Evaluationsmethoden für benutzerzentrierte IT-Sicherheit

vorgelegt von
Diplom-Informatiker
Olaf Kroll-Peters

Von der Fakultät IV – Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des Grads

Doktor der Ingenieurwissenschaften
– Dr.-Ing. –

genehmigte Dissertation

Promotionsausschuß:

Vorsitzender:	Prof. Dr. Axel Küpper
Berichter:	Prof. Dr.-Ing. Sahin Albayrak
Berichter:	Prof. Dr.-Ing. Sebastian Möller
Berichter:	Dr. habil. Roman Englert

Tag der wissenschaftlichen Aussprache: 29.07.2010

Berlin 2010

D 83

Vorwort

Diese Arbeit entstand während meiner Tätigkeit als Wissenschaftlicher Mitarbeiter am DAI-Labor im Fachgebiet Agententechnologien in betrieblichen Anwendungen und der Telekommunikation (AOT) der Technischen Universität Berlin. Dort erhielt ich in diversen Lehrveranstaltungen und Forschungsprojekten die Möglichkeit mich mit den Themen Usability und IT-Sicherheit auseinander zu setzen.

Dort kam ich als Projektleiter der ersten weltweiten Zertifizierung von generischer Sicherheit nach den Common Criteria zuerst mit dem Thema IT-Sicherheit in Berührung. Dabei bemerkte ich, dass IT-Sicherheit nur dann erfolgreich umgesetzt werden kann, wenn Sicherheitsmechanismen auch benutzt werden können. Je einfacher Sicherheitsmechanismen benutzt werden können, desto weniger Fehler werden bei der Benutzung gemacht und umso geringer ist das Bedrohungspotential durch Fehlbedienungen. Von da an faszinierte und leitete mich der Themenkomplex der benutzbaren IT-Sicherheit. In verschiedenen Projekten und Lehrveranstaltungen erforschte ich mit vielen Unterstützern das komplexe Thema der benutzerzentrierten Sicherheit.

Das bildete auch die Basis für diese Arbeit und gab mir die Gelegenheit mich mit meinen Kollegen über die Themen in meiner Arbeit auszutauschen und in vielen fruchtbaren Diskussionen neue Impulse zu erhalten.

Bedanken möchte ich mich daher insbesondere bei Prof. Dr. Ing.- Albayrak, der mir die Gelegenheit zur Anfertigung der Dissertation gab, mir stets mit Rat und Tat beiseite stand und neue Wege in der Forschung eröffnet hat. Ebenfalls möchte ich mich bei Prof. Dr. Ing.- Sebastian Möller, Dr. habil. Roman Englert und Dr. Stefan Fricke für die vielen angeregten Diskussionen, ihre Geduld und Vorschläge zur Verbesserung bedanken.

Bedanken möchte ich mich aber auch bei dem gesamten Team des DAI-Labors und meinen Studenten, vor allem bei den Herren Michael Quade, Stefan Kolm, Christian Nawroth und David Jaschuk für gemeinsame For-

schungsprojekte, Dr. Benjamin Hirsch und Natascha Tiotuico für gemeinsame wissenschaftliche Arbeiten, Dominik Glöckner für alles mögliche, Dr. Karsten Bsufka für die angenehme gemeinsame Leitung diverser Projekte, Volker Eckert, Oliver Raudies und Sven Hoeppner für das Erneuern meiner Energien, Rainer Bye für gemeinsame Gespräche, Christian Scheel für Seelenverwandtschaft, Tim Geissler für gemeinsamen Start in die wissenschaftliche Laufbahn und Thebin Lee für das gemeinsames Schreiben und Diskutieren in der Bibliothek.

Ein weiterer Dank gilt meiner Familie, meiner Mutter Ute Kroll, meinen Brüdern Dirk, Jens und Timm Kroll, insbesondere aber meiner Frau Inga Peters und meinen Kindern Janis und Finja, ohne deren umfangreiche Unterstützung mir diese Arbeit nicht gelungen wäre.

Olaf Kroll-Peters
Berlin, 2010

Kurzfassung

Die Sicherheit von IT-Systemen stellt eine der großen Herausforderungen in der Zukunft dar. Die steigende Verbreitung von IT-Systemen und deren Vordringen in nahezu alle Bereiche des täglichen Lebens macht es unerlässlich, dass Anstrengungen unternommen werden um die Systeme „sicher“ zu betreiben und zu benutzen. Dies bedeutet weiterhin, dass die Bedrohungen, denen die Systeme ausgesetzt sind, möglichst minimiert werden. Neben vielen anderen Bedrohungen, wie z.B. Datenmissbrauch oder Schadsoftware, ist dabei eine potentielle Fehlbedienung oder Nichtbenutzung von Sicherheitsmechanismen durch Benutzer eine der Bedrohungen.

Die vorliegende Arbeit konzentriert sich daher vor allem auf die Bedrohung der IT-Sicherheit von Systemen durch Fehlbedienung oder Nichtbenutzung durch den Menschen. Es wird gezeigt, dass heutige Überprüfungsregularien wie z.B. eine Zertifizierung nach den Common Criteria diese Problemstellung nur ungenügend behandeln. Zunächst wird in der Arbeit daher gezeigt, welche reale Bedrohungslage durch Benutzer vorhanden ist. Um das gezeigte Problem zu lösen sind umfangreiche Maßnahmen notwendig. Einen möglichen ersten Schritt stellt die Bereitstellung von Systemen für Benutzergruppen dar. Aufbauend auf dem gezeigten Problem werden dann Konzepte vorgestellt und prototypisch implementiert, die Ansätze zur Umsetzung benutzerzentrierter IT- Sicherheit, durch Benutzergruppierung mit Fokus auf IT-Sicherheit, zeigen.

Abschließend werden Lösungen aufgezeigt und diskutiert, die das Bedrohungspotential durch die Benutzung von Benutzern minimieren.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1
Einleitung

„πάντα ῥει“

(Heraklit)

Die Informationstechnik (IT) wird in immer weiteren Lebensbereichen eingesetzt um Benutzer zu unterstützen. Konzepte wie das „Ambient Assisted Living“ oder „Intelligente Umgebungen“ zeigen einen Trend bei der veränderten IT-Nutzung an. Bei beiden Konzepten handelt es sich um Arten von Assistenzsystemen. Sie unterstützen Benutzer, indem sie Daten sammeln und personalisiert Dienste bereit stellen.

Beide Konzepte basieren darauf benutzer- und nicht gerätezentriert zu sein. So steht der Benutzer mit seinen Bedürfnissen, Wünschen und Zielen im Mittelpunkt und nicht die zur Verfügung stehenden Funktionen der Systeme. In beiden Konzepten weisen IT-Systeme verschiedene Eigenschaften auf. Sie können autonom arbeiten, autonom Daten sammeln, in die Umgebung integriert sein, für den Benutzer unbemerkt agieren oder auch Strategien für ihre Aktionen aus dem Verhalten der Benutzer ableiten. Die IT-Systeme sollen dem Benutzer optimal assistieren.

Durch die vermehrte und veränderte Interaktion erhalten Benutzer eine höhere Verantwortung im Umgang mit Systemen und Daten. Dieser Umstand motivierte dazu, das Benutzerverhalten hinsichtlich der IT-Sicherheit zu untersuchen. Die Veränderungen der IT-Systeme und des Umgangs mit ihnen werden nun zunächst detaillierter betrachtet um im Anschluss die Bedeutung von „benutzerzentrierter IT-Sicherheit“ fokussiert zu motivieren.

IT-Systeme unterliegen zahlreichen Veränderungen um neuen Einsatzmöglichkeiten gerecht werden zu können. Sie werden zu immer größeren, komplexeren und leistungsstärkeren Netzen zusammen geschaltet, um Daten zu erfassen, auszutauschen, zu generieren und um weitere Funktionen für Benutzer zur Verfügung zu stellen. In Netzen bearbeiten IT-Systeme die Daten von anderen IT-Systemen und generieren so neue weitere Daten. Als Beispiel diene hier die Entwicklung im Automobilbau. Die ersten Informationssysteme in Automobilen zeigten Benutzern nur einfache nicht miteinander gekoppelte Informationen an. So zum Beispiel, dass der Fahrer oder Beifahrer nicht angeschnallt war. Heutzutage befinden sich in den Automobilen leistungsstarke IT-Systeme. Diese stellen zahlreiche miteinander vernetzte Funktionen (Glatteiswarner, Straßenschilderkennung, Tanküberwachung, Tempomat, Routenplaner ...) zur Verfügung. So können die Informationen der Straßenschilderkennung vom Tempomaten weiterverarbeitet werden. Das Verhalten der Benutzer auf die unterschiedlichen Situationen kann gesammelt und zu neuen Informationen verknüpft werden. Aus diesen Daten lassen sich dann Benutzerprofile beziehungsweise Verhaltensmuster generieren für eine individuelle verbesserte Unterstützung.

Jedes Gerät kann Rechenkapazität erhalten und so Daten für ein größeres Netzwerk sammeln. Die Teile der Systeme werden immer kleiner und „ unbemerkter“. Sensoren können dazu unbemerkt auf kleinstem Raum integriert werden.

Weitere Veränderungen sind in Grafik 1.1 illustriert. Sie zeigt die zeitliche Entwicklung bei IT-Systemen. IT-Systeme entwickelten sich von stationären Systemen zu mobilen vernetzten allgegenwärtigen Systemen. Die ersten IT-Systeme waren stationär, nicht miteinander vernetzt, bearbeiteten kleine abgegrenzte Aufgaben und wurden von IT-Experten benutzt. Sie bestanden aus riesigen Apparaturen und füllten ganze Hallen aus.

In der Folgezeit wurde der Funktionsumfang der IT-Systeme erweitert und die Nutzung änderte sich dahingehend, dass sie vernetzt verwendet wurden. Nun arbeiteten auch viele „Nicht-IT-Experten“ in abgegrenzten Umgebungen mit IT-Systemen. Viele Tätigkeiten in Firmen wurden jetzt von IT-Systemen unterstützt.

Viele der stationären IT-Systeme wurden später durch mobile Systeme ersetzt. Die Anzahl der verkauften mobilen PC Systeme (sogenannte Laptops) ist mittlerweile größer als die Zahl der verkauften stationären PC's [19]. Mit der Entwicklung und Verbreitung von mobilen Endgeräten, die eine starke IT-Kapazität aufwiesen, änderte sich wiederum auch die Benutzung der IT-Systeme. Aus Gründen der Bequemlichkeit und des Komforts werden viele

Funktionen, die für stationäre Systeme entwickelt wurden ebenfalls für mobile Geräte bereit gestellt. Oberflächlich sehen die Funktionen gleich aus. Die technische Realisierung und die Rahmenbedingungen sind aber verschieden. So sind Nachrichten innerhalb eines geschützten Unternehmensnetzwerkes anderen Bedrohungen ausgesetzt, als der Versand von Nachrichten aus dem öffentlichen Internet in geschützte Unternehmensnetzwerke.

Zur Zeit verändern sich viele IT-Systeme zu sogenannten allgegenwärtigen Assistenzsystemen. Diese sammeln und analysieren autonom Daten, stellen Dienste bereit und führen Aktionen aus. Teilweise werden dabei Systeme in das Umfeld von Benutzern integriert, ohne dass sich Benutzer der Systeme bewusst sind. Systeme können in Bereichen eingesetzt werden, wo keine Eingaben durch den Benutzer erfolgen. Somit sind die Einsatzmöglichkeiten und Szenarien universeller als bei herkömmlichen Systemen und die Anzahl der Systeme pro Benutzer erhöht sich.

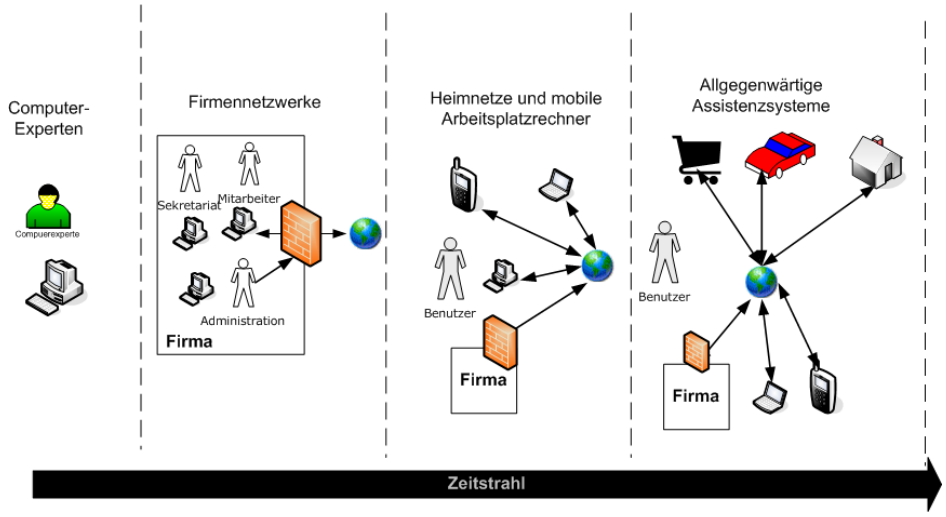


Abb. 1.1: Wandel bei der Benutzung von IT-Systemen

Eine weitere wichtige Veränderung beim Umgang mit den Systemen betrifft die veränderte Bedeutung der IT-Systeme. Immer mehr Geschäfte werden im und über das Internet oder in anderen IT-Systemen abgewickelt. Die IT durchdringt immer weitere Bereiche wo hohe Anforderungen an Ausfallsicherheit oder Vermeidung von potentiellem Fehlverhalten gestellt werden, und ersetzt herkömmliche Systeme. Aus diesem Grund ist die IT-Sicherheit eine der Schlüsselfaktoren für zukünftige Anwendungen [121]. „Nicht-IT“-Systeme werden durch Funktionen von IT-Systemen ergänzt oder komplett abgelöst . Viele Funktionen, die früher ohne IT-Systeme durchgeführt werden konnten, werden heute nur noch mit IT-Unterstützung erbracht. Viele

Aufgaben können ohne fehlerfrei funktionierende Systeme nicht mehr zufriedenstellend, nur mit erheblichem Mehraufwand oder überhaupt nicht mehr gelöst werden. So lassen sich zum Beispiel moderne Automobile bei einer Fehlfunktion der IT-Technik nicht mehr in Betrieb nehmen.

Die Einführung von stationären und vernetzten IT-Systemen in immer weiteren Bereichen hat neben vielen Vorteilen aber auch einige Risiken. Die steigende Bedeutung der Systeme führt dazu, dass der mögliche eintretende Schaden bei einem Ausfall der Systeme oder bei Fehlfunktionen ansteigt. Somit müssen verstärkt Anstrengungen unternommen werden um Fehlfunktionen oder Systemausfälle zu verhindern.

Das Bedrohungspotential der Systeme steigt, da sie über Netzwerke angegriffen werden können. Eindringlinge können Systeme über Netzwerke infiltrieren oder sabotieren. Durch die Verlagerung von realen Gütern in virtuelle Systeme besteht die Möglichkeit, die virtuellen Güter (und damit die realen Güter) zu stehlen. Durch die starke Vernetzung der Systeme ist es Angreifern möglich Angriffe von beliebigen Standorten auszuführen. Sie müssen bei ihrem Angriff nicht mehr direkt vor Ort des Angriffszieles sein, sondern können den Angriff aus der „Sicherheit“ eines weit entfernten Ortes ausführen. Weitere zusätzliche Angriffsoptionen ergeben sich aus den geringen Kosten, die für die Ausführung von Angriffen auf IT-Systeme notwendig sind. Viele Angriffe lassen sich mit einem Rechner, der eine Internet-Verbindung hat, durchführen. Der Schaden durch erfolgreiche Angriffe kann dagegen sehr hoch werden [87]. Der Entwicklungszyklus neuer Angriffsmethoden benötigt immer kürzere Zeiträume. Die Verbreitung neuer Angriffsmethoden wird durch die Informationsübermittlung begünstigt und beschleunigt. Angreifer können ihre wahre Identität und ihre wahren Absichten leicht verbergen. Nicht vorhandene globale Abkommen und juristische Regelungen erleichtern es Angreifern ohne hohe Risiken Angriffe durchzuführen. Zudem steigt die Komplexität der eingesetzten Systeme. Dies erschwert es potentielle Angriffe und Risiken überhaupt zu erkennen.

Der fortschreitende Einsatz von IT-Systemen führt somit unter anderem zu folgenden Veränderungen: Neue Möglichkeiten der Unterstützung, neue Einsatzgebiete, Veränderungen für den Benutzer im Umgang, Veränderungen für die Entwickler/Betreiber, Veränderungen bei den IT-Systemen, mehr Systeme pro Benutzer, Veränderungen der Bedeutung von IT-Systemen und ein erhöhtes Bedrohungspotential. Dadurch verändert sich auch die Rolle des Benutzers bei der Verwendung der Systeme. Diese neue Rolle soll nun im Hinblick auf die Erzielung von IT-Sicherheit beschrieben werden.

1.1 Motivation: Die Rolle des Benutzers bei der Umsetzung von IT-Sicherheit

Um die Vorteile der verbesserten Unterstützung optimal wahrnehmen zu können müssen die Risiken minimiert werden. Daher werden im Bereich IT-Sicherheit Konzepte und Maßnahmen zur Minimierung der Risiken erarbeitet. Die Maßnahmen dienen dazu IT-Systeme möglichst fehlerfrei und ausfallsicher zu betreiben, Missbrauch von Daten zu verhindern und potentielle Angriffe zu vereiteln. Verschiedene Verfahren und Sicherheitskonzepte sollen die Systeme dabei aus unterschiedlichen Bedrohungsperspektiven absichern.

Die zu erzielende Sicherheit von Systemen ist von folgenden Faktoren abhängig: Erkennung der Bedrohungen, Ergreifung geeigneter Gegenmaßnahmen und korrekte Anwendung/Einsatz dieser Maßnahmen. Das Spektrum möglicher Gegenmaßnahmen ist dabei sehr breit und durch die Art der Bedrohungen bestimmt. Es reicht vom Einsatz technischer über organisatorische bis hin zu designgetriebenen Maßnahmen. Die Maßnahmen erhöhen aber nur die Sicherheit der IT-Systeme, wenn sie korrekt und fehlerfrei angewendet und eingesetzt werden. Die Kenntnis einer Möglichkeit zur Email-Verschlüsselung erhöht beispielsweise die Sicherheit bei der Email-Kommunikation nicht, wenn man die Verschlüsselung falsch oder nicht anwendet.

Bei vielen Betrachtungen zu den Bedrohungen von IT-Systemen wurden nur Schadsoftware und böswillige Angreifer (Hacker) als potentielle Bedrohungen untersucht (vgl. [31]). Darauf basierende Gegenmaßnahmen wirken nur gegen Angriffe durch Hacker oder durch Schadsoftware. Ein Beispiel hierfür ist das Buch und die Sichtweise von Bruce Schneier „Applied Kryptografie“ [112]. In diesem schildert er die Möglichkeiten und Anwendungen der Kryptografie. Er kommt zu dem Schluss, dass mit korrekt implementierter Kryptografie ein Höchstmaß an Sicherheit erreicht werden kann. „Es genügt nicht, durch Gesetze geschützt zu werden. Wir müssen uns mit Mathematik schützen.“[1]

Eine neue Sicht über die Bedeutung von technischen Sicherheitsmechanismen und deren Benutzung wird in einem späteren Buch von Schneier sichtbar. Dort wandelte sich seine Meinung bezüglich der Erreichung von Sicherheit allein durch technische Möglichkeiten. In „Secrets & Lies“ [113] kommt er zu der Erkenntnis, dass der Benutzer das wichtigste Glied zur Erreichung von

[1] zitiert aus der deutschen Ausgabe von Secrets & Lies [113]

Sicherheit ist und das technische Möglichkeiten überschätzt werden.

Die neuen Einsatzkonzepte, wie der Einsatz von Assistenzsystemen, machen es notwendig das Verhalten von Benutzern mit in Sicherheitskonzepte einzubeziehen. Die Ausfallsicherheit und die Vermeidung eines möglichen Fehlverhaltens der IT-Systeme kann nicht mehr nur durch Hersteller gewährleistet werden. Auf zahlreiche Systeme haben Hersteller keinen Zugriff. Systeme werden in vielen Situationen einzig durch Benutzer betrieben und genutzt. In diesen Fällen müssen Benutzer mit ihrem Verhalten dafür sorgen das die Systeme fehlerfrei agieren.

In einigen Konzepten, wie dem Konzept der multilateralen Sicherheit [101], wurden Benutzer bereits als Akteure zu Erzielung von Sicherheit integriert. Allerdings wird in diesem Konzept nicht explizit das unwissentlich falsche Handeln von Benutzern untersucht. Die multilaterale Sicherheit geht davon aus, dass sowohl Hersteller als auch Benutzer von Systemen diese „angreifen“ können. Die Angriffsmöglichkeit ergibt sich daraus, dass beide Parteien unterschiedliche Sicherheitsinteressen haben. Jede Partei versucht ihre Sicherheitsinteressen durchzusetzen und kompromittiert dadurch möglicherweise die Interessen der anderen Partei.

Systeme sind aber nicht mehr nur bedroht durch mutwillige Angriffe von „Fremden“ sondern auch durch falsches Handeln der Benutzer. Die falsche Anwendung einer Sicherheitsfunktion stellt ebenso einen Angriff dar, wie die ungeschützte Verfügungstellung von sensiblen Daten. Das bedeutet für Sicherheitskonzepte, dass Benutzer um ihre Verantwortung wissen und sie wahrnehmen können und wollen. Benutzer müssen in der Lage sein sich korrekt zu verhalten. Benutzer dürfen Sicherheitskonzepte nicht unwissentlich oder absichtlich vereiteln und so die Sicherheit von IT-Systemen kompromittieren. Durch den allgegenwärtigen Einsatz der Informationstechnologie sind sich Benutzer der potentiellen Gefahren und Bedrohungen aber häufig nicht bewusst und gehen sorglos mit der IT um ([25],[75]). Der Fokus vieler Benutzer ist nicht darauf gerichtet, wie der Computer sicher funktioniert, sondern nur darauf dass die gewünschte Aufgabe erledigt werden kann. So kaufen viele Benutzer im Internet Waren ohne sich Gedanken zu machen, wie die Transaktion elektronisch gehandhabt wird.

Bei in Firmen genutzten Systemen kann die Verantwortung zum fehlerfreien und ausfallsicheren Betrieb durch Administratoren oder Hersteller übernommen werden. Durch den zum einen mobilen und zum anderen vernetzten Einsatz jetziger Systeme muss diese Verantwortung nun in großem Maße vom Benutzer übernommen werden. Im Gegensatz zu stationären Systemen können Administratoren bei mobilen Systemen weniger globale Schutzmecha-

nismen bereit stellen um den fehlerfreien Betrieb zu gewährleisten. Als Beispiel diene die Bereitstellung einer Firewall bei einem Firmennetzwerk durch die Administration. Die Benutzung mobiler Computer führt zu der Problematik, dass Maßnahmen nicht mehr auf einen vor dem Computer liegenden Zugangspunkt beschränkt sein können. Sobald ein Benutzer mit seinem mobilen Endgerät das gesicherte Firmennetz verlässt muss er die Verantwortung für die Sicherheit seines Systems zu einem Teil selbst übernehmen.

IT-Systeme sind mittlerweile in fast jedem Haushalt zu finden und werden auch von allen Bevölkerungsschichten genutzt. Viele Assistenzsysteme werden für das häusliche Umfeld entwickelt. So besitzt heutzutage fast jeder Haushalt einen Computer, mit dem die Bewohner auch das Internet nutzen. Je mehr Funktionen und Verantwortung durch Benutzer wahrgenommen werden, desto mehr steigt das Fehlerpotential durch den Benutzer. Die Gruppe der Systembenutzer wird aus diesem Grund größer und inhomogener. Heute handelt es sich bei vielen Benutzern um „Nicht-IT-Experten“ und um reine Anwender. Immer mehr Menschen müssen sich immer detaillierter mit IT-Systemen auseinandersetzen. Im häuslichen Umfeld können Schulungen kaum durchgeführt werden und es stehen keine geschulten Administratoren für die Wartung der Systeme zur Verfügung.

Neben der Bedrohung der Systeme durch eine potentielle Fehlbedienung stellt der Umgang der Benutzer mit Daten ein hohes Bedrohungspotential dar. Der erhöhte Komfort durch die Einführung von Assistenzsystemen wird durch eine Datensammlung über das Benutzerverhalten möglich. Dies führt zu einer Veränderung bei der Privatsphäre. Die Daten über die Benutzer können sowohl zur Optimierung der Unterstützung als auch zu erhöhtem Angriffspotential gegenüber dem Benutzer dienen. So können zum Beispiel RFID Chips in Kleidung integriert werden und Kaufhausdiebe entlarven [24] oder aber Einbrüche bei abwesenden Wohnungsinhabern erst ermöglichen. Regelungen müssen erdacht, umgesetzt und durchgesetzt werden, die einen Datenmissbrauch verhindern. Der Datenschutz muss auf diese neue Bedrohungslage angepasst werden [9].

Dies bedeutet, dass die zur Verfügung gestellten Möglichkeiten der Systeme auf die Bedürfnisse und Fähigkeiten der Benutzer angepasst sein müssen. Wenn es die Fähigkeiten des Benutzers nicht zulassen die Systeme fehlerfrei zu bedienen, kann er diese Verantwortung nicht übernehmen. Aus diesem Grund müssen Hersteller von Systemen dafür sorgen, dass die Systeme für die späteren Benutzer benutzbar sind. Benutzer müssen die Bedeutung der Systeme erkennen und sich richtig verhalten können, damit sie durch ihr Verhalten keine Fehlfunktionen oder Ausfälle auslösen oder ein erhöhtes Be-

drohungspotential erzeugen.

Die Einbeziehung der Benutzer in Sicherheitskonzepte stellt Hersteller und Benutzer vor einige Herausforderungen. Die Benutzergruppen werden immer inhomogener und es besteht nicht mehr die Möglichkeit die Benutzer durch Schulungen für eine korrekte Anwendung der Funktionen zu instruieren. Benutzer erkennen häufig nicht die Problematik ihrer Handlungen. Sie sind sich möglicher Gefährdungen nicht bewusst oder vermuten kein eigenes Risiko [126]. Eine weitere Herausforderung besteht im unterschiedlichen Erfahrungswissen der Benutzer und den daraus resultierenden Interpretationsmöglichkeiten von Hinweisen.

Hinweise der Hersteller zum korrekten fehlerfreien Umgang mit den IT-Systemen sind für viele Benutzer nicht eindeutig verständlich. Wenn die Benutzer die Hinweise nicht interpretieren können, führt das wiederum zu einem erhöhtem Fehlverhaltenspotential. Bei jeder Interpretation der Benutzer ist die Möglichkeit gegeben, dass sie Hinweise falsch interpretieren.

Daher muss das Verhalten der Benutzer analysiert und im Anschluss daran müssen Maßnahmen erstellt werden, die Benutzer zu einem eindeutig Fehlverhalten vermeidendem Handeln veranlassen.

Dass die Herausforderungen für die Einbeziehung der Benutzer zur Erzielung von IT-Sicherheit noch nicht zufriedenstellend umgesetzt sind und welche Probleme sich dabei ergeben, soll im Folgenden an Beispielen aus der Realität illustriert werden, um daraus im Anschluss die Ziele dieser Arbeit zu motivieren.

1.1.1 Beispiele für benutzerzentrierte IT-Sicherheit

Ein beliebiger Benutzer möchte einen PC in seinem heimischen Umfeld betreiben. Um den Computer sicher zu betreiben hat er bei der Einrichtung des Systems die folgenden Möglichkeiten:

- Er beauftragt jemanden den Rechner „sicher“ zu konfigurieren und vertraut ihm
- Er konfiguriert ihn selbst „sicher“
- Er tut nichts, da er sich keiner Gefährdung bewusst ist.

Die letzten beiden Möglichkeiten haben ihren Fokus auf der benutzerzentrierten IT-Sicherheit. Wenn der Benutzer sich keiner Gefährdung bewusst

ist, kann er die oben beschriebene Verantwortung für ein sicheres System nicht wahrnehmen. Untersuchungen zeigen, dass Benutzer in hohen Maß davon ausgehen, dass nur andere Benutzer Bedrohungen ausgesetzt sind (vergl. [126]). In diesem Fall haben die Anstrengungen des Herstellers nicht ausgereicht das Bedrohungspotential für den Benutzer zu verdeutlichen.

Wenn der Benutzer seine Verantwortung kennt und sie wahrnehmen will muss er in der Lage sein den Computer richtig zu konfigurieren und anschließend sicher zu betreiben. Die Problematik für viele Benutzer besteht an dieser Stelle in verschiedenen Aspekten. Zum einen werden bei IT-Systemen häufig Begriffe gewählt, die nur „IT-Experten“ geläufig sind (z.B. „Bytelänge für die Verschlüsselung wählen“.). Zum anderen werden viele Begrifflichkeiten im normalen Sprachgebrauch anders verwendet als bei IT-Systemen (z.B. die Verwendung des Begriffes Zone). Weiterhin können viele Benutzer die Auswirkungen ihrer Konfigurationseinstellungen nicht überblicken.

Aber nicht nur die Einrichtung eines Computersystems stellt Benutzer an vielen Stellen vor hohe Anforderungen, sondern auch die normale Benutzung. An vielen Stellen ist die Benutzung bei alltäglichen Aufgaben auf IT-Experten ausgelegt, wie das folgende Beispiel zeigt.

Ein Benutzer erhält während des Schreibens eines Textes die Meldung 1.2[2]. Bei Erscheinen der Meldung bearbeitete der Benutzer gerade eine Datei. Er speicherte seinen Text zu diesem Zeitpunkt nicht aktiv ab. Neben vielen Begriffen aus dem Wortschatz von IT-Experten (z.B. Freigabe remote) enthält die Meldung auch das Problem unterschiedlicher Interpretationsmöglichkeiten. Je nach gewählter Interpretation führt dies zu verschiedenen Handlungen des Benutzers. Die Tabelle 1.1 zeigt mögliche Interpretationen und Handlungen der Benutzer.

Das Beispiel zeigt, dass die Handlungen der Benutzer in Abhängigkeit ihrer Interpretation der Situation sehr unterschiedlich sein können. Die Interpretationen müssen dabei nicht auf korrekten Vermutungen über den Sachverhalt basieren. Die getroffene Wortwahl und fehlende Beispiele geben dem Benutzer nicht die Möglichkeit den Sachverhalt oder Folgen seiner Handlungen eindeutig zu überblicken.

Die Meldung in Abbildung 1.2 ermöglicht verschiedene mögliche Folgezustände. Die Benutzer wählen ihre Handlungen auf Grund von Vermutungen und nicht auf Grund der Kenntnis der Folgezustände[3]. Durch dieses

[2] Diese Meldung erschien bei Verwendung von Windows Word 2007. Bei anderen Programmen sind ähnliche Meldungen integriert.

[3] Eine Untersuchung zu diesem Thema befindet sich im späteren Verlauf dieser Arbeit.

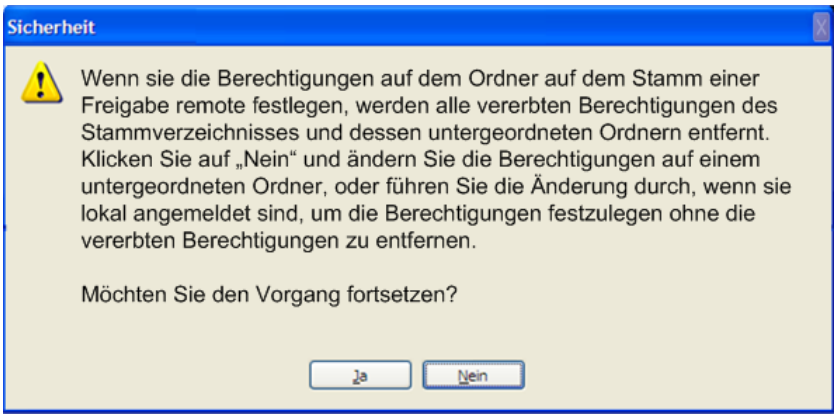


Abb. 1.2: Beispiel einer irreführenden Fehlermeldung

Vorgehen entsteht durch Benutzer ein hohes Risikopotential. Das Risiko besteht darin, dass Benutzer ein fehlerhaftes System, oder sogar dessen Ausfall, durch ihr Handeln erreichen. Besonders an den Stellen wo Benutzer mit „unverständlichen“ Handlungsoptionen konfrontiert werden kann es zu einer falschen Benutzung kommen. Handlungsoptionen sind dabei unverständlich, wenn Benutzer nicht die Ursache von Systemzuständen, deren Folgezustände oder Seiteneffekte erkennen.

Interpretation der Meldung	mögliche Handlung
Fehler des Computers der nichts mit der Tätigkeit zu tun hat	Ignorieren der Meldung
Fehlerhafte Berechtigung im Zielordner	Änderung der Rechte im Zielordner
Fehlermeldung wird nicht verstanden	?

Tab. 1.1: Verschiedene Interpretationsmöglichkeiten für die Fehlermeldung 1.2

Unverständlichen Meldungen führen auch zu einer weiteren Bedrohung. Durch häufige unverständliche Meldungen neigen Benutzer dazu Folgemeldungen vollständig zu ignorieren oder nur teilweise zu lesen. Daher werden kommende wichtige verständliche Meldungen ebenfalls ignoriert.

Durch unverständliche Warn-/Fehlermeldungen ist der Benutzer und das System somit den folgenden Bedrohungen ausgesetzt:

- mögliche Fehlbedienung, mögliche Fehleinschätzung der Situation oder

der Auswirkungen des eigenen Handels, Wahl von falschen (Folge-) Optionen

- Nichtbenutzung von technischen Möglichkeiten, die die Sicherheit erhöhen würden
- der Benutzer reagiert lethargisch auf weitere Fehlermeldungen und liest diese nicht mehr sorgfältig

Um diese Bedrohungen zu minimieren müssen Fehlermeldungen durch den Benutzer eindeutig interpretiert werden können. Sie müssen ihn zu eindeutigen Handlungen führen deren er sich auch bewusst ist. Er muss verstehen was er tut, warum er es tut und was sein Handeln für Folgen auslöst. Eine weitere Problematik von Assistenzsystemen besteht im Umgang von Benutzern mit Daten wie das folgende Beispielszenario zeigt.

Beispielszenario: Das Haus der Zukunft - vernetzte Dienste

Viele Forscher entwickeln IT-Systeme, die in zukünftige Hausumgebungen integriert werden und dort die Benutzer mit zahlreichen Diensten unterstützen. Die Systeme sammeln Daten über das Verhalten der Benutzer um ihre Dienste autonom anzubieten oder auszuführen. Auf der Grundlage der gesammelten und ausgewerteten Daten bieten sie ihre Dienste benutzerspezifisch an und optimieren sie. Beispiele hierfür sind Systeme wie sie in den Forschungsprojekten SerCHo [4] oder dem inHaus Projekt [5] verwirklicht wurden. Es werden Daten für den Benutzer (z.B. alle Informationen zu einem Hobby) und über den Benutzer (Verhalten des Benutzers bei der Benutzung des Systems) gesammelt. Die Daten werden für die Benutzer aufbereitet und ihnen zur Verfügung gestellt oder dienen für andere Dienste als Grundlage. Je mehr Dienste personalisiert angeboten werden können, desto besser können sie den jeweiligen Benutzer individuell unterstützen. Je mehr personalisierte Dienste angeboten werden, desto mehr Daten werden im System benötigt und sind dort vorhanden.

So sind beispielsweise im System SerCHo Dienste integriert, die für die Benutzer personalisiert Fitnesspläne erstellen. Das System sammelt die Daten über den Benutzer (Name, Größe, Gewicht) und generiert aus diesen einen

[4] DAI-Labor *Sercho - Service Centric Home*, http://www.dai-labor.de/projekte/laufende_projekte/sercho/, Zugriff 23.09.2008

[5] Fraunhofer-inHaus-Innovationszentrum *intelligente Raum- und Gebäudesysteme*, http://www.inhaus-zentrum.de/site_de/?node_id=2219, Zugriff 12.02.2009

Fitnessplan. Neben den positiven Aspekten der Unterstützung durch das System zur Erhöhung ihrer Fitness sind die Benutzer durch die Personalisierung Bedrohungen ausgesetzt. Der Gesundheitszustand des realen Benutzers kann hergeleitet werden, wenn seine reale Identität mit seinen Gesundheitsdaten verknüpft werden kann. Eine daraus resultierende Bedrohung bestünde darin, dass eine Versicherung auf Grund des Übergewichtes oder der mangelnden Fitness abgelehnt werden könnte. Weiterhin können die Systeme Daten über das Verhalten der Benutzer sammeln. Diese lassen sich dazu ausnutzen Angriffe direkt gegen den Benutzer auszuführen (personalisierte Phishing- oder Social-Engineering-Angriffe). Des Weiteren sind viele Benutzer der Meinung, dass sie sich nicht um die Verantwortung von Systemen kümmern müssen, die sie nicht kennen und auch nicht überblicken. Wenn der Benutzer aber zum einen nicht versteht, welchen Bedrohungen seine Daten und er selbst ausgesetzt sind und auf der anderen Seite nicht seine notwendige Verantwortung zur Umsetzung von Sicherheitszielen übernimmt, werden potentielle Angriffe erleichtert und das Risiko der Systeme steigt. Ein einfaches Beispiel in diesem Kontext ist die Eingabe von realen Benutzerdaten durch viele Benutzer [36]. Benutzer die sich der Bedrohung bewusst sind und ein Pseudonym eingeben minimieren die Bedrohung der Verknüpfung von System-internen Daten mit ihrer realen Identität.

Neben der Kenntnis der Bedrohungen müssen Benutzer auch einen Überblick über die Assistenzsysteme und deren Möglichkeiten haben. Um effektiv Maßnahmen zum Schutz ihrer Daten zu ergreifen müssen Benutzer wissen, wo ihre Daten bei einer intelligenten Hausumgebung überall verwendet und bedroht werden. Ebenso müssen sie Maßnahmen zur Erzielung höherer Sicherheit kennen und anwenden können.

Somit bieten sich unter Einbeziehung der Benutzer folgende Ansatzpunkte zu einer Verbesserung der IT-Sicherheit. Benutzer müssen die Kritikalität ihrer Daten erkennen. Die Eingabe von kritischen personengebundenen Daten durch den Benutzer (z.B. Verknüpfung der Identität des Benutzers mit seinen Daten) muss ebenso wie die Sammlung von Personen gebundenen Daten auf ein Minimum beschränkt werden. Die Unkenntnis der Benutzer und eine daraus resultierende Nichtbenutzung von technischen Möglichkeiten zur Erhöhung von IT-Sicherheit muss ebenfalls minimiert werden.

Zusammenfassend kann gesagt werden, dass Benutzer die sich nicht über die Bedrohungen und die Kritikalität ihrer Daten bewusst sind bei IT-Systemen ein hohes Bedrohungspotential darstellen. Die Systeme sind auf die Benutzer zentriert und benötigen eine Interaktion mit ihnen. Das schwächste Glied eines Systems bestimmt sein Sicherheitsniveau [82]. Das Sicherheitsniveau

beschreibt dabei die Stärke der Anstrengungen die ein Angreifer unternehmen muss um einen erfolgreichen Angriff durchzuführen. Viele Experten halten den Benutzer für das schwächste Glied [126]. Wenn Benutzer sorglos mit ihren Daten umgehen senken sie das Sicherheitsniveau.

Um das Sicherheitsniveau zu erhöhen müssen im Bereich der IT-Sicherheit Maßnahmen entwickelt werden, die das Verhalten des Benutzers in kritischen Situationen dahingehend beeinflussen, dass er sich Sicherheitsniveausteigernd verhält. Durch die stärkere Verantwortung des Benutzers werden Assistenzsysteme notwendig, die auch „Nicht-IT-Experten“ in die Lage versetzen Systeme korrekt zu verwenden. Obige Schilderung der Sicherheitsproblematik an verschiedenen Beispielen gibt dafür die folgenden Ansatzpunkte:

- Programme müssen so gestaltet werden, dass sie durch Benutzer nicht falsch interpretiert werden. Die verwendeten Begrifflichkeiten müssen durch unterschiedliche Benutzer gleich verstanden werden.
- Benutzer müssen Systeme und deren Möglichkeiten überblicken können.
- Benutzer müssen um ihre Gefährdung, die ihrer Daten und die der Systeme wissen.

Diese Aspekte lassen sich zusammenfassen zu: „Die Systeme müssen durch Benutzer benutzbar werden, um ein Höchstmaß an IT-Sicherheit bieten zu können.“ Benutzer müssen verstehen was sie tun, was von ihnen verlangt wird, welche Verantwortung sie haben und welchen Bedrohungen sie ausgesetzt sind. Diese Aspekte lassen sich zu einer im folgenden beschriebenen Vision von benutzerzentrierter IT-Sicherheit zusammenfassen.

1.1.2 Vision für eine benutzerzentrierte IT-Sicherheit

Vision:
„Intuitiv bedienbare allgegenwärtige IT-Sicherheit“

Das Verhalten des Benutzers ist wie beschrieben eine der Schlüsselfaktoren für die Umsetzung von IT-Sicherheit. Das bedeutet, dass IT-Sicherheit nur dann erreicht werden kann, wenn Sicherheitsfunktionalitäten in IT-Systemen

so bereit gestellt werden, dass Benutzer sie anwenden können und wollen. Für Benutzer stellt die IT-Sicherheit nur selten den primären Aufgabenfokus dar. Somit muss die IT-Sicherheit intuitiv anwendbar sein. Benutzer müssen Einsichten in IT-Sachverhalte, Gesetzmäßigkeiten und IT-Sicherheitsmechanismen haben ohne diskursiven Gebrauch des Verstandes. Dazu gehört auch, dass Interpretationsmöglichkeiten bei der Benutzung von Systemen oder Verständnisprobleme minimiert werden. Einfach verständliche allgemein verfügbare Sicherheit kann nur durch einfache Bedienbarkeit erreicht werden. Je mehr Benutzer bei der Benutzung über ihr Handeln nachdenken müssen, desto mehr Fehler sind möglich und das Ziel der intuitiven IT-Sicherheit wird verfehlt. Benutzer müssen intuitiv wissen welchen Gefahren sie ausgesetzt sind und wie sie diese geeignet abwehren können. Sicherheitsmechanismen müssen allgegenwärtig sein, zum Teil unsichtbar und unbemerkt agieren und von den Benutzern akzeptiert sein. Ob ein System intuitiv handhabbar ist, ist abhängig vom Erfahrungswissen des jeweiligen Benutzers und für viele Menschen unterschiedlich. Aber ein gemeinsames (z.B. kulturell geprägtes) Grundverständnis ist in vielen Bereichen vorhanden und kann verwendet werden.

Mit der Benutzbarkeit von Systemen befasst sich der Bereich der Usability (Gebrauchstauglichkeit). Ein hohes Maß an Usability ist notwendig, damit Benutzer Systeme akzeptieren, die Anweisungen im System verstehen und auch die Folgen ihres Handelns überblicken können. Somit ist ein hohes Maß an Usability notwendig, damit Benutzer auch Sicherheitsfunktionalitäten korrekt anwenden können.

Die Usability-Forschung möchte Programme für Benutzer leicht und intuitiv handhabbar machen. Sie stellt Techniken zur Verfügung, die es ermöglichen zu untersuchen wie leicht und intuitiv Benutzer Programme verwenden. Sie stellt Methoden bereit, die die Belastung für die Benutzer im Bezug auf die Benutzung minimieren sollen. Ein Höchstmaß an Usability ist dabei erreicht, wenn Systeme intuitiv verwendet werden können und die erwarteten Aktionen mit den tatsächlichen Aktionen übereinstimmen.

Wenn Programme durch Techniken des Usability-Engineering leicht und intuitiv handhabbar gemacht wurden, werden dadurch zugleich die Freiräume für Missverständnisse und Interpretationsmöglichkeiten minimiert. Ein korrekt verstandenes System wird weniger Fehler bei der Ausführung nach sich ziehen, als ein System, welches man durch „Raten“ benutzt. Daher leistet die Anwendung von Erkenntnissen aus der Usability-Forschung einen erheblichen Beitrag für die Erzielung von IT-Sicherheit. Durch die steigende Diversität der Benutzer wird dies weiter verstärkt, da althergebrachte Techniken zur

Schulung von Benutzern einen Wandel erfahren[6]. Um das Ziel intuitiver Benutzung vollständig zu erreichen müssten IT-Systeme streng genommen individuell konfiguriert werden, da Menschen unterschiedlich sind, unterschiedliche Erfahrungen haben und unterschiedliche Ziele verfolgen. Dies stößt aber an verschiedene Grenzen (Zeit, Aufwand, Kenntnis der Verschiedenheit der Benutzer). Eine erste praktikable Annäherung besteht darin Benutzer zu Gruppen zusammenzufassen. So können IT-Systeme gruppen-spezifisch konfiguriert werden. Der Aufwand zur Konfiguration wird mit der Minimierung von Interpretationsmöglichkeiten in ein rentables Verhältnis gesetzt. Die Abbildung 1.3 zeigt diesen Zusammenhang zwischen individuellen Lösungen, verschiedenen Lösungen für Gruppen und einer Lösung für alle. Die individuelle Lösung ist am Kosten intensivsten, da für jeden Benutzer die gleichen Kosten aufgewendet werden müssen. Bei einer Lösung für alle müssen dagegen nur Kosten für eine universelle Benutzergruppe aufgebracht werden. Das Potential zur Fehlbedienung steigt invers zum Einsatz der Kosten. Werden die Systeme individuell bereit gestellt, sind die Kosten hoch und Fehlbedienungspotential minimal. Benutzer haben in diesen Fällen Systeme die sie individuell intuitiv benutzen können. Werden dagegen die Kosten minimiert ist das Fehlverhaltenspotential maximal, da alle Benutzer das gleiche System benutzen. Begrifflichkeiten oder Prozesse werden hierbei nicht individuell, sondern für alle gleich bereit gestellt. Ein mittlerer Kostenaufwand ergibt sich durch den Einsatz von Gruppen. Dabei werden Systeme für unterschiedliche Gruppen spezifisch bereit gestellt. Je besser Benutzergruppen das Verhalten ihrer jeweiligen Gruppenmitglieder beschreiben, desto weniger Abweichungen gibt es im Verhalten der Gruppenmitglieder. Somit wird durch eine korrekte Wahl der Benutzergruppen auch das Fehlbedienungspotential gesenkt. Die geeignete Wahl von Benutzergruppen stellt damit einen Kompromiss zwischen notwendigen Kosten und Fehlbedienungspotential dar.

Die Erhöhung der IT-Sicherheit durch Bereitstellung von IT-Systemen für verschiedene Benutzergruppen bringt die folgenden Fragen: Welche Benutzergruppen sind im Kontext von IT-Sicherheit vorhanden? Die Verwendung von wie vielen Gruppen stellt den besten Kompromiss zwischen Kosten und Bedrohungspotential dar? Wie sehen die einzelnen Gruppen aus? Welches sind die wesentlichen Parameter der Gruppen?

Bei herkömmlichen Evaluationsmethoden werden diese Gruppen von „Experten“ bestimmt. Dies beinhaltet aber auch einige Herausforderungen. Experten legen die Anzahl der Gruppen basierend auf ihren bisherigen Erfahrungen fest. Diese Erfahrungen müssen aber nicht unbedingt 100% auf die

[6] Im Internetzeitalter werden die meisten Programm nicht durch Schulungen erlernt.

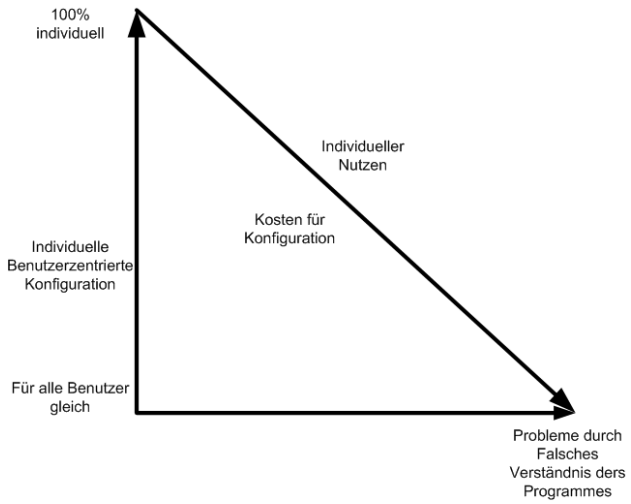


Abb. 1.3: Kosten Nutzen Relation bei der Konfiguration von Systemen

durchzuführende Evaluation passen. Bei der Bestimmung von Gruppen durch Fragebögen spielt es zum einen eine Rolle, ob die richtigen Fragen gestellt wurden, und ob die Versuchspersonen optimal antworten [108]. Ein anderer in der vorliegenden Arbeit beschriebener Ansatz besteht darin, die Benutzergruppen durch Interaktion der Benutzer mit Programmen zu ermitteln. Dieser Ansatz könnte die folgenden Vorteile bieten: Benchmark für Experten, Loslösung von Annahmen, Minimierung von Kosten, schnell durchführbar, Einsparung von Personal und Einbeziehung wichtiger, aber nicht bewusster Parameter.

