gestaltet werden, dass sie schnell und ohne große Mühe aufgenommen und verstanden werden können.

Beispiel: Eine mögliche Umsetzung dieser Forderung könnte so gestaltet sein, dass der Nutzer beim Betreten der Welt von einem NPC oder einem Gamemaster angesprochen wird, der ihm eine kurze Einführung gibt. Betritt der Nutzer die Welt zum ersten Mal, kann diese Einführung etwas ausführlicher gestaltet sein, etwa so dass sie die ersten Schritte gemeinsam durchlaufen. Um aber erfahrene Nutzer nicht zu langweilen, ist es notwendig, dass der erfahrene Nutzer neue Herausforderungen erhält und sich nicht mit

Dingen befassen muss, die er schon kennt (vgl. Flow, Kapitel 3). Gibt es Änderungen bei den Regeln, reicht für erfahrene Nutzer eine kurze Information und das Einholen der Bestätigung.

Für die Wahrung der Fairness ist es außerdem erforderlich, dass es einen Beschwerdekanal gibt, um bei Regelverstößen handeln zu können. Aus Funktionssicht wird vom System verlangt, dass es beim Einreichen von Beschwerden Protokolldaten generiert, verlässliche Zeitstempel erzeugt und einen Alarm auslöst, sodass eine zuständige Stelle informiert wird und handeln kann. Auch hier ist eine Einbettung ins Spielgeschehen sinnvoll, um die Benutzerfreundlichkeit und das Immersionserlebnis positiv zu beeinflussen.

Beispiel: Die Einbettung könnte so gestaltet werden, dass die zuständige Stelle eine „Geschäftsstelle“ in der Virtuellen Welt hat, die der Nutzer aufsuchen kann, um eine Beschwerde vorzubringen. Dort könnte ein NPC oder Gamemaster die Beschwerde entgegennehmen.

Erachtet es die zuständige Stelle für notwendig Sanktionen gegen einen Nutzer zu verhängen, können diese auch in den „Alltag“ der Virtuellen Welt integriert werden.

Beispiel: Kann einem Spieler etwa nachgewiesen werden, dass er unfair agiert, etwa indem er beleidigende Äußerungen macht, erhält er einen Eintrag in seine „polizeiliche Führungsakte“, die von anderen Nutzern eingesehen werden kann. Je nach Schweregrad der Vergehen kann ein Nutzer auch ins virtuelle Gefängnis kommen, sodass er dem Geschehen außerhalb der Gefängniszelle nur zuschauen kann und keine Aktionen machen kann. So können einige Erziehungsmaßnahmen umgesetzt werden, um die Nutzer auf falsches Verhalten hinzuweisen. Die Sperrung des Accounts wird so nur durchgeführt, wenn alle anderen Sanktionen nicht greifen.

9.6 Szenario: Transaktionen

An die Sicherheitsfunktionen des Systems wurde das Ziel definiert Transaktionen nichtabstreitbar zu gestalten (O.NichtabstreitbarkeitTR). Deshalb wurde in den Anforderungen an das System festgelegt, dass es eine Funktionalität bereitstellen soll, die den Nachweis einer Aktion erzeugen kann (vgl. Kapitel 7). Urheberschaftsbeweise und Empfangs-

beweise werden mit kryptografischer Unterstützung mithilfe von Hashfunktionen und digitalen Signaturen erzeugt.

Es ist nicht notwendig und aus Ressourcengründen nicht zu empfehlen, bei allen Transaktionen einen Nachweis zu erzeugen. Ähnlich dem Szenario „Vertrauliche Kommunikation“ wird empfohlen Urheberschafts- und Empfangsbeweise auf Anfrage der Nutzer zu erzeugen.

Für ein ungestörtes Immersions- und Flow-Erlebnis der Nutzer kommt es auch bei der Gestaltung von Nachweisen darauf an, die kryptografischen Funktionen im Hintergrund, für den Nutzer unsichtbar, ablaufen zu lassen. Um dennoch eine Transparenz zu schaffen, sodass der Nutzer die Änderung erkennt, kann mit Symbolen aus der Realwelt gearbeitet werden und der eigentliche Prozess der Signatur in den Handlungsablauf integriert werden.

Beispiel: Ein Nutzer möchte ein wertvolles Gut, zum Beispiel ein virtuelles Gebäude, verkaufen und dabei die Sicherheitsfunktionen des Systems nutzen, um Nachweise über die Handelstransaktion zu erhalten. In Anlehnung an die reale Welt könnte diese Funktionalität als „Notariatsfunktion“ gestaltet sein, bei der beide Handelspartner einen Vertrag vorgelegt bekommen, um ihn mit ihrer digitalen Unterschrift (Signatur) zu unterzeichnen. Im Hintergrund erzeugt das System einen Hashwert des Dokuments und die digitalen Signaturen der Beteiligten.

Damit Nutzer diese Funktionalität benutzen können, müssen sie über die notwendigen Schlüssel verfügen. Um an die Schlüssel zu gelangen, müssen sich die Nutzer eindeutig identifizieren. Soll eine Identifizierung der realen Identität erfolgen, müssen Verfahren zum Einsatz kommen, die das leisten können. Denkbar wäre etwa die Identifizierung mithilfe des elektronischen Personalausweises oder des PostIdent-Verfahrens. Durch Lerneinheiten und Tutorials (Übungen unter Anleitung) wird das Verständnis des Nutzers für den Ablauf eines Prozesses erhöht.

9.7 Szenario: Awareness

Wie bereits in Kapitel 6 erläutert wurde, kann die Durchführung von Awareness-Maßnahmen nicht vom System verlangt werden. Ein kompetentes Verhalten der Nutzer

trägt aber dennoch in großem Maße zur Sicherheit eines Systems bei. Nutzer können sich nur kompetent verhalten, wenn sie die Gefahren kennen und wissen,welches Verhalten richtig ist. Dem Anbieter wird daher empfohlen, seine Nutzer über Sicherheitsgefahren aufzuklären und ihnen aufzuzeigen, welche Handlungen zu einem kompetenten Umgang mit dem System führen.

Das Ziel von Awareness-Maßnahmen ist, den Nutzer zu bewussten und kompetenten Entscheidungen zu befähigen. Die Vermittlung reinen Wissens reicht dafür jedoch nicht aus, sondern erfordert eine offene Kommunikation und eine permanente Auseinandersetzung über den Umgang mit Daten und den Sicherheitsfunktionalitäten (vgl. [Beyer 08]).

Beispiel: Für die Einbindung der Maßnahmen in den Handlungsablauf kann ein NPC den Nutzer bei den ersten Schritten in der Virtuellen Welt begleiten und ihn über die wichtigsten Gefahren aufklären. Alternativ ist die Umsetzung von Awareness-Maßnahmen innerhalb von Quests denkbar.

Es ist wichtig, dass Awareness-Maßnahmen auf keinen Fall so gestaltet werden, dass der Nutzer viel Text lesen muss. Es existieren bereits gute Umsetzungen von Awareness-Maßnahmen in der unternehmerischen Praxis, die als Vorbild für die Gestaltung wirken können (vgl. u.a. [Lardschneider 07], [Schimmer 07], [Mix 07]).

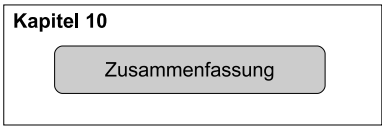
9.8 Szenario: Reputation

Um das Reputationsmanagement der Benutzer zu unterstützen sowie ihre Verlässlichkeit und Vertrauenswürdigkeit zu erhöhen, wird die Einführung eines Bewertungssystems empfohlen. Dort können sich, ähnlich dem Ebay-Vorbild, die Handelspartner gegenseitig bewerten. Das Bewertungssystem muss nicht auf Transaktionen beschränkt sein, sondern kann auch für gutes Verhalten Punkte vergeben bzw. für regelwidriges Verhalten Punktabzug durchsetzen, wobei auch hier wieder Missbrauch verhindert werden muss.

Die Bewertungen der Nutzer müssen für alle anderen Nutzer öffentlich zugänglich sein. Nur so kann Transparenz bezüglich der Vertrauenswürdigkeit der Nutzer erreicht werden.

Kapitel 10

Zusammenfassung



Abschließend beantwortet Kapitel 10 folgende Fragen:

- Welche Erkenntnisse wurden mit der vorliegenden Arbeit gewonnen?
- Wo liegen die Grenzen der Arbeit?
- Wo sieht die Autorin Ansätze für weitere Forschung (Ausblick)?

10.1 Erkenntnisse der Arbeit

Das Ziel der Arbeit ist die Empfehlung von Sicherheitsanforderungen an die Sicherheit Virtueller Welten. Da Virtuelle Welten sozio-technische Systeme sind, ist es notwendig nicht allein die technische Perspektive zu betrachten, sondern insbesondere auch das Nutzerverhalten zu berücksichtigen.

Daher wurde zunächst die Anwendungsdomäne untersucht und aktuelle Virtuelle Welten vorgestellt (vgl. Kapitel 2). Es wurde gezeigt, dass Virtuelle Welten unterschiedliche Handlungsziele erfüllen. Es gibt Virtuelle Welten, deren Fokus auf Unterhaltung liegt (z.B. Onlinerollenspiele, wie Guild Wars), Welten die auf Kommunikation ausgerichtet

sind (z.B. Google Lively) und Welten die den Handel mit virtuellen Gütern fokussieren (z.B. Second Life).

Die Motivation der Nutzung dieser Welten wurde in Kapitel 3 erläutert. Die Untersuchung verschiedener Perspektiven der Nutzungsmotivation hat ergeben, dass Menschen Handlungsziele verfolgen um ihre Bedürfnisse zu stillen. Virtuelle Welten stellen ein Angebot bereit die Handlungsziele zu erfüllen. Sie werden außerdem so gestaltet, dass sie Flow, Immersion, Kontrolle und Spaß unterstützen und die Entwicklung von Fähigkeiten (also Lernen) erlauben. Bei der Gestaltung von Sicherheitsmaßnahmen ist darauf zu achten, dass diese Faktoren für Unterhaltungserleben nicht gestört werden.

In allen Virtuellen Welten existieren Werte mit realer Relevanz, die vor Angriffen geschützt werden müssen. Die Werte wurden im Rahmen der Problemanalyse identifiziert und umfassen den Avatar, Gegenstände, Zahlungsmittel, Fertigkeiten, Level/Erfahrungspunkte, die Welt, die Regeln, Kommunikationsdaten, Transaktionsdaten, Logindaten, Kontaktdaten, Kontodaten und die Reputation der Nutzer. Diese Werte können durch Verlust oder Verletzung der Vertraulichkeit, Integrität, Verfügbarkeit, des Datenschutzes und der Nichtabstreitbarkeit bedroht werden. Es wurde gezeigt, dass bereits Angriffe durchgeführt werden, die genannte Bedrohungen realisieren.

Das Ziel der IT-Sicherheit ist der Schutz bedrohter Werte. Zur Bewertung von IT-Sicherheitsmaßnahmen in Produkten existieren Standards, die eine einheitliche Vorgehensweise bei der Bewertung erlauben. Da Virtuelle Welten auf ein internationales Publikum ausgelegt sind, kommt nur ein internationaler Standard infrage, um eine internationale Anerkennung von Evaluationsergebnissen zu gewährleisten. Die Common Criteria for Information Technology Security Evaluation wurden mit diesem Ziel realisiert und stellen einen Katalog mit Sicherheitsanforderungen bereit.

Aus dem Katalog der Common Criteria wurden Anforderungen an die Sicherheit Virtueller Welten ausgewählt, die zuvor definierte Sicherheitsziele abdecken. Sie betreffen unter anderem die Identifikation und Authentisierung der Nutzer, die kryptografische Unterstützung, die Erstellung von Beweisen und den sicheren Datenverkehr zwischen Client- und Server-Anwendungssoftware (EVG).

Aufgrund ihrer Beschaffenheit erlauben Virtuelle Welten eine gute Integration von Sicherheitsmaßnahmen in den Handlungsablauf. Das heißt, Sicherheitsmaßnahmen können so in die Welt eingebettet werden, dass für Nutzer die Handhabung ganz selbstverständlich erfolgt. Einige Beispiele möglicher Integration in den Handlungs- und Spielablauf wurden in Kapitel 9 dargestellt. Der Prozess der Identifikation und Authentisierung kann beispielsweise von virtuellen Charakteren visualisiert durchgeführt werden.