Diese Arbeit liefert einen ersten Beitrag zur Erzielung von intuitiver IT-Sicherheit, indem Evaluationsmethoden für gruppen-spezifisches Benutzerverhalten zur Minimierung des Fehlverhaltenspotentials untersucht, erstellt und analysiert werden.

1.2 Ziele dieser Arbeit

Die Ziele dieser Arbeit bestehen darin einen ersten Beitrag zur späteren Verwirklichung der oben aufgestellten Vision zu liefern, indem zwei Fragestellungen untersucht werden. Zum einen muss untersucht werden, wie sich Benutzer in sicherheitsrelevanten Situationen verhalten und welchen Bedrohungen sie durch ihr Verhalten ausgesetzt sind. Zum anderen muss der Frage

nachgegangen werden, welche Verfahren geeignet sind, das Verhalten der Benutzer bedrohungsminimierend zu beeinflussen. Die Verwendung geeigneter Benutzergruppen stellt dabei ein adäquates Mittel zur Verfügung um kostensparend Bedrohungssituationen zu minimieren und wird daher detaillierter untersucht.

Aus der Vision, der im vorhergehenden Kapitel vorgestellten Motivation und diesen Zielen ergeben sich die folgenden Fragen, die in dieser Arbeit angesprochen, erörtert und geklärt werden sollen.

- Welche neuen Bedrohungen/Herausforderungen gibt es im Kontext zukünftiger Systeme wie zum Beispiel intelligenter Umgebungen oder ambienter Systeme? Welche Bedrohungen stellen Benutzer dar und in welchen Situationen sind sie bedroht?
- Erkennen Benutzer die Bedrohungen und wie verhalten sie sich in bedrohten Situationen?
- Anhand welcher Kriterien können zukünftige Systeme wie zum Beispiel intelligente Umgebungen oder ambiente Systeme ihre Unterstützung anpassen und optimieren?
- Wird die Problematik der benutzerzentrierten IT-Sicherheit durch heutige Zertifizierungen/Untersuchungsmethoden adressiert?
- Wie können Lösungen für die Problematik benutzerzentrierter IT-Sicherheit aussehen? Wie können Systeme Benutzer bei der Benutzung von IT-Sicherheit unterstützen? Wie kann durch gruppen-spezifische Betrachtung des Verhaltens eine Minimierung des Bedrohungspotentials erreicht werden?

Die folgenden Fragestellungen werden nur am Rand gestreift. Sie sind sie für den Bereich der benutzerzentrierten IT-Sicherheit ebenso wichtig, würden den Diskursbereich allerdings zu sehr vergrößern. Die Fragestellungen: Wie kann die Usability von Mechanismen der IT-Sicherheit durch neue Verfahren, wie zum Beispiel biometrische Authentifizierung, verbessert werden? Welche Aspekte des Datenschutzes sind bei der Untersuchung benutzerzentrierter IT-Sicherheit in welchem Ausmaß relevant? sollten in weiterführenden Arbeiten untersucht werden.

1.3 Zusammenfassung dieses Kapitels

IT-Systeme unterliegen zahlreichen Veränderungen. Diese Veränderungen führen zu Konzepten wie dem Ambient Assisted Living und den intelligenten Umgebungen. In diesen Konzepten assistieren die Systeme dem Benutzer, bieten ihre Dienste personalisiert und autonom an und sind auf eine hohe Interaktion mit ihm angewiesen.

Dies führt dazu, dass der Benutzer eine höhere Verantwortung bei der Umsetzung von IT-Sicherheit innehat. Er kann seiner Verantwortung nur gerecht werden, wenn er die Risiken erkennt und entsprechende Gegenmaßnahmen korrekt anwenden kann. Aus diesem Grunde müssen Assistenzsysteme im Hinblick auf die IT-Sicherheit benutzbar sein um potentielle Bedrohungsrisiken zu minimieren. Neben technischen Möglichkeiten muss der Benutzer wesentlicher Bestandteil bei zukünftigen Überlegungen spielen. Ein potentielles Fehlverhalten der Benutzer muss ebenso minimiert wie ihr Bewusstsein über die Kritikalität von Daten erhöht werden. Dies kann dadurch erreicht werden, dass IT-Sicherheit intuitiv gehandhabt wird.

Um eine intuitive Handhabung von IT-Sicherheit zu ermöglichen muss dass Verhalten der Benutzer analysiert werden. Um eine vollständige intuitive Verwendung umzusetzen müsste das analysierte Verhalten als Grundlage zur individuellen Bereitstellung dienen. Da dies in vielen Fällen aus Kostengründen nicht individuell für jeden Benutzer geschehen kann, müssen die Anwendungen für verschiedene Benutzergruppen bereit gestellt werden. Dadurch wird ein erster Schritt in Richtung intuitiver IT-Sicherheit erzielt. Die geeignete Wahl der Gruppen minimiert das Bedrohungspotential der Systeme durch Fehlbedienungen. Die Benutzung von Benutzergruppen im Kontext von IT-Sicherheit beinhaltet noch einige Fragen, die in dieser Arbeit erläutert werden.

Nach der Problemmotivation werden im folgenden Kapitel die Grundlagen für die angesprochenen Begrifflichkeiten „Trends bei IT-Systemen: Intelligente Umgebungen“, „Sicherheit“ und „Benutzbarkeit“ hergeleitet, eingeführt sowie für diese Arbeit definiert und beschrieben. Nach der Einführung dieser Begriffsbereiche werden die Bedrohungen der IT-Sicherheit an konkreten Studien herausgearbeitet und Gegenmaßnahmen vorgeschlagen und evaluiert.

Den Abschluss der Arbeit bietet eine Zusammenstellung der gefundenen Risiken bei intelligenten Umgebungen, eine Vorstellung einiger konkreter Gegenmaßnahmen sowie ein Ausblick auf zukünftige Forschungsbereiche.

2
Grundlagen

Η αυτόγνωσια ειναὶ ῆ πρώτη όλων τών γνωσέων

(Aristoteles)

In diesem Kapitel werden zunächst reale Beispiele für Trends bei IT-Systemen beschrieben um den Kontext zu zeigen, in welchem benutzerzentrierte IT-Sicherheit in Zukunft stattfindet. Bei diesen Trends zeigt sich, dass immer mehr verschiedene Benutzer immer umfangreicher durch die Systeme unterstützt werden und in immer stärkerem Maße mit diesen interagieren. Die beschriebenen Beispiele für die Trends bei IT-Systemen sind „intelligente Umgebungen“ und „ambiente Systeme“. Nach der Beschreibung von Trends bei IT-Systemen werden die weiteren notwendigen Grundlagen für diese Arbeit vorgestellt. Im speziellen sind dies die Bereiche „IT-Sicherheit“ und „Usability“. Diese beschriebenen Grundlagen liefern die notwendige Basis für die im darauf folgenden Kapitel vorgestellte Relation zwischen den beiden Bereichen IT-Sicherheit und Usability. Im darauf folgenden Kapitel wird dann das Problem der benutzerzentrierten IT-Sicherheit in der Praxis gezeigt und verschiedene Konzepte zur Problembeschreibung und Lösung herausgearbeitet und umgesetzt.

2.1 Trends bei der Unterstützung durch IT-Systeme

Wie im Kapitel 1 beschrieben verändern sich die Einsatzgebiete der Informationstechnologie. Die Informationssysteme werden kleiner und verbreiteter und können so in beliebige (Alltags-) Gegenstände integriert werden. Die Zusammenschaltung dieser Systeme führt zu intelligenten Umgebungen (im englischen „Ambient Intelligence“[39]). Die intelligenten Umgebungen stehen für einen Trend bei IT-Systemen. Da sich durch die Etablierung von intelligenten Umgebungen das Bedrohungspotenzial für Benutzer stark ändert, werden nun kurz intelligente und ambiente Umgebungen erläutert. Durch die veränderte Interaktion mit den Systemen entsteht die Notwendigkeit zu veränderten Evaluationsmethoden.

Intelligente Umgebungen und Ambient Assisted Living

Zukünftige Informationssysteme in Alltagsgegenständen sollen verschiedene Dienste anbieten, die die Benutzer unterstützen. Die Systeme assistieren Benutzern bei ihren Aufgaben, Zielen und Bedürfnissen mit den angebotenen Diensten und werden aus diesem Grund auch Assistenzsysteme genannt. Die Bedürfnisse und Ziele der Benutzer stehen im Vordergrund und nicht mehr die möglichen Funktionen der Geräte. Dazu sammeln die Systeme durch den Einsatz von Sensoren Daten über das Verhalten der Benutzer und passen auf der Grundlage dieser Daten ihre Unterstützung an. Dazu müssen sie erkennen, welche Personen sich in der Umgebung befinden und welche Unterstützung sie benötigen. Die Systeme müssen die Ziele und Aufgaben der Benutzer erkennen und geeignete Unterstützungen anbieten. Zur autonomen Unterstützung benötigen sie zudem die Fähigkeit zur Intentionserkennung und zur Strategieplanung. Systeme mit diesen Eigenschaften werden intelligente Umgebungen (IU) genannt [67].

Intelligente Umgebungen sollen dafür sorgen, dass der Fokus der Benutzer nur auf die Erledigung ihrer eigentlichen Aufgabe gerichtet ist. Benutzer sollen durch die Anwendung von Technologien nicht davon abgelenkt werden. Beispiele hierfür sind intelligente Konferenzräume ([103] oder [67]). Benutzer möchten in diesen Umgebungen die Technik wie Beamer oder Videokonferenzen nutzen um ihre Inhalte zu präsentieren oder sich abzustimmen. Sie möchten sich nicht mit der Einarbeitung von Geräten oder der Behebung von

Fehlfunktionen auseinander setzen.

> **Definition: Intelligente Umgebungen:**
> Bei intelligenten Umgebungen handelt es sich um IT-Systeme, die Benutzer unterstützen, indem sie Daten über die Benutzer sammeln und auf der Grundlage dieser Daten Dienste anbieten. Die angebotenen Dienste sollen die Ziele der Benutzer unterstützen. Aus diesem Grund müssen intelligente Umgebungen die Ziele der Benutzer erkennen (Erkennung der Intention) und Wege zur Zielerfüllung generieren (Entwicklung einer Strategie).

Einen Unterbereich der Intelligenten Umgebungen stellen Systeme des „Ambient Assisted Living“ dar. Bei Systemen aus dem Ambient Assisted Living (AAL) steht der Fokus in erster Linie auf der Unterstützung von Benutzern im alltäglichen Umfeld. Im Bereich AAL werden hauptsächlich Systeme für den Heimbereich entwickelt wie die im Kapitel 1 bereits angesprochenen Beispiele SerCho und inHaus. Ein weiterer wichtiger Schwerpunkt der Entwicklung von Anwendungen im AAL Umfeld ist die Unterstützung der veränderten Benutzerschicht hervorgerufen durch den demografischen Wandel [16]. Studien zeigen, dass die Geburtenzahlen sinken und die Menschen älter werden [117]. Dies führt auch dazu, dass die Benutzer von IT-Systemen im Durchschnitt immer älter werden. Somit müssen Systeme auf Grund des demografischen Wandels auch die immer größer werdende Zielgruppe der älteren Menschen als Benutzer im Fokus haben. Viele AAL-Anwendungen werden daher speziell zur Unterstützung älterer Menschen entwickelt. Ältere Menschen nehmen diese Dienste anders wahr (z.B. Erkennung von Oberflächen mit abnehmender Sehstärke). Außerdem brauchen ältere Menschen andere Dienste als jüngere Menschen (jüngere Menschen bewegen sich mehr, ältere Menschen haben dagegen mehr Erfahrungswissen.)

> **Definition: Ambient Assisted Living:**
> „Unter Ambient Assisted Living (AAL) werden Konzepte, Produkte und Dienstleistungen verstanden, die neue Technologien und soziales Umfeld miteinander verbinden und verbessern mit dem Ziel, die Lebensqualität für Menschen in allen Lebensabschnitten zu erhöhen. Übersetzen könnte man AAL am besten mit Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben. Damit wird auch schon skizziert, dass AAL in erster Linie etwas mit dem Individuum in seiner direkten Umwelt zu tun hat [8].“

Die Veränderungen durch die weitere Etablierung Intelligenter Umgebungen und ambienter Systeme sind in der folgenden Grafik 2.1 illustriert:

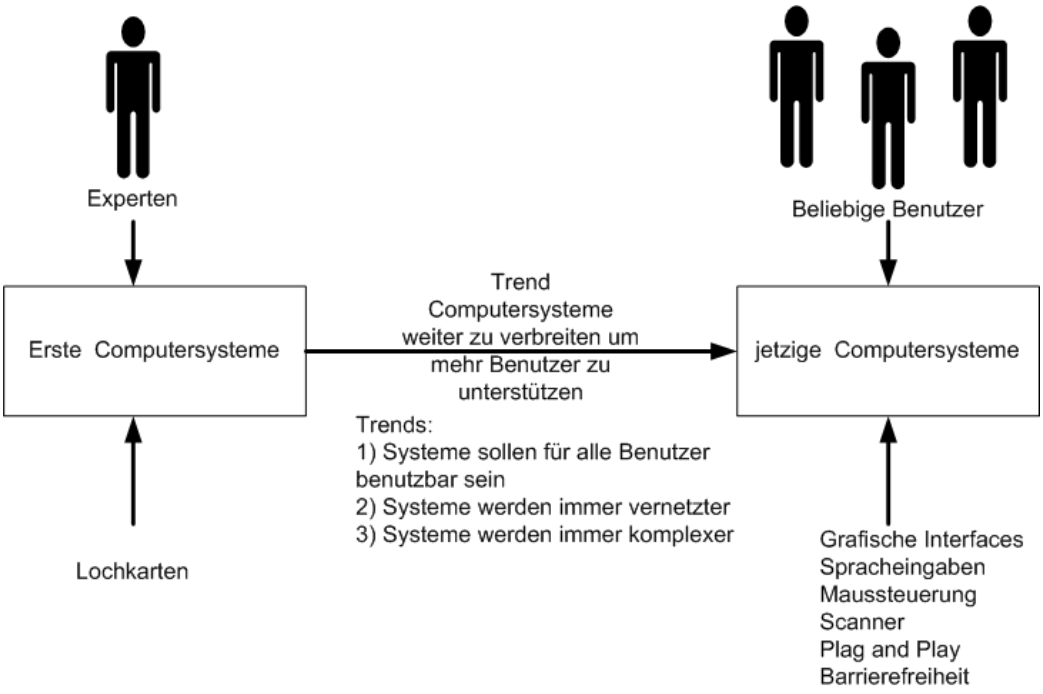


Abb. 2.1: Trends bei Computersystemen

Der Trend bei der Unterstützung durch IT-Systeme, wie z.B. durch intelligente Umgebungen oder speziell Anwendungen im AAL Umfeld, bringt neben den Vorteilen der Unterstützung auch neue Risiken.

Probleme bei intelligenten Umgebungen oder AAL Anwendungen

Mit den Risiken intelligenter Umgebungen befasste sich das Projekt SWAMI (Schutzmaßnahmen in einer Welt intelligenter Umgebungen[1]). Dort wurden verschiedene Szenarien entwickelt, die die Bedrohungslage in intelligenten Umgebungen herausarbeiteten ([43] und [11]).

Die folgenden Faktoren sind laut SWAMI der Auslöser für neue Bedrohungen in intelligenten Umgebungen:

- In IU-Anwendungen werden viele Aktivitäten der Benutzer mit Sensoren erfasst. Diese Daten werden innerhalb der Netzwerke übermittelt um die unterstützenden Dienste zu erbringen.

[1] Originaltitel: Safeguards in a World of Ambient Intelligence

- Die Zahl der Daten wird durch die Sensoren erhöht und die Anzahl der (möglichen) Verknüpfungen der Daten wird erweitert.
- Die Qualität der Daten wird durch immer weitere (verbesserte) Sensoren oder Verknüpfung mit anderen Daten verbessert (genauere Erfassungen, Abgleiche mit anderen Systemen und weitere Medien z.B. Kameras ...).

In SWAMI wurden verschiedene „Dunkle Szenarien“ entwickelt, die verschiedene Risiken und Herausforderungen von Intelligenten Umgebungen zeigen sollten. Diese dunklen Szenarien zeigen dabei negative Auswirkungen, die durch den Einsatz von Intelligenten Umgebungen entstehen könnten, wenn keine geeigneten Gegenmaßnahmen entwickelt werden. Sie dienen dazu potentielle Gefahren zu erkennen, um dann auf Grundlage dieser Gefahren Gegenmaßnahmen zu entwickeln. Dieser Ansatz basiert auf Verfahren zur Risikoanalyse und Bewertung (vgl. [105] oder [69]).

Die Analyse der Szenarien zeigte die Problembereiche Identität, Stress aufgrund von Abhängigkeit, Falsche Verdächtigungen, Kontrollverlust und bösartiger Angriff [43].

Um diese Risiken zu minimieren werden in SWAMI verschiedene Gegenmaßnahmen vorgeschlagen. Die Gegenmaßnahmen entfallen dabei auf die drei Kategorien: Technische, organisatorische und rechtliche Vorkehrungen.

Bevor die realen Risiken im Umfeld Intelligenter Umgebungen untersucht und konkrete Maßnahmen vorgestellt werden, werden nun die Begrifflichkeiten aus den Bereichen IT-Sicherheit und Usability vorgestellt.

2.2 Grundlagen im Bereich IT-Sicherheit

In diesem Abschnitt wird beschrieben, was im Rahmen dieser Arbeit unter IT-Sicherheit verstanden wird und warum IT-Sicherheit immer wichtiger wird. Es werden die grundlegenden Begriffe definiert und die für die IT-Sicherheit von Systemen wichtigen Komponenten geschildert.

2.2.1 Die Bedeutung von IT-Sicherheit und Daten

Informationen waren innerhalb der menschlichen Gesellschaft schon immer ein wichtiges und kostbares Gut. Wie bei Simon Singh in seinem Roman *Geheime Botschaften*[115] zu lesen ist, werden Informationen seit Herodot als äußerst wichtig angesehen und eingesetzt. Informationen dienen zum Nachrichtenaustausch und haben nach Herodot entscheidenden Einfluss über Aufstieg und Niedergang der einzelnen damaligen Königreiche.

Zum Austausch und Speichern von Informationen werden heute Systeme der Informationstechnologie (IT) verwendet. Die Informationstechnologie durchdringt unsere Gesellschaft in einem immer stärkeren und schnelleren Maße. Informationssensitive Maßnahmen und Geschäftsprozesse werden mit der Informationstechnologie durchgeführt und abgebildet. Gewohnte Methoden werden durch adäquate Prozesse in der IT ersetzt oder durch neue Methoden verdrängt. So findet beispielsweise ein großer Teil des Warenverkehrs nicht mehr real sondern virtuell innerhalb von IT-Systemen statt.

Kaufte man sich vor 30 Jahren noch Schallplatten, die physikalisch beim Händler eingetroffen sein mussten, so ist dieser Produktweg heute fast komplett digital ersetzt worden. Audiodaten werden zu einem großen Teil digital über das Internet vermarktet. Viele Prozesse des damaligen Produktverkehrs sind in digitale Prozesse überführt worden und werden heute durch digitalen Datenverkehr realisiert. Der frühere Prozess des Kaufes eines physikalischen Mediums ist durch den digitalen Prozess des Downloads abgelöst worden. Bei vielen Künstlern stehen ihre Werke nur noch digital im Internet zur Verfügung und ohne einen Computer kommt man an diese nur noch über Umwege heran. Da viele Prozesse ins Internet überführt wurden und dort stattfinden, muss ein Umdenken bei der Benutzung des Internets oder anderer IT-Systeme stattfinden.

Dadurch das immer mehr Güter eine Relation zu IT-Systemen haben wird der Schaden im Schadensfall immer größer und die Umsetzung von IT-Sicherheit zunehmend wichtiger [30]. Zugleich interagieren auch immer mehr unterschiedliche Benutzer mit diesen Systemen und die Thematik der Gebrauchstauglichkeit der bereit gestellten Sicherheitsanwendungen und deren Umsetzung bei den Systemen und Anwendungen wird zu einer zentralen Aufgabenstellung um eine hohe Akzeptanz und Benutzerzufriedenheit zu erzielen. „IT Sicherheit ist für die Akzeptanz des E-Commerce ein Schlüsselfaktor für den Kunden“ [114]. Wie in der Einleitung beschrieben können Sicherheitsmechanismen nur dann ihren Zweck bestmöglich erfüllen, wenn die Benutzer die Sicherheitsmechanismen akzeptieren und sie auch korrekt anwenden. Ein sehr gutes Verfahren zur E-Mail Verschlüsselung bringt gegenüber einer unverschlüsselten E-Mail keine Verbesserung, wenn der Benutzer das Verfahren nicht oder falsch anwendet. Somit müssen Benutzer sich der Gefahren bewusst sein und entsprechend handeln[2].

Um den Bedrohungen entgegen zu wirken, sind in Abhängigkeit der Bedrohung verschiedene Maßnahmen möglich und auch nötig. Güter und Waren sind seit jeher Bedrohungen ausgesetzt. Betrüger und Diebe versuchen Waren zu stehlen oder Informationen gewinnbringend gegen Andere einzusetzen. Die Veränderung des Datenverkehrs führt dazu, dass neben bisherigen Bedrohungen bei der Kommunikation und dem Datenverkehr neue Bedrohungen hinzukommen. Die Bedrohungen aus einer Zeit ohne Computer, wie zum Beispiel das Abhören eines Kommunikationskanals beim Telefon oder Betrug beim Warenverkehr, bleiben in der Welt vernetzter Computer von heute bestehen, werden aber um weitere Möglichkeiten mit Hilfe von Computern erweitert. So kann das Ablauschen eines Kommunikationskanals durch einen Computer dahingehend erweitert werden, dass z.B. der Computer das Entschlüsseln eines verschlüsselten Kanals erleichtert. Ein anderes Beispiel ist das Abbuchen von sehr geringen Beträgen (z.B. Rundungsfehler) auf andere Konten. Diese Bedrohung entsteht erst durch den Einsatz von Computern. Diese Beispiele zeigen auch eine Besonderheit von Angriffen mit Hilfe von Computersystemen. Diese Angriffe können permanent ohne Steigerung der Kosten wiederholt werden. Die Kosten für Angreifer sind bei Benutzung von IT-Technologie äußerst gering, der Schaden kann dagegen sehr hoch sein. Beispiele für die Schadensmöglichkeiten befinden sich im Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [26].

Um die Bedrohungen bei IT-Systemen zu minimieren oder sie sogar ganz

[2] Trotz vieler Berichte über verschiedene Attacken, z.B. allgegenwärtige Malware [111] oder auch der falsche Umgang mit Daten bei der Telekom [42], ist das Bewusstsein vieler Benutzer noch nicht sehr ausgeprägt wie spätere Untersuchungen in dieser Arbeit zeigen.

zu eliminieren werden Maßnahmen zur IT-Sicherheit ergriffen. IT-Sicherheit kann nur zum Teil durch technische Verfahren abgedeckt werden. Das Bewusstsein, wie Benutzer mit der Technik umgehen, spielt eine weitere vorrangige Rolle bei der Umsetzung der gewollten Sicherheitsziele.

Den Wandel der Bedrohung zeigt das folgende Beispiel: Wollte früher ein Betrüger die Betriebsgeheimnisse einer Firma stehlen, so musste er sie persönlich in der Firma vor Ort stehlen. Vor Ort musste er die dortigen physikalischen Schutzmechanismen (z.B. Mauern, Schlösser oder Wachschutz) überwinden um dann die realen Daten zu stehlen. Dieser Sachverhalt ist in Abbildung 2.2 illustriert. Heute kann ein Betrüger Betriebsgeheimnisse stehlen, indem er von einem beliebigen Punkt der Welt die Computersysteme der Firma angreift. Dadurch sinkt für ihn persönlich die Gefahr. Er kann durch verschiedene Vorkehrungen seine Identität verbergen. Der Zugriff auf einen erkannten Angreifer ist zudem erschwert, da er sich bei dem Angriff weit entfernt befinden kann. Der Ort von dem aus angegriffen wird und der Ort der angegriffen wird sind verschieden. Die Kosten für Angriffe werden geringer. Reisekosten für Reisen vor Ort entfallen, als Einbruchsmittel reicht ein PC und die Angriffe sind von ein und dem selben Ort aus reproduzierbar und können verschiedene Ziele an verschiedenen Orten angreifen. Diese Problematik ist in Abbildung 2.3 skizziert. Die Abbildung zeigt zudem eine weitere Herausforderung heutiger Systeme. Hatten früher nur bestimmte Personen den unmittelbaren Zugriff auf die Firmengeheimnisse (z.B. Geschäftsführer oder Ingenieure) sind heute die Systeme von nahezu allen Arbeitnehmern (z.B. Geschäftsführer, Werk-Studenten, Sekretärinnen, Entwickler, Administratoren...) einer Firma mit den Systemen auf denen die sensitiven Daten lagern verbunden. Der Zugriff auf die sensitiven Daten wird durch den Administrator mit Hilfe unterschiedlicher Berechtigungen gesteuert. Für die Benutzer innerhalb der Firma kommt eine weitere Herausforderung hinzu. Sie müssen erkennen welche Daten sicherheitsrelevant sind um sich entsprechend zu verhalten. Für das Unternehmen kommt hinzu, dass die Erkennung eines Angriffes erschwert ist.

Es änderte sich zum einen wo Daten gelagert werden und zum anderen, wer Zugriff auf diese Daten hat. Die steigende Anzahl an Informationen führt dazu, dass nicht bei allen Informationen klar ersichtlich ist welche sicherheitsrelevant sind. So kann zum Beispiel der Schichtplan oder das Telefonverzeichnis einer Firma in einem „Social Engineering“ Angriff verwendet werden um an Betriebsgeheimnisse zu gelangen. Kevin Mitnick führte zahlreiche dieser Angriffe in der Realität durch und zeigte, dass nahezu alle Daten für Social Engineering Angriffe verwendet werden können und sicherheitsrelevant sind und geschützt werden müssten [87].

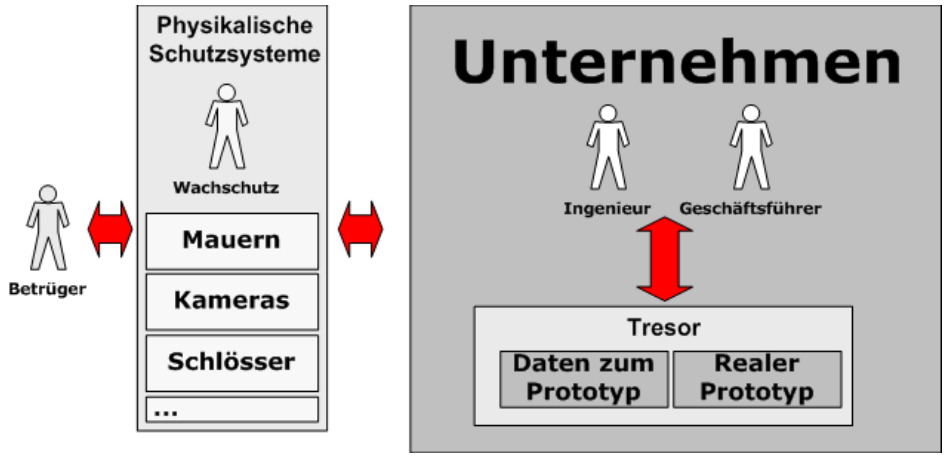


Abb. 2.2: Bedrohungen von Betriebsgeheimnissen ohne Computer

Die Bedeutung der IT-Sicherheit wird bei Müller und Pfitzmann als zentral für die heutige Wirtschaft angesehen. „Ob aber Unternehmen Konstruktions-, Kunden- oder Produktionsdaten austauschen sowie Geldtransaktionen vornehmen oder Privatleute Informationen und Güter über das Internet bestellen und bezahlen, ist eine Frage der Sicherheit der über das Netz bewegten Güter und Dienstleistungen.“[90].

Im Folgenden werden nun die Begrifflichkeiten im Bereich IT-Sicherheit definiert.

2.2.2 Begrifflichkeiten im Bereich IT-Sicherheit

Der Begriff IT-Sicherheit besteht aus den zwei Teilen *IT* und *Sicherheit*. IT steht dabei für Informationstechnologie und ist definiert als: „Informationstechnologie, Abkürzung IT [von englisch information technology], die Technik der Informationserfassung, -übermittlung, -verarbeitung und -speicherung mithilfe von Computern und Telekommunikationseinrichtungen“ [85]. Basierend auf dieser Definition werden in dieser Arbeit unter IT-Systemen sämtliche Computersysteme verstanden.

Für den Begriff Sicherheit lassen sich dagegen verschiedene voneinander stark abweichende Definitionen finden. Häufig wird unter dem Begriff IT-Sicherheit die „Abwesenheit von Gefahren bei IT-Systemen“ aufgefasst (vgl. [89]). Eine andere Definition ist beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu finden: „IT-Sicherheit bezeichnet die Sicherheit aller IT-Systeme. Ziel ist es, unberechtigte Zugriffe auf Computer und Netze zu

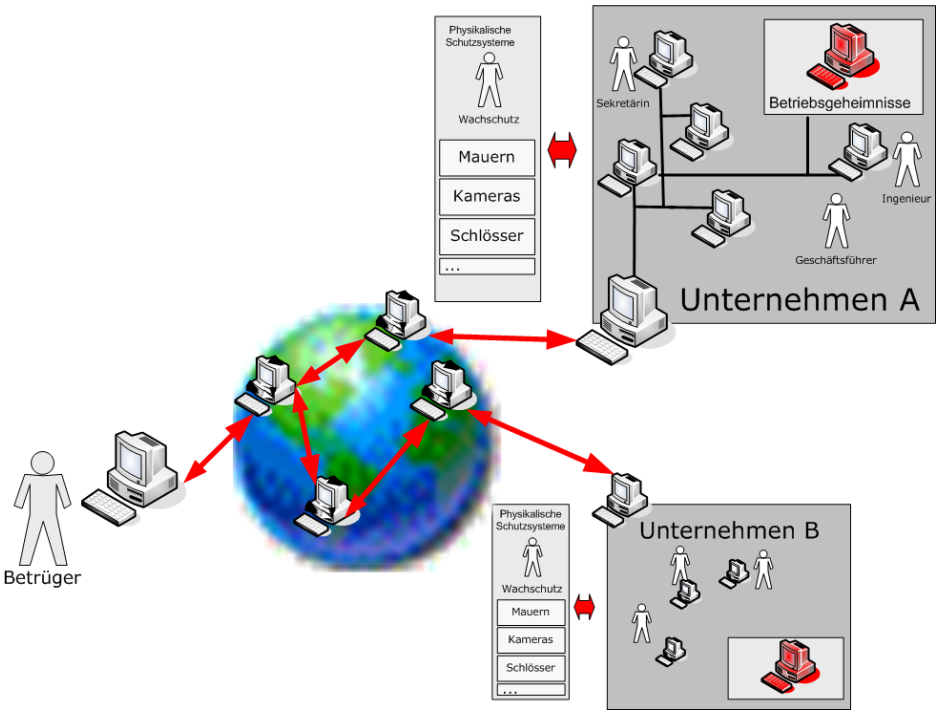


Abb. 2.3: Bedrohungen von Betriebsgeheimnissen auf Computern

verhindern. Dazu müssen sicherheitskritische Software- und Konfigurationsfehler in unsicheren Netzen, zum Beispiel dem Internet, erkannt und beseitigt werden“ [28].

Eine weitere detailliertere Definition von IT-Sicherheit findet sich in der ISO 17799 für Systeme im IT-Sektor. Dort wird der Begriff IT-Sicherheit definiert als: “Informationstechnische Sicherheit ist die Minimierung der Verwundbarkeit von Werten und Ressourcen“ [3]. IT-Sicherheit umfasst somit den Komplex aus möglichen Gegenmaßnahmen gegen Bedrohungen und Angreifer um Schutzziele zu erreichen [88]. Eine ähnliche Definition geben Rannenberg et al.: „Sicherheit besteht bei informationstechnischen (IT-) Systemen darin, dass Schutzziele trotz intelligenter Angreifer durchgesetzt werden können“. [101]

Eckert [38] erweitert die Definition von IT-Sicherheit, indem sie IT-Sicherheit in vier Bereiche unterteilt und diese gesondert definiert. Bei diesen Bereichen handelt es sich um *Funktionssicherheit*, *Informationssicherheit*, *Datensicherheit* und *Datenschutz*. Sie definiert diese Bereiche definiert im Detail folgendermaßen:

- "Unter Funktionssicherheit (engl. safety) eines Systems verstehen wir die Eigenschaft, dass die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt.
- Die Informationssicherheit (engl. security) ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.
- Die Datensicherheit eines Systems (engl. protection) ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen.
- Unter dem Begriff Datenschutz im engeren Sinn (engl. privacy), wie er unter anderem durch das deutsche Bundesdatenschutzgesetz (BDSG)[35] festgelegt wird, versteht man die Fähigkeit einer natürlichen Person, die Weitergabe von Informationen, die sie persönlich betreffen, zu kontrollieren [38]."

Mit diesen Definitionen präzisiert Eckert die Definition der ISO 17799 dahingehend dass sie die *Werte* und *Ressourcen* in verschiedene Kategorien unterteilt. Sie unterscheidet zwischen Informationen und deren Repräsentanten, den Daten. Weiterhin stellt sie fest, dass IT-Sicherheit nicht eine feste Eigenschaft eines Systems ist, sondern als Prozess aufgefasst werden muss, da die Systemeigenschaften sich über die Zeit ändern.

In der deutschsprachigen Literatur werden die Begriffe *Informationssicherheit* und *Security* häufig synonym mit dem Begriff der IT-Sicherheit verwendet (vergl. z.B. [90] oder [37]). In dieser Arbeit wird ebenso verfahren.

Aus den oben gemachten Definitionen lassen sich ebenfalls Ziele zum Schutz der Daten und Informationen ableiten. Diese so genannten Schutzziele sollen im Prozess zur Umsetzung von IT-Sicherheit erreicht und gegen Angreifer aufrecht erhalten werden. Rannenberg et al. benennen in [101] die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Eckert erweitert diese drei Schutzziele um die *Authentizität* und *Verbindlichkeit*. Gerade die Authentizität stellt bei vielen aktuellen und im Folgenden behandelten Sicherheitsproblemen eine Herausforderung dar. Für diese Arbeit werden die fünf Schutzziele wie folgt definiert.

Schutzziele in der IT-Sicherheit

Authentizität stellt sicher, dass Objekte und Personen wirklich die sind, die sie vorgeben zu sein. Man kann dabei zwischen Daten- und Benutzer-Authentizität unterscheiden. Bei Personen überprüft man die Identität der Person, bei Objekten hingegen ihren Ursprungsort (vergleiche Eckert [38]). Mit Authentizität wird sicher gestellt, dass der Benutzer seine wahre Identität nachprüfbar angibt oder dass die Quelle nachgeprüft werden kann, aus der Daten stammen. Aus diesem Grunde ist die Authentizität an eindeutig nachweisbare Merkmale der Personen oder Objekte gekoppelt. Bei Authentizität handelt es sich um Mechanismen zum Schutz vor der Vorspiegelung falscher Identitäten.

Das Schutzziel **Datenintegrität** besagt, dass zu schützende Daten weder unautorisiert noch unbemerkt verändert werden können. Veränderungen an Daten dürfen nur mit entsprechender Berechtigung vorgenommen werden. Dies bedeutet dass Mechanismen zur Datenintegrität Zugriffskontrollen auf die Daten darstellen. Diese regeln wer wie und worauf zugreifen darf und sorgen für die Unversehrtheit, Richtigkeit und Vollständigkeit der Daten.

Informationsvertraulichkeit ist dann gewährleistet, wenn keine unautorisierte Kenntnisnahme (Informationsgewinnung) möglich ist. Das bedeutet auch, dass die eigentliche Kommunikation mit Systemen unbemerkt stattfinden muss, da sich daraus auch Informationen ergeben. Die Mechanismen zur Erzielung von Informationsvertraulichkeit müssen über die bloße „Rechte-Vergabe“ hinausgehen, da dadurch Informationen von berechtigten Personen an Personen, die nicht berechtigt sind, gelangen können. (z.B. wenn sich die Berechtigungen überlappen)

Ein System setzt das Schutzziel der **Verfügbarkeit** um, wenn autorisierte und authentifizierte Benutzer jederzeit auf die Daten zugreifen können. Das bedeutet, dass sämtliche Betriebsmittel, bestehend aus Hardware und Software, in einem funktionsbereitem Zustand sein müssen.

Mit dem Schutzziel der **Verbindlichkeit** wird umgesetzt, dass Aktionen und Absprachen (z.B. Aushandlung elektronischer Verträge) eindeutig zugeordnet und nachgewiesen werden können. Ein Kommunikationspartner kann so im Nachhinein einen Vertrag nicht leugnen.

Können die genannten Sicherheitsschutzziele auch gegen intelligente Angreifer durchgesetzt werden, ist das System gemäß der ISO 17799 aus informationstechnischer Sicht *sicher* [60].

Da es unterschiedliche Mechanismen für die Erzielung der Schutzziele und

unterschiedlich „intelligente“ Angreifer gibt, wird auch noch der Begriff des Sicherheitsniveaus eingeführt.

Sicherheitsniveau: In Anlehnung an die Definition von Markotten in [81] beschreibt das Sicherheitsniveau die Stärke der Mechanismen Angreifern standzuhalten und die Schutzziele jeweils aufrecht zu erhalten. Die Niveaus verschiedener Mechanismen können durch Angriffe gemessen und miteinander verglichen werden. Die Sicherheitsniveaus sagen somit aus, bis zu welcher potentiellen Bedrohung ein Sicherheitsmechanismus sein Schutzziel gewährleistet.

Bedrohungen sind ein weiterer zentraler Aspekt des Themas IT-Sicherheit. Diese können die Nichtumsetzung der Schutzziele oder deren Verletzung durch Angreifer auslösen. Nachdem die Begriffe *IT-Sicherheit*, *Sicherheitsniveau* und *Schutzziele* definiert wurden, werden nun die Begriffe *Bedrohungen* und *Angreifer* näher erläutert.

Angreifer und Bedrohungen von Schutzzielen

Wie zuvor beschrieben dient IT-Sicherheit dazu „Verwundbarkeiten von IT-Systemen zu minimieren“. Jede Verwundbarkeit stellt einen potentiellen Angriffspunkt für einen Angreifer dar. Nach [21, 26ff] kann man bei verteilten Systemen zwischen aktiven (Vortäuschung einer falschen Identität, Wiedereinspielung, Veränderung einer Nachricht, Denial of Service) und passiven (Ausspähen, Nachrichtenverkehrsanalyse) Angriffen unterscheiden.

Alle potentiellen Angriffspunkte sind wiederum eine Bedrohung für die Sicherheit des Systems. Bedrohungen sind nach Eckert [38] definiert als: „Eine Bedrohung (engl. threat) des Systems zielt darauf ab, eine oder mehrere Schwachstellen oder Verwundbarkeiten auszunutzen, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen, oder um die Authentizität von Objekten zu gefährden.“ Somit müssen Mechanismen der IT-Sicherheit sämtliche Angreifer daran hindern die Schutzziele zu gefährden. Um dies zu erreichen muss geklärt werden, welche Angriffspunkte vorhanden sind und welche Angreifer sie mit welchen Angriffen ausnutzen könnten. Abbildung 2.4 zeigt dabei mögliche Angreifer in einem Beispielszenario. Die Grafik zeigt, dass nicht nur ein Angreifer mit böswilligen Zielen eine Bedrohung für die IT-Sicherheit darstellt. Mitarbeiter die aus Unwissenheit falsch handeln stellen ebenfalls eine große Bedrohung dar. Viele Angriffe werden zielgerichtet so aufgebaut, dass sie die natürliche Bedürfnisse der Benutzer ansprechen oder vertrauenswürdige Adressaten vorgaukeln (z.B. große Zeitungen, Informationsdienste oder Banken) und damit

die Benutzer zu fehlerhaften Handlungen verleiten [75]. „Die überwiegende Anzahl von Angriffen und Gefahren (beabsichtigt oder unbeabsichtigt) droht von den eigenen Mitarbeitern! (ca. 86 %). Diese Tendenz ist steigend. So waren es noch vor ca. 5 Jahren ca. 70 % von eigenen Mitarbeitern.“ [57] Eine große Bedrohung bei IT-Systemen besteht zum Beispiel darin, dass berechtigte Mitarbeiter ihre Zugangsdaten unberechtigten Personen mitteilen. Des weiteren zeigt die Grafik, dass Bedrohungen von IT-Systemen und den darauf lagernden sensitiven Daten nicht nur durch Schadprogramme ausgenutzt oder ausgelöst werden können, sondern auch durch verschiedene andere Angriffe. Aus diesem Grunde werden bei Evaluationen der IT-Sicherheit (z.B. Zertifizierungen) verschiedene Bereiche untersucht.

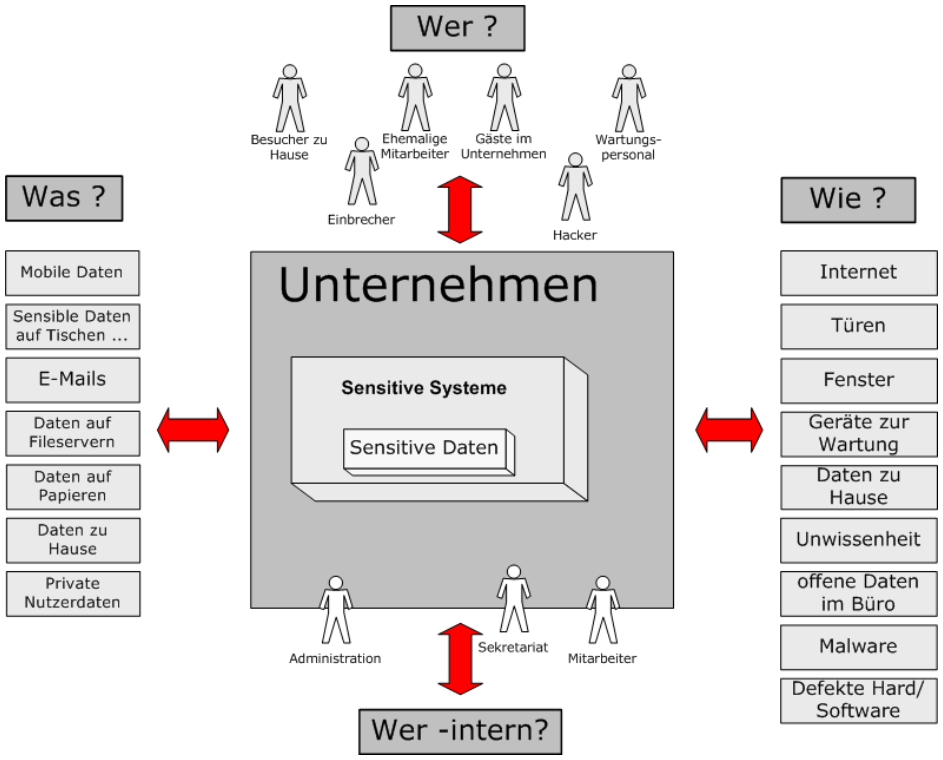


Abb. 2.4: Mögliche Bedrohungen von Betriebsgeheimnissen

Diese Schwachstellen und Verwundbarkeiten sollen durch Maßnahmen der IT-Sicherheit minimiert werden. Für die Entwicklung von Konzepten und Mechanismen zur Minimierung müssen die verschiedenen Angreifer, verschiedenen Angriffspunkte und Angriffstechniken situationsbedingt untersucht werden. Die Tabellen 2.1 und 2.2 zeigen Beispiele für mögliche Angreifer und Bedrohungen.

Potentielle Angreifer
Benutzer
Betreiber
Entwickler
Besucher (zu Hause/in der Firma)
Hacker
Wartungsdienste

Tab. 2.1: Potentielle Angreifer

Art der Bedrohung
Fehlfunktionen
Unwissenheit
Ignoranz
Schadsoftware
Social Engineering
Anruf
Phishing
Naturkatastrophen
Fehlbedienung
Unterschiedliche Erwartungen
physikalischer Einbruch

Tab. 2.2: Verschiedene mögliche Beispielbedrohungen

Die Bedrohungen durch Angriffe aus Tabelle 2.2 lassen sich in zwei große Kategorien unterteilen:

- Bedrohungen durch direkte Angriffe auf Systeme und Daten. Der Angreifer versucht direkt die Daten der sensitiven Systeme zu erhalten oder zu verändern. Ein Beispiel dafür ist das Auslesen eines Adressbuches durch ein Schadprogramm.
- Bedrohungen durch indirekte Angriffe zum Erhalt der Informationen über die Benutzer. Ein Beispiel hierfür sind Social-Engineering-Angriffe, bei denen Angreifer versuchen durch persönlichen Kontakt mit Benutzern Daten zu erhalten. Zum Beispiel der Anruf im Sekretariat einer Firma und der Erfragung von sensitiven Daten. Ein anderes Beispiel ist die benutzerrelevante Datensammlung ohne Einwilligung des Benutzers. Zu diesen Bedrohungen werden in dieser Arbeit auch die Bedrohungen gezählt, die durch falsche Benutzung der Benutzer entstehen.

Damit die zuvor geschilderten Schutzziele trotz dieser Bedrohungen erreicht werden können, müssen verschiedene Gegenmaßnahmen ergriffen werden.

Gegenmaßnahmen

Die Gegenmaßnahmen können dahingehend unterschieden werden, ob es sich um rein technische Gegenmaßnahmen handelt oder um darüber hinausgehende Systeme, die die Einbeziehung de Benutzers erfordern.

Bei **technisch basierten Gegenmaßnahmen** handelt es sich um Systeme, die größtenteils autonom die Angriffe abwehren. Zum Beispiel wehrt eine *Firewall* sämtliche Angriffe ab, für die sie entwickelt wurde. Der Benutzer muss sie zwar konfigurieren, aber nach der Konfiguration arbeitet sie selbstständig.

Benutzerzentrierte Gegenmaßnahmen sind auf ständige Einbeziehung der Benutzer angewiesen. Zum Beispiel kann eine Gegenmaßnahme darin bestehen gewisse Regelungen (sogenannte Policies) für die Firma aufzustellen, wie sich die Mitarbeiter verhalten müssen. Diese Art der Gegenmaßnahmen basieren darauf, dass der Benutzer permanent mit ihnen interagiert oder sie permanent anwendet. Zu diesen Gegenmaßnahmen können auch die Standards und Richtlinien gezählt werden, nach denen *sichere* Systeme oder Software entwickelt und benutzt werden.

Ein weiterer wichtiger Begriff bei der Um- und Durchsetzung von IT-Sicherheit ist das Sicherheitsbedürfnis der Benutzer.

Sicherheitsbedürfnis

Jeder einzelne Benutzer hat eine Vorstellung davon, was ein System in Bezug auf seine Sicherheit leisten kann und muss und welches Feedback er vom System erwartet. Daraus entwickelt sich sein Sicherheitsbedürfnis. Dieses ist immer subjektiv und ist von verschiedenen Faktoren abhängig. Es basiert auf den persönlichen Erfahrungen des Benutzers, der öffentliche Meinung, aktuellen Ereignissen, Politische Rahmenbedingungen, Einschätzung der Wichtigkeit der Anwendung, dem/der Angstpegel/schwelle des Benutzers (ein ängstlicher Benutzer hat ein höheres Sicherheitsbedürfnis, als ein mutiger) und der Kenntnis der Prozesse durch den Benutzer (vergl. [113, 55ff]). Das Sicherheitsbedürfnis eines Benutzers gibt an, wie hohe Anstrengungen er zur Umsetzung von IT-Sicherheit unternimmt und welches Bedrohungspotential er erkennt.

Nachdem die Begrifflichkeiten definiert wurden wird nun der Aspekt der Mehrseitigen Sicherheit besprochen. Dieser erweitert die beschriebene Sicherheitsthematik um den Aspekt, das verschiedene Gruppen verschiedene Zielsetzungen bei der Umsetzung von IT-Sicherheit haben.