Virtuelle Welten bieten außerdem die Chance für Nutzer die Anwendung von IT-Sicherheitsmechanismen spielerisch zu lehren, wie beispielsweise die Verwendung von Verschlüsselungs- und Signaturverfahren. In Virtuellen Welten sind die Nutzer bereit sich ständig neuen Herausforderungen zu stellen und dadurch ihre Fähigkeiten zu entwickeln. So kann beispielsweise die Verschlüsselung einer Nachricht als Quest innerhalb eines Rollenspiels umgesetzt werden.

10.2 Grenzen der Arbeit und Ausblick

Neben diesen Erkenntnissen stößt die Arbeit auf Grenzen. Die Common Criteria sind ein sehr mächtiger Standard, der aber in der Praxis an Grenzen stößt. Die Definition von Anforderungen in einem Schutzprofil muss immer auch unter ökonomischen Gesichtspunkten erfolgen. Es ist nicht zielführend Anforderungen zu definieren, die bei den Entwicklern des Produkts nicht auf Akzeptanz stoßen oder deren technische Umsetzung einen zu hohen Aufwand in sich birgt.

Die Sicherheitsanforderungen in dieser Arbeit stellen daher nur einen Vorschlag dar, der für die spätere Erstellung eines evaluierbaren Schutzprofils dienen kann. Die Sicherheitsanforderungen basieren auf der Problemanalyse und der Definition des Sicherheitsproblems (vgl. Kapitel 6) und wurden so gewählt, dass sie die Sicherheitsziele erfüllen können.

Die Sicherheitsstrategie muss gemäß dem Wert der zu schützenden Güter (Werte, Assets) gestaltet werden. Bei der Definition zu hoher Anforderungen wird die Strategie kaum Akzeptanz erfahren (vornehmlich aus Kosten- und Zeitaufwandsgründen), bei zu niedrigen Anforderungen bleiben eventuell Sicherheitslücken offen.

Es wird von der Autorin als sinnvoll erachtet, dass die vorgeschlagenen Sicherheitsanforderungen in einem Forum mit Entwicklern von Virtuellen Welten, auch unter ökonomischen Gesichtspunkten, abgestimmt werden bevor sie in einem Schutzprofil festgeschrieben werden (zum Beispiel in Form eines Experten-Workshops).

Bevor das Schutzprofil offiziell eingesetzt werden kann, muss es zunächst durch eine zertifizierte Behörde, zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik, geprüft werden.

Des Weiteren muss festgehalten werden, dass eine Zertifizierung der Sicherheit keine transparente Aussage über die Sicherheit eines Produkts treffen kann. Potenzielle Kunden interessiert, wie sicher das Produkt ist. Diese Aussage kann aber nur durch Analyse der Evaluationsdokumentation von Experten beantwortet werden. Hier muss überlegt werden, wie der Zielgruppe die Aussagen über die Sicherheit des Produkts transparent gemacht werden können.

Außerdem entstehen für die Entwickler durch den hohen Evaluationsaufwand nicht unerhebliche Kosten. Insbesondere bei Virtuellen Welten kommt das Problem der Updates zum Tragen. Durch Erweiterungen oder Änderungen an der Software muss die Evaluierung in den entsprechenden Teilen wiederholt werden. Dazu wird empfohlen insbesondere die kritischen Kernelemente festzulegen, die für eine längere Zeit stabil bleiben. Stellt der Anbieter eine Aktualisierung der Software bereit, um für die Nutzer neue Quests zur Verfügung zustellen, betrifft dies nicht die Kernfunktionalität des vertraulichen Datenverkehrs.

Eine Leistung, die diese Arbeit nicht erbringen kann und will, ist die empirische Überprüfung der in Kapitel 3 zusammengestellten Perspektiven der Nutzungsmotivation und die Erforschung der Wirkung und Akzeptanz der in Kapitel 9 aufgestellten Szenarien. An dieser Stelle ist die sozialwissenschaftliche Forschung gefragt.

Diese Arbeit liefert keine Erkenntnisse mit welchem Risiko- und Werteverständnis das Online-Unterhaltungserleben beim Nutzer verbunden ist. Empfindet der Nutzer die identifizierten Werte als wertvoll und schützenswert? Erkennt er die existierenden Gefahren oder sind diese intransparent? Es ist sehr lohnenswert die Beantwortung dieser Fragen

in weiterer Anschlussforschung zu verfolgen. Diese Arbeit eröffnet den Weg zu weiterer interdisziplinärer Forschung zwischen Informatik und Sozialwissenschaft.

Die verzahnte Betrachtung von Nutzerverhalten und technischen Möglichkeiten stellt insbesondere auch eine Herausforderung für Entwickler dar. Die heutige Ausbildung an Universitäten, zum Beispiel im Fach Informatik, ist oftmals noch sehr auf ein Fach fokussiert. Um aber Systeme für Menschen entwickeln zu können, müssen die Entwickler bereits während des Studiums eine interdisziplinäre Ausbildung erhalten und die Betrachtung sozio-technischer Systeme in den Mittelpunkt rücken. Auch die Methoden und Vorgehensmodelle (z.B. Wasserfallmodell, V-Modell, etc.) zur Entwicklung von sozio-technischen Systemen müssen um die Komponente „Nutzerverhalten“ erweitert werden.

Auch im Katalog der Common Criteria fehlt die Benutzersicht völlig. Sicherheitsfunktionen können aber nur wirken, wenn sie von den Benutzern akzeptiert und angewandt werden. Daher schlägt die Autorin die Erweiterung der Common Criteria um eine Anforderungsklasse FUF (User Friendly) vor, um Anforderungen zur Benutzerfreundlichkeit zu definieren. Für den Entwurf dieser Anforderungsklasse müssen die Erkenntnisse der Usability-Forschung Berücksichtigung finden. Insbesondere ließen sich aus einer breiteren Masse von Anwendungssoftware gemeinsame und allgemeingültige Anforderungen zur Benutzerfreundlichkeit ableiten.

Anhang A

T.*	**Bedrohungen**
T.UnbefugtesLesen	Unbefugte können Daten lesen
T.UnbefugteModifikation	Unbefugte können Daten verändern
T.UnbefugtesLöschen	Unbefugte können Daten löschen
T.VerlustVerfügbarkeit	Angreifer führen (automatisiert) zu viele Anfragen auf den Server aus
T.VerletzungDatenschutz	Unberechtigte erlangen Informationen über personenbezogene Daten
T.AbstreitungHandlung	Einem Nutzer kann eine Aktion nicht zugeordnet werden
P.*	**Organisatorische Sicherheitsrichtlinien**
P.Crypt	Verwendung kryptografischer Standards
P.Beschwerdekanal	Einrichten eines Beschwerdekanals
P.Verhaltensregeln	Definition von Verhaltensregeln
P.HinweisWartung	Informationen über Wartungsarbeiten bereitstellen
P.Datenschutzrichtlinie	Definition einer Datenschutzrichtlinie
A.*	**Annahmen**
A.Installation	Ordnungsmäßige Installation und Initialisierung der Anwendung
A.Betriebssystem	Betriebssystem bietet grundlegenden Schutz vor Softwarebedrohungen
A.PhysSchutz	Physischer Schutz des Servers
A.Zeitstempel	Bereitstellung verlässlicher Zeitstempel
A.Sanktionen	Durchsetzbarkeit von Sanktionen
A.Verfügbarkeit	Verfügbarkeit des Netzwerkes und des Servers sind gegeben
A.AuthDaten	Nutzer hält Identifikations- u. Authentisierungsmittel geheim
A.Admin.1	Administratoren des Client-EVG verletzen nicht absichtlich die EVG Sicherheitspolitik
A.Admin.2	Administratoren des EVG sind vertrauenswürdig
A.Regeln	Dem Nutzer sind die Regeln zugänglich und bekannt
A.Datenschutz	Personenbezogene Daten werden vertraulich behandelt
A.Awareness	Der Anbieter führt Awarenessmaßnahmen durch
O.*	**Sicherheitsziele für den EVG**
O.AuthNutzer	Alle Nutzer identifizieren und authentisieren sich
O.ZugriffDB	Zugriff auf Datenbank wird beschränkt
O.GeheimeNachricht	Vertraulichkeit der Daten bei Übertragung zwischen Client und Server
O.IntegritätNachricht	Integrität der Daten bei Übertragung zwischen Client und Server
O.DBCheck	Durchführung Plausibilitätsprüfung vor Datenbankeintrag
O.Regeln	Zustimmung des Nutzers zu geltenden (Verhaltens-)Regeln
O.EinreichenBeschwerde	Beschwerden können eingereicht werden
O.KenntnissBeschwerde	Kenntnis der Verantwortlichen über eine Beschwerde
O.NichtabstreitbarkeitTR	Transaktion ist nicht abstreitbar
O.VollständigkeitTR	Transaktion wird nur vollständig ausgeführt
O.NichtabstreitbarkeitKomm.	Kommunikation ist nicht abstreitbar
O.Pseudonym	Der Nutzer kann unter einem Pseudonym auftreten
O.Zeitstempel	EVG stellt Zeitstempel zur Verfügung
OE.*	**Sicherheitsziele für die Einsatzumgebung**
OE.Installation	Ordnungsmäßige Installation und Initialisierung der Anwendung
OE.Betriebssystem	Betriebssystem bietet grundlegenden Schutz vor Softwarebedrohungen
OE.PhysSchutz	Physischer Schutz des Servers
OE.Zeitstempel	Bereitstellung verlässlicher Zeitstempel
OE.Sanktionen	Durchsetzbarkeit von Sanktionen
OE.Verfügbarkeit	Verfügbarkeit des Netzwerkes und des Servers sind gegeben
OE.AuthDaten	Nutzer hält Identifikations- u. Authentisierungsmittel geheim
OE.Admin.1	Administratoren des Client-EVG verletzen nicht absichtlich die EVG Sicherheitspolitik
OE.Admin.2	Administratoren des EVG sind vertrauenswürdig
OE.Regeln	Dem Nutzer sind die Regeln zugänglich und bekannt
OE.Datenschutz	Personenbezogene Daten werden vertraulich behandelt
OE.Awareness	Der Anbieter führt Awarenessmaßnahmen durch

Tabelle A.1: Sicherheitsstrategie

FAU: Sicherheitsprotokollierung/Audit	
FAU_ARP	Security Audit Automatic Response
FAU_GEN	Generierung der Sicherheitsprotokolldaten
FAU_SAA	Analyse der Sicherheitsprotokollierung
FAU_SAR	Durchsicht der Sicherheitsprotokollierung
FCO: Kommunikation	
FCO_NRO	Nichtabstreitbarkeit der Urheberschaft
FCO_NRR	Nichtabstreitbarkeit des Empfangs
FCS: Kryptografische Unterstützung	
FCS_COP	Kryptographischer Betrieb
FDP: Schutz der Benutzerdaten	
FDP_ACC	Zugriffskontrollpolitik
FDP_ACF	Zugriffskontrollfunktionen
FDP_ITT	EVG-interner Transfer
FDP_ROL	Rückgängig
FDP_SDI	Integrität der gespeicherten Daten
FIA: Identifikation und Authentifizierung	
FIA_AFL	Authentisierungsfehler
FIA_UAU	Benutzerauthentisierung
FIA_UID	Benutzeridentifikation
FMT: Sicherheits-Management	
FMT_MSA	Management der Sicherheitsattribute
FMT_SMR	Rollen im Sicherheitsmanagement
FPR: Datenschutz/Privacy	
FPR_PSE	Pseudonymität
FPT: Schutz der EVG Sicherheitsfunktionen	
FPT_STM	Zeitstempel
FTA: EVG Zugriff/Access	
FTA_TAB	EVG-Zugriffswarnmeldung
FTA_TSE	EVG-Sitzungseinrichtung

Tabelle A.2: Anforderungen

Literaturverzeichnis

[3Sat 08] 3Sat. *Games 2.0 - Der nächste Level, Beitrag der Sendung „Neues“ auf 3Sat am 25.5.08.* abrufbar über die ZDF mediathek, URL: http://www.zdf.de/ZDFmediathek, zuletzt abgerufen am 06.03.09, 2008.