Mehrseitige Sicherheit

Wie zuvor beschrieben, sind IT-Systeme Bedrohungen ausgesetzt. Benutzer und Betreiber wollen sich gegen diese schützen und ein gewisses Maß an Sicherheit erhalten und garantieren. Allerdings entsteht durch die Benutzung von Systemen die Problematik unterschiedlicher Sicherheitsziele. Nach Eckert [38] haben Benutzer die miteinander kommunizieren oder Daten austauschen meist verschiedene Schutzziele. Entwickler und Betreiber stellen in diesem Kontext Benutzer mit speziellen Zielen dar. Um die unterschiedlichen Schutzziele zu untersuchen wurde von Müller und Pfitzmann das Konzept der *Mehrseitigen Sicherheit* eingeführt [90]. Dieses Konzept erweitert den Begriff IT-Sicherheit um zwei weitere Aspekte:

1. Benutzer von IT-Systemen können unterschiedliche Schutzziele haben. Diese unterschiedlichen Sicherheitsanforderungen müssen zur Erzielung optimaler IT-Sicherheit alle berücksichtigt werden.
2. Jeder Benutzer eines IT-Systems ist ein potentieller Angreifer.

Mehrseitige Sicherheit bedeutet somit die Berücksichtigung der Sicherheitsinteressen aller beteiligten Personen [101] und [100].

Um die genannten verschiedenen Schutzziele umzusetzen und Bedrohungen zu erkennen um sie zu minimieren wurden verschiedene Standards und Überprüfungsverfahren im Bereich IT-Sicherheit entwickelt.

2.2.3 Standards und Normen im Bereich IT-Sicherheit

Standards und Normen im Bereich IT-Sicherheit sollen dazu dienen, die Risiken von und durch IT-Systeme durch den Einsatz von angemessenen Maßnahmen auf ein vertretbares Niveau zu reduzieren. 100%ige Sicherheit kann dabei nicht erreicht werden und wird somit auch nicht erwartet. Allerdings sollen durch die Normen im Bereich der IT-Sicherheit die Risiken benannt und durch mögliche Gegenmaßnahmen entschärft werden.

Des Weiteren dienen Normen und Standards im Bereich der IT-Sicherheit dazu, Systeme und Produkte hinsichtlich ihrer Sicherheitseigenschaften vergleichen zu können.

ISO 27002 (ehemals ISO17799)

Die ISO 27002 [5] bietet eine Sammlung von „Best Practices“ zum Erreichen von IT-Sicherheit. Aus diesem Grund kann keine Zertifizierung nach dieser ISO durchgeführt werden.

ISO 27001

ISO 27001 [4] basiert auf dem IT-Grundschutz [27] und ersetzt das Grundschutzzertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die ISO testiert bzw. zertifiziert individuell angemessene IT-Sicherheitsniveaus von IT-Systemen. Viele Ergebnisse und Erfahrungen der ISO 17799 sind in die ISO 27001 eingeflossen [66].

Dies ist eine international zertifizierbare Norm zum IT-Sicherheitsmanagement. Das Ziel der ISO 27001 besteht darin konkrete Anweisungen zum Aufbau eines Informations-Sicherheits-Management-System (ISMS) zu geben.

Ein weiterer wichtiger Standard im Bereich der IT-Sicherheit ist die im folgenden vorgestellte Zertifizierung nach den Common Criteria (CC).

Common Criteria

Nach den Common Criteria (CC) lassen sich sämtliche Arten von Systemen hinsichtlich der IT-Sicherheit zertifizieren. Ein wichtiges Ziel der Zertifizierung nach den CC ist die (weltweite) Vergleichsmöglichkeit mit anderen Systemen. Für Benutzer stellt die Vergleichsmöglichkeit der Sicherheitsfunktionalitäten basierend auf externen Gutachten einen entscheidenden Vorteil dar. Aus diesem Grund wird dieser Standard nun detaillierter vorgestellt.

Der Common Criteria Standard ist ein weltweit anerkannter Standard um Sicherheitsaspekte von Systemen zu definieren, zu beurteilen und zu messen. Dazu werden die zu zertifizierenden Systeme einer systematischen Prüfung im Hinblick auf IT-Sicherheit, der sogenannten Evaluation, unterzogen. Die Sicherheitsfunktionalitäten werden zu Beginn des Prozesses in dem Dokument Security Target (ST) explizit herausgearbeitet und beschrieben. Des weiteren werden diese Sicherheitsfunktionalitäten durch den CC-Prozess zugesichert, da sie einer unabhängigen Evaluation unterzogen und so überprüft werden.

Dies führt zu einem hohen Ausmaß an Vergleichbarkeit zwischen verschiedenen Systemen der gleichen Systemkategorie. Für Benutzer ist der Prozess der Zertifizierung sehr transparent, da jeder Benutzer die Möglichkeit zur Einsicht in den CC-Standard, in die CC-Methodologie und zumindest in die zugesicherten Sicherheitsfunktionalitäten hat. Weitere Informationen und Erklärungen des CC-Standards sind unter [6] zu finden. Neben den zugesicherten Sicherheitsfunktionalitäten werden die Schwachstellen des Systems ebenfalls im Prozess der Zertifizierung untersucht und sind Bestandteil des Zertifizierungsprozesses.

Beim Prozess der Zertifizierung wird ein zu evaluierendes System nach einem standardisierten Verfahren von einer unabhängigen Prüfstelle untersucht. Am Prozess sind drei Gruppen beteiligt. Das Unternehmen, welches ein Produkt entwickelt, Evaluatoren, welche die Prüfungen durchführen und Zertifizierer, die am Ende des Prozesses das Zertifikat vergeben. Der gesamte Prozess gliedert sich in drei Phasen. In der Phase der Vorevaluierung klären die beteiligten Parteien die Rahmenbedingungen der Zertifizierung ab. Bei der Phase Evaluierung wird der Evaluierungsgegenstand (EVG) zahlreichen Tests unterzogen und verschiedene Dokumente werden erstellt. Zum Abschluss wird in Phase Zertifizierung das Zertifikat ausgestellt.

Während des Zertifizierungsprozesses müssen spezielle definierte Dokumente erstellt werden. Diese beschreiben zum Teil Prozesse des zu zertifizierenden Unternehmens und zum anderen die Ergebnisse der Überprüfungen. Die Dokumente beinhalten dabei festgelegte Zusicherungen und Untersuchungen zu dem EVG. Um eine spätere Vergleichbarkeit und eine Detailtiefe der Überprüfungen zu ermöglichen, stehen den Herstellern sieben verschiedene Evaluation Assurance Levels (EALs) zur Verfügung. Je höher der gewählte Level ist, desto detaillierter und umfangreicher werden die Überprüfungen und somit die Dokumente.

Begonnen wird jede Zertifizierung mit der initialen Definition des EVG und der darauf basierenden Erstellung des „Security Target“ (ST). Der Evaluierungsgegenstand wird bei der Zertifizierung in einer konkreten Instanz untersucht und zertifiziert. Im Security Target werden alle Anforderungen und Funktionalitäten in Bezug auf die IT-Sicherheit definiert. Aus diesem Grunde dient das ST als Basis für den gesamten Verlauf und die weiteren Dokumente der Zertifizierung.

Die weiteren einzelnen Dokumentenklassen sind: Sicherheitsvorgaben (ST), Lebenszyklusunterstützung (ALC), Konfigurationsmanagement (ACM), Auslieferung und Betrieb (ADO), Entwicklung (ADV), Handbücher (AGD), Tests (ATE) und Schwachstellenbewertung (AVA). Durch die vorgegebenen

nötigen Dokumente wird der Prozess zeitlich strukturiert, da zwischen den Dokumenten Abhängigkeiten bei der Erstellung bestehen. Außerdem werden verschiedene Sichten auf den EVG untersucht und auf Schwachstellen hin analysiert.

Die Abbildung 2.5 zeigt den zeitlichen Ablauf anhand der erstellten Dokumente bei einer Zertifizierung nach den CC.

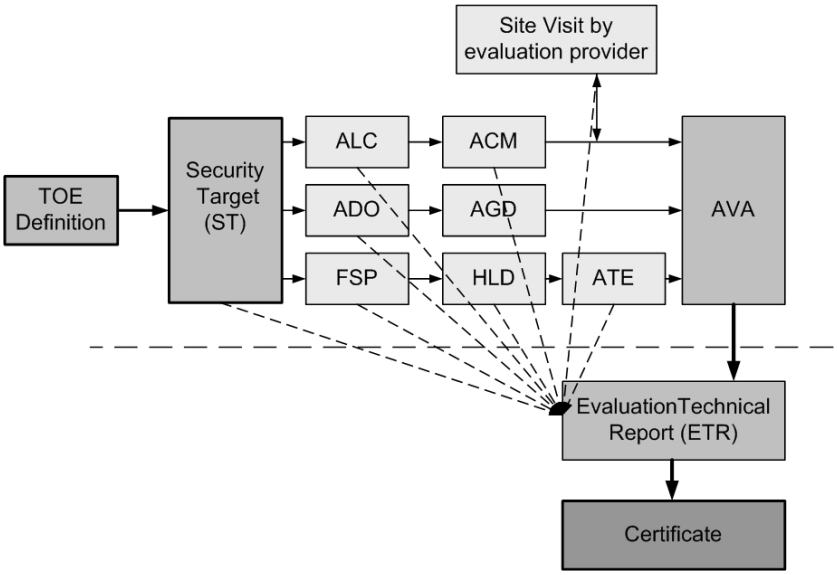


Abb. 2.5: Zeitlicher Ablauf der Zertifizierung von JIAC IV

Fazit zu Normen und Standards im Bereich IT-Sicherheit

Die Standards im Bereich der IT-Sicherheit haben die Sicherheitsfunktionalitäten und den genormten Umgang mit diesen im Mittelpunkt. Sie verschaffen die Möglichkeit verschiedene Systeme hinsichtlich technischer Aspekte miteinander zu vergleichen. Sie gehen aber nicht sehr detailliert auf unterschiedliche Benutzer oder Benutzergruppen und deren unterschiedliches Verhalten ein.

2.2.4 Zusammenfassung von Abschnitt 2.2

Für die vorliegende Arbeit wird der Begriff IT-Sicherheit aus diesen Definitionen abgeleitet und folgendermaßen definiert.

> **Definition IT-Sicherheit:**
> Unter IT-Sicherheit wird der gesamte Komplex aus Verwendung und Interaktion von IT-Systemen mit Benutzern und die daraus resultierenden Bedrohungen, Gefahren und mögliche Gegenmaßnahmen zur Umsetzung von Schutzzielen verstanden.

Sicherheit ist eine nichtfunktionale Anforderung, die meist nicht nur durch den klassischen Programmcode abgedeckt wird. Es müssen weitaus mehr Facetten betrachtet werden. Die Rolle des Benutzers hat dabei einen entscheidenden Einfluss darauf, in wieweit Sicherheits- und Schutzziele umgesetzt werden können.

Aus diesem Grund wird im nächsten Abschnitt der Bereich der Usability erläutert. Dieser untersucht wie „benutzerfreundlich“ Systeme sind.

2.3 Grundlagen im Bereich Usability

Software wird entworfen und implementiert um Menschen bei ihren Tätigkeiten zu unterstützen. Mittlerweile befinden sich Computer in nahezu allen Haushalten und Bereichen des täglichen Lebens. Durch die Verbreitung des Computers müssen diese für nahezu alle Bevölkerungsschichten bedienbar sein. Konnte man früher durch Schulungen für die kleine spezielle Gruppe der Experten Probleme bei der Bedienung der Software beheben, müssen Systeme heute intuitiv für eine viel größere Gruppe an Benutzern bedienbar sein.

Benutzer sollen Software-Systeme anwenden um die gewünschten Aufgaben zu erledigen und Ziele zu erreichen. Verwendet ein Benutzer eine Anwendung, bildet er sich auf Grund seiner Erfahrungen und der Summe seiner Eindrücke ein Urteil darüber, wie gut, wie bedienfreundlich oder „leicht“ er diese Anwendung benutzen kann. Durch die immer größer werdende Programmvielfalt werden Benutzer die Systeme auswählen, die ihre gewohnten Prozesse am besten unterstützen.

Mit der Thematik, wie intuitiv Systeme bedienbar und wie benutzerfreundlich sie sind befasst sich die Wissenschaft der Usability (Gebrauchstauglichkeit)[3]. Der Aspekt der Usability strebt die optimale Unterstützung der Benutzer an, indem er ihre Bedürfnisse und deren Umsetzung analysiert und fördert.

Wenn ein Programm unverständlich oder zu kompliziert zu bedienen ist, wird stattdessen ein anderes Programm gewählt. Die Berücksichtigung der Usability-Eigenschaften, der einfachen, intuitiven und allgemeingültigen Bedienung von Systemen wird aus diesem Grund immer selbstverständlicher werden. Dabei sind die Usability-Eigenschaften für alle Schnittstellen zum Benutzer wichtig (vergleiche [76]).

Weiterhin ist es wichtig, dass der Benutzer ein Feedback seiner Interaktion bekommt, um der Arbeitsweise des Systems zu vertrauen und sich selbst zu vergewissern. Diese und weitere Usability Aspekte finden sich in den 10 Usability-Heuristiken von Jakob Nielsen[4] wieder [95]. Neben diesen allgemei-

[3] Da in der Fachliteratur fast immer der englische Begriff Usability an Stelle des deutschen Gebrauchstauglichkeit verwendet wird, wird in dieser Arbeit ebenso verfahren.

[4] Jakob Nielsen wird als ein führender Experte auf dem Gebiet der Usability angesehen. Auf seiner Website *www.useit.com* finden sich aktuelle Beiträge und Kritiken zu ausgewählten Themen.

nen Kriterien gibt es auch internationale Normen, wie die DIN ISO 9241-11 [2] und DIN ISO 13407 [1], die Vorgaben für die Gestaltung von Software und Interaktionsdialogen machen. Diese sind im Detail feiner ausgearbeitet als Nielsens Heuristiken, können aber auch zu einem anderen Verständnis von Usability führen und zeigen die Komplexität des Begriffs auf [62].

Der Computer ist ein Arbeitsmittel und soll durch Konzepte der Usability auf die besonderen Fähigkeiten und Schwächen seiner Benutzer angepasst werden. Das Ziel besteht darin, dass Benutzer dieses Arbeitsmittel optimal einsetzen können.

In der Literatur werden dabei häufig die Begriffe Usability, Benutzbarkeit und Benutzungsfreundlichkeit synonym verwendet [59]. Aus diesem Grunde erfolgt im Folgenden die Festlegung Begrifflichkeiten für die vorliegende Arbeit.

2.3.1 Definition der Begrifflichkeiten im Bereich Usability

Eine Definition des Begriffes Usability befindet sich in der ISO 9241-11 [2]. Der Begriff Usability wurde dabei in der deutschen Fassung mit mit Gebrauchstauglichkeit übersetzt. Da sich der englische Begriff *Usability* allerdings auch im deutschen Sprachraum etabliert hat, wird er im Folgenden weiter verwendet.

> **Usability gemäß der ISO 9241-11:**
> „Extend to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use“
> **Gebrauchstauglichkeit gemäß der DIN EN ISO 9241-11:**
> „Das Ausmaß in dem ein Produkt durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“[2]

Die Teilbereiche *Effizienz, Effektivität* und *Zufriedenheit* sowie der Begriff *Nutzungskontext* sind in der ISO ebenfalls wie folgt definiert.

Effektivität: „Die Genauigkeit und Vollständigkeit, mit der Benutzer ein bestimmtes Ziel erreichen.“ [2]

Effektivität geht also der Frage nach, ob ein Benutzer eines Programms seine Ziele mit dem Programm erreichen kann und wie genau das Ergebnis mit

dem Ziel übereinstimmt. Das bedeutet das dieser Usability-Aspekt nur auf die Ziele und Arbeitsergebnisse der Benutzer referenziert und nicht auf den eingesetzten Aufwand zur Zielerreichung. In der ISO wird bei diesem Aspekt nicht darauf eingegangen, dass die Ziele der meisten Benutzer bei einer Programmbenutzung unterschiedlich sind.

Das folgende Beispiel soll den Aspekt der Effektivität verdeutlichen. Ein Benutzer möchte seinen eigenen Rechner vor „Schadsoftware“ aus dem Internet schützen. Aus Sicht der Effektivität besteht das Ziel darin dass keine Schadsoftware aus dem Internet auf den eigenen Rechner gelangt. Besonders effektiv sind die Maßnahmen des Benutzers, wenn gar keine Schadsoftware auf den Rechner gelangt. Besonders ineffektiv sind sie, wenn sehr viel Schadsoftware aus dem Internet auf den Rechner gelangt. Über den Aufwand um das Ziel zu erreichen, wird an dieser Stelle aber nichts ausgesagt. Denn auch ein Maßnahme mit sehr geringem Aufwand kann sehr effektiv sein. Eine solche Maßnahme wäre zum Beispiel den Rechner vom Internet zu entkoppeln (dem Betreiben des Rechners ohne Verbindung zum Internet). Allerdings kollidiert diese Maßnahme mit dem dritten oben genannten Aspekt der Usability. Die meisten Benutzer sind nicht zufrieden wenn sie keine Verbindung mit dem Internet haben.

Effizienz: „Der im Verhältnis zur Genauigkeit und Vollständigkeit eingesetzte Aufwand, mit dem Benutzer ein bestimmtes Ziel erreichen.“ [2]

Der Aspekt der der Effizienz untersucht den zur Aufgabenerledigung benötigten Aufwand. Das Effizienzkriterium behandelt die Frage wieviel Aufwand zur Zielerreichung notwendig ist.

Im oben genannten Beispiel sind verschiedene Maßnahmen denkbar, um einen Rechner vor Schadsoftware aus dem Internet zu schützen. So können Benutzer eine Firewall auf dem eigenen Rechner installieren, die Firewall eines verwendeten Zugangsrouters benutzen, ein Betriebssystem verwenden welches nicht so anfällig für Schadsoftware ist oder aber sie verwenden die Sicherheitsmechanismen der Zugangsbrowser. Alle diese Maßnahmen sind mit unterschiedlichem Aufwand verbunden, sollen aber das gleiche Ziel erreichen. Je nach Kontext ist es sogar möglich, dass all diese Maßnahmen die gleiche Effektivität bei unterschiedlicher Effizienz haben. An diesem Beispiel wird auch ein weiterer Aspekt der Effizienz sichtbar. Sie ist abhängig von unterschiedlichem Erfahrungswissen und unterschiedlicher Lernerfahrung der Benutzer. Unterschiedlich trainierte Benutzer haben somit ein unterschiedliches Usability-Empfinden.

Zufriedenstellung: „Freiheit von Beeinträchtigungen und positive Einstellungen gegenüber der Nutzung des Produkts.“ [2]

Zufriedenheit ist eine subjektive Empfindung der Benutzer beim Umgang mit der Software. Sie bezieht auch stark die Persönlichkeit und die bisher gemachten Erfahrungen der Benutzer mit ein. Im oberen Beispiel ist es wichtig, dass die Benutzer zum einen das Gefühl haben sehr effizient und effektiv ihr System gesichert zu haben und zum anderen sich nicht bei ihren Tätigkeiten beeinträchtigt fühlen.

Ob das System wirklich effektiv geschützt ist, zeigt sich erst im Verlauf der Benutzung des Systems. Wenn dann allerdings durch ein Schadsoftwareproblem die Ineffektivität des Systems gezeigt wird, wechselt damit auch die Zufriedenstellung des Benutzers, da er einen Zielkonflikt feststellt.

Nutzungskontext: Nutzungskontext: „Die Benutzer, die Ziele, Aufgaben, Ausrüstung (Hardware, Software und Materialien) sowie die physische und soziale Umgebung, in der das Produkt genutzt wird“ [2].

Die Begriffe Effektivität und Effizienz beziehen sich auf objektiv messbare Eigenschaften einer Anwendung. Der Begriff Zufriedenheit hat dagegen einen subjektiven Bezug zum Benutzer. Alle drei Bereiche werden beim „Nutzungskontext“ einer Anwendung zusammengeführt. Der gesamte Kontext mit all seinen Facetten muss bei der Beurteilung von „Usability“ analysiert und miteinbezogen werden.

Usability Kriterien

Neben der beschriebenen Definition von Usability aus der ISO 9241 gibt es weitere Herangehensweisen für die Erreichung des Zieles benutzer- und bedienerfreundlicher Systeme. So definierte 1993 Nielsen verschiedene Aspekte, die bei der Entwicklung von Systemen umgesetzt werden sollten damit sie ein hohes Maß an Usability aufweisen:

1. „Lernfähigkeit: Wie leicht ist es für die Anwender, grundlegende Aufgaben zu vollenden, wenn sie das erste Mal mit dem Design zu tun haben?
2. Effizienz: Wie schnell können die Anwender Aufgaben erledigen, wenn sie das Design einmal kennen gelernt haben.
3. Leicht erinnerbar: Wie leicht haben es die Anwender, sich wieder zurecht zu finden, wenn Sie nach einer Zeitspanne wieder zum Design

zurückkehren, ohne es benutzt zu haben?

4. Fehler: Wie viele Fehler machen die Anwender? Wie schwerwiegend sind diese Fehler? Und wie leicht können sie sich wieder von diesen Fehlern erholen?

5. Zufriedenheit: Wie angenehm ist es, das Design zu verwenden?“[96]

Diese Kriterien sind bei Untersuchungen über Websites von Nielsen erarbeitet worden, können aber auf fast alle Bereiche der Informationstechnologie übertragen werden. In wie weit sie sich auf Mechanismen übertragen lassen, die zur Herstellung von IT-Sicherheit dienen soll im Verlauf der Arbeit ebenfalls geklärt werden.

Werden die oben beschriebenen Aspekte der Usability umgesetzt erhöht sich nach Nielsen die Akzeptanz des Systems durch die Benutzer, denn diese fünf Bereiche sind wesentliche Bestandteile der Systemakzeptanz. Nielsen erarbeitete in [94] ein Modell der Systemakzeptanz. Die Grafik 2.6 veranschaulicht, welche Bestandteile Nielsen bei der Systemakzeptanz ermittelte und wie wichtig die fünf oben genannten Bereiche der Usability dabei sind.

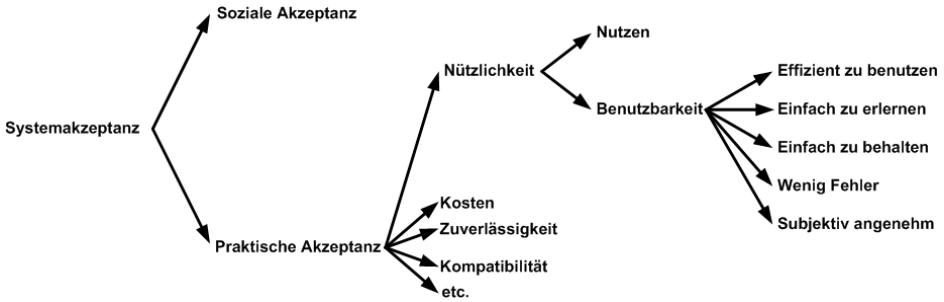


Abb. 2.6: Bestandteile der Systemakzeptanz nach Nielsen [94]

Vorteile durch die Umsetzung „hoher“ Usability

Nachdem beschrieben wurde was Usability ist, und welche Aspekte dabei zu beachten und zu untersuchen sind, werden im Folgenden kurz die entscheidenden Vorteile hoher Usability aufgelistet. Dies zeigt dass die zielgerichtete Entwicklung von Systemen mit hoher Usability (Usability Engineering) notwendig ist. In den zahlreichen Publikationen zur Usability von IT-Systemen (vergleiche [94], [110] , [77] oder [74]) werden die Vorteile guter Usability

genannt. Stellvertretend seien hier die Vorteile die Kalbach [63] beschreibt aufgeführt.

Gute Usability hat nach Kalbach die Vorteile: Usability spart Zeit und Kosten, sie erhöht die Erfolgswahrscheinlichkeit eines Produktes, Usability macht Spass, sie ist ein Qualitätsmerkmal, Usability schafft diverse Wettbewerbsvorteile (Kundenakzeptanz, neue Kunden, höhere Umsätze, Erhöhung des Markenwertes ...) und durch Usability-Tests können neue Ideen generiert werden.

In den oben genannten Publikationen fehlt die Auflistung, dass gute Usability auch zu höherer IT-Sicherheit führen kann. Dies soll am Ende dieser Arbeit ebenfalls als eines der Ergbenisse ermittelt werden.

Um diese Vorteile bei Software-Systemen geniessen zu können müssen Systeme die beschriebenen Aspekte der Usability aufweisen. Die oben beschriebenen Aspekte werden allerdings meist nicht in vollem Umfang durch die Systeme umgesetzt. Meist kommt es zu Problemen, die die Umsetzung der Aspekte verhindern.

Usability-Probleme

Nicht alle Systeme sind durch Benutzer sofort leicht und intuitiv anwendbar. In vielen Fällen kommt es zu Problemen bei der Benutzung. Wie [79] ausführt sind dies aber nicht alles Probleme, die von schlechter Usability des Systemes herrühren.

Eine mögliche Definition für Usability-Probleme befindet sich bei [64] und lautet:

> „Bei einem Usability-Problem handelt es sich um alles, was mit der Fähigkeit des Benutzers interferiert, seine Aufgaben effizient und effektiv zu kompletieren.“

Mögliche Beipiele für schlechte Usability wären demnach:

1. Ein Benutzer schafft es nicht (oder nur mit sehr hohem Aufwand) mit der Software seine Aufgabe(n) zu erledigen.

2. Benutzer erhalten nicht genug Informationen um zu wissen, wo sie in der Anwendung sind, oder was sie als nächstes tun sollen.

3. Die Software verhält sich nicht erwartungskonform.
4. Der Benutzer kann die nächsten notwendigen Schritte nicht durchführen.
5. Bei Fehlern des Benutzers (falsche Eingaben oder falsche Prozessauswahl) muss der Benutzer einen erhöhten Aufwand betreiben, um die eigentliche Aufgabe weiter zu bearbeiten.

Die oben genannten Beispiele können aber nicht ohne Zusatzinformationen als „Usability-Probleme“ klassifiziert werden. Denn ein wichtiger Faktor wird in den oben genannten Beispielen nicht benannt. Dieser besteht in der Auskunft darüber, wie das jeweilige Domänenwissen der Benutzer ist.

Eine weitere Verfälschung der Usability-Eigenschaft kann durch den Einsatz des Systemes in Bereichen erfolgen, für die es nicht konzipiert wurde. Ein Programm welches für schnelles Interagieren eines Administrators über eine Komandokonsole entwickelt wurde, kann die benötigten Eingaben und Ausgaben nicht grafisch für Benutzer mit anderen Anforderungen bereit stellen.

Daher müssen mögliche Usability-Probleme dahingehend untersucht werden, ob sie durch zu unerfahrene Benutzer oder ein falsches Anwendungsgebiet verursacht wurden. Man muss trennen zwischen Problemen, die individuell für einen Benutzer sind und „Usability-Problemen“ die Benutzerübergreifend sind.

> **Definition Usability-Problem:**
> Ein Usability-Problem besteht dann, wenn ein Benutzer mit hinreichendem Erfahrungswissen in der Anwendungsdomäne und bei einer „typischen“ Anwendungssituation seine Ziele nur ineffizient, verbunden mit unangenehmen Empfindungen oder gar nicht ereichen kann.

Um Usability-Probleme zu vermeiden sollten während der Entwicklung eines Systemes die Aspekte der Usability immer beachtet und überprüft werden. Dafür stellt der Bereich des Usability-Engineering geeignete Methoden zur Verfügung.

Usability Engineering

Um Anwendungen mit hoher Usability zu entwickeln, sollte bei der Entwicklung von Systemen von Beginn an auf die Aspekte der Usability geachtet werden. So kann „eine optimale Gebrauchstauglichkeit nur dann gewährleistet werden, wenn entsprechende Kriterien von Anfang an bei der Entwicklung neuer Systeme berücksichtigt werden.“ [110] So wurde neben dem klasisschen Prozess der Softwareentwicklung der Prozes des „Usability Engineerings“ entwickelt. Beide Prozesse sollten eng verzahnt und parallel angewendet werden.

Definition Usability Engineering
Der Begriff „Usability-Engineering“ beschreibt den Prozess um die Eigenschaft Usability zu erreichen. Usability Engineering beinhaltet dafür Konzepte und Richtlinien zum methodischen Vorgehen.

Die Abbildung 2.7 zeigt die drei Hauptbestandteile des Usability-Engineerings. Eine detaillierte Beschreibung zum Usability-Engineering befindet sich zum Beispiel in [94], [106] oder [59].

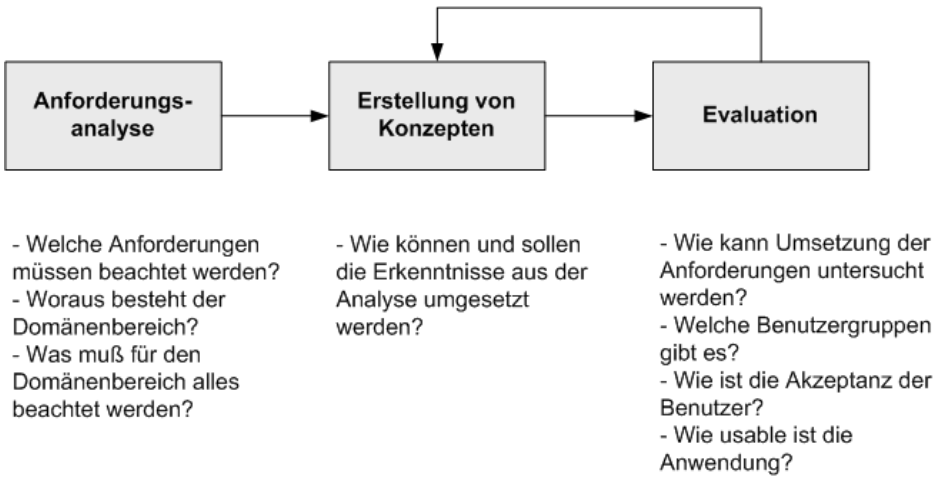


Abb. 2.7: Die einzelnen Elemente des Usability Engineerings in Anlehnung an Sarodnick [110]

Einzelne Benutzer und Benutzergruppen

„Alle Menschen sind gleich“
Voltaire

Durch Maßnahmen des Usability-Engineering sollen Systeme optimal an die Fähigkeiten, das Vorwissen und die Erwartungen von Benutzern angepasst werden. Eine exakte Anpassung an jeden einzelnen Benutzer wäre ideal. Sie ist allerdings aus Kostengründen meist nicht möglich. Aus diesem Grund werden Systeme für verschiedene Benutzergruppen voreingestellt oder angepasst. Bei diesen Benutzergruppen haben dann die Benutzer ähnliche Eigenschaften, Ziele Aufgaben Erfahrungen“ [84]. Viele Interessen und Erfahrungen überlappen sich und damit auch teilweise die Gruppen [78]. Eine klassische Unterteilung der Benutzer besteht dabei in die drei Gruppen: Anfänger, Fortgeschrittener und Experte [118].

Die Anzahl und Zusammensetzung der Benutzergruppen änderte sich im Verlauf der Entwicklung von IT-Systemen. Zu Beginn arbeiteten nur Spezialisten mit IT-Systemen (Computern). Daher waren die Zugänge zum Computer auch auf Spezialisten zugeschnitten. Es gab schnelle effiziente Zugänge, die allerdings auch Schulungen und Einarbeitungsaufwand voraussetzten.

Heute interagieren sehr unterschiedliche Benutzer in vielen verschiedenen Anwendungsgebieten mit IT-Systemen. Das Erfahrungswissen dieser Benutzer ist sehr unterschiedlich, ebenso wie ihre Ziele und ihre Bedürfnisse. Zudem sind individuelle Schlungen zu teuer, um von vielen Benutzern angewendet zu werden. Benutzergruppen sollten zu Beginn der Systementwicklung bekannt sein, damit die Systeme hinsichtlich der Gruppen optimiert weren können. Im Idealfall gehören alle potentiellen Benutzer jeweils genau einer Benutzergruppe an, und das Verhalten des Benutzers weist nur minimal vom „idealen Gruppenmitglied “ seiner Gruppe ab. Dies führt zu neuen Herausforderungen bei der Bestimmung und Verwendung von Benutzergruppen.

Die Aufstellung der Benutzergruppen beinhaltet die folgenden Herausforderungen:

- Die Erstellung der Benutzergruppen muss zu Beginn der Entwicklung erfolgen um sämtliche Phasen der Entwicklung hinsichtlich der Gruppen zu optimieren.
- Klärung der Fragestellungen: Wie sehen die optimalen Gruppen aus? Wieviele verschiedene Benutzergruppen sind optimal? Worin unterscheiden sie sich. Wie sehen die optimalen Gruppenmitglieder aus?

- Die Zuordnung neuer Benutzer zu Benutzergruppen muss schnell zu Beginn der Systembenutzung erfolgen, damit Benutzer von der gruppenzentrierten Anpassung profitieren können.

Aus diesen Gründen versucht man durch verschiedene Verfahren die Anzahl und die Eigenschaften der Benutzergruppen mit Hilfe einer Teilmenge der Benutzer bereits im Vorfeld der Systementwicklung zu ermitteln.

Eine weitere mögliche Lösung besteht darin, die Systeme so zu gestalten dass möglichst wenig verschiedene Benutzergruppen notwendig sind. Eine Möglichkeit besteht darin dass alle unterschiedlichen Benutzer sofort erkennen sollen was ein System macht. Auf diesem Ansatz basiert das „What-You-See-Is-What-You-Get"-(WYSIWYG)-Konzept.

Allerdings stösst dies auf dasselbe Problem der möglichen verschiedenen Interpretationen. Unterschiedliche Benutzer können unterschiedliche Dinge trotz WYSIWYG-Konzept unterschiedlich interpretieren. Aus diesem Grunde wäre ein „What-You-See-Is-What-You-Understand"-(WYSIWYU)-Konzept erfolgsversprechender. Es muss darauf geachtet werden, dass Symbole möglichst ähnlich von vielen Benutzern interpretiert werden. Somit besteht ein Ansatz darin zu ermitteln wo ein gemeinsames Grundverständnis zwischen möglichst vielen Benutzern liegt.

Die Verwendung von Benutzergruppen beinhaltet aber nicht nur Vorteile. Legt man bei der Definition der Benutzergruppen falsche Annahmen zu Grunde, oder lässt wesentliche Aspekte möglicher Benutzergruppen aus, kann dies zu falschen Ergebnissen oder zu falschen Interpretationen führen. Für die geeignete Wahl an Benutzergruppen müssen die folgenden Fragen geklärt werden.

1. Wie viele Benutzergruppen sollen bei der Entwicklung und Evaluation betrachtet werden?

2. Wie sehen die Benutzergruppen aus und welches sind die relevanten Eigenschaften der jeweiligen Benutzergruppe?

Es muss untersucht werden, welche Informationen für die Benutzereinteilung als Grundlage für Entwicklung und Evaluation nötig und welche Relationen bei diesen Informationen vorhanden sind und wie das Fehlverhalten minimiert wird. Diese Informationen können durch verschiedene Verfahren, wie z.B. Fragebögen oder Expertenbefragungen, gesammelt und ausgewertet werden. Einige der wichtigen Evaluationsmethoden werden in Abschnitt 2.3.3

beschrieben, nachdem zunächst die Standards im Bereich Usability detaillierter betrachtet werden.

2.3.2 Standards und Normen im Bereich Usability

In diesem Abschnitt werden einige Standards und Normen aus den Bereichen Usability vorgestellt. Standards und Normen sind wichtig, da sie eine Gruppierung der Benutzer voraussetzen und auch darstellen. So wissen Benutzer, was sich hinter der Papiergröße Din A4 verbürgt, da sie gelernt haben dass es eine spezielle Größe ist. Normen und Standards schaffen so eine gemeinsame Wissensgrundlage für verschiedene Benutzer.

Um die Usability von Systemen untersuchen und bestimmen zu können, müssen geeignete Evaluationsverfahren und Vergleichswerte vorhanden sein. Als Vergleichswerte dienen verschiedene Standards und Normen. Einige seien hier beispielhaft genannt: ISO-Norm 9241 [2], Benutzbarkeitsheuristiken von Nielsen [95], DIN EN ISO 13407 [1], Starys Kriterienkatalog [119] oder der Evaluationsleitfaden EVADIS II [104].

Diese Standards und Normen geben keine konkreten Werte vor, sondern sie sind Empfehlungen für die Entwickler von Systemen. Sie bilden somit Richtlinien nach denen Systeme entwickelt und evaluiert werden können, die die Anpassung der Systeme an Fähigkeiten und Kenntnisse der Benutzer im Fokus haben. Aus diesem Grund geben einige Forscher an, dass diese Normen nicht unbedingt umgesetzt werden müssen um ein hohes Maß an Usability umzusetzen [33]. Nach Markotten [81] dienen die Benutzbarkeitsrichtlinien dazu die Benutzbarkeit der Anwendung zu steigern, Hilfestellung für die Gestaltung der Schnittstellen zu Benutzern zur Verfügung zu stellen und ein Vergleichsmaß für die Evaluation von Benutzer-Schnittstellen bereit zu stellen.

Die Normen im Bereich der Usability sollen Systeme nicht alle gleich machen. Sie sollen dazu führen, dass Aufgaben der Benutzer durch Anwendungen sinnvoll unterstützt werden. Dazu ist es in begrenztem Maß auch wichtig, dass die Normen für Konsistenz und Erwartungskonformität in den Anwendungen sorgen. Dies ist aber nur einer der wichtigen Faktoren und andere Faktoren können im Aufgabenkontext wichtiger sein. Die Anwendung muss immer an den Aufgabenkontext angepasst werden und in ihm gesehen werden. Das erklärt auch den Empfehlungscharakter der Normen.

Neben den Normen existieren zahlreiche Styleguides für die Erstellung von Benutzerschnittstellen. Diese Styleguides dienen dazu konkrete Vorgaben für

die Entwicklung der jeweiligen Anwendung zu machen. Sie geben konkrete Rahmenbedingungen und Gestaltungsrichtlinien vor. Dadurch wird eine gewisse Konsistenz und Erwartungskonformität der jeweilgen Benutzungsschnittstelle erreicht und gewährleistet. Durch Styleguides kann aber nicht erreicht werden, dass die Anwendung auch aufgabenangemessen ist, da der jeweilige Styleguide die zu bearbeitende Aufgabe nicht miteinbezieht.

Viele Forscher, wie z.B. Nielsen, gaben in der Vergangenheit diverse Empfehlungen zur Gestaltung von Benutzungsschnittstellen für Software heraus. Diese Empfehlungen mündeten 1996 in den ersten ISO Normen zur Usability, der DIN EN ISO 9241.

DIN-ISO 9241 Die DIN EN ISO 9241 ist die maßgebliche Norm für die Gestaltung von Systemen mit hoher Usability [110]. Viele Fachbegriffe im Bereich der Usability werden in ihr definiert. Sie besteht aus 17 Teilen. Für die Usability sind vor allem die Kapitel 10 und 11 relevant. Sie befassen sich mit „Grundsätzen der Dialoggestaltung“ und „Anforderungen an die Gebrauchstauglichkeit“.

Im Kapitel 10 der DIN EN ISO[2] werden sieben Grundsätze zur Dialoggestaltung beschrieben.

Aufgabenangemessenheit „Ein Dialog ist aufgabenangemessen, wenn er den Benutzer unterstützt, seine Arbeitsaufgabe effektiv und effizient zu erledigen.“

Selbstbeschreibungsfähigkeit „Ein Dialog ist selbstbeschreibungsfähig, wenn jeder einzelne Dialogschritt durch Rückmeldung des Dialogsystems unmittelbar verständlich ist oder dem Benutzer auf Anfrage erklärt wird.“

Steuerbarkeit „Ein Dialog ist steuerbar, wenn der Benutzer in der Lage ist, den Dialogablauf zu starten sowie seine Richtung und Geschwindigkeit zu beeinflussen, bis das Ziel erreicht ist.“

Erwartungskonformität „Ein Dialog ist erwartungskonform, wenn er konsistent ist und den Merkmalen des Benutzers entspricht, z.B. den Kenntnissen aus dem Arbeitsgebiet, der Ausbildung und der Erfahrung des Benutzers sowie den allgemein anerkannten Konventionen.“

Fehlertoleranz „Ein Dialog ist fehlertolerant, wenn das beabsichtigte Arbeitsergebnis trotz erkennbar fehlerhafter Eingaben entweder mit keinem oder mit minimalem Korrekturaufwand durch den Benutzer erreicht werden kann.“

Individualisierbarkeit „Ein Dialog ist individualisierbar, wenn das Dialogsystem Anpassungen an die Erfordernisse der Arbeitsaufgabe, individuelle Vorlieben des Benutzers und Benutzerfähigkeiten zuläßt."

Lernförderlichkeit „Ein Dialog ist lernförderlich, wenn er den Benutzer beim Erlernen des Dialogsystems unterstützt und anleitet."

Fazit zu Normen im Bereich Usability

Die Normen im Bereich der Usability haben nicht das primäre Ziel Software zu vereinheitlichen, sondern sie sollen dafür sorgen, dass Benutzungsprobleme der Benutzer vermieden oder minimiert werden. Daher beschreiben sie keine konkreten Eigenschaften sondern sprechen Empfehlungen aus.

Erst durch die Evaluierung der beschriebenen Normen, Standards und Richtlinien im Bereich Usability kann fest gestellt werden, ob Systeme auch durch Benutzer benutzbar sind. Daher werden im folgenden Kapitel unterschiedliche Methoden zur Evaluation von Systemen vorgestellt

2.3.3 Evaluierungsmethoden

Einer der Bestandteile des Usability-Engineerings ist die Evaluation von Usability-Aspekten einer Anwendung. Die Anwendung wird dabei nach verschiedenen später in diesem Kapitel näher beschriebenen Aspekten untersucht. Die Bewertung der Usability-Eigenschaften und die anschließende Optimierung dieser Aspekte ist ohne Evaluation nicht möglich.

Im folgenden Kapitel werden einige der wichtigsten Methoden für eine Usability-Evaluation vorgestellt. Bevor die eigentlichen Evaluierungsmethoden im Detail beschrieben werden, werden zunächst noch die Grundlagen und Definitionen beschrieben.

Definitionen im Bereich Evaluierungsmethoden

Der Begriff Evaluation wird im Bereich des Usability-Engineerings in unterschiedlichen Kontexten unterschiedlich definiert. So wird der Begriff zum Beispiel von Wottawa [124] folgendermaßen definiert: "das Sammeln und Kombinieren von Daten mit einem gewichteten Satz von Skalen mit denen entweder vergleichende oder numerische Beurteilungen erlangt werden sollen". Die Deutsche Gesellschaft für Evaluation e.V (DeGEval) definiert dagegen den Begriff Evaluation wie folgt: „Evaluation ist die systematische Untersuchung des Nutzens oder Wertes eines Gegenstandes [17]." In dieser Arbeit wird der Begriff „Evaluation" wie folgt verwendet:

> **Definition Evaluation:**
> Eine Evaluation ist eine systematische Untersuchung, die analysiert welche Usability-Aspekte bei einer Anwendung umgesetzt wurden. Die Evaluation erstellt eine nachvollziehbare Bewertung des untersuchten Gegenstandes, so dass dessen Gebrauchstauglichkeit möglichst genau bestimmt werden kann. Eine Evaluation zeigt die Schwachstellen und Problembereiche einer Anwendung in Bezug auf ihre Usability-Eigenschaften auf. Je nach verwendeter Evaluationsmethodik werden unterschiedliche Usability-Bereiche analysiert und verschiedene Problembereiche untersucht.

Die Usability-Aspekte einer Anwendung können durch unterschiedliche Arten von Evaluationen überprüft werden. Die Evaluationsmethoden können dabei in zwei Arten unterteilt werden [110]. Zum einen können **„Empirische Usability-Evaluationsmethoden"** durchgeführt werden, zum anderen kann die Anwendung durch **„Expertenbasierte Usability-Evaluationsmethoden"** untersucht werden. Diese Aufteilung ist in Grafik 2.8 dargestellt.

Bei den empirischen Usability-Evaluationsverfahren wird die zu untersuchende Anwendung von realen Nutzern bedient. Dabei wird die Benutzung mit verschiedenen Untersuchungsmethoden beobachtet, gemessen und untersucht. So können z.B. Benutzer den Gebrauch einer Anwendung in der Praxis (aus-) testen und bewerten wenn sie eine reale Aufgabe lösen. In diesem Fall handelt es sich dann um *„Usability-Testmethoden"*.

Bei den Expertenbasierten Usability-Evaluationsmethoden beurteilen „Gutachter", so genannte „Usability-Experten", die Anwendung nach speziellen Kriterien. In der Literatur [53] ist dafür auch der Begriff *„Usability-Inspektion"* vorhanden.

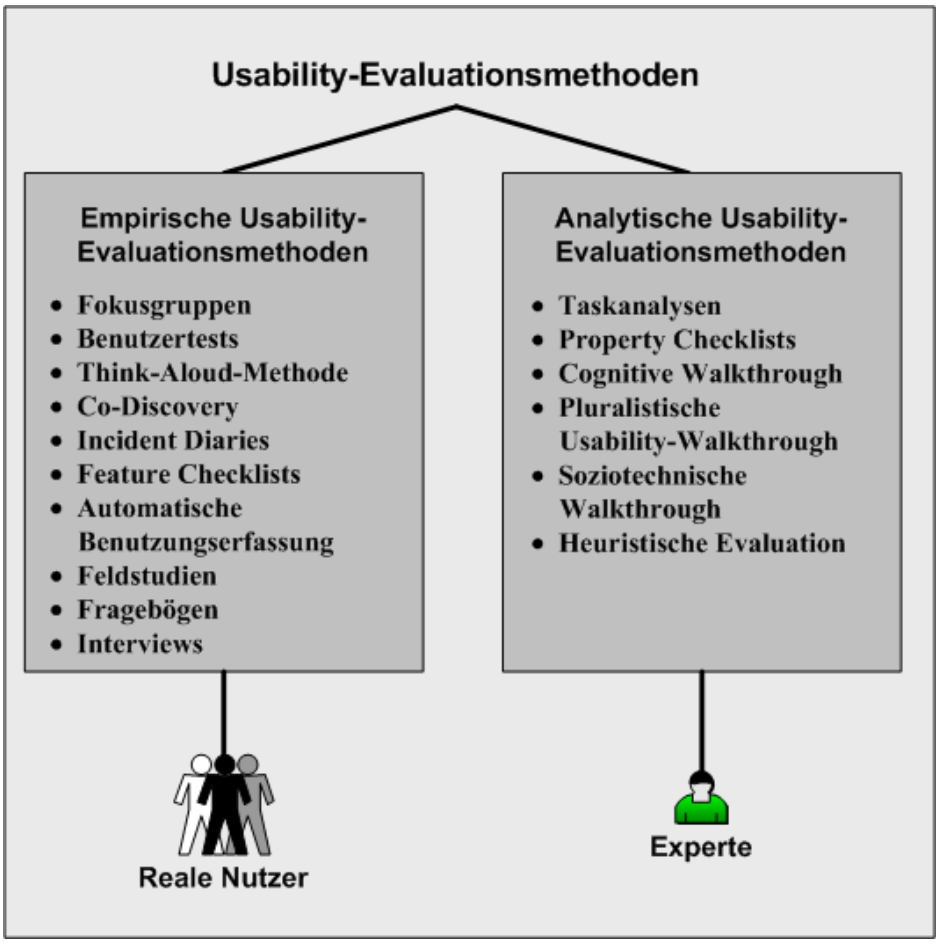


Abb. 2.8: Unterschiedliche konkrete Evaluationsmethoden

Gemäß der Deutschen Gesellschaft für Evaluation sollen Evaluationen immer die vier folgenden grundlegenden Eigenschaften aufweisen: Nützlichkeit, Durchführbarkeit, Fairness und Genauigkeit.

Evaluationen werden immer durchgeführt um bestimmte Fragestellungen zu beantworten. Die Beantwortung der Fragestellungen stellt dabei das Evaluationsziel dar. Evaluationsziele können sowohl im Ermitteln von konkreten Maßen und Werten bestehen, als auch im Finden von allgemeinen Usability-Problemen. So kann zum Beispiel gemessen werden, wie viel Zeit ein Benutzer benötigt um eine Aufgabe in einem Dialog zu lösen. Oder es wird untersucht werden, ob der Benutzer mit dem Dialog zufrieden ist. Nach [29] sollen die Evaluationsziele zu Begin der Entwicklung einer Anwendung von dem gesamten Projektteam ermittelt werden. Dadurch können von allen beteiligten Entwicklergruppen eigene Evaluationsziele eingebracht werden (z.B.