[Aarseth 04] Espen Aarseth. *Genre Trouble.* URL: http://www.electronicbookreview.com/thread/firstperson/vigilant, zuletzt abgerufen am 06.3.09, 2004.

[ALS 08] ALS. *Alliance Library System, Second Life Library.* http://www.infoisland.org/about, zuletzt abgerufen am 03.03.2008, 2008.

[Amann 92] Esther Amann & Hugo Atzmüller. *IT-Sicherheit - Was ist das?* Datenschutz und Datensicherung (heute: Datenschutz und Datensicherheit), Vieweg Verlag, Wiesbaden, Vol. 6, Seiten 286–292, Juni 1992.

[Banavar 00] H. Banavar. *Security Issues in Multiplayer, Distributed Network Games.* URL: http://ww2.cs.fsu.edu/ banavar/research/NSPaper.htm, zuletzt abgerufen am 14.03.09, 2000.

[Bartle 96] Richard Bartle. *Hearts, Clubs, Diamonds, Spades: Players who suit MUDs.* Journal of MUD Research, URL:

http://www.brandeis.edu/pubs/jove/HTML/v1/bartle.html, 1996.

[Bartle 01] Richard Bartle. *Avatar, Character, Persona. Immerse yourself...* Muddled Times, Ausgabe vom August 2001, online abrufbar: URL: http://mud.co.uk/richard/acp.htm, zuletzt abgerufen am: 28.11.2008, 2001.

[BBCNews 07] BBCNews. *'Virtual theft' leads to arrest: A Dutch teenager has been arrested for allegedly stealing virtual furniture from „rooms" in Habbo Hotel, a 3D social networking website.* BBC News Online vom 14 November 2007. URL: http://news.bbc.co.uk/1/hi/technology/7094764.stm, zuletzt abgerufen am 13.1.2009, 2007.

[Beyer 06] Anja Beyer. *Security Aspects in Online Games.* In Klaus P. Jantke & Gunther Kreuzberger (Hrsg.), Knowledge Media Technologies, First International Core-to-Core-Workshop, Dagstuhl Castle, Germany, Nr. 21 in IfMK Diskussionsbeiträge, Seiten 41–46. TU Ilmenau, 2006.

[Beyer 07a] Anja Beyer. *Security in Online Games - Case Study: Second Life.* In Florida AI Research Symposium (FLAIRS-07), Key West, FL, USA, May 2007.

[Beyer 07b] Anja Beyer & Klaus P. Jantke. *When the Real Criminal gets Virtual, the Virtual Crime gets Real.* 1st Computer Security Conference, Myrtle Beach, SC, USA, April 2007.

[Beyer 08] Anja Beyer, Gunther Kreuzberger, Marcel Kirchner & Jens Schmeling. *Privacy im Social Web - Zum kompetenten Umgang mit persönlichen Daten im Web 2.0.* DuD (Datenschutz und Datensicherheit), Vol. 32/Nr. 9, Seiten 597–600, 2008.

[Beyer 09] Anja Beyer & Michael Müller. *Virtueller oder Realer Gauner - Sicherheit in Online Spielen.* In Digitale Spiele: Herausforderung & Chance - Beiträge der Tagungen LIT 2006 und 2007, Seiten 157–164. vwh-Verlag, 2009.

[Birchall 95] D. Birchall & L. Lyons. Creating Tomorrows Organization. Unlocking the benefits of future Work. Pitman, London, 1995.

[Blascovich 02] J. Blascovich, J. Loomis, A. Beal & K. Swinth et al. *Immersive virtual environment technology as a methodological tool for social psychology.* Psychological Inquiry, Vol. 13(2), Seiten 103–124, 2002.

[Blizzard 08] Blizzard. *World of Warcraft zählt jetzt mehr als 11,5 Millionen Abonnenten weltweit (Stand Dezember 2008).* URL: http://eu.blizzard.com/de/press/081223.html, zuletzt abgerufen am 23.2.09, 2008.

[BMG 09a] BMG. *Bundesministerium für Gesundheit. Fragen und Antworten zur elektronischen Gesundheitskarte.* URL: http://www.die-gesundheitskarte.de/fragen_und_antworten/testphase/details/herausgabe_eGK.html, zuletzt abgerufen am 16.3.2009, 2009.

[BMG 09b] BMG. *Bundesministerium für Gesundheit. Informationen vom Bundesministerium für Gesundheit zur deutschen elektronischen Gesundheitskarte.* URL: http://www.die-gesundheitskarte.de, zuletzt abgerufen am 16.1.2009, 2009.

[BNetzA 09] BNetzA. *Bundesnetzagentur.* URL: http://www.bundesnetzagentur.de/enid/Veroeffentlichungen/Algorithmen_sw.html, zuletzt abgerufen am 16.03.09, 2009.

[Bourdieu 92] Pierre Bourdieu. Die verborgenen Mechanismen der Macht. Ökonomisches Kapital - Kulturelles Kapital - Soziales Kapital. Vsa, Margareta Steinrücke (Herausgeber), 1992.

[BSI 09a] BSI. *Bundesamt für Sicherheit in der Informationstechnik, Algorithmenempfehlungen.* URL: http://www.bsi.bund.de/esig/kryptoalghistorie.htm, zuletzt abgerufen am 16.03.09, 2009.

[BSI 09b] BSI. *Bundesamt für Sicherheit in der Informationstechnik. Common Criteria Leitfaden.* http://www.bsi.bund.de/cc/cc_leitf.pdf, zuletzt abgerufen am 06.03.09, 2009.

[BSI 09c] BSI. *Bundesamt für Sicherheit in der Informationstechnik. Evaluation Assurance Level (EAL).* URL: http://www.bsi.bund.de/cc/eal_stufe.htm, zuletzt abgerufen am 20.1.2009, 2009.

[BusinessWeek 06] BusinessWeek. *My Virtual Life.* Artikel vom 1.5.06, URL: http://www.businessweek.com/magazine/content/06_18/b3982001.htm, zuletzt abgerufen am 06.03.09, 2006.

[Cassidy 05] Butch Cassidy. *The Time has Come for Action, We will be ignored no longer.* Forumsbeitrag von „ButchCassidy“ vom 25.11.05, URL: http://www.iwnation.com/Forums/index.php?showtopic=17450&st=0, zuletzt abgerufen am 17.01.09, 2005.

[Castronova 05] Edward Castronova. Synthetic Worlds: The Business and Culture of Online Games. The University of Chicago Press, 2005.

[Castronova 07] Edward Castronova. *Effects of Botting on World of Warcraft.* URL: http://virtuallyblind.com/files/mdy/blizzard_msj_exhibit_7.pdf, zuletzt abgerufen am 25.1.09, 2007.

[CC 06] CC. *Common Criteria for Information Technology Security Evaluation.* http://www.commoncriteriaportal.org, zuletzt abgerufen am 14.3.09, 2006.

[CCPart1 06] CCPart1. *Common Criteria Part 1: Introduction and General Model.* Version 3.1 Revision 1, URL:

http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R2.pdf, zuletzt abgerufen am 14.3.09, September 2006.

[CCPart2 06] CCPart2. *Common Criteria Part 2: Security functional components*. Version 3.1 Revision 2, URL: http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf, zuletzt abgerufen am 14.3.09, September 2006.

[CCPart3 06] CCPart3. *Common Criteria Part 3: Security assurance components*. Version 3.1 Revision 2, URL: http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R2.pdf, zuletzt abgerufen am 14.3.09, September 2006.

[Chen 05] Y.-C Chen, J.-J Hwang & R. Song et al. *Online Gaming Cheating and Security Issue*. International Conference on Information Technology: Coding and Computing (ITCC'05), Vol. 1, Seiten 518–523, 2005.

[ContextAds 09] ContextAds. *About ContextAds: Advertising for Second Life*. URL: http://www.slcontextads.co.uk/about.asp, zuletzt abgerufen am 23.1.09, 2009.

[Csikszentmihalyi 91] Mihaly Csikszentmihalyi. Flow: The Psychology of Optimal Experience. Harper Perennial, 1991.

[Csikszentmihalyi 00] Mihaly Csikszentmihalyi. Beyond boredom and anxiety: experiencing flow in work and play. Jossey-Bass Inc., 2000.

[Dibbell 06] Julian Dibbell. Play Money Or, How I Quit My Day Job and Made Millions Trading Virtual Loot. Basic Books, 2006.

[Directive 95] Directive. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with*

regard to the processing of personal data and on the free movement of such data, 1995.

[Ducheneaut 04] Moore R.J. Ducheneaut N. *The Social Side of Gaming: A study of Interaction Patterns in a Massively Multiplayer Online Game*. Proceedings of ACM CSCW'04 Conference on Computer-Supported Cooperative Work, Vol. 6, Nr. 3, Seiten 360–369, 2004.

[Duden 07a] Duden. *Duden - Das große Fremdwörterbuch: Herkunft und Bedeutung der Fremdwörter*. Dudenverlag, Bibliographisches und Institut Brockhaus AG, 2007.

[Duden 07b] Duden. *Duden - Deutsches Universalwörterbuch*. Dudenverlag, Bibliographisches Institut und Brockhaus AG, 2007.

[Ebay 09] Ebay. *Auktionen in der Kategorie Onlinespiele*. URL: http://games.shop.ebay.de/items/Onlinespiele__W0QQ_sacatZ1654?_npmv=3, zuletzt abgerufen am 15.03.09, 2009.

[Eckert 04] Claudia Eckert. IT-Sicherheit, Konzepte-Verfahren-Protokolle. Oldenbourg Verlag München, 2004.

[Enisa 08] Enisa. *Enisa Survey Results: Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds*. URL: http://www.enisa.europa.eu/doc/pdf/other/survey_vw.pdf, zuletzt abgerufen am 14.3.09, 2008.

[Eskelinen 01] Markku Eskelinen. *The Gaming Situation*. The International Journal of Computer Game Research, Vol. 1, Nr. 1, Seiten online, http://www.gamestudies.org, 2001.

[Frasca 98] Gonzalo Frasca. *Ludology meets Narratology*. URL, http://www.ludology.org/articles/ludology.htm, zuletzt abgerufen am 28.02.2008, 1998.

[Fritz 04] Jürgen Fritz. Das Spiel verstehen. Eine Einführung in Theorie und Bedeutung. Juventa Verlag Weinheim, 2004.

[Früh 03] Werner Früh. Theorie der Unterhaltung: ein interdisziplinärer Diskurs. Halem Verlag Köln, 2003.

[GMG 03] GMG. *Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz), Gesetz vom 14.11.2003, in Kraft getreten 1.1. 2004.* Bundesgesetzblatt Jahrgang 2003 Teil I Nr. 5, ausgegeben am 19.11.2003, URL: http://217.160.60.235/BGBL/bgbl1f/bgbl103s2190.pdf, 2003.

[Heeks 08] Richard Heeks. *Current Analysis and Future Research Agenda on „Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games.* Working Paper of the Development Informatics Group UK, URL: http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp32.pdf, zuletzt abgerufen am 13.1.2009, 2008.

[Heim 98] M. Heim. Virtual Realism. Oxford University Press, 1998.

[Hogben 08] Giles Hogben. *Virtual Worlds, Real Money: Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds.* ENISA Position Paper, URL: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_security_privacy_virtualworlds.pdf, November 2008.

[Huizinga 06] Johann Huizinga. Homo Ludens - Vom Ursprung der Kultur im Spiel. Rowohlts Enzyklopädie, 2006. Bibliographisch ergänzte Neuausgabe des 1956 erschienen Titels, Originalausgabe des Jahres 1938 erschien unter dem Titel „Homo Ludens".

[IGE 08] IGE. *Webseite von Internet Gaming Entertainment.* URL: http://www.ige.com/, letzter Abruf am 28.11.2008, 2008.

[Jakobsson 06] M. Jakobsson. *Virtual worlds and social interaction design.* PhD thesis, Umeå University, Department of Informatics, 2006.

[Jantke 06] Klaus P. Jantke. *Digital Game Knowledge Media (Invited Keynote).* In 3rd International Symposium on Ubiquitous Knowledge Network Environement, Volume of Keynote Speaches, Seiten 53–83, Sapporo, Japan, Feb 28 - March 1 2006.