Designer, Software-Entwickler, Tester usw.).

> **Definition Evaluationsziel:**
> Das Evaluationsziel ist die Beantwortung der jeweiligen Fragestellung. Nach [46] kann man drei grobe Klassen von Fragestellungen bei der Evaluation unterscheiden: *Was ist besser? Wie gut ist es? Was ist schlecht?*

Jede Evaluation wird von einem Evaluator geleitet. Der Evaluator ist die Person, die eine Evaluation plant, vorbereitet und durchführt. Der Evaluator muss sich nicht aktiv an einer Evalution beteiligen. Er kann auch nur die Planung und Analyse durchführen. Neben dem Evaluator sind bei einer Evaluation noch verschiedene andere „Rollen“ an Personen beteiligt (Moderator, Benutzer/Tester oder Experte). Bei jeder Evaluationsmethode sind nicht unbedingt alle Rollen beteiligt.

Die besten Optimierungsergebnisse für die Benutzbarkeit werden durch die Kombination von empirischen mit analytischen Verfahren erzielt. In Abbildung 2.8 sind einige konkrete Usability-Evaluationsmethoden und ihre zugehörigkeit zur jeweiligen Klasse dargestellt. Abbildung 2.9 zeigt die nach Nielsen wichtigsten Evaluierungsverfahren. Einige von diesen werden im Folgenden detaillierter beschrieben.

Empirische Evaluierungsverfahren

Bei Empirische Evaluierungsverfahren testen Testpersonen, die vorzugsweise aus der Zielgruppe für die Anwendung stammen, das Programm unter möglichst realen Bedingungen. Dazu versuchen sie mit der Anwendung reale Aufgaben zu erledigen (z.B. Authentifizierung vor einer Transaktion oder das Auffinden von benötigten Informationen). Bei einem Benutzertest wird die fertige Anwendung oder ein erster Prototyp durch Testpersonen getestet. Bei den Testern handelt es sich nicht um die Entwickler. Die Testpersonen testen anhand bestimmer Fragestellungen die fertige Anwendung und sollen beim Test ein möglichst umfangreiches Feedback abgeben. Durch dieses Feedback werden dann Usability-Probleme lokalisiert.

Um Daten zur Optimierung der Benutzbarkeit zu erhalten werden die zwei folgenden Verfahren eingesetzt. Zum einen werden die Testpersonen während der Tests meist beobachtet. Dies gibt Aufschlüsse darüber wie sie sich bei der Benutzung verhalten und wo mögliche Benutzungsprobleme auftreten

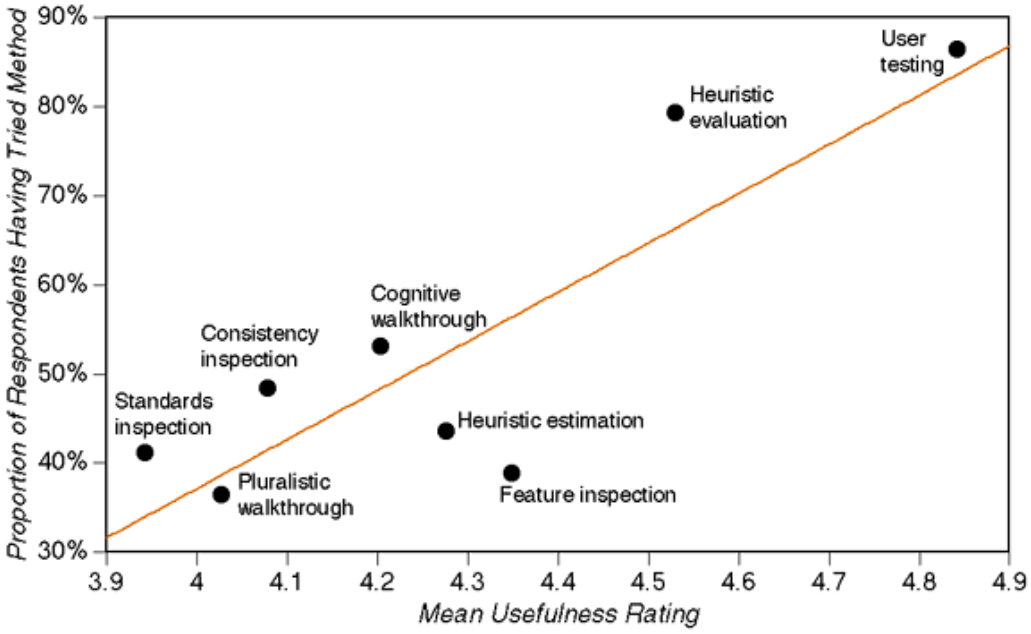


Abb. 2.9: Die wichtigsten Usability Evaluationsverfahren nach Nielsen [94]

können. Zum anderen werden die Testpersonen nach dem Test befragt. Dadurch erhält man Feedback darüber, wo eine Testperson selbst Probleme bei der Handhabung gesehen hat. Beide Arten von Problemen können dann gewichtet und eliminiert werden. Die Usability-Tests sollten aus Kostengründen entwicklungsbegleitend durchgeführt werden. Dazu werden während der ersten Phasen „Benutzungsschnittstellen-Dummys“ verwendet. Die Kosten, die durch die Durchführung der Tests enstehen, sind meist geringer als das eingesparte Geld für die Behebung der Fehler in den ersten Projektphasen. Bevor man einen Benutzertest durchführt, müssen die Ziele, die man mit der Durchführung verfolgt, geklärt werden. Im Folgenden werden einige der empirischen Evaluationsverfahren genauer vorgestellt.

Think-Aloud-Methode: Die Think-Aloud-Methode [116] ist eine einfache und kostengünstige Methode um Anwendungen auf ihre Benutzbarkeit zu untersuchen. Benutzer aus der späteren Zielgruppe, für die die Anwendung implementiert wird testen die Anwendung. Sie erhalten dazu konkrete Aufgaben, die sie mit Hilfe der Anwendung lösen sollen. Bei der Benutzung erzählen die Testnutzer dann in lauten Worten, was sie gerade tun. Sie sollen ihre Gedanken, Gefühle, Meinungen und Erwartungen, die sich bei der Benutzung des Programms ergeben, laut aussprechen. Diese Informationen

werden aufgezeichnet oder protokolliert und später ausgewertet. Diese Untersuchung kann bereits mit einem der ersten Prototypen durchgeführt werden. Die komplette fertige Implementation der Anwendung muss dafür nicht zur Verfügung stehen. Man gewinnt durch die Methode Eindrücke von dem Probleme und dem Problemlöseverhalten der „Endbenutzer“. Es werden vor allem folgende Informationen gewonnen: Warum tut ein Benutzer gerade etwas? Wie versucht ein Benutzer ein Problem/Aufgabe zu lösen? Was erwartet ein Benutzer gerade im Programm? Ist die Beschriftung innerhalb des Progerammes für den Benutzer verständlich?

Die Benutzer müssen allerdings gegeignet instruiert werden, damit sie auch die Informationen vermitteln die man benötigt. Außerdem müssen sie animiert werden ständig Informationen zu geben. Die Think-Aloud-Methode sollte mit ungefähr 5 verschiedenen [44] Benutzern durchgeführt werden. Um eine Vergleichbarkeit der dabei gemachten Beobachtungen zu erhalten wird in der Praxis am Ende meist eine Befragung der Teilnehmer durchgeführt. Diese Befragung dient dazu das Hintergrundwissen der Versuchsteilnehmer zu erfahren und gegebenenfalls mit in die Bewertung einfliessen zu lassen.

Analytische Evaluierungsverfahren

Bei den analytischen Evaluierungsverfahren testet ein Experte oder eine Gruppe von Experten das Programm. Man spricht daher auch von Expertengutachten oder Inspektion. Die Benutzbarkeit einer Anwendung wird dabei nach einem vorher festgelegten Kriterienkatalog untersucht. Trotz des fest definierten Kriterienkatalogs sind bei einer Inspektion sehr viele Freiheitsgrade vorhanden. Dies resultiert aus dem unterschiedlichen Erfahrungswissen der Usability-Experten. Die Kriterien müssen immer im Gesamtkontext der Aufgabenerledigung gesehen werden. Sie sind jedoch nicht fest definiert. So wird das Kriterium:“einfache Navigation bei der Authentifizierung“ unterschiedlich interpretiert. Ein Experte der schon mit vielen Authentifizierungsverfahren zu tun hatte wird sich bei der Benutzung andere Fragen stellen als ein Experte, der zwar Usability-Kriterien, aber nicht die Hintergründe von Authentifizierungen kennt. Die evaluierenden Experten sind nicht direkt am Entwicklungsprozess der Software beteiligt [45]. Um subjektive Meinungen einzelner Experten zu minimieren sollte die Anzahl der Evaluatoren zwischen drei bis fünf liegen. Außerdem wird durch eine höhere Anzahl von „Gutachtern“ auch eine größere Anzahl an Fehlern aufgedeckt. Allerdings steht eine noch höhere Anzahl an Experten nicht mehr in einem befriedigendem Verhältnis zu den ermittelten Fehlern. Nielsen untersuchte dies bei Heurstischen Evaluationen [94] und kam zu dem Ergebnis in Grafik 2.10.

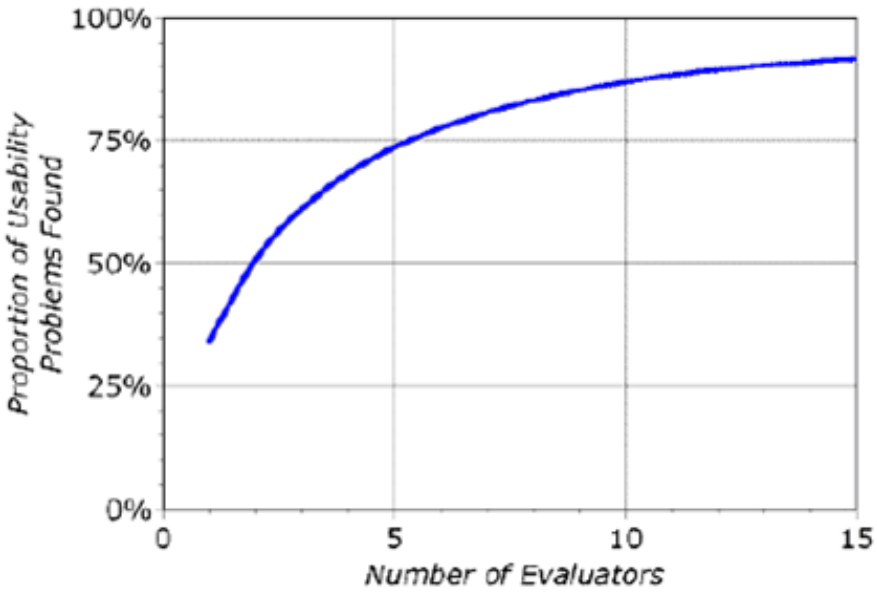


Abb. 2.10: Abhängigkeit der gefundenen Fehler von der Anzahl der Evaluatoren aus Nielsen [94]

Die Gutachtergruppe sollte aus Fachexperten und Usability-Spezialisten bestehen. Dies hat den Vorteil, dass zum einen die Einarbeitung in das Fachthema und zum anderen die Einarbeitung in die Usability-Methoden minimiert werden. Durch Expertengutachten sollen schon in einem frühen Stadium des Entwicklungsprozesses Rückmeldungen zum Benutzbarkeitsaspekt der Software erfolgen. Dies ist zum Beispiel durch Verwendung von Papier-Prototypen oder aber auch durch das fertige Gesamtsystem möglich. Expertengutachten haben den Vorteil, dass die Ergebnisse zumeist schneller und auch billiger vorliegen, als bei Tests mit eigentlichen Benutzern. Dies liegt auch darin begründet, dass zu einer befriedigenden Benutzbarkeitsanalyse nur eine geringe Anzahl an Experten nötig ist.

Expertengutachten lassen sich unterteilen in:

- *Freie Expertengutachten*
  Die Evaluatoren führen ihre Tests nach allgemeinen Richtlinien durch.
- *Strukturierte Expertengutachten*
  Die Evaluatoren untersuchen das Programm mit detailierten Check-Listen um die Erfüllung und Umsetzung von Richtlinien und Standards zu überprüfen.

- *Modellbasierte Expertengutachten*
  Die Evaluatoren untersuchen das Programm durch ein Modell der Benutzungsoberfläche. An diesem Modell werden vordefinierte Evaluationstests ausgeführt.

Mit diesen Methoden werden Schwachstellen in der Aufgabenangemessenheit aufgedeckt. Zugleich werden Bedienprobleme für die Experten ersichtlich.

Die Evaluation wird in vier Schritten durchgeführt:

- *Schritt 1: Aufgaben*
  Im ersten Schritt wird erläutert, wer mit dem System arbeiten soll und welche Ziele im und mit dem System erreicht werden sollen.
- *Schritt 2: Funktionale Beschreibung*
  Bei diesem Schritt werden die Prozesse zur Umsetzung der Aufgaben beschrieben. Dies wird in Grobdialogen skizziert.
- *Schritt 3: Syntaktischer Durchlauf*
  Die Evaluatoren gehen alle Funktionen durch, um zu überprüfen, ob die jeweilige Bedeutung klar ist. Außerdem überprüfen sie den Aufruf und den Ablauf der Funktionalitäten hinsichtlich Bedienerfreundlichkeit und Feedback des Systems.
- *Schritt 4: Ein-/Ausgabe*
  Im letzten Schritt bewerten die Experten alle Elemente (z.B. Menüs, Rück- oder Fehlermeldungen). Unter anderem werden folgende Aspekte bewertet: Benennung, Gruppierung und Farbgestaltung der Elemente. Dies soll immer aus der Sicht der späteren Benutzer erfolgen.

Eine Überprüfung auf die Verwendung von richtigen Eingabeelementen und Tastenbelegungen bildet den Abschluss der Evaluation. Inspektionen können zwar auch projektbegleitend durchgeführt werden, werden aber meist vor den eigentlichen Usability-Tests durchgeführt

Im Folgenden werden nun einzelne analytische Evaluierungsverfahren vorgestellt und erläutert.

Cognitive Walkthrough (CWT): Der Cognitive Walkthrough dient dazu Handlungsabläufe von Benutzern zu untersuchen. Diese Methode wurde von Wharton entwickelt und beschrieben ([127], [80] und [128]). Der Fokus liegt darauf zu untersuchen, wie die Handlungsabläufe der Benutzer von dem System intuitiv unterstützt werden. Es soll herausgefunden werden, wie gut sich ein typischer Benutzer in einem Programm zurecht findet. Der Cognitive Walkthrough wird dabei zu Beginn der Entwicklung durchgeführt. Daher beinhaltet der CWT ein hohes Einsparpotential, da nötige Änderungen an der Software erkannt werden, bevor mit der Implementierung begonnen wird.

Beim Cognitive Walkthrough versetzt sich ein Usability-Experte in die Rolle eines Benutzers und führt dessen Arbeitsschritte durch. Er soll sich dabei nach Möglichkeit genau wie ein „Standard-Benutzer“ verhalten, indem er zum Beispiel auch keine Handbücher liest, sondern intuitiv das Programm verwendet. Dabei ist es wichtig, dass der Usability-Experte weiß, welche Ziele und Aufgaben ein Benutzer hat und erledigen möchte, welche Aktionen er ausführt und über welches Hintergrundwissen er verfügt. Diese Informationen werden während der ersten Arbeitsschritte eines CWT erarbeitet und im weiteren verlauf der Evaluation weiter verwendet.

Bei einem CWT werden die vier Phasen *1) Definition des Inputs 2) Beschreibung der Aufgabe und Aufteilung in detaillierte einzelne Handlungssequenzen 3) Protokollierung kritischer Informationen 4) Revision der Benutzungsschnittstelle* durchgeführt.

Definition des Inputs: Die folgenden Grundlagen werden für einen CWT benötigt und daher spätestens in diesem Arbeitsschritt erstellt.

1. Erstellung einer Beschreibung des Systems. Dies ist textuell oder durch einen Prototypen möglich. Im Idealfall existiert beides. Aus den Dokumenten sollte bereits ersichtlich sein, wo welche Funktionalität im späteren Programm vorhanden ist und wie sie umgesetzt sein sollte.

2. Die Aufgaben/Ziele, die der Benutzer mit dem System bearbeiten möchte, müssen beschrieben sein.

3. Die zum Erreichen der Ziele bzw. der Bearbeitung der Aufgaben benötigten Aktionen müssen ermittelt werden. Sie werden in Aktionslisten die die Erledigung einzelner Aufgaben ergeben zusammen gefasst.

4. Es muss beschrieben werden, welches Hintergrundwissen bei einem „Standard-Benutzer“ vorausgesetzt werden kann.

Handlungssequenzen der Aufgabe: Die im vorangegangenen Arbeitsschritt erstellten Aktionslisten werden nun analysiert. Es soll überprüft werden, ob die ebenfalls erstellten Aufgaben durch den Benutzer erledigt werden können. Dazu wird jede Aktion der Aktionsliste auf die vier fehlenden Punkte untersucht:

1. *Wird der Benutzer versuchen den richtigen Effekt zu erzielen?*
   Als wichtigster Schritt bei der Untersuchung der einzelnen Aktionen wird zuerst überprüft, ob die zur Verfügung stehende Aktion den gewünschten Effekt hat. Der Benutzer soll die Aktion, die er als nächstes benötigt, erkennen. Dabei sind zum einen besonders das Hintergrundwissen und zum anderen die Erfahrung des Benutzers mit dem System wichtig. Zusätzlich soll das System den Benutzer zum richtigen Handeln anleiten.

2. *Wird der Benutzer erkennen, dass die korrekte nächste Aktion zur Verfügung steht?*
   Hierbei wird überprüft, ob der Button, Menueintrag o.ä., welcher die gewünschte nächste Aktion auslöst für den Benutzer sofort sichtbar ist. Ansonsten müssen ihm andere Informationsquellen, wie zum Beispiel Erfahrungswissen, zur Verfügung stehen. Bei dieser Frage wird nur untersucht, ob die Aktion für den Benutzer sichtbar ist und nicht ob er die Aktion als solche erkennt.

3. *Wird der Benutzer die zur Verfügung stehende Aktion als die erkennen, die er als nächstes benötigt?*
   Auch wenn ein Benutzer das Richtige tun will und weiß, dass dies möglich ist, muss er trotzdem nicht die richtige Aktion auswählen. Denn es bleibt die Frage, ob der Benutzer den Auslöser der nächsten Aktion als selbigen erkennt. Er muss den Zusammenhang zwischen diesen beiden Informationen herstellen. Der Benutzer könnte diese fehlende Verbindung aufgrund seiner Erfahrung (z.B. weil alle anderen Möglichkeiten weniger vielversprechend erscheinen) oder einer Eigenschaft des Systems (z. B. Gute Beschriftung der Buttons) herstellen.

4. *Wird der Benutzer nach Ausführen der korrekten Aktion ein Feedback erhalten und wird dieses für ihn verständlich sein?*
   Wenn die richtige Aktion vom Benutzer ausgelöst wurde sollte das System ihm dies auch mitteilen. Das Vertrauen des Benutzers in das System soll durch diese Maßnahme gesteigert werden.

Wenn eine der Fragen (oder mehrere) bei einem Aktionsschritt negativ beantwortet werden, soll der Evaluator trotzdem mit der Untersuchung fortfahren und den nächsten Aktionspunkt der Liste abarbeiten.

Protokollierung der kritischen Informationen: In diesem Arbeitsschritt werden zwei Arten von Informationen notiert und gesammelt:

- Das Hintergrundwissen, welches beim Benutzer während jedes Arbeitsschrittes vorhanden sein muss.
- Alle Aktionen (und Daten über sie), die zu einer möglichen Fehlbedienung führen (inklusive einer Begründung für die falsche Bedienung).

Revision der Benutzungsschnittstelle: Wenn ein Aktionsschritt in Phase 2 des CWT gescheitert ist, sollte eine Überarbeitung der Benutzungsschnittstelle erfolgen. Dabei sind die folgenden Möglichkeiten eines Problems vorhanden.

1. *Der Benutzer versucht nicht den richtigen Effekt zu erzielen.*
   Um dieses Problem zu lösen sind die folgenden Möglichkeiten denkbar. Die fehlgeschlagene Aktion könnte beseitigt werden, indem sie mit einer anderen Aktion kombiniert, oder bereits vom System übernommen wird. Der Benutzer könnte aber auch einen Hinweis darauf erhalten, welches der nächste richtige Effekt ist. Die Schnittstelle kann auch dahingehend geändert werden, dass für den Benutzer klarer ist, wieso und welche Aktion als nächste auszuführen ist.
2. *Der Benutzer erkennt nicht, dass die gewünschte Aktion zur Verfügung steht.*
   Zur Problembehebung kann das benötigte Bedienelement „sichtbarer“ positioniert werden.
3. *Der Benutzer stellt keine Verbindung zwischen der korrekten Aktion und dem gewünschten Effekt her.*
   Dafür sollte die Beschriftung bzw. grafische Hinweise so angepasst werden, dass der Zusammenhang für den Benutzer ersichtlicher ist.
4. *Der Benutzer erhält keine ausreichende Rückmeldung über seine Aktion.*
   Das Feedback muss so angepasst werden, dass dem Benutzer zwei Tatsachen mitgeteilt werden. Zum einen, dass seine Aktion etwas auslöste und zum anderen was sie auslöste.

Ein CWT hat die Vorteile: eine einfache Durchführbarkeit, er ist billig, er kann bereits in einer sehr frühen Entwicklungsphase eingesetzt werden und die Benutzung der Anwendung wird zielorientiert untersucht.

Seine Nachteile sind dagegen, dass nicht die späteren Benutzer sondern „Experten“ testen, dass für jede Aufgabe ein eigener CWT erstellt werden muss und dass er bei größeren Projekten sehr umfangreich ist.

Neben den geschilderten Verfahren gibt es noch viele weitere Verfahren für Usability Evaluation (z.B. Co-Discovery [65], Incident Diaries Methode [95], Fragebögenmethode [110], Pluralistische Usability-Walkthrough [110] oder [18], Soziotechnischen Walkthrough [55], die Heuristische Evaluation [93] und [98]). Da es nicht das alleinige Verfahren gibt, was ein Maximum an Usability Problemen aufdeckt, sollten verschiedene Verfahren kombiniert werden. Durch die Anwendung mehrerer Verfahren werden zwar auch mehr Probleme aufgedeckt, aber die Kosten für die Untersuchung steigen ebenfalls. Diese Kosten kann man senken indem man die Evaluierungsmethoden zum Teil automatisiert.

Automatische Evaluierungsmethoden

Automatisierte Usability-Evaluierungsverfahren haben gegenüber manuellen Testverfahren die Vorteile der geringeren Personalkosten, dem konsistenten Aufdecken von Usability-Problemen, dem schnellen und einfachen Vergleich ähnlicher Designs sowie der schnellen Durchführung der Evaluation.

Demgegenüber haben automatische Verfahren aber auch Nachteile. Sie müssen sehr detailliert vorbereitet werden und benötigen auch ein Feedback durch Menschen. Daher sollten automatische Testverfahren nach [58] nur in Verbindung mit herkömmlichen Evaluierungsverfahren eingesetzt werden. Die Anwendung verschiedener Verfahren deckt zudem meistens auch unterschiedliche Usabilityprobleme auf.

Nach [58] lassen sich automatische Evaluierungstools in folgenden Bereichen Automatic Capture Methods, Automatic Analysis Methods, Inspection Methods, Inquiry Methods, Analytical Modelling Methods und Simulation Methods benutzen.

Als Beispiel wird im Folgenden das automatische Usasbilityevaluationsprogramm UsAGE vorgestellt, um den Stand der Technik auf diesem Gebiet zu zeigen und außerdem darzustellen, welche Vor- und Nachteile bestehen und wo Verbesserungspotential vorhanden ist.

Abb. 2.11: Das Tool UsAGE [123]

Bei dem Tool Usage [123] werden Eingaben eines Experten mit denen eines Benutzers verglichen. Der Grundgedanke, der dem Tool UsAGE zu Grunde liegt besteht darin, dass ein Experte weiss, welche Aktionen er ausführen kann und was diese Aktionen bewerkstelligen. Der „normale Benutzer“ kennt nicht die Anwendung und wird an all den Stellen, die ihm nicht intuitiv erscheinen zögern. Genauso an allen Stellen, bei denen er die Bezeichnung als nicht korrekt empfindet. Durch eine Normierung und einen Vergleich der jeweiligen einzelnen Lösungszeiten für jede einzelne Aktion, lassen sich Usability-Probleme extrahieren.

Zu Beginn wird eine detaillierte Aufgabe entwickelt, die mit der zu evaluierenden Anwendung zu lösen ist. Diese Aufgabe müssen dann sowohl Experte als auch „normaler Benutzer“ mit der zu evaluierendnen Anwendung lösen. Ihr Lösungsweg wird durch das Tool Usage mitprotokolliert und kann danach verglichen werden. Für den Vergleich zwischen den beiden Lösungswegen steht in UsAGE eine grafische Repräsentation wie in Abbildung 2.11 zur Verfügung.

Nachteile von UsAGE

- Der Moderator muss einen Match zwischen der grafischen Ausgabe und den eigentlichen Problemen herstellen.
- Keine detaillierte Zeitachse in der grafischen Ausgabe vorhanden.
- Falsche Zuordnung von Ausgabeelementen zur eigentlichen Anwendung
- Es ist nur möglich jeweils einen Graphen eines Experten mit einem Graphen eines „unerfahrenen Benutzers“ zu vergleichen.

Automatische Usabilityevaluierungsverfahren bieten eine gute Ergänzung zu herkömmlichen Evaluierungsverfahren. Sie können gut eingesetzt werden, um zu einen Konsistenzprobleme aufzudecken oder zum anderen schnell verschiedene Designversionen einer Anwendung miteinander zu vergleichen. Sie können allerdings nicht eingesetzt werden, wenn es um die Erfassung wichtiger qualitativer oder subjektiver Informationen der Benutzer geht.

Fazit zu den Evaluationsverfahren

Eine große Anzahl an unterschiedlichen Evaluationsverfahren ist vorhanden. Die Ergebnisse der Verfahren unterscheiden sich dabei ebenso wir das Vorgehen. Der Grund liegt darin, dass die Verfahren die Usability aus verschiedenen Blickwinkeln untersuchen. Ein Vergleich der Ergebnisse ist aus demselben Grund schwierig. Alle Evaluationsmethoden können einen wesentlichen Beitrag zur Verbesserung der Usability eines Systems liefern. Um die Stärken zu kombinieren und die Schwächen zu eliminieren sollten daher Verfahren möglichst kombiniert und früh einsgesetzt werden.

2.3.4 Zusammenfassung des Kapitels 2.3

In diesem Abschnitt wurden die Grundlagen aus dem Bereich Usability, die für die vorliegende Arbeit wichtig sind vorgestellt und definiert. Die Kernaussage des Abschnitts bestand dabei darin, dass Usability eine Eigenschaft von Systemen ist, die massgeblich über deren Einsatz durch Benutzer entscheidet. Somit ist es für Entwickler und Betreiber von Systemen wichtig zu wissen, wie diese Eigenschaft gemessen werden kann. Eine Messung der Eigenschaft Usability kann dann dazu verwendet werden die Akzeptanz der Benutzer durch Optimierung der gemessenen Parameter zu erhöhen. Dies kann wiederum dazu verwendet werden, die Akzeptanz von Sicherheitsmechanismen durch gezielte Optimierung ihrer Usabilityparameter zu erhöhen. Zugleich können aber auch Usability-Untersuchungen Fehlbedienungen aufzeigen und somit Schwachstellen lokalisieren. Die Messungen werden durch verschiedene Evaluationsverfahren durchgeführt, die unterschiedliche Usability-Probleme ermitteln.

Zusammenfassend wird der Begriff Usability für die vorliegende Arbeit wie folgt definiert.

> **Definition Usability:** Usability ist eine Eigenschaft eines Systems oder eines Produktes und entscheidet über seine Nützlichkeit, Verwendung und Anwendung für und durch Benutzer.

Nachdem nun die Grundlagen aus den Bereichen Usability und IT-Sicherheit einzeln beschrieben und definiert wurden, wird im folgenden Kapitel die Beziehung zwischen diesen beiden Bereichen erläutert und der Themenkomplex der benutzerzentrierten IT-Sicherheit beschrieben.

3
Benutzerzentrierte IT-Sicherheit

χαλεπὰ τὰ καλά

(Überlieferung nach Plutarch)

Nachdem im letzten Kapitel die Trends bei IT-Systemen und die Bereiche Usability und IT-Sicherheit behandelt wurden, wird in diesem Kapitel die besondere Relation zwischen Usability und IT-Sicherheit herausgearbeitet und daraus die Notwendigkeit der benutzerzentrierten IT-Sicherheit hergeleitet.

Eine häufige Annahme bei der Betrachtung der beiden genannten Bereiche besteht darin, dass Benutzbarkeitskriterien zum Teil gegensätzlich zu den Sicherheitsinteressen wirken.

„The more secure a system is, the harder it is to use. The harder it is to use a system, the less secure it will be. [72] “

Aus dem Zitat von Brian R. Krause wird diese Einschätzung deutlich. Durch die Entwicklung, durch die zur Verfügungstellung und durch die Etablierung von Sicherheitsfunktionen soll die Benutzbarkeit von Systemen sinken. Zu dieser Einschätzung führt die Überlegung, dass Sicherheitsfunktionen zusätzlich zu dem weiteren Funktionsumfang von Systemen bereit gestellt und durch die Benutzer verwendet werden müssen.

Die in Kapitel 1 geschilderten Veränderungen, die gesteigerte Bedeutung von IT-Systemen sowie die steigenden Bedrohungen durch Schadprogramme machen es zudem notwendig, dass sich zum einen immer mehr und zum anderen immer unterschiedlichere Benutzer mit IT-Sicherheit auseinander setzen. Ein Erfolg zur Erzielung von IT-Sicherheit kann dabei nur dann erreicht werden,

wenn diese Benutzer die Sicherheitsanwendungen korrekt einsetzen. Die Sicherheitsanwendungen müssen zu diesem Zweck durch unterschiedliche Benutzer benutzbar sein. Dies steht in Gegensatz zu der oben geschilderten Einschätzung von Brian R. Krause und führt zu der Annahme, dass Sicherheit ohne Benutzbarkeit durch Anwender nicht umsetzbar ist.

Wie aktuell das Thema der Einbeziehung des Benutzers in Fragen der IT-Sicherheit ist, zeigen Veranstaltungen wie der *Safer Internet Day*. Dort betonen Experten wie Stefan Grosse vom Bundesamt für Sicherheit in der Informationstechnik den Stellenwert von Benutzern. „Software-Hersteller und Online-Dienste-Anbieter sollten ihre Produkte sicherer und einfacher bedienbar machen“ ...„Die Nutzer sind immer noch weit weg von dem, was wir uns vorstellen.“[68]. Trotzdem wird das Thema „benutzbare Sicherheit“ nur in wenigen Publikationen wie z.B. Cranor et al. [32] behandelt.

Um Sicherheitsanwendungen benutzbarer zu gestalten, sind verschiedene Überlegungen notwendig. Die steigende Komplexität und die steigende bereitgestellte Informationsmenge führt dazu, dass Benutzer die Systeme und das Systemgeschehen immer weniger überblicken können. Benutzer benötigen somit geeignete Steuerungs- und Kontrollelemente, um aktiv zur Sicherheit beitragen zu können. Diese Elemente müssen den Kriterien der Usability genügen, da sie sonst durch die Benutzer ignoriert, nicht verwendet, abgeschaltet, nicht in vollem Umfang genutzt oder umgangen werden.

Bereits 1975 beschrieben Saltzer und Schroeder das Konzept der Psychlogical Acceptance [109]. Sie kommen im Rahmen ihrer Untersuchung über die Randbedingungen zur Entwicklung sicherer Systeme zu dem Schluss, dass Sicherheitsmechanismen einfach zu bedienen sein müssen, um von Benutzern verwendet zu werden. Sicherheitsfunktionen von Systemen müssen in erster Linie ein hohes Maß an Usability aufweisen um verwendet zu werden [51].

Wenn Benutzern nicht klar ist, wo die Probleme eines Systems liegen und welche Handlungen die Systemsicherheit kompromittieren könnten, müssen diese „möglichen“ Handlungen auf ein Minimum reduziert werden. Dies wird gerade durch intuitives Handeln und kleine Fehlermöglichkeiten erreicht. Benutzer sollten erst dann unsichere Zustände herbeiführen können, wenn sie sich dessen bewusst sind und verstehen was sie tun. Wenn die Erfahrung und das Empfinden gegenüber Sicherheitsmechanismen nicht berücksichtigt wird kann das dazu führen, dass zwar Gegenmaßnahmen ergriffen werden, diese aber durch falsche Anwendung nicht zur Erhöhung sondern zur Verminderung des Sicherheitsniveaus eines Systems führen [41].

Für unterschiedliche Benutzer muss die Benutzbarkeit von Systemen ver-

schiedene Aspekte berücksichtigen, da sie unterschiedliche Ziele und Erfahrungen besitzen. Zu umfangreiche individuelle Konfigurationsmöglichkeiten beheben das Problem nicht, denn jede Konfigurationsmöglichkeit bietet wieder eine neue weitere Fehlerquelle.

Die Möglichkeit jedes einzelnen Benutzers zur Einflussnahme auf die Sicherheitsfunktionen steht auch aus einem weiteren Grund in Gegensatz zur gewünschten Sicherheit des Systems. Das schwächste Glied in einem Sicherheitssystem definiert das Sicherheitsniveau des gesamten Systems [82]. Aus diesem Grund muss die Sicherheit System übergreifend sein. Sie muss unabhängig davon sein, welche Benutzer mit dem System interagieren und welche Erfahrungen und Ziele der Benutzer vorliegen. So soll die Infrastruktur einer Bank z.B. nicht dadurch kompromittiert werden können, dass einige Benutzer mit ihrem Account zu sorglos umgehen und durch ihren Umgang eine Bedrohung für das Gesamtsystem erschaffen. Hinzu kommt, dass die Begrifflichkeiten im Bereich IT-Sicherheit nicht klar definiert umrissen und für jeden Benutzer gleich gefasst sind. Da Benutzer die Begrifflichkeiten unterschiedlich interpretieren und auch verschiedene Vorstellungen davon haben, was ein System tut und welche Implikationen Benutzerhandlungen haben, ist den meisten Benutzern nicht klar, welche Implikationen ihr Handeln hat (vergleiche [41]). Um dieses Bedrohungspotential zu minimieren, sollten die Systementwickler daher Systeme entwickeln, die ein hohes Maß an intuitiver Handhabung beinhalten und nur einen kleinen Fehlerspielraum durch verschiedene Interpretationen bieten.

Die intuitive Handhabung ist auch aus Gründen der menschlichen Aufmerksamkeitsleistung und Aufnahmekapazität notwendig, da diese begrenzt ist. Die Sicherheitsaspekte einer Anwendung und die dazu notwendigen Handlungen haben für den Benutzer meist einen untergeordneten Stellenwert. Sein Hauptfokus liegt auf der eigentlichen Aufgabenerledigung. Wenn beispielsweise ein Benutzer im Internet eine Reise buchen will, überlegt er wohin die Reise gehen soll, oder wie die günstigsten Tarife sind. Die wenigsten Benutzer überlegen in dieser Situation ob ihre Suchergebnisse gespeichert oder gegen sie verwendet werden könnten. Die Sicherheitsmechanismen sollten daher möglichst gut intuitiv benutzbar sein, damit Benutzer ihre Aufmerksamkeit vollkommen auf die eigentlichen Aufgaben verwenden können. Wenn die Mechanismen als nicht intuitiv wahrgenommen werden, werden sie von vielen Benutzern nicht verwendet. Beim E-Mail Versand sind die Risiken bekannt. Um die Risiken kümmern sich aber die wenigsten Benutzer, da für sie meist der Nutzungskomfort mehr zählt. So werden trotz besseren Wissens nur ca 5% der Mails verschlüsselt übertragen [99].

Ein weiterer Grund für das besondere Verhältnis zwischen IT-Sicherheit und Usability liegt in dem „Wesen“ von Sicherheit und Sicherheitsanwendungen. Einige Kriterien der Usability aus Kapitel 2.3.1, wie zum Beispiel „Fehlertoleranz“, „Feedback“ und „Lernen“ können nicht uneingeschränkt auf Sicherheitsanwendungen angewendet werden. So besteht ein großer Unterschied zwischen Sicherheitsfunktionen und anderen Funktionen darin, dass Sicherheitsfunktionen nur dann korrekt funktionieren, wenn sie immer korrekt durchgeführt werden. Werden sicherheitskritische Fehler begangen, ist dass Ausmaß einer tatsächlichen Bedrohung sehr schwer einzuschätzen. Wird eine Email unverschlüsselt versandt, kann nicht gesagt werden, wie viele Informationen abgehört wurden. Das Kriterium der *Fehlertoleranz* kann daher bei sicherheitskritischen Anwendungen nur an sicherheitsunkritischen Stellen angewendet werden. Um diesen Zwiespalt zu lösen, könnte das Usability-Kriterium der Fehlertoleranz in Fehlervermeidung geändert werden.

Auch das Kriterium *Feedback* der Anwendung stellt eine Herausforderung dar. Zwar kann das System den Benutzern bei ihren Interaktionen ein Feedback geben, aber ob ihre Aktionen erfolgreich waren, kann nicht mitgeteilt werden. Erst wenn der Fehlerfall eintritt, kann die Unwirksamkeit der Handlungen mitgeteilt werden. Wenn Bedrohungen durch eine abgehörte Email auftreten, kann daraus geschlossen werden, dass die Vorkehrungen des Benutzers nicht ausgereicht haben oder falsch gehandhabt wurden.

Ebenfalls stellt das *Erlernen* der Arbeitsweise von Sicherheitsanwendungen ein Problem dar. Zum einen kann nur eingeschränktes Feedback gegeben werden und zum anderen kann eine einmalige Fehlbenutzung durch erneutes Ausführen nicht korrigiert werden. So bringt das erneute verschlüsselte Senden einer Email, die zuvor fälschlicherweise unverschlüsselt gesendet wurde, keine Verbesserung der Sicherheit. Bereits beim ersten Versenden könnte sie abgehört worden sein.

Das Fazit der Betrachtung beider Bereiche kann daher nur lauten, dass IT-Sicherheit ohne Usability nicht optimal umgesetzt werden kann. Einige mögliche Lösungen und die damit verbundenen Herausforderungen um Sicherheitsanwendungen benutzbarer zu gestalten sollen nun vorgestellt werden.

Benutzergruppen

Eine Möglichkeit Sicherheitsanwendungen für Benutzer leichter verwendbar zur Verfügung zu stellen ist die Verwendung von Benutzergruppen. Dabei werden die Systeme für unterschiedliche Benutzer(-gruppen) mit unterschiedlichen Sichten und Konfigurationen bereit gestellt. Für jedes Gruppenmitglied soll dadurch eine suboptimale Anpassung an seine Kenntnisse, Erfahrungen und Ziele erreicht werden. Eine Einteilung in Gruppen hat gegenüber der individuellen Konfiguration den Nachteil, dass das Fehlverhalten für die einzelnen Mitglieder der Gruppe erhöht wird, da sich jedes Gruppenmitglied ein wenig anders verhält als das „ideale“ Gruppenmitglied. Allerdings können die Kosten für die Bereitstellung und Wartung drastisch gesenkt werden. Daher muss bei Anwendungen im Sicherheitskontext auch berücksichtigt werden, dass die Gruppen ein mögliches Fehlerpotential oder Fehlverhalten beinhalten und diese geeignet minimiert werden.

Eine weitere Herausforderung bei der Bereitstellung der Systeme für spezielle Benutzergruppen besteht in der Auswahl und Bestimmung der jeweiligen Benutzergruppen. Es muss geklärt werden, wie sich die unterschiedlichen Benutzergruppen zusammen setzen, wie sie sich gegeneinander abgrenzen, wie ihr jeweiliges Verhalten ist, welches ihre Erwartungen und Ziele sind und welche Wahl an Benutzergruppen das Fehlbedienungspotential und Bedrohungsrisiko bestmöglich senken. Viele dieser Fragen können bei den primären Aufgaben der Systeme meist durch Feldanalysen beantwortet und validiert werden. Bei Querschnittsfunktionalitäten oder -aspekten, die für eine sehr inhomogene Menge von Benutzern gelten, stellen diese Fragen dagegen eine hohe Herausforderung dar. Während sich die Ziele und die Erwartungen der Benutzer hinsichtlich der primären Aufgabe ähneln, können sich die Ziele und die Erwartungen bei den Querschnittsfunktionen stark unterscheiden. Die Entwicklung von Sicherheitsfunktionalitäten stellt einen solchen Querschnittsaspekt dar. Bei der Versendung einer Email haben alle Benutzer das primäre Ziel ihre Email zu versenden. In Abhängigkeit ihrer Ziele und Erfahrungen unternehmen die Benutzer aber unterschiedliche Anstrengungen für den sicheren Versand und sind sich unterschiedlicher Bedrohungen bewusst. Durch die Erkenntnisse und Forschungen auf dem Gebiet der „Multilateralen Sicherheit“ ist bekannt, dass Benutzer oft verschiedene und gegensätzliche Sicherheitsziele verfolgen, die aus unterschiedlichen Sicherheitsbedürfnissen und Erfahrungen resultieren. Diese müssen bei der Bildung von Gruppen zur Erzielung optimaler Sicherheit mit berücksichtigt werden.

Die Hinleitung zu den richtigen Eingaben minimiert mögliche Fehler. Wenn der Benutzer seine gewohnten Prozesse durchführen kann, ohne nach dem

Sinn von möglichen Abweichungen nachzudenken, wird er dies einfach tun. Durch Benutzergruppeneinteilungen und -einstellungen müssen also die Systemeigenschaften abgedeckt werden, bei denen sich die jeweiligen Gruppenmitglieder alle in einem gewohnten Umfeld befinden.

Eine benutzergruppenzentrierte Gestaltung von Software darf dabei nicht das Ziel verfolgen, Benutzergruppen bei der Benutzung von sicherheitsrelevanter Software zu entmündigen, sondern sie bestmöglich zu unterstützen. Der meist verfolgte Ansatz, spezielle Konfigurationsmöglichkeiten und Funktionalitäten für ungeübte Benutzer zu verstecken birgt einige Nachteile und Risiken:

Falsche Annahme über das Ziel des Benutzers: Bei der Einschränkung des Systemumfanges durch Defaultkonfigurationen werden bereits einige Annahmen über das Ziel der Benutzergruppe gemacht, die nicht unbedingt mit den wahren Zielen der Benutzer übereinstimmen müssen. Durch die Unterstützung für bestimmte Ziele, ohne die Herangehensweise unterschiedlicher Benutzer zu berücksichtigen, wird ein neues erhöhtes Fehlerpotential geschaffen.

Späteres Lernen der Funktionalitäten wird erschwert: Werden einige Funktionen zu Beginn der Interaktion mit einem Programm versteckt, führt dies nicht zwangsläufig dazu, dass sie verwendet werden, sobald sie benötigt werden. Durch eine gewohnheitsmäßige Benutzung werden erweiterte Funktionen oft nicht benutzt. Die Hauptaufgabe von Systemen besteht darin, Benutzer zu unterstützen. Um dies zu erreichen, muss der Benutzer betrachtet werden und ihm an jeder Stelle eine bestmögliche Unterstützung angeboten werden. Dies kann nicht dadurch erreicht werden, dass seine Freiheiten beschnitten werden, sondern nur dadurch, dass die Unterstützung optimal für ihn bereit gestellt wird.

Nicht Berücksichtigung des Sicherheitsbedürfnisses: Das Sicherheitsbedürfnis der Benutzer richtet sich nicht unbedingt nach ihrer Kenntnis der IT-Sicherheit. Daher dürfen Konfigurationseinstellungen nicht nur abhängig von der Kenntnis sein, sondern müssen in Abhängigkeit der Ziele, der Bedürfnisse und der Erfahrungen der Benutzer erfolgen.

Durch die Bereitstellung von Programmen für Benutzergruppen kann die IT-Sicherheit verbessert werden, wenn dadurch die Programme besser auf die Ziele, Kenntnisse und Erfahrungen der Benutzer angepasst werden. Allerdings müssen die Fragen: *Welche und wie viele Benutzergruppen gibt es, wie sehen sie im Detail aus und wie verhalten sie sich?* zuvor geklärt werden ohne, dass durch die Wahl der Benutzergruppen eine Entmündigung der Benutzer stattfindet.

Gemeinsame Basis für das Systemverständnis

Einen weiteren Ansatzpunkt zur Verbesserung von Systemsicherheit durch Usability stellt das Verständnis der Systeme dar. Das Verständnis und die Benutzbarkeit eines Systems ist für einen Benutzer A, einen Benutzer B, einen Administrator oder einen Entwickler jeweils unterschiedlich, geprägt vom gesellschaftlichen Hintergrund, den jeweiligen Erfahrungen und Zielen. Über die verschiedenen Anwendergruppen muss die IT-Sicherheit verknüpft werden. Daher ist es wichtig, eine gemeinsame „Verständnis-Basis“ bei der Erstellung von Systemen zu haben und zu verwenden. Diese Basis muss nicht für alle Menschen gleich sein, aber je ähnlicher sie ist, desto leichter ist das gemeinsame Verständnis und umso leichter werden Missverständnisse bei der Bedienung vermieden. Verstehen nahezu alle Benutzer unter einer Bezeichnung ungefähr das Gleiche, werden Fehlinterpretationen verringert, im Gegensatz zu Bezeichnungen, die mehrfach interpretierbar sind.

Somit ist es nicht nur wichtig Systeme gruppenspezifisch bereit zu stellen, sondern auch möglichst eine geringe Anzahl an Gruppen anzustreben.

Aspekte der Sicherheitsanwendungen

Systeme sollen sicherer gemacht werden, indem man durch verschiedene „Sicherheitsfunktionalitäten“ dem Benutzer Aufgaben auferlegt, die es einem potentiellen Angreifer schwerer machen, die Integrität des System zu „bedrohen“. So müssen sich zum Beispiel Benutzer in vielen Institutionen mit Zugangsberechtigungen an den Systemen autorisieren. Dies findet klassischer Weise mit Passworten und Benutzeridentifikationskennungen statt. Dabei sollten Benutzer verschiedene Faktoren bei der Wahl des Passwortes berücksichtigen, damit es ein gewisses Sicherheitsniveau erreicht. Das Passwort sollte nicht zu kurz sein, die Bestandteile sollen aus verschiedensten Kategorien stammen (Kleinbuchstaben, Zahlen, Ziffern und Großbuchstaben), sich nicht lexikographisch einordnen lassen und regelmäßig gewechselt werden.

Das Wechseln des Passwortes in einem Turnus (z.B. alle drei Monate) trägt jedoch nicht dazu bei, dass Systeme benutzerfreundlicher werden. Daher sollte bei vielen Systemen geklärt werden, ob ein Passwort benötigt wird, oder ob man die Zugänge nicht anders regeln könnte (z.B. der Benutzer kennt ein leichter zu merkendes Geheimnis).

Sicherheitsanwendungen machen nur dann Sinn, wenn sie verwendet werden können. Ein Beispiel sei hier, dass das Verbergen einer Funktionalität

„SMTP-Over-Pop deaktivieren“ [1] nicht zur Sicherheit beiträgt, sondern maximal den Schaden begrenzt. Die Sicherheit kann nur dadurch erhöht werden, dass der Benutzer die Funktion versteht und in der richtigen Situation sie korrekt einsetzt.

Der Benutzer sollte nicht die Wahl und die Nötigung haben, sich einen Workaround bei der Benutzung des Systems zu erstellen. Er sollte sofort die richtige Bedienreihenfolge anwenden.

Die permanente Konfrontation mit Auswahl oder Bestätigungsdialogboxen (z.B. „Ja“ oder „Nein“) bringt das Problem, dass der Benutzer häufig nicht weiss, was er da gerade auswählt, einträgt oder welchen Prozess er damit auslöst. Es stellt sich daher häufig an dieser Stelle die Frage, ob man den Benutzer überhaupt involvieren sollte. Auf der anderen Seite benötigen Benutzer Interaktionen mit dem Programm, um Vertrauen in es zu bekommen. Die Auswahl dieser Dialogboxen sollte daher nicht das Ziel verfolgen, die Möglichkeit zur Kompromittierung der Systemsicherheit durch den Benutzer zu minimieren, sondern ein Feedback bzw. Informationen für Benutzer zu bieten.

Das Klicken um ein System sicherer zu machen muss ersetzt werden durch das Klicken um ein System unsicherer zu machen. Der Standardweg sollte nicht darin liegen, ein System durch Konfigurationen oder zusätzliche Mechanismen sicherer zu machen, sondern im Möglichen unsicherer machen eines Systems durch Wegnahme von Sicherungsmechanismen. Die Konditionierung der Benutzer auf Schnelligkeit oder andere gewünschte Attribute eines Systems, die sofort offensichtlich für Benutzer sind, muss zugunsten nicht offensichtlicher Kriterien, wie z.B.der Sicherheit, geändert werden.

Eine Möglichkeit zur Verbesserung von IT-Sicherheitsmechanismen in Systemen stellten Balfanz, Durfee und Grinter 2004 vor [15]. Sie automatisierten viele Konfigurationsschritte und ermöglichten so für die Benutzer einen Zeitgewinn. Dieser Zeitgewinn führte wiederum zu positiven Rückmeldungen über das System.

Um Benutzer bei der IT-Sicherheit zu integrieren, muss man nicht nur Wissen vermitteln, sondern man muss ein Anreizsystem schaffen, welches Benutzer für richtiges Verhalten belohnt und für falsches Verhalten bestraft. Benutzer sind sich häufig nicht über die weitreichenden Gefahren bewusst, die falsches

[1] Diese Funktion ist in einem großen Betriebssystem integriert. Die später in dieser Arbeit vorgestellten Experimente zeigten aber, dass kaum jemand die Funktion anwenden konnte.

Handeln hervorrufen kann[2]. Wenn Benutzer beispielsweise auf ihrem eigenen Rechner Malware , durch die sie bei ihrer Arbeit nicht behindert werden, nicht eliminieren tragen sie doch zu einer Gefährdung bei, da sich die Malware so verbreiten kann.

Bei der Entwicklung von Sicherheitsanwendungen sind spezielle Einflüsse auf die Benutzbarkeit zu beachten, die umgesetzt werden müssen. Nach [83] sind dies die Folgenden: Es handelt sich bei Sicherheitsanwendungen um unwiderrufliche Aktionen (zeitpunktbezogene Aktionsfehler und zeitraumbezogene Konfigurationsfehler). Das schwächstes Glied bestimmt das Sicherheitsniveau, Sicherheit wird von vielen Benutzern als nachrangiges Ziel gesehen. Häufig gibt es nur eine Erstbenutzung, die zudem einen hohen Abstraktionsgrad aufweist. Die Fehlerkontrolle ist schwierig, und für die Benutzung von Sicherheitsanwendungen ist Vertrauen die Voraussetzung.

Bei der Optimierung eines Systems hinsichtlich der beiden Bereiche Usability und IT-Sicherheit müssen also Benutzer-spezifische (bei der Benutzbarkeit) Aspekte in einen globalen Aspekt der gewünschten IT-Sicherheit einbezogen werden. Die Usability soll und muss individuell angepasst und entwickelt werden. Trotzdem müssen alle Grundbedürfnisse in einem Konsens zusammengefasst werden.

Diese Betrachtungen führen zu der folgenden Überlegung. Wenn Benutzer mit einem System interagieren, wird das Bedrohungspotential durch Fehlbedienungen oder falsche Erwartungen (oder Systemverständnis) durch Usability-Maßnahmen minimiert. Weiterhin muss die Sicherheit in die Systeme von Beginn an integriert werden und darf nicht erst später zusätzlich durch weitere Funktionen hineingebracht werden. Der Benutzer stellt mit seinem Verhalten also eine wesentlichen Parameter für die Umsetzung hoher Systemsicherheit bereit.

Dass das Erreichen von hoher IT-Sicherheit häufig mit dem Erreichen guter Usability zusammenhängt, kann an folgendem Beispiel gezeigt werden.

Ein Benutzer der seine Firewall selbst administriert muss wissen, welche Ports er dabei frei gibt. Ebenso darf er nicht durch häufige Warnmeldungen der Firewall dazu verleitet werden, zu viele Ports freizuschalten um diese Warnmeldungen zu umgehen. Durch das Freischalten weiterer Ports würde er das Bedrohungspotential erhöhen.

[2] Dies wird auch in den später beschriebenen Experimenten gezeigt.

Zusammenfassung

Die Interaktionen bezüglich der Sicherheit müssen bei Systemen sensibel durchgeführt werden, um Bedrohungen oder Schäden durch das Eintreffen falscher Erwartungen zu minimieren. Aus diesem Grund sind Systeme notwendig, die von den Benutzern verstanden und bedient werden können. Dies ist nur durch die Umsetzung von Maßnahmen aus dem Bereich Usability möglich. Somit müssen beide Bereiche gemeinsam bei der Entwicklung und dem Betrieb von Systemen umgesetzt werden. Dabei geht die Usability nach [51] vor die IT-Sicherheit.

IT-Sicherheit muss dabei in Systeme von Beginn an integriert werden und darf nicht erst später zusätzlich hineingebracht werden. Sicherheitsmechanismen sollten die Benutzungsmöglichkeiten der Systeme nicht einschränken sondern absichern/unterstützen.

Eine Kenntnis der verschiedenen Benutzergruppen und die Einbeziehung des spezifischen Gruppenverhaltens kann dazu genutzt werden, die Usability der Systeme zu steigern und sie somit sicherer zu machen.

Sicherheitsanwendungen haben einige besondere Aspekte (Fehlervermeidung, Lernproblematik, Feedbackproblematik...), die bei der Umsetzung hoher Usability bedacht werden müssen.

> **Fazit:** IT-Systeme, die Interaktionen mit Benutzern haben, müssen ein Höchstmaß an Usability aufweisen, um ein Höchstmaß an IT-Sicherheit erreichen zu können.

Um diesen Aspekt vertieft betrachten zu können, wird für diese Arbeit der Begriff der benutzerzentrierten IT-Sicherheit wie folgt definiert:

> **Definition benutzerzentrierte IT-Sicherheit:**
> Unter der benutzerzentrierten IT-Sicherheit werden alle Maßnahmen und Aspekte verstanden, die die Erhöhung der IT-Sicherheit erreichen indem die Interaktion von Benutzern mit Systemen betrachtet und unter Usability-Aspekten verbessert wird.

4

Fallstudien zur benutzerzentrierten IT-Sicherheit

„Bei einem Spiel kann man einen Menschen in einer Stunde besser kennen lernen als im Gespräch in einem ganzen Jahr“

(Überlieferung nach Platon)

Wie im Kapitel 1 beschrieben, sind Benutzer in vielen Lebenssituationen darauf angewiesen, dass IT-Systeme korrekt funktionieren. Ein Ausfall oder eine Fehlfunktion der IT-Systeme führt zu starken Beeinträchtigungen für die Benutzer. Durch ihr Verhalten können Benutzer die korrekte Funktion der Systeme unterstützen oder aber auch selbst Beeinträchtigungen auslösen.

Benutzer sind bei der Anwendung von IT-Systemen meist drauf fokussiert, ihr primäres Ziel zu erreichen. Sie richten ihre Aufmerksamkeit nur auf das angestrebte Ziel und beachten Bedrohungen ihrer Privatsphäre oder Daten nicht [122]. Bemerken sie die negativen Auswirkungen nicht, oder treffen die Auswirkungen erst zu einem späteren Zeitpunkt ein, werden von ihnen keine Maßnahmen ergriffen.

Ein Ziel bei der Entwicklung neuer Systeme muss darin bestehen, alle Arten von Beeinträchtigungen zu mildern oder sogar ganz auszuschließen. Dies kann aber weder durch alleinige Maßnahmen auf Benutzerseite noch allein durch den Hersteller erreicht werden. Nach Nielsen [97] muss sich der Umgang mit der IT-Sicherheit grundlegend ändern. Die Verantwortung für einwandfrei

funktionierende Systeme darf den Benutzern nicht allein auf gebürdet werden, da die Systeme zu kompliziert seien, als dass sie jeder Benutzer verstünde.

Allein durch Verfahren und Produkte auf Herstellerseite können einwandfrei funktionierende Systeme allerdings auch nicht gewährleistet werden. Gerade das Internet und die dadurch schnelle Verbreitung von Informationen macht es für Hersteller unmöglich, bei vielen Systemen alle Fehlfunktionen zu unterbinden. Hersteller haben nicht auf alle Randbedingungen beim Einsatz ihrer Software Einfluss und können somit nicht mehr umfassend Fehlfunktionen durch Maßnahmen auf ihrer Seite ausschließen. Viele Fehlfunktionen werden durch unbedachte oder unerfahrene Benutzer ausgelöst. So können beispielsweise Benutzer ihre Email-Systeme mit Filtern so konfigurieren, dass ungewollte Emails gefiltert werden. Hersteller übernehmen meist eine grobe Vorfilterung der Emails und überlassen es dem Benutzer ein „Finetuning“ der Filter durchzuführen. Eine falsche Konfiguration der Filter durch den Benutzer kann dazu führen, dass mehr erwünschte Emails gefiltert werden, als ohne Konfiguration. Je nach Ziel des Benutzers, könnte er sein System so konfigurieren, dass er nur einen Bruchteil der gewünschten Emails erhält, ohne dies zu bemerken.

Somit müssen Benutzer ebenso in die Vermeidung von Fehlfunktionen und Ausfällen miteinbezogen werden. Benutzer und Entwickler müssen jeweils einen Teil der Verantwortung übernehmen. Die konsequente Miteinbeziehung der Benutzer und ihrer daraus resultierenden Verantwortung beim Umgang mit IT-Systemen minimiert das Fehlverhaltens und Ausfallpotential der Systeme. Dazu müssen Benutzer von ihrer Verantwortung wissen und dieser auch gerecht werden können. Um dies zu erreichen, müssen während des gesamten Usability-Engineering-Prozesses (vergleiche Kapitel 2.3.1) Maßnahmen bezüglich der IT-Sicherheit ergriffen werden. Diese Maßnahmen müssen dazu führen, dass Benutzer ihre Verantwortung erkennen, sie wahrnehmen wollen und auch umsetzen können.

Um das Bedrohungspotential von Systemen zu minimieren, werden Systeme hinsichtlich ihrer Schwachstellen nach verschiedenen Evaluierungsmethoden untersucht. Eine der möglichen Evaluierungsmethode stellt die in Kapitel 2.2.3 beschriebene Zertifizierung nach den Common Criteria (CC) dar. Dass Benutzer im Kontext der Zertifizierung nach den CC äußerst wichtig sind, wird von den Zertifizierungsstellen betont. Das Bundesamt für Sicherheit in der Informationstechnik (BSI), die oberste Zertifizierungsinstanz für den Zertifizierungsstandard der CC in Deutschland, schreibt in seinen Hinweisen [22] für Hersteller von Software:

“Ziel muss es deshalb sein, informationsverarbeitende Systeme so zu ent-

werfen, herzustellen und einzusetzen, dass ein angemessener Schutz z.B. gegenüber Bedienungsfehlern und Manipulationsversuchen gegeben ist.“

Die Zertifizierung [23] des Agentenframeworks JIAC IV [34],[56] nach den Common Criteria zeigte, dass die Interaktion von Benutzern mit dem zu untersuchenden System nur ansatzweise untersucht wurde ([47] und [56]). Die Abbildung 4.1 zeigt das durch die Zertifizierung untersuchte System[1]

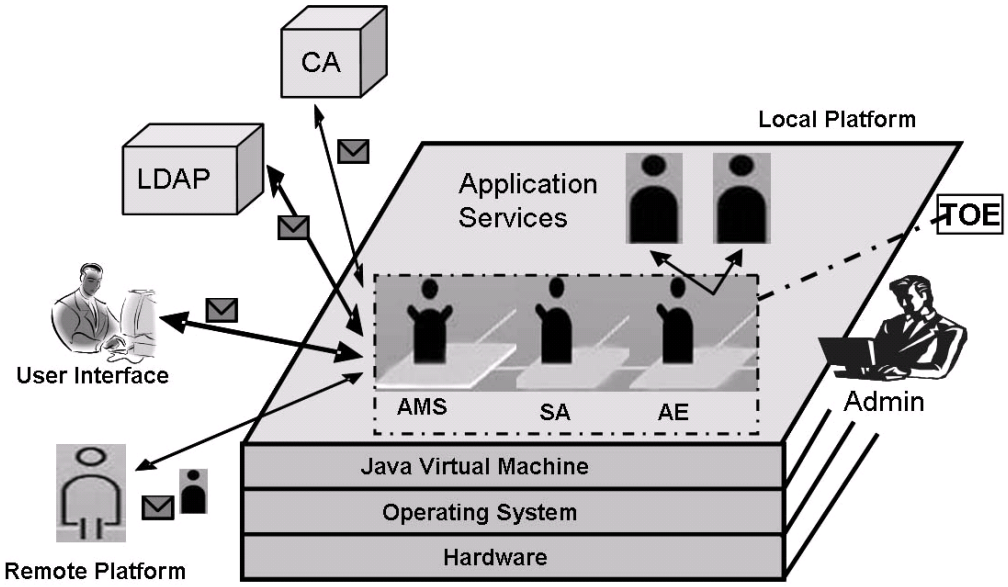


Abb. 4.1: Evaluierungsgegenstand JIAC IV [47]

Obwohl in dem abgebildeten System Benutzer mit diesem interagieren, wird der Untersuchungsfokus allein auf technische Umsetzungen und Rahmenbedingungen gelegt. Die CC verlangen ein hohes Maß an Sicherheitsbewusstsein innerhalb des entwickelnden Unternehmens. Auf Benutzerseite wird das Vorhandensein oder die Schaffung eines Sicherheitsbewusstseins in den CC nicht beachtet. Die CC untersuchen, ob Handbücher für Administratoren (Konfiguration des Systems) und Benutzer (Benutzung des Systems) vorhanden sind. Sie überprüfen aber nicht, ob dies auch fehlerfrei angewendet werden oder wie Benutzer ihre Verantwortung wahrnehmen. Die CC gehen von der Prämisse aus, dass diese zwei Handbücher korrekt angewendet werden, wenn dies möglich ist.

[1] Mit der Zertifizierung von JIAC IV wurde zum ersten Mal ein Framework mit generischer Sicherheit zertifiziert. Eine andere Zertifizierung von generischer Sicherheit wurde bei der IAIK-JCE durchgeführt. Die Zertifizierung der IAIK-JCE CC Core, Version 3.1 erfolgte fasst zeitgleich, erhielt aber das Zertifikat ein wenig früher [120]. Bei vorangegangenen Evaluationen wurden Firewalls, Chipkartenleser oder Betriebssystemteile evaluiert.

Dass diese Untersuchungssicht nicht ausreicht wird in den folgenden Fallstudien gezeigt und beschrieben. Die Fallstudien untersuchen die Wichtgkeit der Einbeziehung der Benutzer zur Erzielung von Systemsicherheit. Sie untersuchen die Herausforderungen der benutzerzentrierten Sicherheit aus unterschiedlichen Blickwinkeln. Darüber hinaus zeigen sie wo Ansatzpunkte für Lösungen sind, um die Systeme „sicherer“ zu machen, indem die Interaktion von Benutzer und System verbessert wird.

Alle Fallstudien wurden im Rahmen der Tätigkeit als wissenschaftlicher Mitarbeiter am DAI-Labor durchgeführt. Aus diesem Grunde handelte es sich bei den Versuchsteilnehmern größtenteils um Mitarbeiter des Labors und Studenten der von mir betreuten Veranstaltungen. Jeder Versuchsteilnehmer nahm nur an genau einer der Studien teil und musste auch einen Fragebogen ausfüllen. Wie beispielsweise bei [106], [110] oder auch [20] beschrieben ist, hängt die Qualität der Ergebnisse und Aussagen von Fragebögen entscheidend mit der Qualität der Vorüberlegungen, Planungen und Durchführungen der Versuche und Fragebögenevaluationen zusammen. Aus diesem Grunde wurde für alle vorgenommenen Fragebögenevaluationen das im Anhang A beschriebene Prozedere gewählt und angewendet.

Im Folgenden werden nun die einzelnen Untersuchungen, Fallstudien und implementierten Systeme vorgestellt. Nachdem die Betrachtung der oben geschilderten Zertifizierung gezeigt hatte, dass dort die Einbeziehung der Benutzer nicht untersucht wird, zeigen die zwei folgenden Fallstudien zunächst den Bedarf nach der Mitwirkung von Benutzern auf. Sie zeigen wo das Bedrohungspotential und die Herausforderungen durch leichtfertigen Umgang von Benutzern mit IT-Systemen liegen, und dass sich viele Benutzer ihrer Verantwortung nicht bewusst sind.

Im Anschluss daran wird in mehreren Stufen eine Evaluationsmethode erarbeitet, die das Verhalten von Benutzern untersucht.

4.1 Bewusstsein der Benutzer über das Bedrohungspotential ihrer Daten

Menschen sollen durch heutige IT-Systeme Lösungen erhalten, die sie in immer mehr Bereichen des Alltags unterstützen und die ihre Aufgaben und Arbeiten erleichtern. Wie im Kapitel 2.1 beschrieben geht ein Trend bei der Unterstützung zu „ambienten“ IT-Systemen. Diese arbeiten wie jegliche IT-Systeme mit Daten, welche verschiedenen Gefahren ausgesetzt sind. Daher werden Maßnahmen ergriffen, um unterschiedliche Sicherheits- oder Schutzziele zu erreichen und Gefahren zu minimieren.

Bei diesen Sicherheitszielen handelt es sich um die im Kapitel 2.2 vorgestellten Sicherheitsziele (z.B. Authentizität, Datenintegrität, Informationsvertraulichkeit, Vermeidung von unzulässigem Informationsfluss oder Anonymisierung und Pseudomisierung). Benutzer können durch eine falsche Benutzung der Systeme Fehler verursachen und so gegen diese Ziele wirken. Dies führt zu einer Beeinträchtigung der IT-Sicherheit. Somit bedroht jede Benutzung durch Benutzer die Sicherheit des Systems. Um diesem Trend bei IT-Systemen Rechnung zu tragen, muss der Benutzer mit in IT-Sicherheitskonzepte einbezogen werden. Einen Ansatz bietet die Untersuchung darüber wie bewusst sich Benutzer möglicher Gefahren sind, was die folgende Idee zeigt.

4.1.1 Die Idee von der Bedrohung der IT-Sicherheit durch die Benutzer bei ambienten Systemen

Benutzer müssen sich Bedrohungen bewusst sein und sie erkennen (können), um aktiv Maßnahmen gegen sie zu ergreifen. Um diese Idee zu untersuchen, werden nun einige im Folgenden beschriebenen Hypothesen evaluiert.

Auf der Idee basierende Hypothesen

Benutzer sind sich der Gefahren bei zukünftigen modernen Systemen, wie sie ambiente Systeme darstellen, zu wenig oder nicht bewusst, um auf sie reagieren zu können, sodass sie daher ungewollte Sicherheitsbedrohungen verursachen. Weiterhin sind sie sich über das gleiche Risiko in verschiedenen Domänen unterschiedlich bewusst.

Diese Hypothesen basieren auf dem folgenden Gedankengang: Die Eigenschaft ambienter Systeme in die Umgebung eingebettet zu sein, führt zu dem Problem, dass Benutzer häufig mit ihren Daten zu sorglos umgehen. Dies resultiert daraus, dass sie die Systeme wegen der Einbettung in die Umgebung zu wenig wahrnehmen, ihre Aufmerksamkeit durch den fortdauernden Kontakt sinkt, und sie auch nicht nachzuvollziehen können, welche Daten und Datenverknüpfungen durch die Benutzung gewonnen werden können. Eine weitere Vermutung liegt darin, dass durch die Etablierung der Systeme in neuen Domänen ein neues Bedrohungspotential entsteht, da Benutzer Systeme in unterschiedlichen Domänen unterschiedlich risikoreich ansehen, auch wenn die Systeme die gleichen Daten benutzen.

Nachfolgend wird für die Thematik, wie bewusst sich der Benutzer möglicher Gefahren ist, der englische Begriff (User) Awareness verwendet. Die Problematik der User Awareness bei herkömmlichen IT-Systemen wird z.B. in [92] und [40] behandelt und in verschiedenen Studien gezeigt wie z.B. [26] oder [102]. Die erste Studie beschreibt, dass die Problematik der „User Awareness“ zu zahlreichen Bedrohungen führt. Der Fokus des Berichtes liegt dabei auf den Bedrohungen, denen die PC's der Benutzer ausgesetzt sind (z.B. durch Viren oder Phishing). Die zweite Studie zeigt, dass viele Benutzer mit den Passwörtern zu diesen Systemen nicht verantwortungsbewusst umgehen. Bei beiden Studien wurde die Interaktion der Benutzer mit privaten oder vom Arbeitgeber gestellten Systemen analysiert.

Im Rahmen dieser Arbeit wurde zu dieser Thematik ebenfalls ein Konzept entwickelt und eine Untersuchung durchgeführt. Im Gegensatz zu den vorgestellten Studien wird in dem entwickelten Konzept untersucht, wie sich Benutzer verhalten, wenn sie nicht mit privaten PC's oder PC's ihrer Arbeitgeber interagieren, sondern mit öffentlich zugänglichen Systemen.

Zur Überprüfung der Hypothesen entwickeltes Konzept

Um die oben aufgestellten Hypothesen zu evaluieren, wurde das folgende Konzept entwickelt: Benutzer sollen dazu animiert werden mit einem öffentlich zugänglichen System zu interagieren und dabei Daten preis zugeben. Es ist dabei wichtig, dass das System öffentlich ist, weil die Benutzer so nicht abschätzen können, was alles mit den Daten gemacht wird. Um das Bewusstsein der Benutzer in Bezug auf die Sensibilität der eingegebenen Daten zu untersuchen, müssen zudem reale nicht sofort offensichtliche Bedrohungen im System existieren und zum anderen muss es Benutzern möglich sein, Daten einzugeben, die die oben genannten Sicherheitsziele umsetzen, und welche, die sie verletzen. Um die zweite Hypothese zu überprüfen, sollte zudem für das System eine Domäne gewählt werden, die mit der Domäne „Geld oder Banken“ verglichen werden kann. Da in vielen Untersuchungen (z.B. [26]) diese Domäne gewählt wird um das Bedrohungspotential von IT-Systemen zu zeigen, ist hier das Bewusstsein bei vielen Benutzern ausgeprägter.

4.1.2 Praktische Evaluation des aufgestellten Konzeptes

Um das entwickelte Konzept und die aufgestellten Hypothesen der User Awareness bei ambienten Systemen zu untersuchen wurde ein Experiment bei einer konkreten Anwendung im Healthcare Bereich durchgeführt.

Systeme im Healthcare Bereich sind von zwei Arten von Risiken bedroht. Zum einen können Fehlfunktionen bzw. von Außen hervorgerufene Störungen das Leben oder die Gesundheit des Benutzers direkt bedrohen. Diese Bedrohungen werden im Folgenden nicht weiter betrachtet, da sie durch Maßnahmen auf Herstellerseite unterbunden werden müssen.

Zum anderen sind die Daten im System fast immer personengebunden. Diese Daten sind als sensibel einzustufen, da sie Benutzer persönlich betreffen und von Angreifern gegen sie verwendet werden könnten. Einem potentiellen Angreifer ist es so möglich den Benutzer „persönlich“ anzugreifen. Dieser Angriff ist dann möglich, wenn die Möglichkeit der Datenverknüpfung von Identität und persönlichen Daten gegeben ist. Diese Bedrohung entsteht in vielen Fällen durch das falsche Verhalten der Benutzer. Benutzer ermöglichen die Verknüpfung von Identität und persönlichen Daten durch Eingabe ihrer sensibler Daten auch in Situationen, wo die Eingabe der wahren Identität nicht notwendig ist. Je mehr Daten dabei vom Benutzer bekannt sind oder eingegeben werden, desto leichter ist die Ermittlung seiner Identität und ein umso höheres Bedrohungspotential entsteht.

So könnten beispielsweise Benutzer einen schlechteren Lebensversicherungsabschluss erhalten, wenn der Versicherer Kenntnis über Bluthochdruck des Versicherten hätte. Somit stellt die Verknüpfung der Tatsache, dass eine Person Bluthochdruck hat, mit ihrer Identität, eine reale Bedrohung dar. Auf diese Bedrohungen können Benutzer aktiv einwirken, indem sie zum Beispiel in einem System zur Messung von Vitaldaten ein Pseudonym wählen und möglichst wenig personengebundene reale Daten eingeben.

Die konkreten Probleme und Bedrohungen sind somit:

- Benutzer geben Daten ein, die eindeutig mit ihrer Identität verknüpft werden können.
- Benutzer geben mehr Daten preis als notwendig sind.
- Die Benutzer ergreifen keine Maßnahmen um ihre Daten zu schützen.

Um die Bedrohungen zu minimieren, müssen Benutzer ein Bewusstsein entwickeln, dass es sich auch im Healthcare Bereich um einen Bereich mit sensiblen Daten handelt, und dass sie diese Daten nicht uneingeschränkt preisgeben dürfen. Um die Sicherheit der Daten (und der IT-Systeme) zu erhöhen, muss untersucht werden, wie das Bewusstsein der Benutzer im Umgang mit ihren Daten ist und wie dieses weiter gesteigert werden kann.

Dazu diente das folgende Experiment. Es untersucht, welcher Gefahren und Bedrohungen sich Benutzer im Umfeld eines Healthcare-Systems bewusst sind und wie sie sich verhalten.

Das entwickelte System

Bei dem untersuchten System handelt es sich um den „Smart Health Assistent“ (SHA). Das Software-System SHA wurde als persönlicher virtueller Trainer in der Gesundheitsdomäne entwickelt. Beim SHA handelt es sich um eine Webapplikation, die den Benutzer hinsichtlich seiner Fitness berät. Durch externe Geräte lassen sich verschiedene Vitalparameter (z.B. Blutdruck, Puls) messen und im System verwenden. Basierend auf diesen Werten gibt das System Vorschläge für Trainingseinheiten und Ernährung. Die Abbildung 4.2 zeigt einen Überblick über das System. Das System setzt auf einem Agenten-Framework auf und wurde als Multi-Agent-System (MAS) realisiert. Dieser Ansatz wurde gewählt, weil die Eigenschaften von MAS-Architekturen wie Modularität, Skalierbarkeit, Adaptivität und Verteilung besonders bei der Umsetzung von eingebetteten und ambienten System Vorteile gegenüber anderen klassischen Ansätzen [12] [61] bieten.

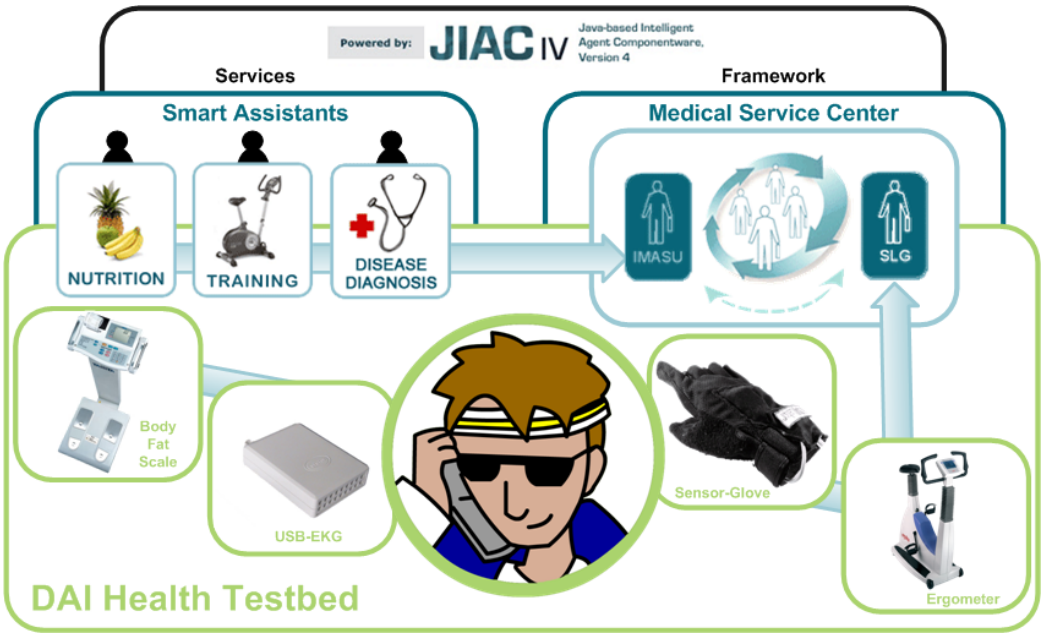


Abb. 4.2: Das SHA-System

Das durchgeführte Experiment

Das Experiment untersuchte, ob sich Benutzer des SHA der Problematik die aus Verknüpfung ihrer Daten und ihrer realen Identität entsteht, bewusst sind.

Um die aufgestellten Hypothesen zu evaluieren, sollte das Experiment zunächst die folgenden Fragestellungen untersuchen:

`Frage:1` Wissen Benutzer, dass sie bei der SHA-Anwendung mit sensiblen Daten umgehen?

`Frage:2` Welche der verwendeten Daten schätzen Benutzer als sensibel ein, und welche dieser Daten möchten sie weitergeben?

`Frage:3` Wie unterscheidet sich das Empfinden der Sensibilität der Daten in verschiedenen Domänen? (z.B. Bankenbereich im Vergleich zum Healthcare Bereich).

`Frage:4` Lässt sich das Bewusstsein durch Hinweise im Programm steigern?

Der Versuch bestand aus verschiedenen Schritten, die in Abbildung 4.3 skizziert sind.

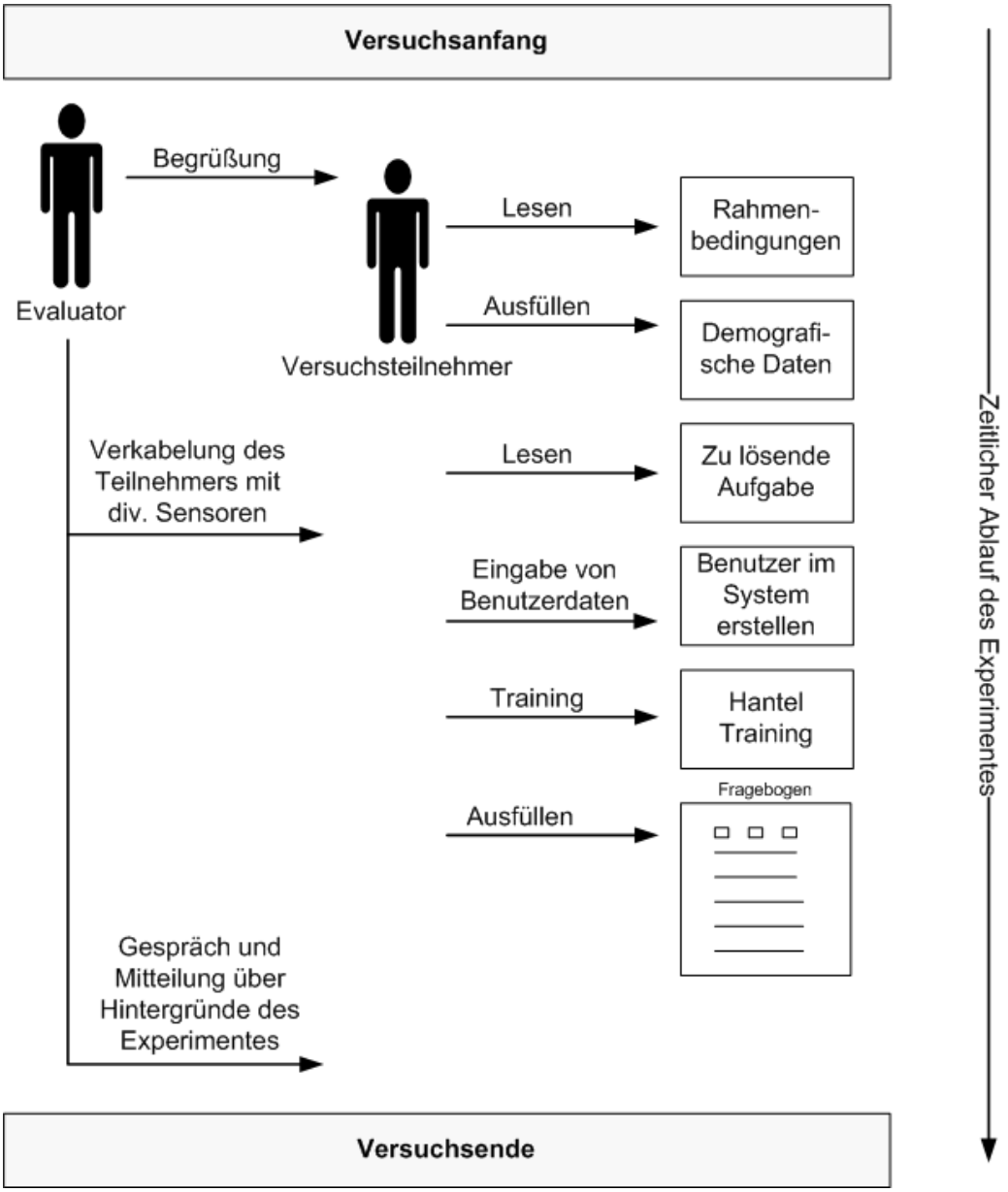


Abb. 4.3: Der Versuchsablauf zur Untersuchung der Awareness beim SHA-System

Die Versuchsteilnehmer erhielten zu Beginn des Versuches eine kurze Situations- und Aufgabenbeschreibung sowie den Fragebogen aus Anhang A. In dieser wurde ihnen gesagt, dass sie ein Fitnessprogramm testen sollten, um den Entwicklern Aufschlüsse darüber zu geben, wo die Benutzbarkeit verbessert werden könnte. Den Benutzern wurde zu diesem Zeitpunkt nicht gesagt, dass ihr Umgang mit sensiblen Daten ebenfalls Gegenstand des Experimentes sei. In dem ersten Teil des Fragebogens sollten sie ihre demografischen Daten (z.B. Alter, Beruf...) eintragen. Durch diese Daten war es nicht möglich die Benutzer einwandfrei zu ermitteln. Die gemessenen Daten konnten nicht mit der Identität der Benutzer zweifelsfrei verknüpft werden. Zusätzlich wurde ihnen die folgende Situation geschildert. In dieser sollten sie die SHA-Anwendung verwenden und hinsichtlich der Usability evaluieren.

Die Benutzer sollten sich vorstellen, bei einem Arzt einen Prototypen der SHA-Anwendung zur Verbesserung ihrer Fitness zu sehen. Dies kann als Analogie zu vielen anderen ambienten Diensten, die Benutzer alltäglich umgeben, gesehen werden.

Die Versuchsteilnehmer waren zur Dateneingabe per Zufall in drei Gruppen aufgeteilt worden. Gruppe 1 erhielt das Programm ohne Hinweis auf die Sensibilität der Daten. Gruppe 2 erhielt das Programm mit dem im Fließtext der Begrüßung eingebetteten Hinweis, dass einige der Daten bei der Anmeldung sensibel seien. Gruppe 3 erhielt das Programm mit dem gleichen aber stark hervorgehobenen Hinweis.

Im ersten Schritt des praktischen Versuchs mussten sie eine Anmeldung am System durchführen. Dazu mussten sie einige Daten eingeben. Einige der Daten waren dabei als „Mussfelder“ und einige als „optionale Felder[2]“ gekennzeichnet.

Als Pflichteingaben waren von allen drei Gruppen die Eingabefelder „Nachname“, „Vorname“, „Geschlecht“, „Größe“ und „Gewicht“ auszufüllen. Es gab für diese Daten allerdings keinerlei Plausibilitätskontrollen. Zusätzlich konnten weitere freiwillige personengebundene Daten eingegeben werden, wie z.B. die E-Mail Adresse, Telefon.

Nach Eingabe dieser Daten wurden den Benutzern Sensoren angelegt, und sie sollten einige Fitnessübungen durchführen (Hanteltraining, Kniebeugen ...), um Daten für die angelegten Sensoren zu liefern. Welche Daten die Sensoren maßen, und welche Daten dadurch ins System gelangen könnten, wurde nicht erwähnt. Ebenso wenig wurde gesagt, wozu die Daten dienten. Als Ziel für die

[2] Im System gab es an keiner Stelle einen Hinweis darauf, wozu die Daten verwendet wurden.

Geschlecht	Anzahl
weiblich	18
männlich	40

Tab. 4.1: Geschlecht der Teilnehmer

Alter	Anzahl
≤ 25	28
26-30	10
31-40	11
41-50	5
51-60	4

Tab. 4.2: Alter der Teilnehmer

Beruf	Anzahl
Student (Info.)	18
Angestellte(r)	14
sonstiger Student	17
Auszubildende(r)	1
Hausfrau	3
arbeitssuchend	2
keine Angabe	3

Tab. 4.3: Tätigkeit der Teilnehmer

Dateneingabe wurde den Benutzern mitgeteilt, dass ein Fitnessplan erstellt werden sollte.

Es bestand für die Versuchsteilnehmer keinerlei Notwendigkeit bei der Systembenutzung reale Daten einzugeben. Nach Beendigung des praktischen Anteils beantworteten die Benutzer den Fragebogen. Dort waren auch Fragen integriert, ob die Benutzer die Daten im System als sensibel einschätzten (z.B. Frage 8, 9 und 10).

Ergebnisse des Experimentes

An dem Experiment nahmen insgesamt 58 Versuchsteilnehmer teil. Die Tabellen 4.1, 4.2 und 4.3 zeigen die Stammdaten der Versuchsteilnehmer.

Die erste Fragestellung, die bei der Auswertung untersucht wurde, war, wie viele Benutzer reale Daten in ein ihnen unbekanntes System eingaben. Das Ergebnis ist in Abbildung 4.4 dargestellt. Im Fragebogen wurden dazu die Teilnehmer in Frage 5 gefragt, bei welchen der folgenden Daten sie im Programm ihre realen Daten eingegeben hatten.

Die Abbildung 4.4 zeigt, dass eine hohe Zahl der Benutzer reale sensible Daten ins System eingab. Die Ergebnisse der drei Versuchsgruppen unterscheiden sich dabei kaum. Der unterschiedliche Hinweis auf die Problematik der Daten hatte keinen Einfluss auf das Versuchsverhalten der unterschiedlichen Gruppen. Das bedeutet, dass die Hinweise von den Benutzern entweder nicht beachtet wurden, oder dass sich die Benutzer nicht bewusst darüber waren, welche Daten wie sensibel sind. Zu sehen ist auch, dass das Bewusstsein einer möglichen Bedrohung bei dieser Anwendung aus dem Healthcare-Bereich nicht sehr hoch war. Die Benutzer gaben bei den „Mussfeldern“ im Durchschnitt ca. 86% reale Daten ein. Sie achteten darauf, welche Felder als

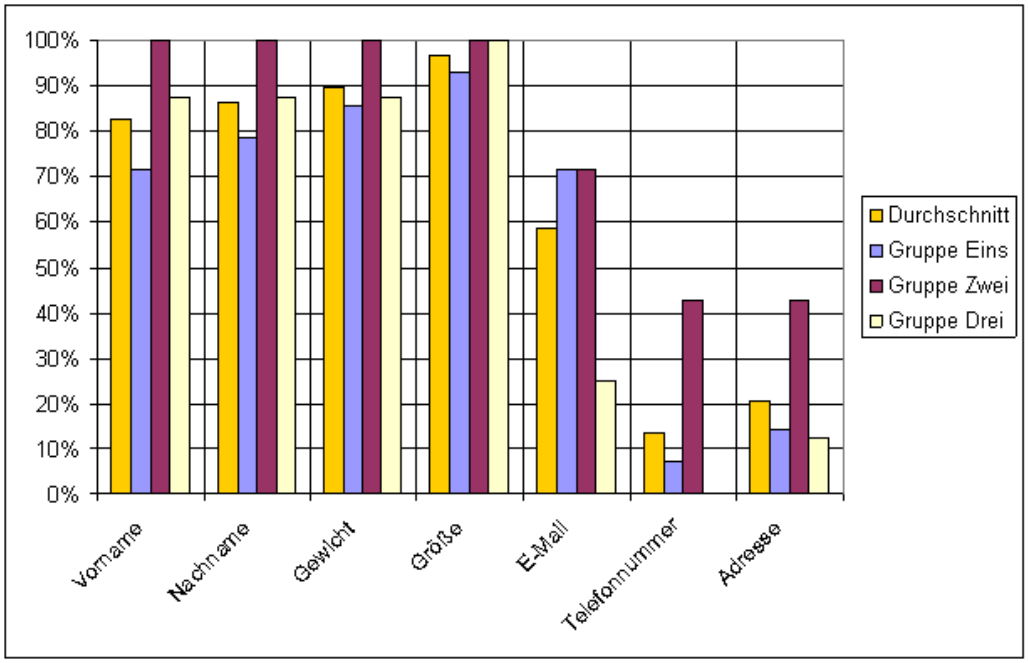


Abb. 4.4: Eingabe realer Daten

Pflichtfelder oder optionale Felder gekennzeichnet waren und leiteten daraus ab, welche Daten das Programm scheinbar benötigte und welche Daten es scheinbar generierte.

Die Abbildung 4.5 zeigt den Anteil der Benutzer, die reale Daten eingaben, welche die Bestimmung eines möglichen Übergewichts und die Zuweisung zu ihrer Identität ermöglichten. Dabei handelte es sich um alle Benutzer, die sowohl die Relation zwischen Größe und Gewicht, als auch genug Daten zur Bestimmung ihrer Identität eingaben. Diese konkrete Bedrohung steht stellvertretend als Beispiel für viele andere mögliche Bedrohungen. Sie zeigt, wie sensible Daten gegen Benutzer verwendet werden können. Andere Bedrohungen würden sich aus den potentiellen Sensordaten ergeben. Diese könnten ebenfalls dazu benutzt werden, das Risiko für Krankheiten zu ermitteln (z.B. Blutdruck) oder den Benutzer durch die Ausnutzung der Kenntnis des Aufenthaltsortes zu verfolgen. Das Beispiel zeigt, dass die Eingabe von sensiblen persönlichen Daten im medizinischen Kontext sehr gefährlich ist, da simple Daten (z.B. Größe und Gewicht) so kombiniert werden können, das reale Bedrohungen entstehen.

Nur 6 der 58 Versuchsteilnehmer gaben ihre Daten so in das System ein, dass es nicht möglich war, ihre Identität mit den persönlichen Daten zu ver-

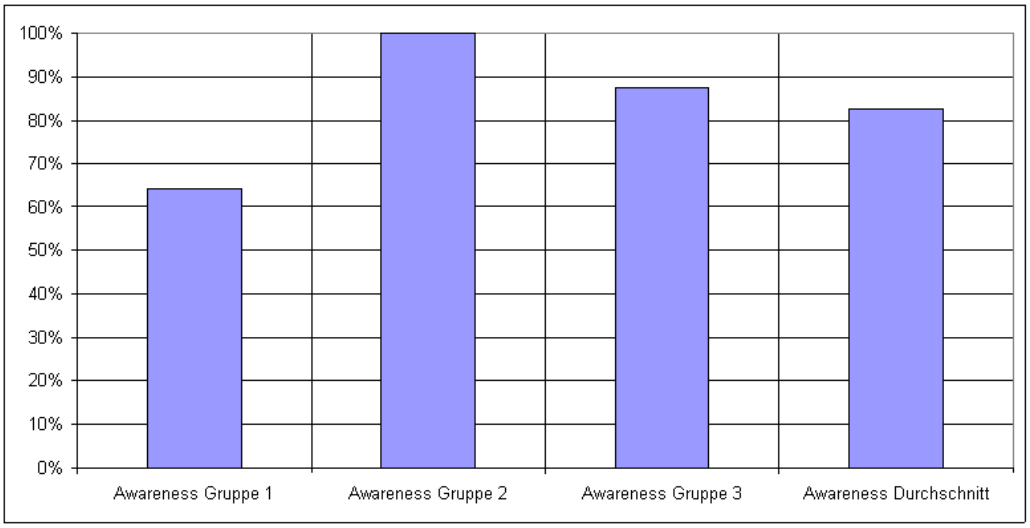


Abb. 4.5: Awareness bei der Dateneingabe

knüpfen. Allerdings waren sich mehr Benutzer der Sensibilität der Daten bewusst, wie ein Ergebnis des Fragebogens in Abbildung 4.6 zeigt. Über 60% der Benutzer stuften ihre eigene Identität als sensibel ein. Auf die Frage welche Daten an den „Arbeitgeber“ übermittelt werden dürften, antworteten die Versuchsteilnehmer bei 98% der Daten, dass sie nicht übermittelt werden dürften.

Weiterhin wurde untersucht, ob das Sicherheitsbedürfnis und die Sicherheitswahrnehmung in Abhängigkeit zur gewählten Domäne stehen. Dazu gab es im Fragebogen Fragen zum Umgang mit Geld. Da die in der Presse verbreiteten Bedrohungen meist auf Geld abzielen, sind Benutzer in dieser Domäne sensibilisiert. Die Abbildung 4.7 zeigt die Ergebnisse der Frage 9. Sie zeigt, dass sich Benutzer in unterschiedlichen Domänen verschieden bedroht fühlen.

Nur 9 Teilnehmer fragten während des Versuches, welche Daten durch die Sensoren gemessen würden. Allerdings gaben auch von diesen 9 einige genug Daten ein, um sensible Daten mit ihrer Identität zu verknüpfen. Diese 9 Versuchsteilnehmer hatten einen vagen Verdacht, dass ihre Daten sensibel seien. Sie handelten aber nicht alle entsprechend.

27,5% der Teilnehmer fragten direkt im Anschluss an den Versuch was mit den Daten geschieht und ob sie der Öffentlichkeit zugänglich gemacht würden. Allerdings fragten diese Teilnehmer nicht nach, welche Daten das System genau erhoben hatte.

Die zu Beginn des Experimentes aufgestellten Fragestellungen lassen sich aus

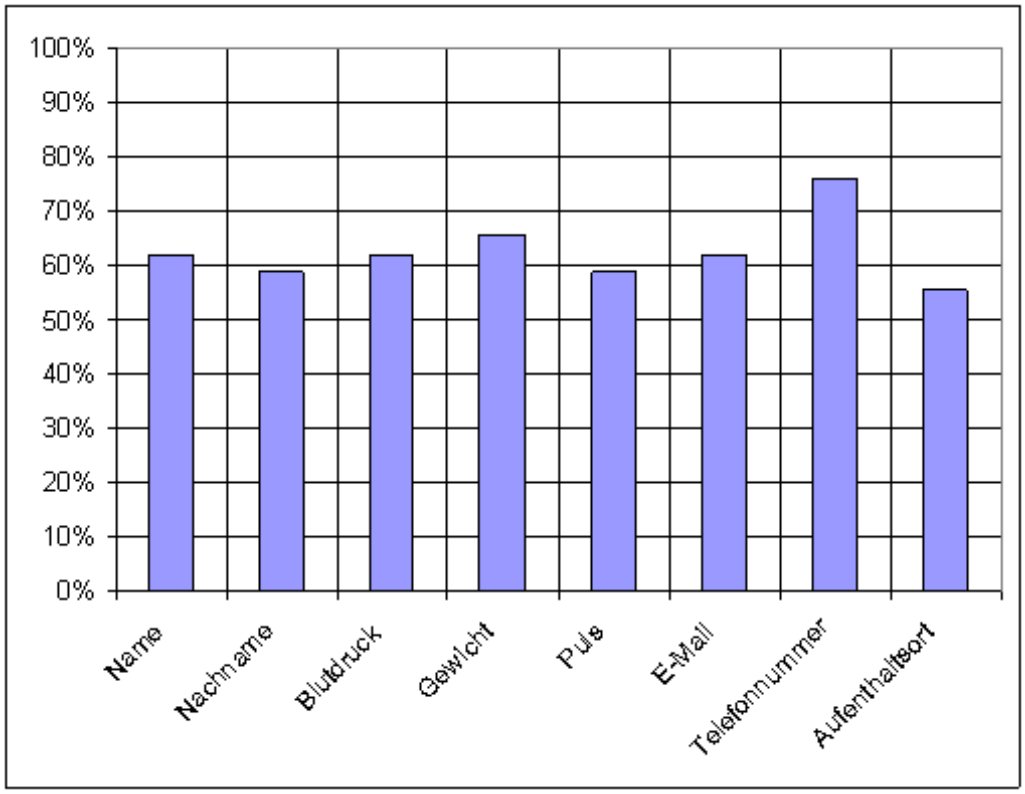


Abb. 4.6: Geschätzte Sensibilität der Daten

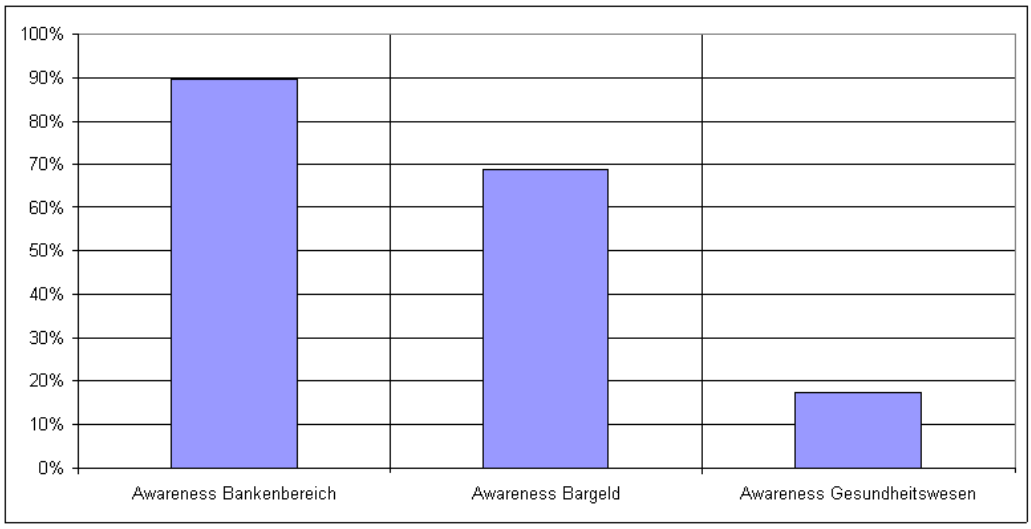


Abb. 4.7: Awareness in verschiedenen Domänen

den gemachten Ergebnissen wie folgt beantworten:

`Antwort auf Frage:1` Die Benutzer erkannten unbewusst, dass sie mit sensiblen Daten umgingen. Die Daten, die sie eingaben, klassifizierten sie als sensitiv. Allerdings mussten sie aktiv nachdenken, um die Problematik zu erkennen.