[Juul 03] Jesper Juul. *The Game, the Player, the World: Looking for a Heart of Gameness.* URL: http://www.jesperjuul.net/text/gameplayerworld, zuletzt abgerufen am 28.02.2008, 2003.

[Kirmse 97] C. Kirmse & A. Kirmse. *Security in Online Games.* Gamasutra http://www.gamasutra.com, originally published in Game Developer, July 1997.

[Klaß 06a] Christian Klaß. *Second Life - Hacker griff auf Kundendaten zu. Betreiber lässt alle Nutzer aus Sicherheitsgründen Passwörter ändern.* golem.de news vom 11.9.2006, URL: http://www.golem.de/0609/47726.html, zuletzt abgerufen am 13.1.2009, 2006.

[Klaß 06b] Christian Klaß. *Softwarefehler: World of Warcraft schmeißt Linux-Nutzer raus. Fälschliche „Erkennung“ von Cedega als Cheating-Tool.* golem.de news vom 16.11.06, URL: http://www.golem.de/0611/48983.html, zuletzt abgerufen am 13.01.2009, 2006.

[Köhnlein 05] Jan Köhnlein. *Sicherheit in verteilten virtuellen Umgebungen.* PhD thesis, Technische Universität Hamburg-Harburg, 2005.

[Koll 07] Koll. *Virtuelle Welten warten noch auf Sicherheitsstandards.* Computerzeitung, Vol. 38, Nr. 32, Seite 8, August 2007.

[Koster 05] R. Koster. A Theory of Fun for Game Design. Paraglyph Press, Inc., Scottsdale, AZ, USA, 2005.

[Krüger 07] Bertolt Krüger. *Protection Profile electronic Health Card (eHC) (elektronische Gesundheitskarte (eGK)).* 27.1.2007, BSI-PP-0020-V2-2007, URL: http://www.bsi.bund.de/cc/pplist/pplist.htm, zuletzt abgerufen am 20.1.2009, 2007.

[Lardschneider 07] Michael Lardschneider. *Security Awareness - Grundlage aller Sicherheitsinvestitionen. Bei der Münchner Rückversicherungs-Gesellschaft.* DuD (Datenschutz und Datensicherheit), Vol. 31, Nummer 7, Seiten 492–497, 2007.

[LG 08] LG. *Webseite von Live Gamer.* URL: http://www.livegamer.com/, letzer Abruf am 28.11.2008, 2008.

[LifeGamer 08] LifeGamer. *The Trusted Source for Virtual Trading.* URL, http://lifegamer.com, zuletzt abgerufen am 03.03.2008, 2008.

[Linden 06] Robin Linden. *Copyrights and Content Creation in Second Life.* Blog-Beitrag vom 13. November 2006, URL: http://blog.secondlife.com/2006/11/13/copyrights-and-content-creation-in-second-life/, zuletzt abgerufen am 25.1.2009, 2006.

[Lober 05] Dr. A. Lober & O. Weber. *Money for Nothing? - Handel mit Spiel-Accounts und virtuellen Gegenständen.* c't, Vol. 20, Seiten 178–180, 2005.

[Lober 07] Andreas Lober. Virtuelle Welten werden real - Second Life, World of Warcraft und Co: Faszination, Gefahren, Business. Heise Zeitschriftenverlag, 2007.

[Maslow 77] Abraham H. Maslow. Motivation und Persönlichkeit. Walter-Verlag Olten und Freiburg im Breisgau, 1977. Das Buch ist 1954 unter dem Titel 'Motivation and Personality' bei Harper and Row, New York erschienen.

[Matt 05] Bishop Matt. Introduction to Computer Security. Pearson Education, 2005.

[MDB 08] MDB. *Webseite von Markee Dragon Broker.* URL: http://www.markeedragon.net/, letzer Abrufam 28.11.2008, 2008.

[Merkow 05] Mark S. Merkow & Jim Breithaupt. Computer security assurance using the common criteria. Delmar Learning, Clifton Park, New York, 2005.

[Mix 07] Markus Mix & Miriam Pingel. *Be better-Be secure. Security Awareness in der Bosch-Gruppe.* DuD (Datenschutz und Datensicherheit), Vol. 31, Nummer 7, Seiten 498–501, 2007.

[mmogchart.com 08] mmogchart.com. https://mmogchart.com, zuletzt abgerufen am 05.03.08, 2008.

[Müller 01] Günter Müller & Martin Reichenbach (Hrsg.). Sicherheitskonzepte für das Internet. Springer Verlag, 2001.

[Murray 98] Janet Murray. Hamlet on the Holodeck: The Future of Narrative in Cyberspace. MIT Press, 1998.

[NCsoft 09] NCsoft. *Offizielle Webseite des MMORPG „Guild Wars“.* URL: http://de.guildwars.com/, zuletzt abgerufen am 02.03.2009, 2009.

[NIST 09] NIST. *National Institute of Standards and Technology, FIPS (Federal Information Processing Standard) Publications.* URL: http://csrc.nist.gov/publications/PubsFIPS.html, zuletzt abgerufen am 16.03.09, 2009.

[Ochel 05] David Ochel. *Evaluierung von IT-Sicherheit: Garantiert sicher.* iX, Heise Zeitschriftenverlag, Vol. 5, Seiten 132–135, 2005.

[Parlament 95] EU Parlament. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal da-*

ta and on the free movement of such data. Official Journal of the European Communities No L. 281, S. 31-39, online abrufbar: URL: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, 23. November 1995.

[Pfitzmann 04] A. Pfitzmann. Multilateral Security. Galileo, 2004.

[Porteck 06] Stefan Porteck. *Second Life: Programm ermöglicht virtuelles Klauen.* http://www.heise.de/newsticker/meldung/81088, veröffentlicht: 15.11.2006, zuletzt abgerufen am 13.1.09, 2006.

[Register 06] Register. *Trojan targets World of Warcraft gamers.* URL: http://www.theregister.co.uk/2006/05/08/wowcraft/, zuletzt abgerufen am 23.1.2009, 2006.

[Robbins 07] Sarah „Intellagirl“ Robbins. *Second Life Education Research.* http://www.secondlife.intellagirl.com, 2007.