`Antwort auf Frage:2` Die Benutzer schätzten alle Daten als sensitiv ein. An ihren „Arbeitgeber“ wollten sie keine der eingegebenen Daten weitergeben.

`Antwort auf Frage:3` Der Healthcare Bereich war positiv besetzt. Daten im Bankenbereich wurden dagegen als kritisch betrachtet.

`Antwort auf Frage:4` Durch bloße Hinweise ließ sich das Bewusstsein nicht steigern oder entwickeln.

Im Anschluss an das Experiment wurde mit allen Teilnehmern ein kurzes Gespräch geführt, bei dem 100% angaben, dass sie die Daten des Experiments größtenteils für sensibel hielten. Die hohe Quote ist darauf zurückzuführen, dass im Gespräch auf die potentiellen Bedrohungen hingewiesen wurde. Alle Teilnehmer forderten darauf hin, dass ihre Daten nicht weitergegeben werden sollten.

4.1.3 Zusammenfassung und Wertung der Hypothesen

Neben einem höheren Komfort führt die Eigenschaft ambient zu sein bei Systemen und Diensten auch zu neuen Sicherheitsbedrohungen. Einige der neuen Bedrohungen werden durch die veränderte Interaktion von Benutzern mit Systemen hervorgerufen. Früher interagierten Benutzer explizit mit Systemen. Sie gaben bewusst Daten in Systeme ein und waren sich der Bedrohungen der jeweiligen Daten bewusst. Bei ambienten Systemen interagieren sie nun häufig implizit. An vielen Stellen werden die Daten unbewusst eingegeben oder allein durch das Verhaltens des Benutzers erhoben und gesammelt. Benutzer nehmen diese ambienten Systeme kaum wahr und sind sich bei der Benutzung der Systeme nicht unbedingt der möglichen Gefahren bewusst, die die Benutzung betreffen. Zum Beispiel ist die Erstellung von Käuferprofilen und Bewegungen ausgehend von der Sammlung von RFID Signalen denkbar.

Daher muss von Hersteller- und Betreiberseite nicht nur dafür gesorgt werden, dass die Systeme die Daten „sicher“ behandeln, sondern der Interaktion mit den Benutzern muss besondere Beachtung geschenkt werden.

Eine weitere Bedrohung bei ambienten Systemen besteht darin, dass sie in vielen neuen Domänen eingesetzt werden. Während Daten im Bankenbereich kaum weiter gegeben werden, werden persönliche Daten im Healthcare Bereich oder anderen Domänen schnell weiter gegeben. Zum einen, weil Benutzer sich keiner Bedrohungen bewusst sind, zum anderen antworteten die Befragten, dass die Domäne Healthcare positiv besetzt ist. So erfolgte die Dateneingabe ins System auch dann, wenn die Benutzer im Nachhinein fragten, ob die Daten nicht weiter verbreitet würden. Sie waren sich einiger Bedrohungen bewusst, negierten diese aber. Der Versuch zeigte, dass es nicht ausreicht auf die Sensibilität der Daten hinzuweisen. Wenn Benutzer gegenüber Programmen positiv eingestellt sind, geben sie Daten ein, ohne über die Gefährdung nachzudenken.

Die beiden Hypothesen, dass *sich Benutzer der Gefahren bei ambienten Systemen zu wenig oder nicht bewusst sind, um auf diese reagieren zu können und dadurch Sicherheitsbedrohungen verursachen*, und dass sie sich *über das gleiche Risiko in verschiedenen Domänen unterschiedlich bewusst sind*, wurden durch das Experiment belegt.

Eine Möglichkeiten zur Erhöhung der IT-Sicherheit besteht daher darin, Benutzer für die Problematik von Daten bei allen IT-Systemen zu sensibilisieren. Bei dem Experiment zeigte sich, dass durch Hinweise im System dies nur ungenügend geschieht. Somit muss auch eine Diskussion in der Öffentlichkeit zur Sensibilisierung dieser Thematik beitragen. Weiterhin müssen Entwickler und Betreiber von Systemen dafür sorgen, möglichst wenige personengebundene Daten im System zu verwenden. Eine Möglichkeit wäre es, eine Entkopplung der Daten von der Identität des Benutzers anzustreben, indem virtuelle Personen als Platzhalter für reale Personen verwendet werden.

Zusammenfassend wurden durch das Experiment die folgenden Ergebnisse festgestellt:

- Benutzer geben sensible Daten ein, weil sie häufig mit keiner Bedrohung rechnen. Den Benutzern ist die Sensibilität ihrer Daten teilweise unklar.
- Bedrohungen werden erst wahrgenommen, wenn man aktiv über die Daten nachdenkt.
- Es reicht als Prävention nicht aus, auf die Sensibilität der Daten hinzuweisen.

- Unterschiedliche Domänen werden unterschiedlich wahrgenommen.
- Durch die Häufigkeit an Dateneingaben im täglichen Leben sind viele Benutzer in vielen Bereichen so konditioniert, dass sie sensible Daten einfach eingeben.

Zur Erzielung von IT-Sicherheit dürfen also nicht nur technische Maßnahmen ersonnen werden, sondern der Umgang der Daten durch den Benutzer muss ebenfalls analysiert werden. Es muss Awareness geschaffen werden bei den Benutzern und Entwicklern. Awareness bei den Benutzern, dass sie mit sensiblen Daten umgehen und dass zahlreiche Bedrohungen existieren. Awareness bei den Entwicklern, dass Benutzer hinsichtlich der Bedrohungen sensibilisiert werden müssen, und dass zur Erreichung von Awareness nicht einfache Hinweise ausreichen, sondern ein komplexes Problem gelöst werden muss.

Im diesem Experiment wurde das Verhalten der Benutzer untersucht, durch dass sie unbewusst Bedrohungen auslösen können. In dem nächsten Experiment wird untersucht, wie Benutzer sich verhalten, wenn sie in IT-Systemen explizit auf gerade eintretende Bedrohungen hingewiesen werden. Im Gegensatz zu dem soeben vorgestellten Experiment wird nun ein Konzept vorgestellt, bei dem Benutzer bei der Benutzung mobiler Endgeräte permanent verschiedenen Bedrohungen ausgesetzt und auf diese hingewiesen werden.

4.2 Das Verhalten von Benutzern bei eintretenden Bedrohungen

Nachdem im letzten Experiment untersucht wurde, wie Benutzer mit ihren Daten umgehen, und ob sie sich deren Bedrohungen bewusst sind, wird in diesem Kapitel untersucht, wie Benutzer sich verhalten, wenn Bedrohungen eintreten.

Der im Kapitel 1 beschriebene Trend bei der Veränderung der Systeme (kleiner, unbemerkter und mobiler) bringt die Notwendigkeit, dass sich Benutzer mit Bedrohungen und Bedrohungshinweisen auseinander setzen und geeignet auf sie reagieren. Ein Beispiel für diesen Trend stellen Telefone dar. Vor 30 Jahren waren nahezu sämtliche Telefone stationär und nur wenige Benutzer hatten die Gelegenheit drahtlose Systeme zu verwenden. Heute haben dagegen sehr viele Benutzer drahtlose Mobiltelefone. Mobiltelefone stellen somit ein Beispiel für den Trend zu allgegenwärtigen IT-Systemen dar.

Die Überführung von Prozessen stationärer IT-Systeme auf mobile Endgeräte führt zu neuen Bedrohungen. Neue Schutzkonzepte müssen die fest installierten Schutzsysteme von stationären Systemen ergänzen oder ersetzen. So können zum Beispiel fest stationierte Arbeitsplatz-Systeme durch Firewalls oder Intrusion-Detection-Systeme vor Angreifern aus dem Web geschützt werden. Dieser Schutz kann aber in dieser Form nicht mehr aufrecht erhalten werden, wenn die Arbeitsplatzrechner durch mobile Endgeräte ersetzt werden. Mobile Endgeräte werden durch die Benutzer an verschiedenen Standorten eingesetzt und erhalten so Zugang zu verschiedenen Netzen. Diese Netze sind nicht alle gleich abgesichert und bieten nicht alle den gleichen Zugangsschutz (als Beispiel diene hier der unterschiedliche Zugang zum WWW über ein Heimnetz oder über das geschützte Firmennetz).

Durch die Veränderung des Schutzes der Systeme ändert sich auch die Verantwortung des Benutzers. In Firmennetzen teilt sich der Benutzer die Verantwortung mit Administratoren. Im heimischen Netz hat er dagegen die alleinige Verantwortung Bedrohungen zu minimieren oder zu beseitigen. Aus diesen Gründen steigt die Verantwortung des Benutzers für ein sicheres System bei Verwendung mobiler Endgeräte. Auch die Verantwortung der Hersteller steigt. Sie müssen Sicherheitsfunktionalitäten bereit stellen, die nicht nur durch Experten bedient werden können. Bei der klassischen Firmen-Firewall gibt es meist Experten (z.B. die Systemadministratoren der Firma), die für eine korrekte Installation, Konfiguration und den Betrieb sorgen. Bei

mobilen Endgeräten für eine breite Nutzerschicht (z.B. Mobiltelefone oder Laptops) müssen unterschiedlichste Benutzer in der Lage sein Bedrohungen zu erkennen, sich bedrohungsminimierend zu verhalten und die Sicherheitsfunktionalitäten korrekt einzustellen.

Um die Erhaltung des Sicherheitsniveaus durch verschiedene Benutzer zu gewährleisten, muss die Bedienung durch die Hersteller auf eine breitere inhomogene Benutzerschicht zugeschnitten werden. Sie müssen die folgenden Fragen klären, um ihre Produkte gemäß der Ergebnisse optimieren zu können.

- Wie verhalten sich Benutzer in Bedrohungssituationen?
- Welche unterschiedlichen Benutzergruppen lassen sich separieren?
- Wie können die Benutzergruppen optimal unterstützt werden, um ein Mindestmaß an Bedrohungen durch Benutzer zu erhalten?

Die Beantwortung dieser Fragen ist eine sehr komplexe Herausforderung. Untersuchungen zeigen, dass einige Benutzer Bedrohungen realisieren und Gegenmaßnahmen anwenden und andere dies nicht tun [41], [129], [54].

Diese Voraussagen über das Verhalten von Benutzern in sicherheitsrelevanten Situationen existieren nur in einigen wenigen Bereichen. So wird meist untersucht, wie Personen reagieren, wenn sie mit Geld interagieren oder wenn sie sich eines Angriffes bewusst sind. Wie die Untersuchung 4.1 zeigte, handeln Benutzer jedoch im Alltag in vielen Domänen ohne ihren Fokus auf die IT-Sicherheit zu legen. Untersuchungen über ihr Verhalten, wenn sie die Bedrohung nicht erkennen oder sich der Bedrohung nicht bewusst sind, fehlen. Die Schwierigkeit für aussagekräftige Evaluationen besteht dabei darin, dass die Benutzer sich der Untersuchungssituation nicht bewusst sein dürfen, da sie sich sonst anders verhalten, als wenn sie im Alltag Entscheidungen fällen (vergl. [107]). Daher wurde die folgende Idee entwickelt, die das Verhalten der Benutzer in Bezug auf IT-Sicherheit untersucht, während der Fokus der Teilnehmer auf andere Domänen gerichtet ist.

4.2.1 Die Idee der „unfokussierten“ Evaluation des Benutzerverhaltens in sicherheitsrelevanten Situationen

Wenn Benutzer nach der Wichtigkeit von IT-Sicherheit befragt werden, geben sie meist an, dass für sie die IT-Sicherheit sehr wichtig ist (vergleiche Experiment in 4.1). Ob sich Benutzer auch entsprechend verhalten, kann nur untersucht werden, wenn sich die Teilnehmer der Untersuchung aus Blickwinkel der IT-Sicherheit nicht bewusst sind. Bei Untersuchungen sollten die Teilnehmer daher auch mit einem Diskursbereich konfrontiert werden, der von ihnen nicht sofort als „sicherheitsrelevant“ eingestuft wird (vergl. [107]). Auch eine spielerische Fortbildung der Benutzer kann sicherheitsrelevant sein, da einige Bedrohungsszenarien denkbar sind. So werden Wissenslücken der Benutzer offenbart, und sie würden durch diese Lücken für einige Tätigkeiten bei potentiellen Arbeitgebern nicht in Frage kommen. Um das Verhalten der Benutzer in diesen Situationen zu untersuchen, um Gegenmaßnahmen zu entwickeln, wurde die folgende Idee entwickelt.

Das „alltägliche“ Verhalten der Benutzer in Bezug auf IT-Sicherheit muss in Situationen untersucht werden, wo sie sich diesem Untersuchungsfokus nicht bewusst sind. Eine Untersuchung zur IT-Sicherheit sollte eine Komponente beinhalten, die den Fokus der Teilnehmer auf eine andere Domäne lenkt.

Auf der Idee basierende Hypothesen

Auf der geschilderten Idee basieren die folgenden Hypothesen, die in diesem Abschnitt untersucht werden sollen.

Wenn Benutzer gefragt werden, hat für sie die IT-Sicherheit einen sehr hohen Stellenwert, sie verhalten sich aber nicht dementsprechend. Ihr Verhalten weist eine geringere Wertung der IT-Sicherheit auf. Außerdem verhalten sich Benutzer in Bezug auf die IT-Sicherheit anders, wenn ihr Fokus auf einer anderen Aufgabenerledigung liegt. Sie sind so konditioniert, dass sie die IT-Sicherheit der Aufgabenerledigung unterordnen.

Zur Überprüfung der Hypothese entwickeltes Konzept

Benutzer interagieren mit einem System und erhaltene eine Aufgabe, die ihren Fokus auf andere Bereiche als die IT-Sicherheit lenkt. Während der Aufgabenerledigung werden Bedrohungen der IT-Sicherheit ausgelöst. Diese erschweren aber verhindern nicht die Aufgabenerledigung und führen zu einer möglichen Systembeeinträchtigung. Das Verhalten der Benutzer wird dahingehend untersucht, wie sie mit Bedrohungen umgehen.

4.2.2 Praktische Evaluation des aufgestellten Konzeptes

Um diese Hypothesen zu adressieren, wurde im Rahmen dieser Dissertation das im Folgenden vorgestellte Werkzeug MEGSA (Mobile, Education, Gaming, Security Application) entwickelt und in verschiedenen Lehrveranstaltungen an der Technischen Universität Berlin eingesetzt und evaluiert. MEGSA stellt eine Plattform mit Wissensspielen für mobile Endgeräte bereit. Damit können Benutzer sich durch „mobiles Spielen“ an unterschiedlichen Orten und zu beliebigen Zeiten fortbilden. Der mentale Fokus der Benutzer wird dabei auf die Domäne Fortbildung gelenkt. Außerdem beinhaltet MEGSA für Evaluatoren Komponenten zur Untersuchung des unterschiedlichen Sicherheitsverhalten und Bewusstseins der Benutzer bei Benutzung mobiler Endgeräte.

Das implementierte MEGSA System

Bei der Entwicklung von MEGSA wurden die folgenden Ziele verfolgt:

- Ziel 1: Verbesserung des Lernverhaltens von Lernenden.
- Ziel 2: Untersuchung von Benutzerverhalten in Bezug auf IT-Sicherheit, ohne dass sich Benutzer dieser Untersuchung bewusst sind.
- Ziel 3: Ermittlung von Aspekten zur Gruppierung verschiedener Benutzer durch ihr Verhalten in Bezug auf IT-Sicherheit.

Für den Benutzer sollte dabei nur das Ziel 1: *Verbesserung des Lernverhaltens von Lernenden* ersichtlich sein. Mit Hilfe verschiedener Spiele konnten sie z.B. auf ihrem Mobiltelefon ihr Wissen in verschiedenen Anwendungsdomänen erweitern. Ohne die Erreichung dieses Zieles wäre die Umsetzung

der anderen beiden Ziele nicht möglich gewesen. So richteten die Teilnehmer ihren Fokus auf ihre Weiterbildung und dachten nicht darüber nach, ob sie sich in einer bedrohten Umgebung befänden. Ergebnisse zu Untersuchungen, wie das System Lernen von Studenten fördert, sind in [73] beschrieben und werden hier nicht weiter erläutert.

Abbildung 4.8 zeigt die unterschiedlichen Bestandteile und Aufgaben des umgesetzten MEGSA Systems.

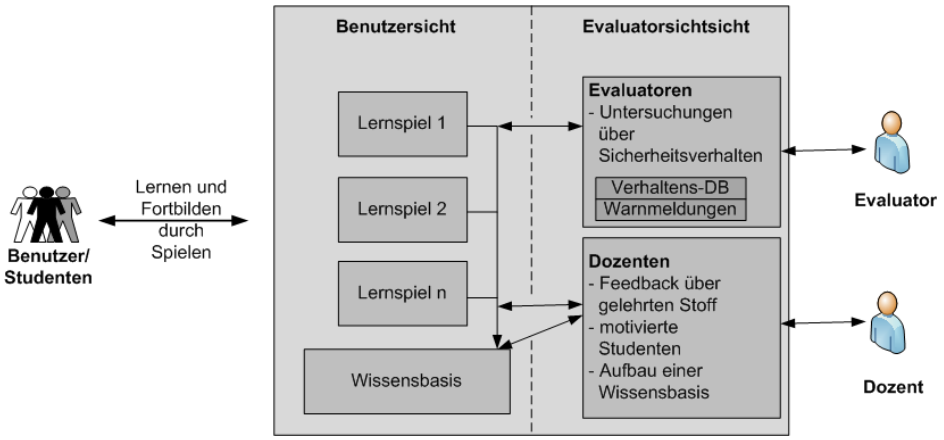


Abb. 4.8: Bestandteile von MEGSA

Während die Teilnehmer ein „Spiel“ spielen und sich fortbilden, werden sie durch den Evaluator unbewusst verschiedenen virtuellen Bedrohungen ausgesetzt. Verschiedene Warn- oder Fehlermeldungen erscheinen und müssen bearbeitet werden. Das Verhalten der Benutzer in diesen Situationen wird in einer Datenbank mitprotokolliert und kann ausgewertet werden. Der Fokus der Teilnehmer liegt auf dem Erreichen eines hohen Highscore. Sie bearbeiten die Meldungen nur unbewusst. Somit beeinflussen diese Meldungen unbewusst das Verhalten der Benutzer. Eine Analyse dieses Verhaltens gibt dann Aufschluss darüber, wie sich Benutzer verhalten, wenn sie sich der Bedrohung nicht bewusst sind. Die Erkenntnisse können anschließend dazu benutzt werden, um Fehler- und Warnmeldungen des Systems dahingehend zu ändern, dass das Fehlverhalten der Benutzer minimiert wird.

Das durchgeführte Experiment

In einem Raum befanden sich jeweils ein Versuchsteilnehmer und ein Evaluator. Zu Beginn des Versuches händigte der Evaluator dem Versuchsteilnehmer einen Beschreibung des Versuches und der Aufgabenstellung aus. Zugleich erklärte er dem Teilnehmer mündlich, dass er ein Programm zur Lernverbesserung im Hochschulbereich unter Usability-Aspekten testen sollte.

Die Aufgabenbeschreibung enthielt die eigentliche Aufgabe und zusätzlich noch einen Fragebogen zur Bewertung des Testprogramms und zu Angaben über den Teilnehmer. Die Aufgabenbeschreibung (inklusive des Fragebogens) ist im Anhang A vorhanden. Der Teilnehmer las nun die Aufgabenstellung und konnte zu dieser Fragen an den Evaluator stellen. Nachdem der Teilnehmer die Aufgabe verstanden hatte, übergab der Evaluator ihm ein mobiles Endgerät. Auf diesem war das zu evaluierende Programm zur Fortbildung durch Lernen installiert. Die Abbildung 4.9 zeigt das Konzept und den Spielablauf des ersten umgesetzten Spieles. Weitere Ergebnisse und Details MEGSA aus „Lernverbesserungssicht“ sind in [73] beschrieben.

Der Teilnehmer löste nun seine Aufgabe mit dem mobilen Endgerät. Während er seine Aufgabe löste erschienen zufällig einige Fehlermeldungen (siehe Anhang B) auf dem Display des Endgerätes und störten die Erledigung der Aufgabe. MEGSA protokollierte das Verhalten der Teilnehmer mit diesen Meldungen in einer Datenbank zur späteren Auswertung. Nachdem die Teilnehmer ihre Aufgabe erledigt hatten, füllten sie den Fragebogen aus. Während des gesamten Versuches konnten die Versuchsteilnehmer an den Evaluator Fragen stellen. Falls sich die Frage dabei auf eine der Fehlermeldungen bezog, antwortete der Evaluator, dass er das Programm nicht programmiert hätte und nichts über die technischen Hintergründe wüsste.

Dieser gleich bleibende Ablauf der Versuche mit MEGSA ist in Abbildung 4.10 zur besseren Veranschaulichung bildlich dargestellt.

Um unterschiedliche Aspekte zu untersuchen, wurden verschiedene Experimente mit MEGSA durchgeführt, die jeweils einzelne Experiment-Hypothesen überprüfen sollten. Die Tabelle 4.4 zeigt die verschiedenen Experimente und die variierten Aspekte. Alle Experimente dauerten 30 Minuten mit Ausnahme des Experimentes Nr. 2. Die weiteren Variationen werden nun detaillierter beschrieben.

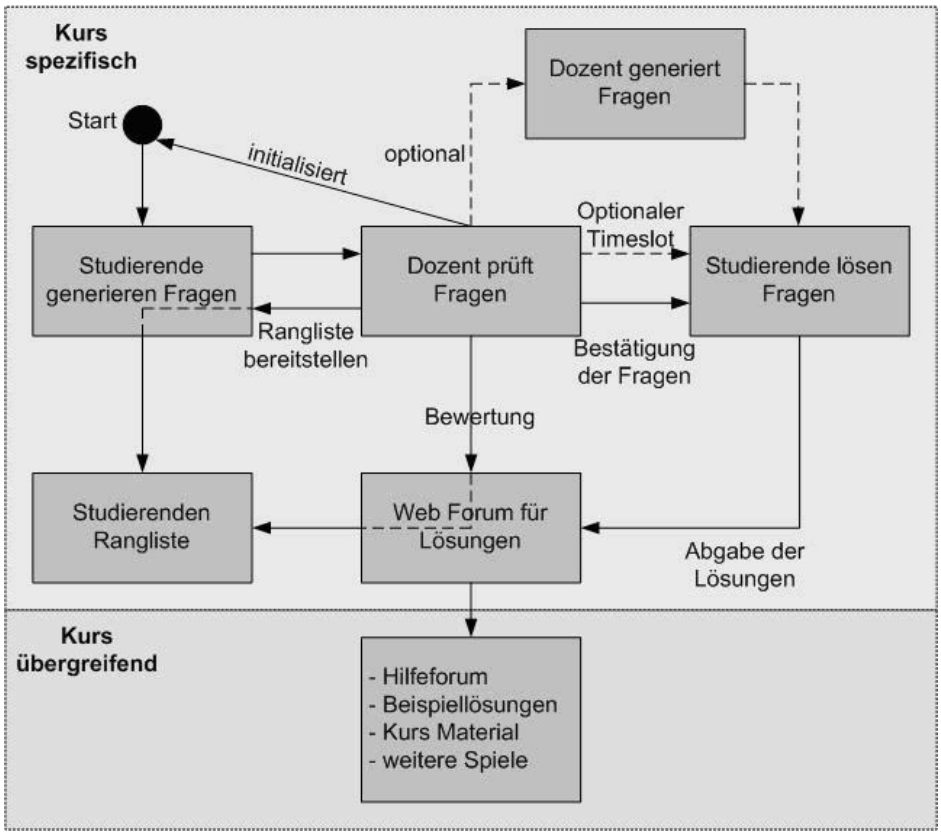


Abb. 4.9: Konzept des ersten in MEGSA implementierten Lernspieles

Experiment	Untersuchungsfokus	variierte Aspekte
Experiment 1	Akzeptanz	keine
Experiment 2	Zeitdruck	Zeit für Lösen der Aufgabe wird variiert
Experiment 3	Häufigkeit	Häufigkeit der Meldungen wird variiert
Experiment 4	visuelle Aspekte	Aussehen der Meldungen wird variiert
Experiment 5	Diskursbereich	Teilnehmer kann beliebigen Diskursbereich wählen
Experiment 6	Einsatzumgebung	Teilnehmer kann System an beliebigem Ort anwenden

Tab. 4.4: Unterschiedliche Experimente mit MEGSA

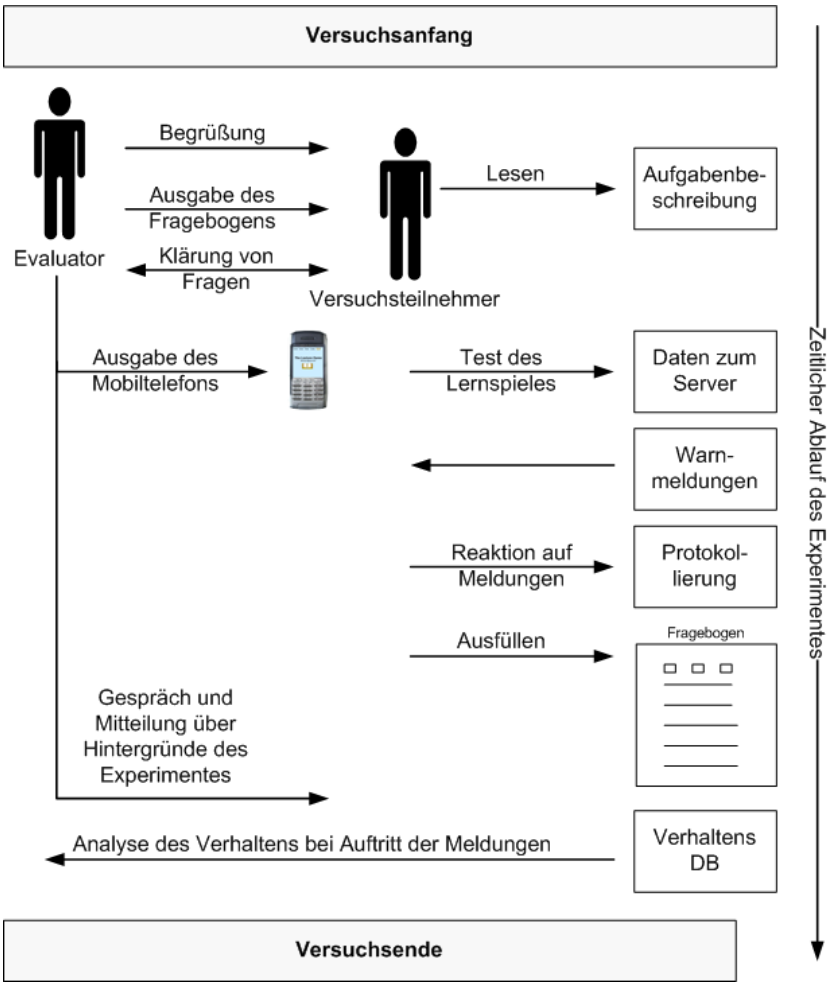


Abb. 4.10: Ablauf der Experimente mit MEGSA

Die einzelnen unterschiedlichen Experimente

MEGSA Experiment 1: Im ersten Experiment sollte untersucht werden, wie die Akzeptanz der Anwendung durch die Benutzer ist. Nur wenn die Benutzer die Anwendung akzeptieren, kann ihr Verhalten in Bezug auf die Sicherheit in Alltagssituationen durch MEGSA vorhergesagt werden, da sie freiwillig nur Systeme verwenden, die sie akzeptieren.

Bei diesem Experiment testet jeder einzelne Versuchsteilnehmer das System unabhängig und selbstständig und kann jederzeit Rückfragen an den anwesenden Evaluator stellen. Per Zufallsgenerator werden die Fehlermeldungen ausgewählt und in einem zufälligen zeitlichen Abstand (im Durchschnitt alle 5 Minuten) eingeblendet.

Die zu überprüfende Experiment-Hypothese besteht darin, dass das MEGSA System von den Versuchsteilnehmern akzeptiert wird.

MEGSA Experiment 2: In diesem Experiment soll untersucht werden, welchen Einfluss Zeitdruck auf das Verhalten der Teilnehmer hat. Aus diesem Grunde werden die Versuchsteilnehmer dieses Experimentes in drei Gruppen aufgeteilt. Die erste Gruppe hat nur 15 Minuten Zeit die Aufgabe zu lösen. Der zweiten Gruppen stehen dafür 30 Minuten und der dritten Gruppe sogar 45 Minuten zur Verfügung.

Die zu überprüfende Experiment-Hypothese besteht darin, dass Zeitdruck Benutzer dazu verleitet weniger auf Warnhinweise zu achten und somit zu einem erhöhtem Bedrohungspotential führt.

MEGSA Experiment 3: In diesem Experiment wird die Häufigkeit der Warnmeldungen variiert. Die Versuchsteilnehmer werden in zwei Gruppen aufgeteilt. Eine Teilnehmergruppe erhält bei der Aufgabenerledigung 5 Warnmeldungen (im Durchschnitt alle sieben Minuten jeweils eine). Eine zweite Benutzergruppe erhält dagegen ca. alle 3 Minuten eine Warnmeldung (insgesamt 10 Warnmeldungen.). Um eine bessere Vergleichbarkeit der Gruppen zu gewährleisten, sind die ersten fünf Warnmeldungen in beiden Gruppen identisch. Die zweiten 5 Warnmeldungen der zweiten Gruppe sind innerhalb der Gruppe wieder identisch.

Es besteht die Experiment-Hypothese, dass Benutzer bei einer Zunahme an Warnhinweisen diese ignorieren.

MEGSA Experiment 4: In diesem Experiment wird das Aussehen der Warnhinweise verändert. Damit soll die Experiment-Hypothese untersucht werden, dass Benutzer auf deutlich erkennbare Warnhinweise anders reagieren als auf nicht hervorgehobene Warnhinweise.

Die Benutzer bekommen dazu alle während des Experimentes die gleichen fünf Warnmeldungen. Zwei dieser Warnmeldungen haben aber ein geändertes Design. Die Abbildung 4.11 zeigt das Aussehen der geänderten Warnmeldungen.

Abb. 4.11: Unterschiedlich aussehende Warnmeldungen

MEGSA Experiment 5: In diesem Experiment wird die Aufgabe für die Benutzer leicht verändert. Bei dieser Aufgabe müssen sie nicht mehr Fragen zu einem bestimmten Diskursbereich eingeben, sondern sie können beliebige Fragen eingeben und lösen.

Der Grundgedanke dieses Experimentes besteht darin, dass sich Benutzer in Domänen, wo sie sich besonders gut auskennen, anders verhalten als in Domänen, an denen sie teilnehmen müssen. Durch die eigene Wahl einer Domäne für die Teilnahme bei diesem Experiment ist zu erwarten, dass Domänen gewählt werden, in denen sich die Teilnehmer besonders gut auskennen.

Zu evaluieren ist die Experiment-Hypothese, dass Benutzer in dieser Situation mehr Aufmerksamkeit auf Warnmeldungen richten können.

MEGSA Experiment 6: Mit diesem Experiment soll untersucht werden, welchen Einfluss die Einsatzumgebung auf den Aufmerksamkeitsfokus der Teilnehmer hat. Aus diesem Grunde verwenden die Teilnehmer dieses Experimentes das System in ihrer heimischen Umgebung. Es soll überprüft werden, ob die Teilnehmer in einer für sie angenehmen Umgebung den Fehlermeldungen mehr Aufmerksamkeit schenken.

4.2.3 Evaluation und Ergebnisse

An dem Versuch mit MEGSA nahmen insgesamt 187 Versuchsteilnehmer teil. Jeder Teilnehmer nahm genau an einem Experiment teil. Alle erhielten dabei die Aufgabe, die reale Umsetzung des oben beschriebenen Spieles in Bezug auf die Usability des Systems zu untersuchen. Um die Usability des Systems zu beurteilen, bekamen sie dazu alle die gleiche Aufgabe gestellt. Die Aufgabe lautete, dass sie jeweils neue Fragen eingeben und beliebige Frage im System lösen sollten. Als Diskursbereich für die Experimente 1-4 und 6 wurde der Bereich Grundlagen der Informatik gewählt. Alle Versuchsteilnehmer erhielten das gleiche mobile Endgerät. Die Tabelle 4.5 zeigt die unterschiedliche Anzahl an Teilnehmern bei den einzelnen Versuchen.

Experiment	**1**	**2**	**3**	**4**	**5**	**6**	**Gesamt**
Teilnehmer	66	36	27	17	19	22	**187**
Meldungen	494	217	197	103	116	128	**1255**

Tab. 4.5: Grunddaten der Testphasen

Ergebnisse der einzelnen Experimente

MEGSA Experiment 1
Am ersten Experiment nahmen 66 Versuchsteilnehmer teil. Die Tabellen B.1 und B.2 im Anhang B zeigen einige ihrer Stammdaten.

Dieses Experiment wurde als Vorexperiment zu den anderen Experimenten durchgeführt, da ohne Akzeptanz der Lernanwendung von MEGSA die weiteren Experimente keine Ergebnisse bezüglich des Einsatzes von Systemen in Alltagssituationen gehabt hätten.

Ausgewertet wurde die Frage D.8 des Fragebogens. Von den 66 Teilnehmern antworteten 56, dass sie das System als spannend oder sinnvoll ansehen. Somit würden es in der Praxis vermutlich 84% der Teilnehmer benutzen. Nachdem die Vorevaluation einen so hohen Wert erbracht hatte, wurden die Experimente 2-6 durchgeführt. Am Ende wurde dann die Zustimmung der Teilnehmer aller Experimente für das System erneut berechnet.

Die Akzeptanz aller Teilnehmer für das System war sehr hoch. Von den insgesamt 187 Teilnehmern beschrieben 163 das System (unter dem Aspekt des Einsatzes zum besseren Lernen in der Hochschullehre) als sinnvoll und/oder spannend. Dies entspricht ca. 87% der Teilnehmer. Sowohl bei der direkten Zielgruppe (Studenten) mit 89,78% (123 der 137 studentischen Teilnehmer) als auch dem restlichen Teil der Versuchsteilnehmer mit 80% (40 der 50 Teilnehmer) gab es eine deutlich positive Resonanz auf das System. Die Abbildung 4.12 zeigt die genauen Ergebnisse der Frage D.8 des Fragebogens.

Eine Auswertung hinsichtlich des Studienfaches zeigte, dass Studierende der Informatik das System meist als sinnvoll aber nicht als spannend bezeichneten. Studierende anderer Fachrichtungen klassifizierten dagegen das System sowohl als spannend als auch sinnvoll. Dies ist damit zu erklären, dass Informatiker während des gesamten Studiums mit Informationssystemen in Berührung kommen. Aus diesem Grunde sehen sie in einem solchen System bei einem Experiment von 30-45 Minuten noch keine spannende Interaktion.

Fast alle Studierenden wollten das System in der Lehrveranstaltung benutzen. Bei den Studierenden der Informatik gaben 97% bei Frage D.5 die Note 1 oder 2 an. Bei den übrigen Studierenden waren es noch 93%.

MEGSA Experiment 2

An diesem Experiment nahmen 36 Versuchsteilnehmer teil. 13 Teilnehmer bekamen für die Erledigung der Aufgabe 15 Minuten Zeit, 10 Teilnehmer erhielten 30 Minuten und 13 Teilnehmer erhielten wiederum 45 Minuten Zeit.

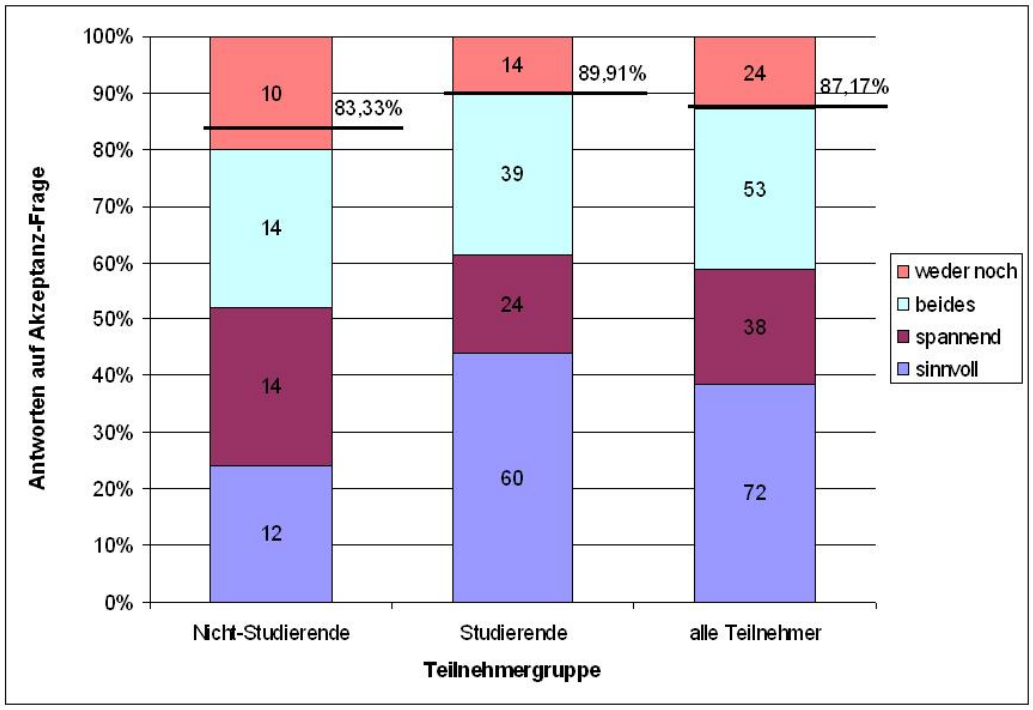


Abb. 4.12: Akzeptanz von MEGSA über alle Experimente berechnet

Jeder Teilnehmer konnte sein eigenes Ergebnis zu den Ergebnissen aller Teilnehmer (inklusive Experiment 1) in Relation setzen, da der Highscore und der erzielte Rang permanent eingeblendet wurden. Allerdings wussten die Teilnehmer nicht, dass andere Teilnehmer ein unterschiedliches Zeitkontingent hatten. Dieses Experiment zeigte, dass eine Verkürzung des Zeitkontingentes sich negativ auf das Sicherheitsbewusstsein der Teilnehmer auswirkte. Je weniger Zeit die Benutzer hatten, desto weniger Zeit verwendeten sie auf das Lesen der Warnhinweise. Der Zeitdruck führte dazu, dass sie die Warnmeldungen schneller „weggeklickten“ als die Teilnehmer, die mehr Zeit hatten. Im Durchschnitt klickten die Teilnehmer mit 15 Minuten Bearbeitungszeit die Warnmeldungen bereits nach 2,87 Sekunden weg. Die Teilnehmer, die 30 Minuten Zeit hatten, verwandten für die Warnmeldungen dagegen durchschnittlich 3,49 Sekunden und die Teilnehmer mit 45 Minuten Bearbeitungszeit sogar 3,65 Sekunden. Diese Ergebnisse sind in Abbildung 4.13 grafisch dargestellt.

Ein weiteres Indiz für die Beeinträchtigung des Sicherheitsbewußtseins durch den Zeitdruck ist die Auswahl der Optionen bei den Warnmeldungen. In 88,24% der aufgetretenen Meldungen wählten die 13 Teilnehmer, die 15 Mi-

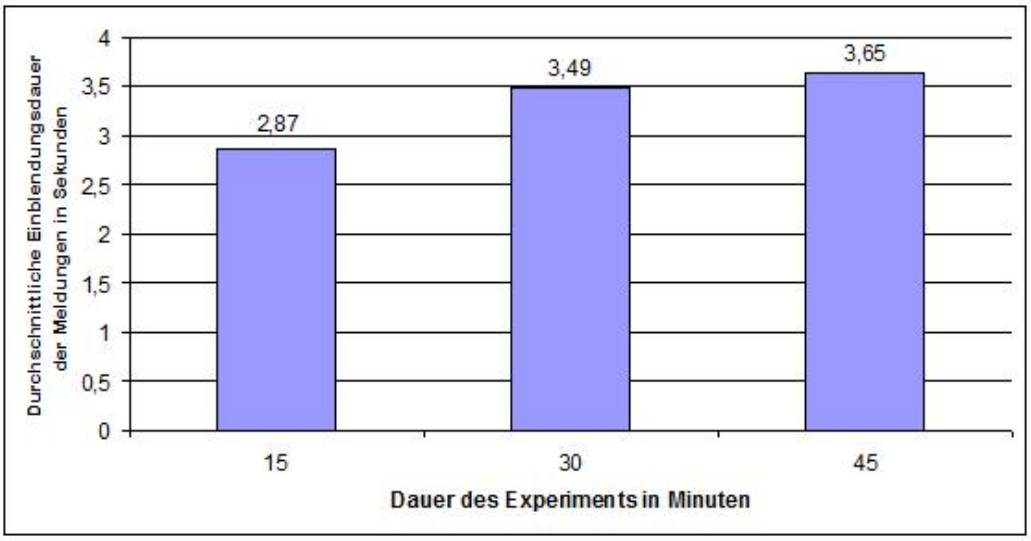


Abb. 4.13: Durchschnittliche Verweildauer der Meldungen in Abhängigkeit der Zeitspanne zur Erledigung der Aufgabe

nuten Zeit zur Aufgabenerledigung hatten, die „Continue“ Möglichkeit der Warnmeldung (bei 30 von 34 Meldungen wurde diese Option gewählt). Diese Option stand für das niedrigste Sicherheitsbewußtsein.

MEGSA Experiment 3

An diesem Experiment nahmen 27 Teilnehmer teil. 13 von ihnen erhielten im Durchschnitt alle sieben Minuten eine Warnmeldung. Die zweite Gruppe bestand aus 14 Teilnehmern. In dieser Gruppe wurden die Meldungen im Durchschnitt alle drei Minuten eingeblendet. Zusätzlich kann für die Berechnungen aus den Teilnehmern bei Experiment 1 [3] eine dritte Gruppe gebildet werden, die die Meldungen im Durchschnitt alle fünf Minuten erhielt.

In diesem Experiment konnten zwei Ergebnisse festgestellt werden. Zum einen änderte sich die Anzahl der Teilnehmer, die sich beim Evaluator erkundigten, ob die Warnmeldungen zum Versuch gehörten (Abbildung 4.14).

Die Abbildung zeigt, dass sich deutlich mehr Versuchsteilnehmer erkundigten, ob die Warnmeldungen zum Versuch gehörten, als die Auftrittshäufigkeit im Durchschnitt bei drei Minuten lag. In diesem Experiment erkundigten sich elf von vierzehn Teilnehmern nach den Meldungen (dies entspricht etwa 78,57%). Im Gegensatz dazu erkundigten sich nur 15,38% (2 von 13) Teilnehmern nach den Meldungen als sie nur etwa alle sieben Minuten erschienen.

[3] Die Versuchsbedingungen waren hier nahezu identisch.

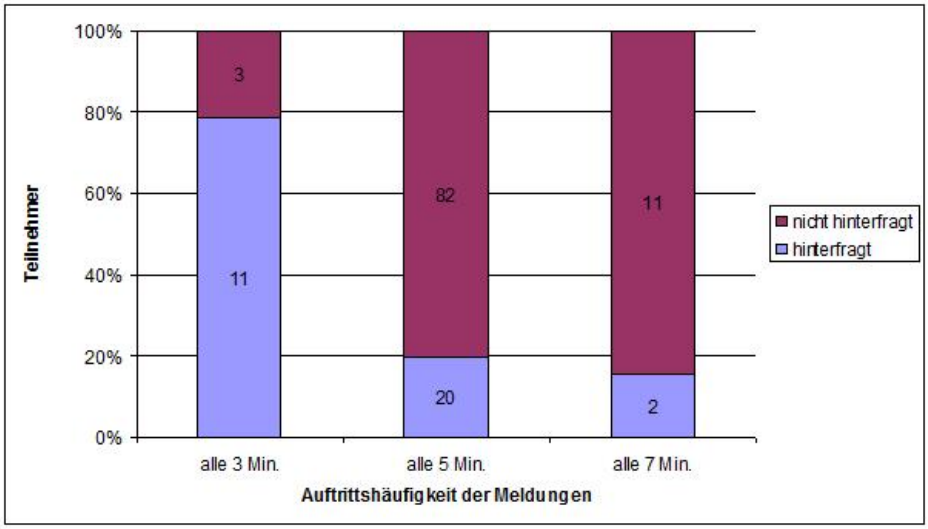


Abb. 4.14: Nachfrage der Teilnehmer in Abhängigkeit der Auftrittshäufigkeiten der Meldungen

Ein ähnlicher Wert ist bei der dritten Gruppe mit 19,70 % zu verzeichnen (13 von 66).

Auf Grund dieses Ergebnisses wurden bei allen weiteren Experimenten Meldungen im Durchschnitt alle fünf Minuten eingeblendet.

Ein weiteres Ergebnis zeigte die Dauer, mit der Meldungen gelesen wurden. Mit Ausnahme der zehnten Meldung wurden alle Meldungen nur einmal präsentiert. Trotzdem verwendeten die Teilnehmer immer weniger Zeit zum Lesen der Meldungen. Dieses Ergebnis bestätigt die Hypothese, dass die Benutzer durch zu viele Meldungen „abstumpfen“ und auch nicht mehr wichtige Meldungen lesen.

MEGSA Experiment 4

An diesem Experiment nahmen 17 Versuchsteilnehmer teil. Bei diesen handelte es sich nur um Studenten. Das Verhalten bei der Interaktion mit MEGSA wurde mit den Studierenden aus Experiment 1 verglichen. Im Gegensatz zu den Teilnehmern aus dem ersten Experiment erhielten die Teilnehmer dieses Versuches zwei Warnmeldungen mit geändertem Design. Im Verhalten bei beiden Gruppen konnte kaum ein Unterschied festgestellt werden. Die Zeiten, bis ein Button gewählt wurde, unterschieden sich im Durchschnitt nur um ca. 100 Millisekunden. Dies kann daran liegen, dass die Meldungen zum Teil nicht verschieden genug waren bzw., dass die verschiedenen Meldungen sofort als irrelevant durch die Teilnehmer klassifiziert wurden.

Einige Versuchsteilnehmer 17,65 % (3 von 17) erkundigten sich nach dem Versuch, warum die Meldungen zueinander im Design unterschiedlich ausgesehen hatten.

MEGSA Experiment 5

An diesem Experiment nahmen 19 Studierende teil. Bei der Eingabe von Fragen und Antworten war die Aufgabenstellung dahingehend geändert worden, dass die Studierende beliebige Fragen aus einem ihrer Hobbys stellen konnten. Somit wurden die Fragen schneller generiert als bei festgelegten Diskursbereichen (im Vergleich zu Experiment 1-4). Warnmeldungen wurden bei dieser schnellen Eingabe an Daten ebenfalls schnell „weggeklickt“, da sich die Studierenden in den Themen, die sie besonders interessierten, nicht durch das Programm behindern lassen wollten. Sie verwendeten im Durchschnitt für die Meldungen lediglich 2,88. Bei den Experimenten 1 - 4 waren dies im Durchschnitt noch 3,28 Sekunden.

MEGSA Experiment 6 Am letzten Experiment mit MEGSA nahmen 22 Studierende teil. In ihrer gewohnten Umwelt verwendeten die Studierenden mehr Zeit zum Lesen von Warnmeldungen als in dem Untersuchungslabor. Im Durchschnitt wurden die Meldungen nach 3,84 Sekunden beendet. Die Ergebnisse des fünften und sechsten Experimentes sind in Abbildung 4.15 grafisch dargestellt.

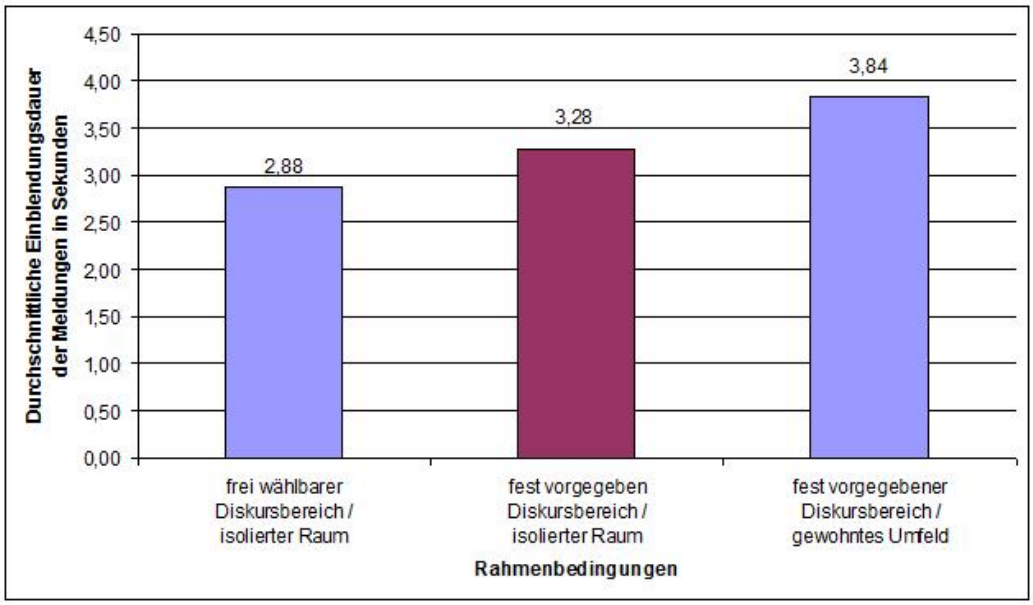


Abb. 4.15: Durchschnittliche Bearbeitungsdauer der Meldungen in Abhängigkeit des Diskursbereichs und Umfeldes

Auch die Wahl der Optionen veränderte sich im gewohnten häuslichen Umfeld. So wurden im Experiment 5 80,17% der Meldungen (93 von 116) mit „Continue“ beantwortet. In den Experimenten 1 - 4 waren dies 84,37% (853 von 1011). Dies ist eine ähnliche Tendenz wie die Einblendungsdauer. Im sechsten Experiment wurde die „Continue“ Option nur 73,44% (94 von 128) gewählt. Dies sind rund 10% weniger als in den Experimenten 1-4. Benutzer reagieren somit im eigenen Umfeld bewusster auf Warnmeldungen. Diese Ergebnisse sind in Abbildung 4.16 abgebildet.

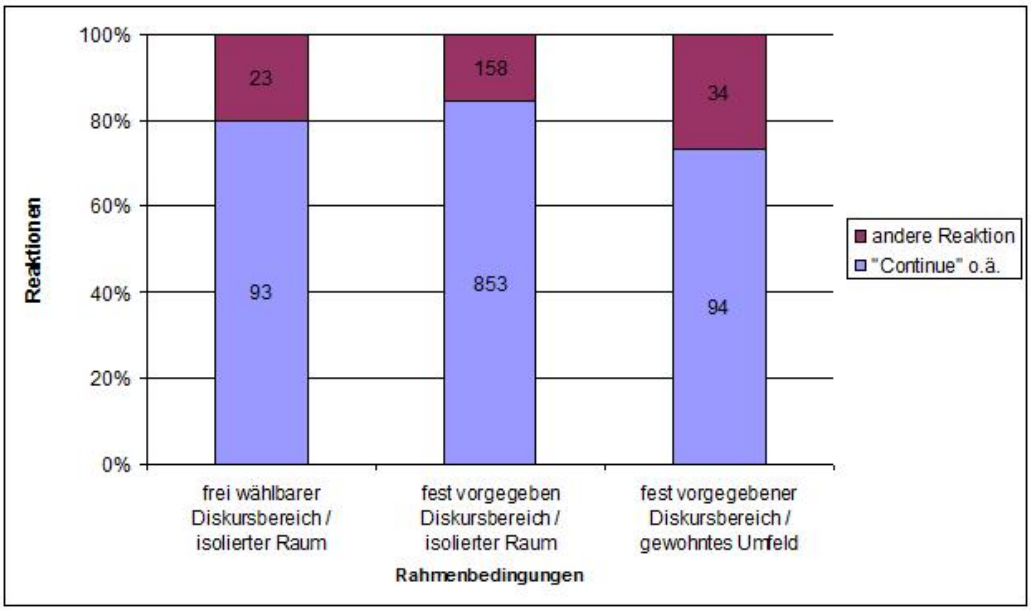


Abb. 4.16: Wahl der „Continue“ Option in Abhängigkeit des Diskursbereichs und Umfeldes

Die Untersuchung der Experiment-Hypothesen ergab, dass die Experiment-Hypothesen 1-3 belegt, wohin gehend die Experiment-Hypothesen 4 und 5 nicht belegt werden konnten. Bevor davon ausgehend die Betrachtung der allgemeinen Hypothesen erfolgt, werden nun noch einige weitere Ergebnisse der Experimente vorgestellt.

MEGSA weitere Ergebnisse

Die Auswertung der Frage C.10 (siehe Tabelle 4.6) ergab, dass nahezu sämtliche Teilnehmer den Diskursbereich IT-Sicherheit als wichtig empfanden. Allerdings verhielten sie sich nicht alle dementsprechend, wie die nächsten Ergebnisse zeigen.

Die unterschiedlichen Typen an Warnmeldungen (siehe Anhang B) benutz-

Großes Interesse	Wichtig	Nicht so wichtig	Ist mir egal	Keine Angabe
118	58	2	3	6

Tab. 4.6: Selbsteinschätzung des Sicherheitsbewusstseins

ten die Teilnehmer unterschiedlich. Dieses Verhalten ist in Abbildung 4.17 graphisch dargestellt.

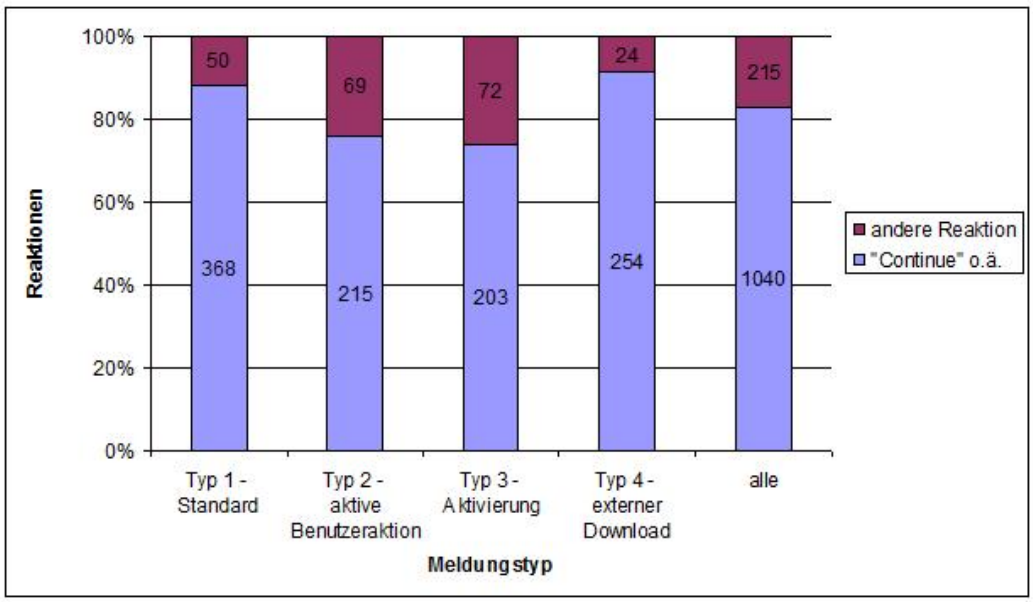


Abb. 4.17: Reaktionen der Teilnehmer in Abhängigkeit des Typs der Warnmeldungen

Beim ersten Typ an Warnmeldungen wählten 88,04% (368 von 418) der Teilnehmer den „Continue“ Button. Dies kann damit erklärt werden, dass die Teilnehmer diese Meldungen bereits von ihren eigenen Systemen kennen und kaum noch wahrnehmen oder beachten.

Die Meldungen des zweiten Typs wurden mit 75,70% (215 von 284) ebenfalls durch Wahl der „Continue“ Option ebenfalls häufig „weggeklickt“. Die Teilnehmer erklärten ihr Verhalten auf Nachfrage damit, dass sie die Meldungen als nicht sicherheitskritisch eingestuft hätten.

Ein ähnlicher Wert für die „Continue“ Option ist bei Meldungen des Typs drei zu ersehen. Dort wählten die Versuchsteilnehmer bei 73,82% (203 von 275) diese Option. Aus sicherheitstechnischer Sicht ist diese hohe Zahl zu

begrüßen, da durch diese Option andere Programme nicht berechtigt werden einen Angriff durchzuführen.

Die höchste Wahl der Option „Continue“ gab es bei Präsentation von Meldungen des Typs 4. Dort wurde die Option 91,37% (254 von 278) ausgewählt. Auf Nachfrage erklärten die Teilnehmer ihre Wahl meist damit, dass der Text zu umfangreich war, und sie lieber das Programm weiter benutzt hätten.

Ein weiteres Ergebnis ergibt die Analyse und Einteilung der Benutzer hinsichtlich verschiedener Benutzergruppen. Insgesamt wurden fünf verschiedene Gruppen gefunden und die Teilnehmer darin klassifiziert. Die Teilnehmer wurden dabei in die Gruppen eingeteilt, deren Merkmal sie bei mehr als 49%[4] der Möglichkeiten ausgewählt hatten. Wenn ein Benutzer zwei Merkmale gleich häufig gewählt hatte, wurde er in die sicherheitskritischere Gruppe eingeordnet.

Verhaltensmuster 1 Benutzer dieser Kategorie öffneten Programmanhänge (z.B. *.zip), autorisierten unbekannte Programme und gaben unbekannte Ports frei. Diese Benutzer agierten dabei sehr sicherheitskritisch. 11% der Benutzer verhielten sich so.

Verhaltensmuster 2 Benutzer dieser Eingruppierung verwendeten die „Continue“ Option ohne sich mit der Bedrohung auseinander zu setzen. Damit reagierten auch sie sicherheitskritisch. Sie nehmen Warnmeldungen nicht mehr war und reagieren nicht auf aktuelle Angriffe. Dieses Verhalten ist als sicherheitskritisch einzustufen. 76% der Versuchsteilnehmer wiesen dieses Verhalten auf.

Verhaltensmuster 3 Benutzer mit diesem Muster aktivierten häufiger die „inform support“ Option um Hilfe zu holen.
7% der Versuchsteilnehmer kann dieses Verhalten zugeordnet werden.

Verhaltensmuster 4 Mit der Option „Close game“ oder „Reboot mobile“ wurde von 2% der Versuchsteilnehmer sicher reagiert.

Verhaltensmuster 5 Die Reaktionen der Versuchsteilnehmer können keinem der anderem Verhaltensmuster zugeordnet werden.
4% der Benutzer wurden in diese Kategorie eingeordnet.

[4] Eine Abweichung von dieser Regel war die Einteilung von Benutzern in Verhaltensmuster 1. In dieses wurden alle Benutzer eingeteilt, die dieses Verhalten mindestens einmal aufwiesen.

Von diesen Verhaltensmustern ausgehend wurden die folgenden Benutzergruppen gebildet.

Benutzergruppe 1 Der Benutzer hat *kein Sicherheitsbewusstsein.*

Benutzergruppe 2 Der Benutzer hat *kaum ein Sicherheitsbewusstsein.* Die Aufgabenerledigung steht für ihn an erster Stelle.

Benutzergruppe 3 Der Benutzer *hat Sicherheitsbewusstsein*, ist mit der Situation aber *überfordert.* Aus diesem Grund versucht er Hilfe zu erhalten.

Benutzergruppe 4 Der Benutzer hat *ein hohes Sicherheitsbewusstsein.* Er ist eines bestehenden Risikos bewusst und versucht dieses zu minimieren.

Benutzergruppe 5 Der Benutzer weist ein nicht eindeutiges Verhalten auf und kann keiner der Gruppen zugeordnet werden.

4.2.4 Zusammenfassung und Wertung der Hypothesen

Mit MEGSA (Mobile Education Gaming Security Application) wurde in diesem Abschnitt ein System vorgestellt, welches das Verhalten von Benutzern mobiler Endgeräte in alltäglichen Situationen hinsichtlich der IT-Sicherheit untersucht, ohne dass sich der Benutzer dessen bewusst ist.

Es wurden 6 verschiedene Experimente mit unterschiedlichen Rahmenbedingungen beschrieben. An diesen nahmen insgesamt 187 Testpersonen teil.

Die Auswertung der Ergebnisse ergab, dass viele der Versuchsteilnehmer Warnhinweise oder -meldungen meist ignorierten, da ihr Aufmerksamkeitsfokus auf die Erledigung einer anderen Aufgabe gerichtet war. Trotzdem gaben sie bei der ebenfalls durchgeführten Befragung an, dass ihnen IT-Sicherheit sehr wichtig ist. Die Untersuchung unterschiedlicher Designs bei den Warnmeldungen ergab in der durchgeführten Variation keine klaren Ergebnisse. Das Bewusstsein der Benutzer konnte durch unterschiedliche Meldungsdesigns nicht gesteigert werden. Dies kann aber auch an den gewählten Variationen gelegen haben. Die zu Beginn dieses Kapitels aufgestellten Hypothesen, dass Benutzer der IT-Sicherheit zwar einen hohen Stellenwert zuweisen, sich aber anders verhalten, konnte gezeigt werden. Die Teilnehmer ordneten ihr Sicherheitsbewusstsein einer anderen Aufgabe unter. Vom Design der durchgeführten Experimente wäre es ohne Einschränkungen möglich gewesen, sowohl die Aufgabe zu erledigen als auch ein hohes Sicherheitsbewusstsein umzusetzen. Die Teilnehmer hätten in allen Situationen die „Inform

Support“ Option wählen können. Kritisch an dieser Stelle ist anzumerken, dass die Probanden nicht ihr eigenes Mobiltelefon verwendeten, sondern ein von der Universität überlassenes. Dafür waren sie auch verantwortlich. Weitere Studien müssen daher klären, wie sich das Verhalten ändert, wenn die eigenen Geräte benutzt werden. Allerdings änderten sich die Ergebnisse im Verhalten kaum, als einige der Probanden die Mobiltelefone in der heimischen Umgebung benutzten und somit bei einem Schaden der Geräte haften hätten müssen.

Das vorgestellte System eignet sich, um das Verhalten von Benutzern bei sicherheitskritischen Situationen zu untersuchen, ohne dass sich die Benutzer dessen bewusst sind. Solange nicht zu viele Warnmeldungen generiert wurden, bemerkten die Versuchsteilnehmer die Untersuchung ihres sicherheitsrelevanten Verhaltens nicht. Erst bei einer gesteigerten Häufigkeit fragten die Teilnehmer bei dem Versuchsleiter nach.

Die Analyse des Verhaltens dieser Testpersonen ergab verschiedene Verhaltensmuster der Teilnehmer, aus denen sich die folgenden verschiedenen Benutzergruppen klassifizieren ließen:

1. Benutzer hat kein Sicherheitsbewusstsein,
2. Benutzer hat kaum Sicherheitsbewusstsein,
3. Sicherheitsbewusstsein ist vorhanden, Benutzer ist aber mit Situation überfordert,
4. Sicherheitsbewusstsein und Kenntnis der Maßnahmen sind beim Benutzer vorhanden,
5. das Verhalten des Benutzers kann keiner der anderen Gruppen eindeutig zugeordnet werden.

Die Auswertung in MEGSA ergab, dass die meisten Benutzer über kein oder über kaum Sicherheitsbewusstsein verfügen. Sie stellen die Erledigung von anderen Aufgaben in den Vordergrund und messen dem Thema IT-Sicherheit bei alltäglichen Aufgaben keinen hohen Stellenwert bei.

Aus diesem Grund müssen für technische Maßnahmen[5] zur Erhöhung der IT-Sicherheit, die eine Interaktion mit Benutzern benötigen, Rahmenbedingungen für einen optimalen Einsatz geschaffen werden. Zum einen muss das

[5] z.B. Firewalls, IDS, Email-Verschlüsselung, Systeme zur Authentifizierung oder Autorisierung ...

Sicherheitsbewusstsein der Benutzer gesteigert werden, und sie müssen potentielle Risiken und Bedrohungen erkennen. Zum anderen müssen Benutzer aber auch die technischen Hilfsmittel und Maßnahmen korrekt bedienen können.

Das MEGSA Konzept und die Erkenntnisse aus den Experimenten können dazu verwendet werden, Systeme sicherer zu machen, indem die Benutzung neuer Sicherheitsmaßnahmen dadurch untersucht werden kann, ohne dass sich Benutzer dieses Untersuchungsfokus bewusst sind. So kann untersucht werden, durch welche Maßnahmen der mentale Fokus der Benutzer von der eigentlichen Aufgabenerledigung auf die zusätzlich sichere Interaktion mit Systemen gelenkt werden kann oder durch welche Maßnahmen Benutzer unbewusst sichere Aktionen tätigen. Allerdings bietet sich hier auch neues Risikopotential, denn Designer von Schadsoftware können diese Ergebnisse ebenso verwenden, indem sie Schadsoftware erstellen, die die Unterordnung des Sicherheitsbewusstseins unter einen anderen mentalen Fokus ausnutzt, wie dies in Ansätzen bereits bei SPAM oder Phishing-Attacken ausgenutzt wird.

Ein weiterer Aspekt bei einer Weiterentwicklung des MEGSA Systems könnte darin bestehen, dass Benutzergruppen autonom gruppiert werden und Sicherheitsmaßnahmen gruppenspezifisch bereit gestellt werden, um dadurch die Sicherheit zu erhöhen. Aus diesem Grunde wurde die im Folgenden vorgestellte Idee entwickelt. Diese dient zur autonomen Gruppierung von Benutzern anhand ihrer Interaktion mit IT-Systemen.

4.3 Benutzergruppierung durch Untersuchung der Interaktion

Die Ergebnisse aus Abschnitt 4.1 und Abschnitt 4.2 zeigen, dass von Benutzern ein großes Bedrohungspotential durch ihre Unkenntnis und Fehleinschätzung der Situation ausgeht. Diesem Bedrohungspotential kann von Herstellerseite entgegen gewirkt werden, wenn Systeme so entwickelt werden, dass die Erfahrung des jeweiligen Benutzers verwendet wird, um die Situation richtig einzuschätzen und sich entsprechend zu verhalten. Allerdings sind alle Benutzer verschieden und haben unterschiedliches Erfahrungswissen. Eine Anpassung an jeden einzelnen Benutzer ist aus Kostengründen nicht möglich (vgl. Abschnitt 1.1.2). Einen Kompromiss stellt die Anpassung und Bereitstellung der Systeme für unterschiedliche Benutzergruppen dar.

Bei herkömmlichen Evaluierungsmethoden, wie z.B. Fragebögen, werden Benutzer anhand von Kriterien aus Vorevaluationen (vgl. Abschnitt 2.3.3) in verschiedene Benutzergruppen gruppiert. Wenn allerdings nicht die relevanten Kriterien durch den Evaluator zur Gruppierung verwendet wurden, führt dies zu Abweichungen und Problemen. In diesem Fall kann das Verhalten eines Gruppenmitglieds erheblich vom angenommenen Verhalten der Gruppe abweichen. Benutzt beispielsweise ein Evaluator das Kriterium K_1 = „Beruf der Versuchsteilnehmer“ zur Trennung der Gruppen, erhält er andere Gruppen, als wenn er die Gruppen nach dem Kriterium K_2 = „auf dem heimischen Computer benutztes Betriebssystem“ trennen würde. Wenn nun ein Programm in Abhängigkeit von K_1 optimiert wird, das Verhalten der Benutzer aber in Abhängigkeit von K_2 variiert, ist dass Fehlbedienungspotential durch die Optimierung nicht zwangsläufig minimiert.

Nach Nielsen [93] und Sarodnick [110, 136 ff] ist es auch Experten nicht möglich, alle Kriterien ausreichend zu berücksichtigen, da sie einige Kriterien bei der Erstellung des Evaluierungsrahmens zu stark, manche zu schwach und andere in Unkenntnis ihrer Bedeutung überhaupt nicht gewichten und verwenden. Viele Hersteller führen nur eine sehr einfache Gruppierung durch, indem sie Programme für die Gruppen: „Anfänger“, „Normaler Benutzer“ und „Experte“ bereitstellen (vgl. [118]). Aus der in Kapitel 2.3.1 beschriebene Wichtigkeit von Benutzergruppen entsteht jedoch die Notwendigkeit die Fragen: *Welche Gruppen gibt es?* und *Wie sehen sie aus?* detailliert zu klären, um ein Höchstmaß an IT-Sicherheit durch gruppenspezifische Anpassungen erreichen zu können. Dieser Gedankengang führte zu folgender Idee.

4.3.1 Die Idee von der Verbesserung der IT-Sicherheit durch Analyse der Benutzerinteraktion

Die gruppenspezifische Bereitstellung der Systeme verbessert die IT-Sicherheit, wenn durch Bildung der Gruppen das Fehlbedienungspotential minimiert wird. Für Gruppen mit ähnlichem Verhalten können Sicherheitsmechanismen gruppenindividuell angepasst werden, um die Fehlbenutzung zu minimieren. Speziell auf diese Gruppen zugeschnittene Benutzungsaspekte (z.B. GUI's oder Bezeichnungen oder Default-Kongfigurationen) erhöhen das Sicherheitsniveau, da sie einer potentiellen Fehlbenutzung entgegen wirken. Die Benutzer verhalten sich innerhalb ihrer Gruppe ähnlich bzw. nahezu oder vollkommen gleich. Sie verstehen ungefähr das Gleiche unter den Funktionen und haben ähnliche Erwartungen und Ziele. Jeder Benutzer weist innerhalb seiner Gruppe nur eine minimale Abweichung bei seinem Verhalten zum angenommenen Gruppenverhalten auf.

Es müssen somit Aspekte gefunden werden, die die Anzahl und die Zusammensetzung der Benutzergruppen bestimmen. Die Untersuchung von Benutzerinteraktion und deren Gruppierung stellt einen möglichen Schritt dazu dar. Die Untersuchung und Gruppierung sollte dabei weitestgehend autonom erfolgen, damit subjektive Einflüsse durch die Sicht des Evaluators minimiert werden und um die zuvor beschriebenen Probleme zu vermeiden. Um die Idee von der Verbesserung der IT-Sicherheit durch gruppenspezifische Voreinstellungen zu untersuchen, wurden die folgenden Hypothesen aufgestellt und evaluiert.

Die Idee stützende Hypothesen

Durch die Untersuchung der Interaktion von Benutzern mit Programmen lassen sich Gruppierungen zur Verbesserung der IT-Sicherheit und Hinweise für Verbesserungen der Usability finden. So lassen sich gruppenspezifische Sicherheitsbedrohungen minimieren. Außerdem ergibt die Untersuchung des Verhaltens der Benutzer bei Anwendungen andere Benutzergruppen als die Gruppen: *Experte, Normaler Benutzer und Anfänger*. Es lassen sich so andere eindeutige Gruppen mit speziellen Attributen finden.

Zur Überprüfung der Hypothesen entwickeltes Konzept

Um die aufgestellten Hypothesen und Fragestellungen zu untersuchen wurde, die folgende Konzeptidee von der Verbesserung der IT-Sicherheit durch Untersuchung des Verhaltens entwickelt, die im weiteren Verlauf der Arbeit die Grundlage für die Untersuchungen bildet.

> **Konzeptidee:** Beliebige Benutzer interagieren mit einem Programm. Die Interaktion wird protokolliert. Die Protokolldaten werden durch mathematische Verfahren analysiert und gruppiert. Evaluatoren erhalten visuell aufbereitete Gruppierungen, mit denen sie neue Kenntnisse sammeln oder alte Erfahrungen abgleichen können. Aufgrund der gefundenen Gruppierungen werden zudem Schwachstellen bei der Verwendung sichtbar, deren Behebung die IT-Sicherheit verbessert.

Mit den Ergebnisses aus der Umsetzung dieser Idee können Erkenntnisse aus Befragungen oder anderen Evaluationsmethoden ergänzt und verifiziert werden. Die Umsetzung dieser Idee bei einem System zeigt allerdings nur eine Momentaufnahme im Verhalten der Versuchsteilnehmer. Durch Lernen können Versuchsteilnehmer ihr Verhalten und somit die Gruppenzugehörigkeit verändern. Diese Methode kann aber anzeigen, ob viele unterschiedliche Gruppen vorhanden sind. Je nach Wahl verschiedener mathematischer Verfahren kann die Zahl der Gruppen zu Beginn der Auswertung festgelegt werden oder erst durch das unterschiedliche Verhalten der Versuchsteilnehmer bestimmt werden.

Nach Ermittlung der Gruppen muss es das Ziel sein durch Usability-Maßnahmen für ein höheres gemeinsames Verständnis und eine Verringerung der Anzahl der Gruppen zu sorgen, da dadurch das Fehlbedienungspotential gesenkt wird.

4.3.2 Praktische Evaluation des aufgestellten Konzeptes

Um diese Idee und die aufgestellten Hypothesen zu untersuchen, wurde im Rahmen dieser Arbeit das System SUESA (System for Usability Evaluation in Security Applications) im DAI-Labor der Technischen Universität Berlin entwickelt und in mehreren Lehrveranstaltungen eingesetzt und evaluiert. Das System dient dazu verschiedene Aspekte des Verhältnisses von Benutzergruppen und IT-Sicherheit zu untersuchen. Im Fokus stehen dabei die

Fragestellungen wie und in welche Gruppen Benutzer bei der Interaktion mit Sicherheitsmechanismen gruppiert werden können.

Das entwickelte System

Das Konzept von SUESA lässt Benutzer mit einer Software interagieren, zeichnet ihre Interaktionen mit einem „Eventrecording“-Werkzeug auf, separiert aus diesen Daten verschiedene Benutzergruppen und zeigt Ansatzpunkte zur Verbesserung der IT-Sicherheit auf. Die gefundenen Gruppen und mögliche Ansatzpunkte werden so aufbereitet, dass ein Evaluator diese Daten geeignet interpretieren kann.

Das „Eventrecording“-Werkzeug erzeugt für jeden Benutzer einen mehrdimensionaler Interaktionsvektor. Jede mögliche Interaktion stellt dabei eine Dimension des Vektors dar. Dies können zum Beispiel die Eingaben bei unterschiedlichen Menüs oder die Betätigung von Buttons sein. Um eine detailliertere Untersuchung zu ermöglichen, kann dieser Vektor für die spätere Untersuchung wiederum in verschiedene Untervektoren zerlegt werden.

Zum Beispiel kann nur betrachtet werden, welche Checkboxen bei einem Programm ausgewählt wurden. Der zugehörige Untervektor wäre dann $\overrightarrow{Checkboxen} = (C_{Box1}, C_{Box2}, ..., C_{Box(n)})$.

Die Vektoren dienen in SUESA als Eingabevektoren für die mathematischen Verfahren zur Gruppierung wie z.B. Self Organizing Maps (SOMs) (vgl. [71, 70]) oder dem Expectation Maximization (EM) - Algorithmus (vgl. [86], [130], [14]).

Die Gruppierung der Benutzer durch SUESA kann für sämtliche Bereiche der IT dienen und ist nicht auf die IT-Sicherheit beschränkt, da Benutzer anhand ihres Verhaltens in Gruppen eingeteilt werden. In dieser Arbeit wurde als Diskursbereich allerdings der Bereich IT-Sicherheit fokussiert betrachtet und soll im Folgenden behandelt werden.

Die gefundenen Gruppen können verwendet werden, um verschiedene Problembereiche der Usability und IT-Sicherheit zu identifizieren. Dazu ist es allerdings zur Zeit noch notwendig weitere Informationen aus anderen Evaluationsmethoden zu verwerten. Zum einen muss geklärt werden, warum ein Benutzer einer Gruppe zugewiesen wurde und zum anderen durch welche Gruppierungen Problembereiche angezeigt werden.

Für diese Arbeit wurde dazu die Kombination von SUESA mit Fragebögen gewählt. So lassen sich verschiedene Attribute zu den Gruppen finden. SUE-

SA findet die Anzahl der Gruppen und welche Benutzer den jeweiligen Gruppen zurechenbar sind. Die Fragebogenmethode ermittelt, wodurch sich dann die Benutzergruppen gegeneinander abgrenzen. Diese Abgrenzungskriterien können bei weiteren Untersuchungen mit SUESA voraus gesetzt werden und müssen dann nicht erneut erhoben werden.

Die Abbildung 4.18 zeigt diesen schematischen Aufbau des SUESA-Konzeptes.

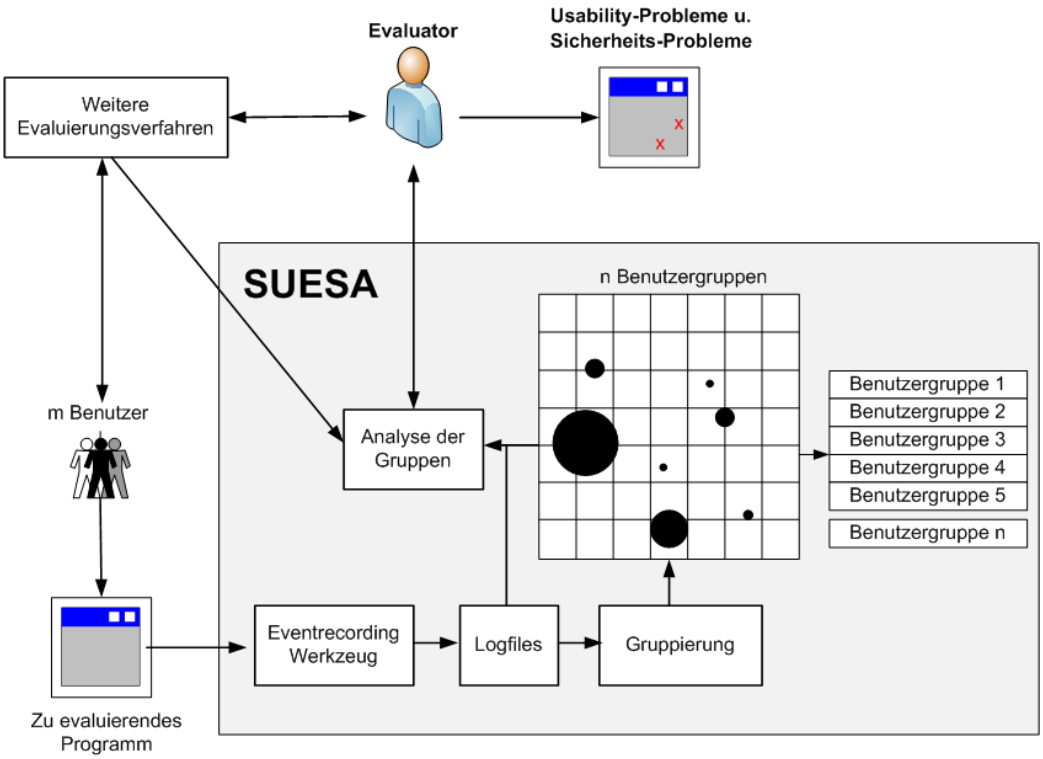


Abb. 4.18: SUESA: System for Usability Evaluation in Security Applications

Die Verwendung und Einbindung von SUESA in Evaluationen kann konzeptionell in zwei Phasen unterschieden werden. Bei der ersten Phase handelt es sich um eine Datengewinnung und bei der zweiten Phase um eine Datenverarbeitung.

Zur Datengewinnung erhalten Versuchsteilnehmer eine Aufgabe, die sie mit Hilfe eines zu evaluierenden Programms lösen sollen. Durch das eingebundene „Eventrecording-“ Werkzeug von SUESA werden die Aktionen der Benutzer dabei in einem Logfile mitprotokolliert. In dem Logfile sind dann die folgenden Daten der Benutzung gespeichert: die Reihenfolge der gewählten Aktionen des Benutzers, seine Navigation durch das Programm, die Zeit die er

zwischen seinen Aktionen benötigt und die Ergebnisse, die seine Handlungen auslösen.

Bei der Phase der Datenverarbeitung werden diese Logfiles dann analysiert, um verschiedene Benutzergruppen zu separieren. Die Daten der Logfiles werden dazu so aufgearbeitet, dass sie als Eingabevektoren für die Benutzerklassifizierung dienen. Die Zeiten, die die Benutzer benötigten, werden normiert, um zu stark abweichende Daten bewerten zu können. Klassifizierungsalgorithmen unterteilen dann die Benutzer in verschiedene Gruppen, indem sie die Eingabevektoren verwenden. Nach Bildung der Gruppen können diesen einzelne Attribute zugewiesen werden.

Optional können bei diesem Ablauf bei der Phase der Datengewinnung weitere Daten durch andere Evaluierungsmethoden erhoben werden. So kann zum Beispiel im Anschluss an die oben geschilderte Datengewinnung durch die Mitprotokollierung eine weitere Datengewinnung durch die Befragung der Benutzer mit einem Fragebogen erfolgen. Mit Hilfe der Daten aus dieser zusätzlichen Datengewinnung können die Klassifizierungsergebnisse von SUESA validiert oder um weitere Attribute ergänzt werden.

Die implementierte „SUESA“-Komponente

Die implementierte SUESA-Komponente besteht aus mehreren Teilen. Zuerst werden die Interaktionen der Benutzer durch die eingebundene Eventrecording Open Source Software Jacareto[10] aufgezeichnet. Diese ermöglicht das Aufzeichnen, Abspeichern und Abspielen von Interaktionen mit grafischen Oberflächen, die auf Java basieren. Die Daten in den Protokolldateien liegen dabei im XML-Format vor. Die aufgezeichneten Protokolldateien beinhalten auch nicht benötigte Zusatzinformationen, auf die eine Reduktionskomponente angewendet wird, um die Eingangsvektoren für die Analyse zu erstellen. Der nächste Bereich von SUESA analysiert die Eingangsvektoren und erstellt die Gruppierungen der Benutzer und stellt sie grafisch dar. Der letzte Bereich in SUESA bietet einige Funktionen zur Interpretation der Gruppen an. Diese Bestandteile und deren zeitliche Verwendung ist in Abbildung 4.19 grafisch abgebildet.

Zur Gruppierung der Benutzer wurde im Prototyp von SUESA als erstes das SOM Verfahren implementiert, da mit diesem Ansatz umfangreiche Ergebnisse für Gruppierungsprobleme vorliegen. Der SOM Ansatz wurde von Kohonen entwickelt [71, 70]. Es handelt sich dabei um ein Verfahren der künstlichen neuronalen Netze. In diesen wird unüberwachtes und Wettbewerbslernen eingesetzt, um meist mehrdimensionale Eingangssignale in weniger dimensionale Ausgangssignale zu transformieren. Dabei werden ähnliche

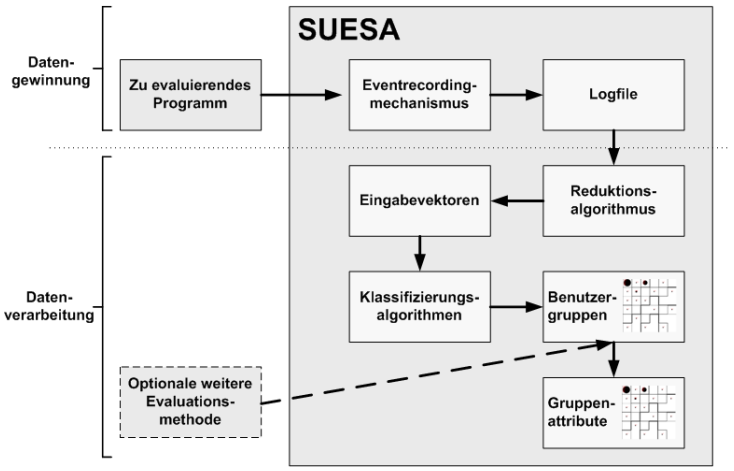


Abb. 4.19: Zeitliche Einbindung und Ablauf einer Evaluation mit SUESA

mehrdimensionale Signale, analog zu biologischen Systemen (z.B. Karten im Gehirn), in dicht beieinander liegende planare Strukturen abgebildet. Auch für Aufgaben im Bereich der IT-Sicherheit wird der SOM Ansatz bereits für eine Reihe von Gruppierungsaufgaben benutzt. So wird zum Beispiel die Anomalieerkennung in Intrusion Detection Systemen (IDS) mit Hilfe des SOM Ansatzes erforscht [13].

Die Benutzung von SOMs bietet darüber hinaus die folgenden Vorteile [71]:

- Abbilden von mehrdimensionalen Eingabevektoren auf zweidimensionale Karten
- Möglichkeit zur Gruppierung ohne vorherige Kenntnis der Anzahl der Gruppen
- Keinerlei Kenntnis über die Gruppen notwendig

Die gesammelten hochdimensionalen Daten werden durch SOMs auf ein leicht überschaubares visuelles Feedback für den Evaluator transformiert. In diesem Feedback ist es für den Evaluator leicht möglich die einzelnen Gruppen voneinander zu unterscheiden.

Die Gruppierung der Eingangsvektoren wird beim SOM Algorithmus nach folgendem Muster durchgeführt: Ein beliebiger Testvektor wird zufällig ausgewählt und dem verwendeten Kohonen Netz präsentiert. Das Netz ändert sich in Abhängigkeit des dargebotenen Vektors und lernt dadurch die Eingangsvektoren abzubilden. Wenn die Änderungen für den gewählten Testvektor durchgeführt wurden, wird ein neuer Testvektor dem Netz präsentiert,

und es lernt erneut. Die Lernrate wird über die Zeit immer weiter verringert, damit der Algorithmus terminiert und die Änderungen immer detaillierter durchgeführt werden. Die Eingangsvektoren werden dem Netz solange präsentiert (auch mehrfach), bis eine Abbruchbedingung erreicht ist. Eine detailliertere Beschreibung des verwendeten SOM Ansatzes ist im Anhang C.3 zu finden.

Für die Gruppierung der Benutzer wurden in SUESA die zwei Gruppierungsarten: „Gruppieren anhand der benötigten Zeit“ und „Gruppieren basierend auf getätigten Entscheidungen“ implementiert.

Gruppierung in Abhängigkeit der benötigten Zeit

In SUESA können Benutzer in Abhängigkeit der Zeit, die sie für eine Aufgabe benötigten, gruppiert werden. Dafür wurde eine Gauß-Glocken Funktion implementiert, die das “gewinnende“ Neuron[6], das BMU (best matching unit), und die benachbarten Neuronen verändert. Je näher ein Neuron dabei an dem Gewinner liegt, je mehr wird es durch den Eingangsvektor modifiziert. In Formel 4.1 ist die implementierte Gauß-Glocken Funktion beschrieben. Bei ω_i handelt es sich um das Erregungszentrum und bei ω_k um ein anzupassendes Neuron auf der Karte. Allerdings werden nur die Neuronen angepasst, die sich innerhalb der Nachbarschaft befinden.

$$\gamma(\omega_i, \omega_k) = \begin{cases} e^{-\left(\frac{d(\omega_i,\omega_k)^2}{\sigma^2}\right)}, d(\omega_i, \omega_k) \leq \sigma \\ 0, sonst \end{cases} \tag{4.1}$$

Neben der Möglichkeit nach der Zeit zu gruppieren bietet SUESA auch die Möglichkeit, die Benutzer gemäß ihrer getroffenen Entscheidungen zu gruppieren.

Gruppierung in Abhängigkeit der getroffenen Entscheidungen

Bei der Gruppierung gemäß der getroffenen Entscheidungen wird in SUESA ein anderer Eingabevektor für die Lernverfahren verwendet. Dieser wird in Abhängigkeit des zu untersuchenden Verhaltens durch den Reduktionsalgorithmus erstellt. Soll zum Beispiel untersucht werden, welche Buttons und welche Hilfeoptionen die Benutzer auswählten, enthält der Eingabevektor einen Eintrag für jede potentielle Button-Auswahl und für jede potentielle Hilfeauswahl. Kann der Benutzer 10 Buttons wählen und dazu 10 Hilfetexte auswählen, enthält der Vektor 20 Elemente.

[6] Neuronen sind die elementaren Bestandteile des künstlichen neuronalen Netzes, welches die SOM zur Berechnung verwendet.

Für die Gruppierung hat der Eingabevektor eines Benutzers eine „Eins“, wenn der Benutzer diesen Button/Hilfetext betätigte und eine „Null“, wenn er dies nicht tat. Aus dem zu untersuchenden Verhalten der Benutzer wird somit ein Bitvektor als Eingangsvektor erstellt. Daher kann zur Bestimmung des Abstands zwischen dem Eingangsvektor und den Kartenneuronen der *Hamming-Abstand* benutzt werden. Der Hamming-Abstand besagt dabei, an wie vielen Stellen sich zwei Vektoren voneinander unterscheiden. Beide Vektoren müssen dazu die gleiche Anzahl an Elementen besitzen. Die Formel 4.2 zeigt die allgemeine Berechnung des Hamming-Abstandes.

$$h(x, y) = \|x \otimes y\| \tag{4.2}$$

Der Hamming-Abstand wurde bei der Implementierung dieser Variante in SUESA ebenfalls benutzt, um die BMU zu bestimmen. Im Anhang C.3 sind die Modifikationen, die für die reale Verwendung notwendig waren, beschrieben.

Implementierte Oberflächen in SUESA

Bei der Implementierung der eigentlichen SUESA-Anwendung (Gruppierung der Interaktionsdaten) wurden drei Menüs erstellt. Abbildung 4.20 zeigt das Fenster mit den Hauptfunktionalitäten zur Gruppierung. Hier können verschiedene Eingaben zur Erstellung der Gruppierung eingegeben werden.

In zwei weiteren Menüs können Angaben zu einer detaillierteren Analyse der Gruppierungen und zur Speicherung der Ergebnisse eingegeben werden. Diese beiden Menüs sind im Anhang C.2 abgebildet und dort beschrieben.

Im Folgenden werden nun ein real mit SUESA durchgeführtes Experiment und seine Resultate vorgestellt.

Der durchgeführte Versuch mit SUESA

Mit dem oben vorgestellten Prototypen wurde eine Untersuchung durchgeführt, um die aufgestellten Hypothesen zu untersuchen. An dieser praktischen Erprobung nahmen zum einen Studenten der Lehrveranstaltungen IT-Sicherheit und IT-Sicherheit und Qualitätsmanagement und zum anderen noch Versuchspersonen aus dem privaten Umfeld der Studenten teil. Für die Umsetzung des Experimentes wurde der folgende Versuchsaufbau gewählt.

Versuchsaufbau und Ablauf

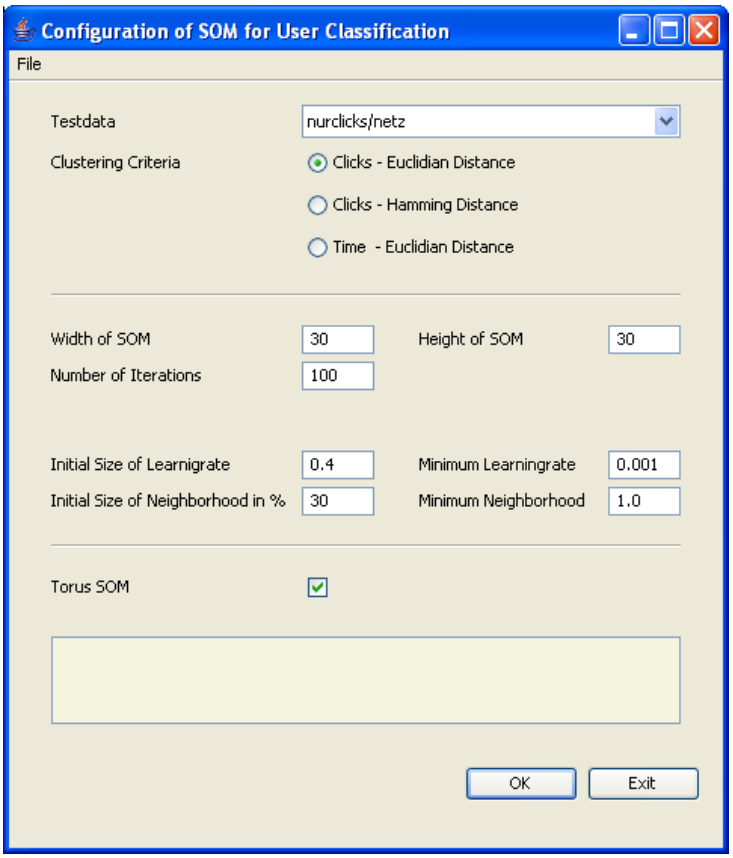


Abb. 4.20: Menü zum Starten der Gruppierung in SUESA

Die Versuchsteilnehmer erhielten zu Beginn des Versuches einen Fragebogen (siehe Anhang A). In diesem war zunächst die Aufgabenstellung beschrieben. Nach Lesen der Aufgabenstellung sollten sie ein *Absicherungsprogramm* starten und damit die Aufgabe lösen. Das Absicherungsprogramm war speziell für die Evaluation erstellt worden, entsprach in seinem Aussehen aber einem realen Produkt. Dann gruppierte SUESA die Interaktionsdaten, und die gefundenen Gruppen wurden durch einen Evaluator mit Hilfe einiger Werkzeuge in SUESA interpretiert.

Um zusätzlich eine Gruppierung hinsichtlich des selbst empfundenen Sicherheitsbedürfnisses durchzuführen, mussten die Teilnehmer dieses selbst bestimmen (siehe C.2). Die zu lösende Aufgabe lautete:

Stellen Sie sich vor, Sie haben den vor Ihnen befindlichen Computer soeben für Ihr privates Umfeld erworben. Sie möchten mit diesem auch im Internet arbeiten. Sie erhalten nun ein Programm, mit dem Sie alle sicherheitsrele-

vanten Einstellungen vornehmen können. Konfigurieren Sie den Computer bitte so, dass er Ihrem Sicherheitsbedürfnis entsprechend eingerichtet ist.

Das „Absicherungsprogramm“

Das Absicherungsprogramm hatte die Aufgabe, das Verhalten der Versuchsteilnehmer im Kontext von IT-Sicherheit zu stimulieren, indem es sie mit verschiedenen Konfigurationsmöglichkeiten aus dem Bereich der IT-Sicherheit konfrontierte. Für das Programm diente das verbreitete Sicherheitskonfigurationsprogramm XP-AntiSpy [7] als Vorbild. Diesem wurden einige Bezeichnungen, Hilfen und Optionen entnommen und in dem Sicherungsprogramm grafisch nachgebildet.

Die erste Oberfläche im Absicherungsprogramm beinhaltete einen Text, den jeder Benutzer lesen musste und der ihm die Verwendung des Programmes und die Erstellung eines Passwortes beschrieb. Dieser Schritt wurde gewählt, damit alle Versuchspersonen die identische Aufgabenstellung und Startposition hatten. Nach der Erstellung von Benutzer und Passwort beinhaltete das Absicherungsprogramm die vier Konfigurationsbereiche *Allgemein, Netzwerk, Email* und *Browser*. Dort hatte jeder Versuchsteilnehmer die Möglichkeit insgesamt 20 verschiedene Konfigurationseinstellungen zu tätigen. Die Funktionalität der verschiedenen Menüs wurde nicht nachimplementiert.