[Roush 07] Wade Roush. *Second Earth - The World Wide Web will soon be absorbed into the World Wide Sim: An immersive, 3-D visual environment that combines elements of social virtual worlds like Second Life and new mapping applications like Google Earth. What happens when the virtual and real worlds collide?* Technology review, Vol. 110, 4, Seiten 38–49, 2007.

[Rymaszewski 07] Michael Rymaszewski. Second Life: The official Guide. Wiley Publishing, Indianapolis, New Jersey, 2007.

[Schiller 00] Friedrich Schiller. Über die ästhetische Erziehung des Menschen. Reclam, Stuttgart, 2000.

[Schimmer 07] Klaus Schimmer. *Sicherheit beginnt im Kopf. Sensibilisieren - aber wie?* DUD (Datenschutz und Datensicherheit), Vol. 31, Nummer 7, Seiten 510–514, 2007.

[Schmitz 07] Tobias Schmitz. *MMORPGs heute und morgen: World of Warcraft forever?* In Virtuelle Welten werden real, Second Life, World of Warcraft & Co, Faszination, Gefahren, Business, Seiten 21–32. Heise Zeitschriftenverlag GmbH & CoKG, 2007.

[Scholz 00] C. Scholz. Strategische Organisation-Multiperspektivität und Virtualität. Moderne Industrie, Landsberg/Lech, 2nd, revised edition edition, 2000.

[Schweiger 07] Wolfgang Schweiger. Theorien der Mediennutzung. VS Verlag für Sozialwissenschaften, 2007.

[SecondLife 06] SecondLife. *Webseite der Virtuellen Welt Second Life.* http://www.secondlife.com, abgerufen am 05.01.07, 2006.

[SecondLife 07a] SecondLife. *Islands in Second Life.* http://secondlife.com/community/land-islands.php, 2007.

[SecondLife 07b] SecondLife. *Number of Second Life Residents.* URL: http://www.secondlife.com/whatis/economy_stats.php, zuletzt abgerufen am 31.01.2007, 2007.

[SecondLife 08] SecondLife. *Webseite der Virtuellen Welt Second Life.* http://www.secondlife.com, zuletzt abgerufen am 03.03.2008, 2008.

[Smed 01] J. Smed, T. Kaukoranta & H. Hakonen. *Aspects of Networking in Multiplayer Computer Games.* In Proceedings of International Conference on Application and Development of Computer Games in the 21st Century, Seiten 74–81, 2001. URL: http://www.tucs.fi/Publications/proceedings/pSmKaHaa.php.

[Sophos 07] Sophos. *Mal/Iframe-F.* URL: http://www.sophos.com/security/analyses/viruses-and-spyware/maliframef.html, 2007.

[Stallings 08] William Stallings & Lawrie Brown. Computer Security - Principles and Practice. Upper Saddle River NJ, Pearson Prentice Hall, 2008.

[Sutton-Smith 97] Brian Sutton-Smith. The Ambiguity of Play. Harvard University Press, Cambridge, 1997.

[Symantec 06] Symantec. *Infostealer.Wowcraft.D.* URL: http://www.symantec.com/security_response/writeup.jsp?docid=2006-061911-0328-99&tabid=1, zuletzt abgerufen am 23.1.2009, 2006.

[Taylor 06] T.L. Taylor. Play Between Worlds - Exploring Online Game Culture. Massachusetts Institute of Technology (MIT) Press, Cambridge, London, 2006.

[te Wildt 07] Dr. Bert Theodor te Wildt. *Pathological Internet Use: Abhängigkeit, Realitätsflucht und Identitätsverlust im Cyberspace.* In Virtuelle Welten werden real - Second Life, World of Warcraft & Co: Faszination, Gefahren, Business. Heise Zeitschriften Verlag, 2007.

[Trist 51] Eric Trist & Ken Bamforth. *Some social and psychological consequences of the long wall method of coal getting.* Human Relations, Vol. 4, Seiten 3–38, 1951.

[VE 08] VE. *Virtual Environments Blog.* URL: http://www.virtualenvironments.info, zuletzt abgerufen am 04.03.2008, 2008.

[Vhs 09] Vhs. *Webseite der Volkshochschule Goslar in Second Life.* URL: http://www.vhs-sl.de/, zuletzt abgerufen am 02.03.2009, 2009.

[Voiskounsky 04] A.E. Voiskounsky, O.V. Mitina & A.A. Avetisova. *Playing Online Games: Flow Experience.* Psychology, Vol. 2, Nr. 3, Seiten 259–281, 2004.

[Waldo 08] Jim Waldo. *Scaling in games and virtual worlds.* ACM Queue (Architecting tomorrows computing), Vol. November/Dezember, Seiten 10–16, 2008.

[Wesener 04] Stefan Wesener. Spielen in virtuellen Welten - Eine Untersuchung von Transferprozessen in Bildschirmspielen. VS Verlag für Sozialwissenschaften, 2004.

[Whitten 05] A. Whitten & J.D. Tygar. Why jonny can't encrypt. a usability evaluation of pgp 5.0, Kapitel 34, Seiten 679–702. O'Reilly, 2005.

[Williams 05] Tad Williams. Otherland 1. Stadt der goldenen Schatten. Heyne Verlag, 2005.

[WoW 06] WoW. *Webseite des Spiels World of Warcraft.* URL: http://www.wow-europe.com, abgerufen am 05.01.07, 2006.

[Wünsch 06] Carsten Wünsch. Unterhaltungserleben: ein hierarchisches Zwei-Ebenen-Modell affektiv-kognitiver Informationsverarbeitung. Halem Verlag Köln, 2006.

[Yan J.J 02] Choi H.-J. Yan J.J. *Security issues in online games.* The Electronic Library, Vol. 20, Nr. 2, Seiten 125–133, 2002.

[Yee 06] George Yee, Larry Korba, Ronggong Song & Ying-Chieh Chen. *Towards Designing Secure Online Games.* In 20th International Conference on Advanced Information Networking and Applications (AINA 2006), 18-20 April 2006, Vienna, Austria, Seiten 44–48, 2006.

[ZDNet 05] ZDNet. *Cheaters slam 'Everquest II' economy.* Onlineartikel vom 11. August 2005, URL: http://news.zdnet.com/2100-1040_22-144176.html, zuletzt abgerufen am 25.1.2009, 2005.