Eine der Oberflächen des Absicherungsprogramms zeigt Abbildung 4.21. Diese Oberfläche war zum Konfigurieren der Browser-Einstellungen vorgesehen. Im Anhang C.1 befinden sich zur Veranschaulichung sämtliche weiteren Oberflächen.

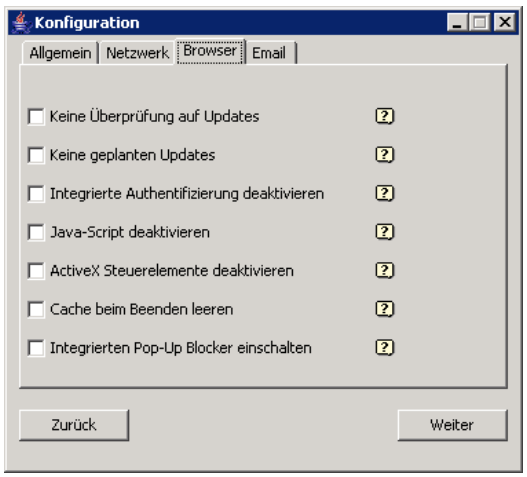


Abb. 4.21: Oberfläche zur Konfiguration der Browser-Einstellungen beim Absicherungsprogramm

Hinter jeder Konfigurationsmöglichkeit befand sich ein Fragezeichensymbol, mit dem die Benutzer Hilfetexte zu den Konfigurationseinstellungen anschauen konnten. Auf diese Möglichkeit eine Hilfe zu verwenden wurden die Versuchsteilnehmer zu Beginn des Versuches durch den Evaluator explizit hingewiesen. Bei Anwahl dieses Hilfesymbols erhielt der Benutzer Informationen zu der jeweiligen Konfigurationsmöglichkeit. Diese Hilfemöglichkeit wurde integriert, um die später beschriebene Untersuchung über Unsicherheit durchzuführen (siehe 4.4). Die Hilfetexte waren dabei ebenfalls dem Vorbild XP-AntiSpy entnommen.

Als eine Konfigurationsmöglichkeit war die Option SMTP-Over-Pop[7] im Konfigrationsbereich Email in den Versuch integriert, da Sie den meisten Benutzern unbekannt war und somit auch dass Verhalten in Bezug auf die bereit gestellte Hilfe und die Unsicherheit bei der Benutzung untersucht werden konnte. Zugleich wurde ein sehr wenig informativer Hilfetext angezeigt, um auch das Verhalten bei unzureichender Unterstützung durch das System zu analysieren. Der Hilfetext lautete: *Setzen Sie diese Einstellung nur, falls Ihr Provider dies erfordert.*

Nachdem die Versuchsteilnehmer die Aufgabe mit dem Programm gelöst hatten, füllten sie den Rest des Fragebogens aus. Während der Versuchsdurchführung befanden sich jeweils ein Testteilnehmer und der Evaluator im Raum. Der Teilnehmer konnte jederzeit Fragen an den Evaluator stellen. Die Interaktionsdaten der Versuchsteilnehmer wurden durch SUESA aufgezeichnet und anschließend gruppiert. In einem weiteren Schritt wurden dann die Gruppierungsergebnisse mit den Ergebnissen des Fragebogens in Beziehung gesetzt.

SUESA protokollierte alle Eingaben der Benutzer und bereitete sie auf. Die Resultate von SUESA und die Ergebnisse des Fragebogens werden nun vorgestellt und dann in Beziehung gesetzt.

[7] SMTP-Over-Pop wird für die Authentifizierung beim Versenden von Emails eingesetzt. Diese Funktion ist nicht standardmäßig im SMTP Protokoll aktiviert.

Ergebnisse des Experimentes

Mit SUESA können verschiedene Varianten an Ausgabekarten erzeugt werden. Konkrete Ausgabeergebnisse sollen im Folgenden an einer Fallstudie gezeigt werden bei der der oben beschriebene Versuchsablauf verwendet wurde.

Nachdem alle 35 Versuchsteilnehmer die Aufgabe gelöst und ihren Fragebogen ausgefüllt hatten, bereitete SUESA die Interaktionsdaten für Evaluatoren auf. Bevor die von SUESA erstellten Karten gezeigt und interpretiert werden, werden zunächst einige Ergebnisse des Fragebogens vorgestellt, die bei der spätere Untersuchung benötigt werden.

Ergebnisse aus den Fragebögen

Der Fragebogen bestand aus zwei Teilen. Im ersten Teil wurden die Stammdaten der Versuchsteilnehmer und ihr persönliches Verhältnis zu Computern und IT-Sicherheit erhoben. Im zweiten Teil wurden dann Fragen speziell zum verwendeten Testprogramm gestellt. Diese lieferten Aussagen über die Übersichtlichkeit und Handhabung des Testprogramms. Die Fragen in beiden Teilen wurden so gewählt um später Aussagen über die mit SUESA gefundenen Gruppen hinsichtlich ihres Verhaltens bei der Benutzung von IT-Sicherheitsmechanismen zu treffen.

Trotz dem hohen Anteil an Studenten aus dem Bereich Informatik schätzten nur zwei Teilnehmer ihr Wissen über sicherheitsrelevante Software als „sehr gut“ ein. Gute Kenntnisse gaben 14 Teilnehmer an, Grundkenntnisse 13 und 4 keine Kenntnisse. Zwei Teilnehmer gaben keine Einschätzung ab. 24 von 35 Teilnehmern administrieren ihren eigenen PC selbst.

Weiterhin wurden die Versuchsteilnehmer dahingehend befragt, welchen Stellenwert sie der IT-Sicherheit des eigenen PC beimessen. Neun Versuchsteilnehmer gaben dabei an, dass ihnen die Sicherheit ihres eigenen Computers sehr wichtig ist, für 14 war sie wichtig, 10 Teilnehmer legten nur Wert darauf, dass der Computer funktioniere und 2 Teilnehmer gaben keine Antwort.

Dieses Ergebnis zeigt, dass trotz der in Kapitel 2.2 beschriebenen Wichtigkeit von IT-Sicherheit vielen Benutzern nur der Komfort ihres Systems wichtig ist. Dieses Ergebnis deckt sich mit den Ergebnissen des letzten Abschnittes 4.2 Die Antworten auf die Fragestellung 3 können so interpretiert werden, dass viele Benutzer sich keiner persönlichen Bedrohung bewusst sind.

Neben den Fragen zu den Stammdaten der Versuchsteilnehmer im ersten Teil des Fragebogens wurden im zweiten Teil einige Fragen zu dem verwendeten Absicherungsprogramm gestellt, deren Ergebnisse nun vorgestellt werden.

Diese Fragen sollten dazu dienen, potentielle Fehlbedienungen mit den durch SUESA gefundenen Gruppen in Bezieghung setzen zu können.

Die Tabellen 4.7 und 4.8 zeigen wie intuitiv die Versuchsteilnehmer mit dem Absicherungsprogramm zu recht kamen (Fragen 1 und 3).

Wie bewerten Sie die Bezeichnungen der Einstellungen?	Anzahl
1 (Eindeutig)	10
2	14
3	6
4	1
5 (Verwirrend)	3
Keine Angabe	1

Tab. 4.7: Bewertung der Bezeichnungen

Wie bewerten Sie die allgemeine Übersichtlichkeit der Anwendung?	Anzahl
1 (Sehr gut)	14
2	11
3	5
4	2
5 (Sehr schlecht)	1
Keine Angabe	2

Tab. 4.8: Selbsteinschätzung der Übersichtlichkeit

Sie zeigen, dass die meisten der Versuchsteilnehmer mit dem Programm keine großen Probleme hatten, da sie die Bezeichnungen und die Übersichtlichkeit als gut bewerteten. Dies ist insofern wichtig, als dass Benutzer Handlungen tätigen sollten, deren Sinn sie verstehen sollten. Wenn die Teilnehmer dagegen ihre Entscheidungen nur durch „Raten“ getroffen hätten, wäre eine Gruppierung nicht sinnvoll gewesen.

Drei Versuchsteilnehmer fanden die Bezeichnungen allerdings verwirrend. Eine detaillierte Befragung dieser drei Personen ergab, dass eine Person keinen eigenen PC besaß und nur sehr einfache Kenntnisse mit Computern gesammelt hatte und eine weitere Person auf Grund eines Sprachproblems mit den Bezeichnungen im Programm nicht zurecht kam.

Weitere Ergebnisse der Fragebogenauswertung befinden sich im Anhang C.4.

Die Ergebnisse der Befragung im Fragebogen können dahingehend zusammen gefasst werden, dass die Versuchsteilnehmer die grafische Oberfläche des Testprogramms als benutzerfreundlich einstuften. Allerdings waren die Fragen dazu nur sehr grob gestellt worden. Wenn die Beurteilung und Verbesserung der Usability des Testprogramms im Fokus gestanden hätte, müssten die Fragen detaillierter zum Evaluierungsgegenstand gestellt werden. Die Fragen dienten jedoch nur dazu die Ergebnisse der automatischen Gruppierung von SUESA zueinander in Beziehung zu setzen.

Ergebnisse der erstellten Karten in SUESA

Im Folgenden werden Ergebnisse vorgestellt, die unter Verwendung des euklidischen Abstandes[8] erzielt wurden. Die Abbildung 4.22(a) zeigt eine erstellte Karte nach Abschluss des Lernverfahrens bei Untersuchung des Email-Konfigurationsdialogs. Die Karte zeigt die fertige Gruppierung der Benutzer anhand ihrer Interaktionsdaten nach insgesamt 10000 Lernschritten. Jede Farbe steht für eine Gruppierung. Die Zahlen innerhalb der Kreise geben die jeweiligen Teilnehmer der Gruppe an.

Auf Grund der zufälligen Initialisierung der Neuronen war die Karte zunächst ungeordnet. Der erste zufällig gewählte Testvektor passte die Neuronen in der Nachbarschaft der BMU an. Durch das exponentielle Absinken der Lernrate und der Nachbarschaftsgröße sowie der geeigneten Wahl der initialen Werte beider Parameter wurde eine schnelle Sortierung erreicht. Wie Kohonen [71] beschreibt, gibt es keine festen Regeln für die Wahl der initialen Parameter. Diese müssen durch Ausprobieren und Erfahrungswerte gefunden werden.

(a) Ergebnis nach 10.000 Schritten (b) Untrainierte Bereiche

Abb. 4.22: Darstellung der Interaktionsdaten in einer SOM (euklidischer Abstand)

Interpretation der Ausgabekarte

Die abgebildete Ausgabekarte gibt das Ergebnisse als Torus wieder. Aus diesem Grund sind die Randbereiche bei der Interpretation miteinander zu verbinden.

[8] Auf die Darstellung der Karten unter Verwendung des Hamming Abstandes wird verzichtet, da die Karten sich zwar im Aussehen unterscheiden, aber die Zuordnung der Teilnehmer zu den einzelnen Gruppen identisch war.

Die unterschiedlichen Farben innerhalb der Ausgabekarten entsprechen jeweils einer Gruppierung. Die gleichen Testvektoren werden durch die SOM auf den gleichen Bereich der Ausgabekarte abgebildet. Ähnliche Testvektoren werden in dicht nebeneinander liegenden Bereichen abgebildet. Je unähnlicher sich die Testvektoren sind, desto weiter entfernt werden sie auf der Ausgabekarte abgebildet. Die Ähnlichkeit der Testvektoren wird durch ihre Entfernung und nicht durch ähnliche Farbwahl gekennzeichnet. Dies bietet den Vorteil, dass Evaluatoren schnell Ähnlichkeiten bei den ermittelten Gruppierungen sehen können (auch in Schwarzweißbildern).

Für eine weitere verbesserte Interpretation wurde diese Version der Implementation dahingehend erweitert, dass untrainierte Bereiche transparent dargestellt werden können wie Abbildung 4.22(b) zeigt.

Der Evaluator kann nun verschiedene Attribute der Gruppen visuell darstellen lassen. Dazu verwendet er die Analysedialoge von SUESA. Die Abbildung C.6 im Anhang zeigt als Beispiel den Auswahldialog für die Untersuchung der Interaktionen bei der Email-Konfiguration. Mit diesem Dialog lassen sich Aspekte der Gruppen zeigen, indem nur die jeweiligen Gruppen angezeigt werden, bei denen die eingegebene Merkmalskombination zutraf. Dadurch kann sowohl gemeinsames als auch unterschiedliches Verhalten der Gruppen sichtbar gemacht werden.

Erstellte Karten der verwendeten Zeit in SUESA

SUESA bietet auch die Möglichkeit, die verwendete Zeit in einem Dialog als SOM darzustellen. Die Abbildung 4.23 zeigt eine Ausgabekarte (Zeit über den gesamten Versuch gemessen) für die verwendete Zeit bei Verwendung des euklidischen Abstandes. Bei Gruppierungen nach der Zeit handelt es sich im Gegensatz zu den Gruppierungen nach den gewählten Optionen nicht um die Reduktionen von Merkmalsvektoren. Die benötigte Zeit stellt in diesem Falle einen eindimensionalen Vektor dar.

Im Gegensatz zu den anderen Gruppierungen (vergleiche Abbildung 4.22(a)) entstehen bei dieser Art der Gruppierung kaum Gruppen mit mehreren Teilnehmern. Dies kommt daher, dass die verwendeten Zeiten selten gleich sind. Trotzdem kann die Ähnlichkeit des Verhaltens der Benutzer durch diese Art der Karte grafisch dargestellt werden. Je mehr Zeit die Benutzer in dem jeweiligen Dialog verbracht haben, desto dunkler wird der Vektor auf der Ausgabekarte dargestellt. Die Benutzer(-gruppen), die sehr wenig Zeit in dem untersuchten Bereich (z.B. die gesamte Aufgabe oder nur ein spezieller Dialog) verbracht haben, sind dagegen sehr hell dargestellt. Durch den Evaluator können nun Beziehungen zwischen der benötigten Zeit und den Gruppierun-

gen aus den Untersuchungen über die getätigten Einstellungen hergestellt werden. Dies soll an einem Beispiel verdeutlicht werden.

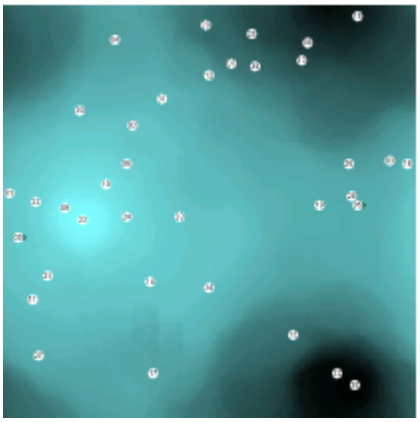
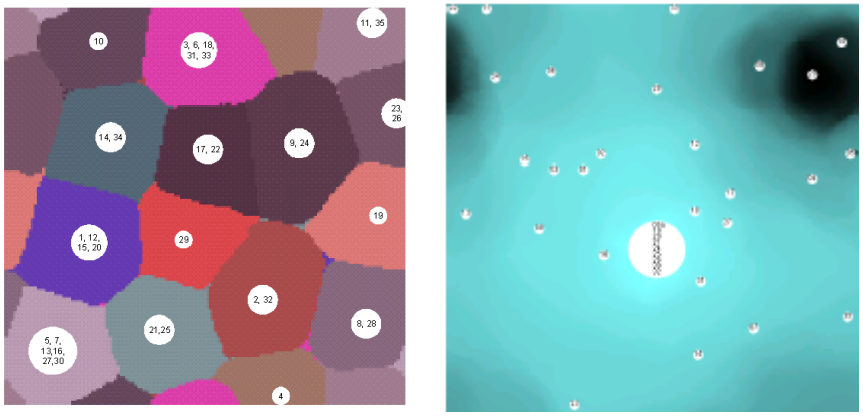


Abb. 4.23: SOM der verwendeten Zeiten (euklidischer Abstand) über das gesamte Experiment

Die Analyse nach Benutzergruppen in Abbildung 4.22 wurde um eine Analyse der benötigten Zeiten der Benutzer für einzelne Menüs erweitert. Die Gegenüberstellung mit dem Ergebnis für das Menü Email-Konfiguration ist in Abbildung 4.24 dargestellt.



(a) Gruppierung nach gewählten Optionen

(b) Darstellung der benötigten Zeiten der Email-Konfiguration

Abb. 4.24: Gegenüberstellung von SOMs nach Optionen und Zeiten

Nur einige wenige Benutzer sind in dunklen Bereichen der Ausgabekarte abgebildet. Dies bedeutet, dass die meisten Benutzer gar keine Zeit (weiß dargestellter Bereich) oder wenig Zeit (hell dargestellte Bereiche) in diesem Dialog

verwendeten. Die Gegenüberstellung der Ergebnisse mit dem Ergebnis aus 4.22 zeigt, dass für eine Gruppe hier ein Usability Problem vorlag, da eine Gruppe das Menü übersah (die Gruppe der Teilnehmer). Aus diesem Grund liegt für diese Gruppe dann zugleich ein Sicherheitsproblem vor, da sie die dort vorhandenen Maßnahmen nicht wahrnehmen können.

Die Benutzer dieser Gruppe bewerteten die Übersichtlichkeit der grafischen Oberfläche allerdings mit gut bis sehr gut. Das Aufgabenziel der Anwendung bestand in der möglichst sicheren Konfiguration des eigenen Systems. Diese Benutzer haben das Aufgabenziel nicht erreicht, weil sie Teile der Anwendung nicht erkannt haben. Sie erkennen diese Nichterreichung aber nicht. Aus diesem Grunde müssen Sicherheitsanwendungen auch dahingehend evaluiert werden, ob Benutzer in der Lage sind sie zu erkennen und zu benutzen.

Ein weiteres Ergebnis besteht darin, dass nur sehr wenig Benutzer viel Zeit in diesem Dialogschritt benötigten. Die Grafik in Abbildung 4.25 zeigt die Benutzer die im Intervall [0.33,1.0][9] liegen. Von diesen Benutzern verwendete nur ein Benutzer keinen Hilfeaufruf im Dialog. Die evaluierte Anwendung kann nun dahingehend untersucht werden, an welchen Stellen die Benutzer viel Zeit benötigten und wie dies verbessert werden kann. Wenn nur einige Benutzer in einem Dialog viel Zeit benötigen, spricht das dafür, dass diese Benutzer diesen Dialog nicht als intuitiv empfanden. Wenn der Dialog nicht intuitiv ist, ist das Fehlbenutzungspotential höher.

Abb. 4.25: Benutzergruppen die bei der Email-Konfiguration viel Zeit benötigten

Weitere Ergebnisse in SUESA

Bisher wurde gezeigt, dass mit SUESA Gruppierungen ausgehend von dem

[9] 1.0 entspricht der maximal benötigten Zeit

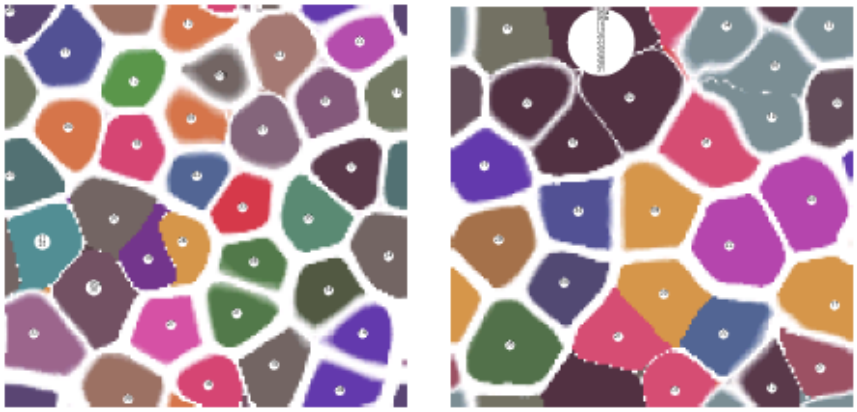
Verhalten der Benutzer gebildet werden können. Außerdem wurden Interpretationen der Ergebnisse und die Zuweisung von Merkmalen zu den Gruppen gezeigt. In diesem Abschnitt werden nun noch einige weitere Ergebnisse sowie Herausforderungen des Systems beschrieben.

Die weiteren Dialoge des Absicherungsprogramms wurden wie der beschriebene Beispieldialog (Email-Konfiguration) mit SUESA analysiert. Die Erstellung und Art der Interpretation der Ausgabekarten für diese Dialog ist analog zu dem skizzierten und wird hier daher nicht beschrieben. Über alle Dialoge wurde vor allem zwei große Benutzergruppen sichtbar. Die eine Benutzergruppe ignoriert dabei an jeder Stelle die angebotene Hilfefunktion, während eine andere große Gruppe jeden Hilfetext las.

Die detaillierte Betrachtung (Fragebogen) und Befragung von Testpersonen und Analyse ihres Verhaltens zeigte, dass das Verhalten der Testpersonen nicht von trivialen Parametern abhängt. Eine Testperson gab an, als System-Administrator in einem Unternehmen tätig zu sein. Aus diesen Gründen musste sie über sehr gute Kenntnisse auf dem Gebiet der IT-Sicherheit verfügen. Die Analyse der Ausgabekarten zeigte, dass diese Person sehr viel Zeit auf die Konfiguration und das Lesen der Hilfetexte verwendete. Dagegen verwendete ein weiterer Benutzer (ebenfalls Systemadministrator) wenig Zeit für die Konfiguration und las kaum Hilfetexte. Beide Versuchsteilnehmer konfigurierten das System nahezu identisch. Eine Unterscheidung anhand der benötigten Zeit (sehr unterschiedlich) oder der Erfahrungen durch den Beruf (sehr ähnlich) hätte bei diesen beiden Benutzern hinsichtlich der Gruppen für eine optimale IT-Sicherheit nicht ausgereicht.

Im Verlauf des SUESA-Versuches wurde neben einzelnen Dialogen auch die gesamte Anwendung hinsichtlich Benutzergruppen analysiert. Die Abbildung 4.26 zeigt die Gruppierung über die gesamte Anwendung. Die linke Grafik zeigt dabei die Gruppierung über sämtliche getätigten Konfigurationen. Die rechte Grafik zeigt dagegen die ausgewählten Hilfeoptionen. In beiden Fällen gab es 2^{20} Möglichkeiten bzw. potentiell mögliche Gruppierungen (und 35 Teilnehmer die auf diese Gruppen verteilt wurden.) Je dichter die Gruppen beieinander liegen, je ähnlicher war das Verhalten der Benutzer. In der linken Grafik wird dies durch sehr eng zusammen liegende Gruppen deutlich. Dies sind die Teilnehmer die Teile der Anwendung übersahen. Diese Benutzer sind ebenfalls als große Gruppierung in der rechten Grafik dargestellt.

Die Ergebnisse durch die Gruppierung werden undeutlicher, je größer die analysierten Teile des untersuchten Systems werden. Eine Untersuchung einzelner Bestandteile des Systems kann in den Ausgabekarten eher die Schwachstellen aufzeigen als die Untersuchung eines gesamten Systems.



(a) getätigte Konfigurationen (b) ausgewählte Hilfe

Abb. 4.26: Darstellung der getätigten Konfigurationen und ausgewählten Hilfe

4.3.3 Bewertung der aufgestellten Hypothesen und Zusammenfassung

Systeme sollten so gestaltet sein, dass sie die Benutzer zu korrektem Verhalten animieren. Benutzer haben allerdings unterschiedliches Wissen, Erwartungen und unterschiedliche Ziele. Aus diesem Grunde verhalten sich Benutzer selten gleich. Allerdings kann davon ausgegangen werden, dass sie sich ähnlich verhalten, wenn ihr Wissen und ihre Ziele ähnlich sind. Diese Benutzer mit ähnlichem Verhalten können zu Gruppen zusammengefasst werden. Daher werden Programme häufig für verschiedene Benutzergruppen angeboten. Eine optimale Einteilung der Benutzer in verschiedene Gruppen kann nur erfolgen, wenn ihr Vorwissen, ihre Erfahrungen und ihr Verhalten zur Kategorisierung verwendet werden.

Bei vielen Systemen werden Basisgruppen (z.B. Anfänger, normaler Benutzer und Experte) definiert, und die Benutzer sollen durch Lernerfolge zu Benutzergruppen mit erweiterten Fähigkeiten wechseln. Im Sicherheitsumfeld stellt die Anpassung der Systeme in Abhängigkeit von Lernerfolgen aber ein Problem dar. Benutzer die Fähigkeiten erlernen machen beim Erlernen Fehler. Fehler oder falsche Handlungen können Systeme aber sofort kompromittieren. Gibt der Benutzer beispielsweise persönliche Daten in ein System ein und lernt erst dann, dass dies ein Sicherheitsproblem darstellt, sind seine persönlichen Daten weiterhin bedroht, auch wenn er nun seine Daten nicht erneut eingibt. Aus diesem Grund müssen die Benutzergruppen bei sicherheitsrelevanten Funktionen bereits ohne Lernerfolge möglichst optimal zugewiesen

werden um Bedrohungen zu minimieren. Das Verhalten der Benutzer bei der Benutzung sicherheitsrelevanter Funktionen sollte gleich oder möglichst ähnlich zu dem angenommenen Verhalten sein.

Die automatische Gruppierung von Benutzern im Diskursbereich IT-Sicherheit anhand ihres Verhaltens wurde mit dem vorgestellten System SUESA untersucht. Das System ist in der Lage, Benutzer automatisch hinsichtlich ihres Interaktionsverhaltens in verschiedene Gruppen zu gruppieren. Die Ergebnisse wurden bei einer realen Fallstudie mit dem Fokus auf IT-Sicherheit gezeigt und miteinander verglichen.

Es zeigte sich, dass durch eine automatische Gruppierung mit SOMs, bei der keine vorgegebene Anzahl an Benutzergruppen festgelegt wird, sehr viele verschiedene Gruppen im Diskursbereich IT-Sicherheit gefunden wurden. Die Hypothese: *„Die Untersuchung des Verhaltens der Benutzer bei Anwendungen ergibt andere Benutzergruppen als die Gruppen: Experte, Normaler Benutzer und Anfänger“* wurde somit belegt. Eine durch viele Hersteller vorgenommene Gruppierung in die drei Benutzergruppen Anfänger, normaler Benutzer und Experte löst die Herausforderung der Programmanpassung durch Einführung von Benutzergruppen also nur sehr vage. Das Bedrohungspotential bleibt weiterhin sehr hoch, da sich Benutzer nicht gemäß dieser drei Gruppen, sondern viel individueller, verhalten. Zudem führt diese Einteilung nach Harris [52] zu verschiedenen weiteren Problemen, wie z.B. dazu, dass die Optionsvielfalt (im Expertenmodus) von der eigentlichen Aufgabenerledigung abhält.

SUESA gruppierte die realen Benutzer, und es konnten einige Merkmale und Gründe für die unterschiedlichen Gruppierungen gefunden werden. Diese reichen aber nicht aus, die Gruppen eindeutig zu bestimmen, so dass die zweite Hypothese: *„Durch die Untersuchung der Benutzerinteraktion lassen sich andere eindeutige Gruppen mit speziellen Attributen finden“* nicht belegt werden kann. Es konnten zwar einige Attribute gefunden werden, aber nicht unbedingt die relevanten und alle.

Trotzdem kann die vorgestellte Betrachtung und Untersuchung von Gruppen die Hypothesen: *„Die Untersuchung der Benutzerinteraktion kann gruppenspezifische Sicherheitsbedrohungen liefern.“ und “Durch die Untersuchung der Interaktion lassen sich Hinweise für Verbesserungen der Usability finden.”* belegen. Bei dem Experiment zeigte sich, dass einige Usability-Probleme mit SUESA gefunden werden konnten. Diese Usabilityprobleme führten dazu, dass einige Benutzer einige Systembestandteile überhaupt nicht oder falsch verwendeten. Diese beiden Vorgehensweisen stellen Bedrohungen für die IT-Sicherheit dar und müssen vermieden werden.

Weitere Möglichkeiten zur Erhöhung der IT-Sicherheit durch ein solches System bestehen darin, verschiedene Programmversionen hinsichtlich der Anzahl von Benutzergruppen zu überprüfen. So vermindert beispielsweise eine von einer größeren Gruppe korrekt verstandenen Bezeichnung eine potentielle Fehlbedienung. Mit SUESA gefundene Gruppierungen können so anzeigen, wo ein gemeinsames Grundverständnis (oder auch Unverständnis) eines untersuchten Systems vorliegt. Zusätzlich können mit SUESA einzelne Benutzer als Repräsentanten für unterschiedliche Benutzergruppen ausgewählt werden, um Testevaluationen durch repräsentativer Benutzertests zu ermöglichen.

Die vorgestellte Untersuchung mit SUESA zeigte, dass die Hypothese: *„Durch die Untersuchung der Interaktion von Benutzern mit Programmen lassen sich Gruppierungen zur Verbesserung der IT-Sicherheit finden.“* dadurch belegt wurde, dass gruppenspezifische Probleme gefunden wurden, deren Behebung zur Verbesserung der IT-Sicherheit führt. Allerdings zeigte die Untersuchung auch, dass bereits sehr viele Benutzergruppen bei der Benutzung eines sehr kleinen Programms gefunden wurden. Dies bedeutet, dass eine Anpassung für jede einzelne Gruppe nicht möglich bzw. kostengünstig ist.

Auch wenn die Ergebnisse zunächst aus dem Bereich sicherheitsrelevanter Software kommen, kann diese Methode und die damit erzielten Ergebnisse auch auf andere Bereiche übertragen werden.

SUESA zeigte, dass die alleinige Analyse nach getätigten Entscheidungen in einem Programm zur Einteilung der Benutzer nicht ausreicht. Aus diesem Grund wird im Folgenden ein System vorgestellt, bei dem die Gruppierung der Benutzer durch einen weiteren Aspekt erweitert wird.

4.4 Erhöhung der IT-Sicherheit durch Analyse von Unsicherheit

In diesem Abschnitt soll das Konzept der Verbesserung von IT-Sicherheit durch Gruppierung von Interaktion um eine weitere Idee ergänzt werden. Das im letzten Abschnitt vorgestellte Konzept gruppierte Benutzer anhand verschiedener Kriterien bei der Benutzung von Software. Zu diesen Kriterien gehörten die benötigten Zeiten bei der Erledigung von Aufgaben und die ausgewählten Einstellungen. Diese Kriterien sollen nun um Hinweise ergänzt werden, an welchen Stellen die Benutzer unsicher bei ihrem Verhalten waren.

Im Fokus von IT-Sicherheit stellen Handlungen, bei denen sich Benutzer unsicher waren, ein erhöhtes Bedrohungspotential dar, da an diesen Stellen das Fehlbedienungspotential höher ist.

4.4.1 Die Idee von der Optimierung der IT-Sicherheit durch Beobachtung von Unsicherheit

Die Sicherheit von Systemen ist wie zuvor beschrieben zum einen durch Angriffe auf die Systeme bedroht, aber auch durch Fehlverhalten seiner Benutzer. So können Angreifer versuchen schützenswerte Daten zu erspähen, indem sie Schutzmechanismen überwinden. Die gleichen Daten können aber auch durch Fehlverhalten auf Seiten der Benutzer freigegeben werden. Die Bedrohung, die durch die Benutzer dabei für die Systeme ausgeht, kann aktiver oder passiver Natur sein. Aktiv bedeutet in diesem Kontext, dass die Benutzer absichtlich die Daten bedrohen, indem sie die Daten stehlen oder sabotieren. Diesem Sachverhalt wird durch Anwendung der Theorie der Multilateralen Sicherheit ([100],[101]), bei der jeder Benutzer eigene Interessen hat und somit als Angreifer gilt, Rechnung getragen. Dieser Aspekt der Bedrohungen durch Benutzer wird im Folgenden nicht weiter betrachtet.

Eine weitere Bedrohung geht von passiven Angriffen durch die Benutzer aus. Ein passiver Angriff liegt vor, wenn der Benutzer unabsichtlich das System angreift. Benutzer stellen eine passive Bedrohung für Systeme dar, wenn sie Systeme falsch interpretieren, falsche Erwartungen über die Auswirkungen ihres Handelns haben oder sich unsicher verhalten. Während die ersten zwei Kategorien immer einen Angriff darstellen, stellen unsichere Handlungen eine potentielle Bedrohung dar. Unsichere Handlungen beinhalten die Möglich-

keit, ein Fehlverhalten zu erzeugen. Die folgenden Schwachstellen bilden die Möglichkeit für passive Angriffe. Benutzer interpretieren ein System falsch und tätigen falsche Entscheidungen, sie überblicken die Folgen ihrer Handlungen nicht, oder sie sind sich unsicher bei der Benutzung.

Ein Erkennen dieser Schwachstellen und deren Minimierung stellt eine Verbesserung der IT-Sicherheit dar. Während das im letzten Abschnitt vorgestellte Konzept die Benutzer anhand der ersten zwei Schwachstellen gruppierte, wird nun ein Konzept vorgestellt, welches die „Unsicherheit“ beim Verhalten der Benutzer untersucht.

Die Idee besteht darin, protokollierte Interaktionsdaten dahingehend zu untersuchen, ob sich darin potentiell unsichere Handlungen zeigen lassen. Eine geeignete Aufbereitung der Stellen, an denen sich Benutzer „unsicher“ verhielten, gibt Evaluatoren Anhaltspunkte wo die Systemsicherheit verbessert werden kann. Die Benutzung an diesen Stellen kann dann durch Maßnahmen des Usability-Engineerings so umgestaltet werden, dass sich Benutzer sicherer bei ihren Handlungen sind, die richtigen Entscheidungen treffen und verstehen was ihr Handeln für Konsequenzen hat. Dies kann z.B. dadurch erfolgen, dass Benennungen geändert werden, Bearbeitungsreihenfolgen verändert oder zusätzliche Hilfen angeboten werden. Durch die Vermeidung von Fehlverhalten der Benutzer wird die Sicherheit der Systeme erhöht.

Um diese Idee zu evaluieren wird im folgenden Abschnitt die folgende Hypothese untersucht.

Auf der Idee basierende Hypothese

Aus den Daten, die bei der Protokollierung des Verhaltens im letzten Abschnitt gesammelt wurden, lassen sich weitere Aspekte zur Minimierung von Bedrohungen bzw. zur Erhöhung der IT-Sicherheit extrahieren. Eines dieser Kriterien kann die Unsicherheit bei getätigten Entscheidungen sein.

Zur Überprüfung der Hypothesen entwickeltes Konzept

Um die oben aufgestellte Hypothese zu untersuchen wird in dieser Arbeit das folgende Konzept verwendet:

Benutzer interagieren mit einem beliebigen System. Die Interaktion wird protokolliert und anschließend hinsichtlich Unsicherheit analysiert. Dazu werden die Ergebnisse für Evaluatoren aufbereitet und interpretiert.

Die Beobachtung des Verhaltens bei der Interaktion der Benutzer mit einer Anwendung kann wertvolle Informationen darüber liefern, ob sie mit der Anwendung zufrieden sind und wo potentielle Probleme bei der Benutzung liegen. Daher wird das Verhalten der Benutzer mit unterschiedlichen Verfahren analysiert und interpretiert. Verschiedene Datengewinnungsmethoden werden bei den unterschiedlichen Evaluierungsmethoden in Kapitel 2.3.3 eingesetzt. Je nach Evaluierungsverfahren können zum Beispiel Daten durch Befragung (Fragebögen oder Interviews), Eyetracking oder Eventrecording gesammelt und analysiert werden. Beim Eventrecording werden dabei verschiedene Eingaben des Benutzers aufgezeichnet, um später analysiert werden zu können. Dazu gehören zum Beispiel Tastatureingaben, Mausbewegungen oder aber auch die Betätigung eines Joysticks.

In diesem Abschnitt wird als Technik die Untersuchung des Mausbewegungsverhaltens verwendet. So können zum einen die protokollierten Daten des letzten Abschnittes verwendet werden und zum anderen kann die Benutzung der Maus bei Computersystemen relativ leicht untersucht werden.

4.4.2 Praktische Evaluation des aufgestellten Konzeptes

Ein Verfahren zur Untersuchung des Mausbewegungsverhaltens bilden dabei die sogenannten *Mousemaps*. Mit Hilfe von Mousemaps werden die Mausbewegungen der Benutzer aufgezeichnet und visualisiert. Mousemaps sind 2-dimensionale Grafiken, auf der die Mausbewegungen einer Person dargestellt werden. Mousemaps liefern nur eine Darstellung der Mausbewegungen, jedoch keine Interpretation. Der Vorteil von Mousemaps gegenüber anderen Methoden wie einer Videoaufzeichnung (vergleiche [50]) besteht darin, dass sie weniger Speicherplatz benötigen und trotzdem eine übersichtliche Darstellung zur Interpretation liefern [48] und [91]. Als Nachteile stehen dem gegenüber, dass nicht alle Systeme eine Maus als Steuerungssystem verwenden, und dass sich einige Aspekte (z.B. auf und zuklappen von Dialogen) durch Mousemaps schlecht visuell darstellen lassen.

Für die Untersuchung in dieser Arbeit werden Mousemaps auf Grund der Vorteile, und weil sie sich aus den bereits erhobenen Daten erstellen lassen, verwendet. Sie sollen nicht alle Schwachstellen eines Systems ermitteln. Sie dienen nur als ein Verfahren um zu belegen, dass sich Aspekte für „Unsicherheit“ und somit Schwachstellen in IT-Systemen durch Analyse des Verhaltens finden lassen. Aus den im letzten Abschnitt aufgezeichneten Daten werden zur besseren visuellen Darstellung und Evaluation Mousemaps generiert. Diese Mousemaps werden dann dahingehend untersucht, ob sich Merkmale für

eine potentielle unsichere Benutzung oder „bedrohliche“ Situationen erkennen lassen.

Mit Mousemaps können Probleme an der Gebrauchstauglichkeit der Software erkannt werden, da einige Anwender beim Lesen eines Textes die Maus bzw. den Mauszeiger als Lesehilfe benutzen. Ein Indiz für ein Problem an der Lesbarkeit ist das wiederholte Verfolgen einzelner Zeilen. [91]. Somit können verschiedene Usability-Richtlinien mit Mousemaps überprüft werden. So zum Beispiel die Einhaltung des Konzeptes der zusammen liegenden Buttons.

Ein weiterer Aspekt der Gebrauchstauglichkeit, der durch Mousemaps analysiert werden kann, ist das Effizienzkriterium [2]. Das Effizienzkriterium ist die Minimierung der Steuerbewegungen. Diese sind durch die Strecke, die mit der Maus zurückgelegt wurde, als Distanz messbar. Voraussetzung ist dabei, dass die Maus das dominante Steuerinstrument ist. Die Effizienz kann nur mit der Distanz bewertet werden, wenn die Person nicht nur mit den Augen nach Komponenten auf der graphischen Oberfläche sucht, sondern auch Suchbewegungen mit der Maus tätigt.

Neben den Aspekten der Usability können Mousemaps einen weiteren Aspekt visualisieren. Sie können verschiedene unbewusste Aspekte im Verhalten von Benutzern anzeigen, wie zum Beispiel entspannte Normalzustände, Stress, Zeitdruck oder Sicherheit bei der Betätigung ([48] und [49]). Die Anwahl von Aktionen durch direkte Anwahl der Betätigung (z.B. Sofortiges Betätigen eines Buttons) zeigt dabei Sicherheit bei der getroffenen Entscheidung an. Demgegenüber zeigt ein Verweilen über den Steuerelementen oder das nicht direkte Anwählen der Elemente oder das wiederholte Betätigen (Wechsel zwischen *„Einstellung ein“* und *„Einstellung aus“*) eine Unsicherheit bei der Benutzung an.

Im Kontext der Evaluation des Verhaltens von Benutzern können Mousemaps verschiedene Arten von Bedrohungen anzeigen. Sie können sicherheitsrelevante Usability-Probleme aufdecken und unsicheres Verhalten der Benutzer anzeigen. Im Folgenden wird ein implementierter Prototyp sowie eine damit gemachte Untersuchung vorgestellt, bei der die Mausbewegungen von Benutzern bei der Benutzung sicherheitsrelevanter Funktionen bezüglich der Sicherheit untersucht wurden. Das System erstellt aus den Protokolldateien des letzten Abschnittes Mousemaps und stellt Möglichkeiten zur weiteren Untersuchung bereit.

Das implementierte System

Im Folgenden wird das System GAMJA (Generate and Analyze Mousemaps from Jacareto-XML-Files) vorgestellt, welches die mit SUESA aufgenommenen Interaktionsdaten hinsichtlich der Mausbewegungen der Benutzer analysiert. Abbildung 4.27 zeigt den konzeptionellen Aufbau des Systems.

Mit GAMJA werden die Mausbewegungen von Benutzern eines Systems in Form von Mousemaps dargestellt. Benutzer interagieren mit einem zu testenden Programm. Ihre Mausbewegungen werden dabei mit dem Open Source Programm Jacareto aufgenommen[10]. Aus den von Jacareto generierten XML Dateien werden Mousemaps erstellt. Weiterhin liefert GAMJA neben den eigentlichen Mousemaps auch weitere Analysedaten für die spätere Interpretation.

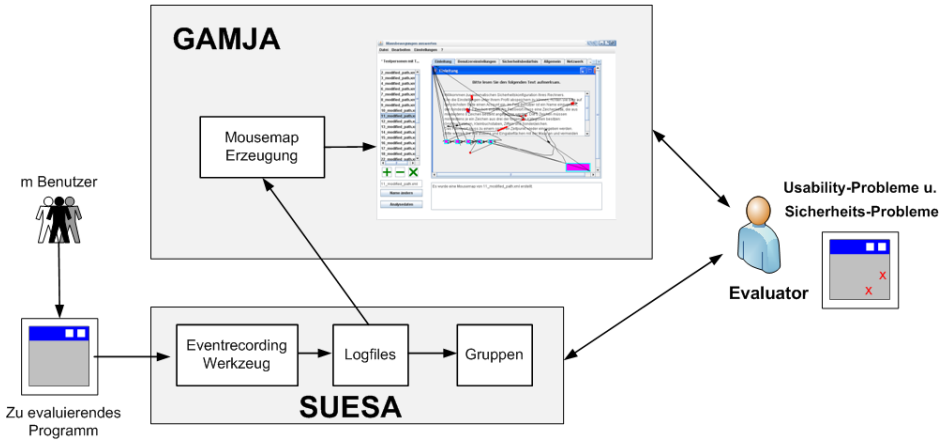


Abb. 4.27: GAMJA: Generate and Analyze Mousemaps from Jacareto-XML-Files

Nach Erstellung der Logfile-Dateien (XML-Dateien) in SUESA filtert das System GAMJA diese nach den, zur Erstellung einer Mousemap, relevanten Daten. Aus diesen wird für jeden Benutzer eine Mousmap erstellt. Anschließend können die Mousmaps verglichen und analysiert werden.

Die Oberfläche des Systems sowie eine geöffnete Mousemap ist in Abbildung 4.28 zu sehen. Bei den aus den XML-Dateien erstellten Mousemaps werden Mausbewegungen als normale Linien dargestellt. Je dicker die Linien desto höher ist die benötigte Zeit für die Strecke. Um zu verhindern, dass die Linien zu dick werden und dadurch die Mousemap unübersichtlich wird, verändert sich zusätzlich noch die Farbgebung. Die Farbgebung kann vom Benutzer

[10] Bei der realen Implementation wurde die für SUESA entwickelte Event-Recording-Komponente verwendet und eingebunden.

frei gewählt werden. Wird eine Komponente auf der graphischen Oberfläche mit dem Mauszeiger fokussiert, wird dieses Element eingerahmt. Die Farbe des Rahmens ist ebenfalls frei wählbar. Wenn eine Komponente angewählt wurde, wird diese wiederum mit einer selbst gewählten Farbe ausgefüllt.

GAMJA zeigt die Mausbewegungen in verschiedenen Fenstern der graphischen Benutzeroberfläche auf unterschiedlichen Mousemaps an. Die Mousemaps befinden sich in einzelnen Tabs bzw. Reitern. Zusätzlich wird für jede Versuchsperson ein Analyseblatt erstellt, auf diesem stehen dem Usability-Experten Daten zur Analyse zur Verfügung. So wird zum Beispiel die zurückgelegte Strecke angezeigt. Die zurückgelegte Strecke könnte zu Vergleichszwecken mit bloßem Auge nicht genau ermittelt werden. Über alle Versuchspersonen werden die Daten ebenfalls gesammelt um Durchschnittswerte zu generieren. Bei der Betrachtung von Mousemaps und der Zuhilfenahme der Analysedaten durch einen Usability-Experten kann dieser Probleme mit der Gebrauchstauglichkeit aufdecken. Zusätzlich können bestimmte Kriterien automatisch analysiert und bewertet werden, so dass eine automatisierte Benutzerklassifizierung durch ein Programm mit Hilfe der Mausdaten stattfinden kann. Auch eine automatisierte Analyse bezüglich der Gebrauchstauglichkeit ist im begrenzten Umfang möglich. Zum Beispiel Ermittlung von Durchschnittsberechnungen für Mausdistanzen und deren Varianz.

Diese Daten können dann bei Programmen aus dem IT-Sicherheitskontext zur Ermittlung und Behebung von Bedrohungen benutzt werden, wie das folgende Experiment zeigt.

Das durchgeführte Experiment

GAMJA wurde mit dem Fokus entwickelt, Sicherheitsprobleme zu ermitteln und anzuzeigen. Aus diesem Grunde ist der Versuchsaufbau analog zu dem Versuchsaufbau mit dem System SUESA (vergleiche Abschnitt 4.3). Nur die Analyse der Daten unterscheidet sich.

Versuchsaufbau und Ablauf

Die Versuchspersonen erhielten einen Fragebogen und mussten mit Hilfe des im Abschnitt 4.3 vorgestellten Testprogramms einen Computer konfigurieren. Bei der Konfiguration mit Hilfe des Testprogramms waren einige Parameter eingebunden, bei denen alle Versuchsteilnehmer unsicher bei der Einstellung sein sollten. Diese dienten dazu, Referenzwerte für unsicheres Verhalten der Benutzer zu erhalten. Als Beispiel diene hierzu die Konfiguration der Option: *SMPT-Over-Pop aktivieren?*. Demgegenüber gab es Einstelloptionen, die als

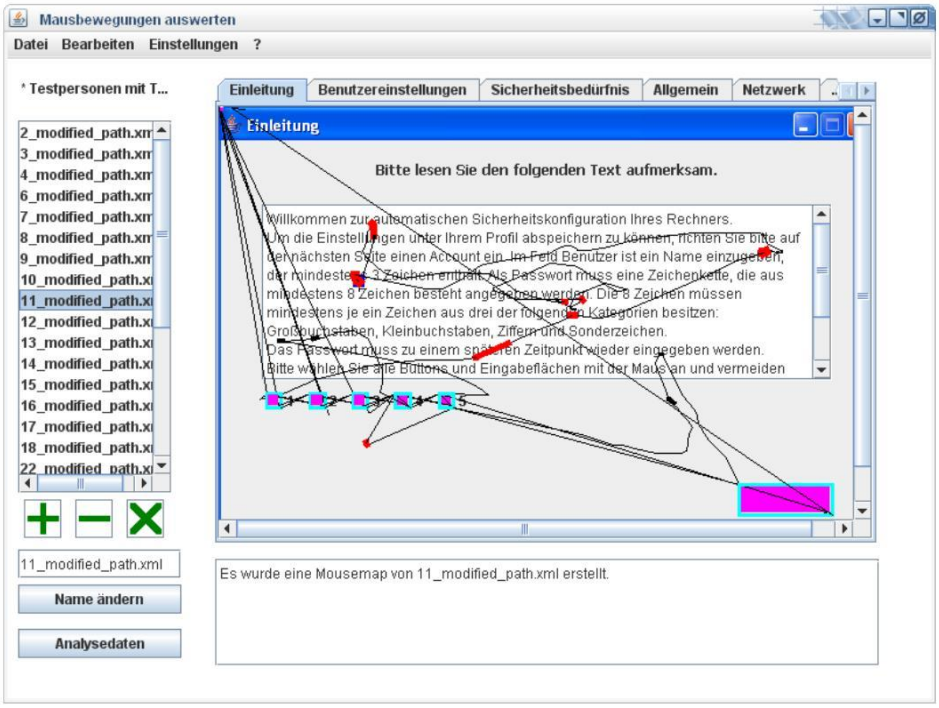


Abb. 4.28: Mousemap in GAMJA

Referenz für sicheres Verhalten dienen sollten: *SPAM Filter aktivieren?*.

In den Fragebögen waren zu diesem Zweck Referenzfragen integriert.

- Referenzfrage: Welche Auswirkungen hat die Einstellung: SMPT-Over-Pop aktivieren?
- Referenzfrage: Welche Auswirkungen hat die Einstellung: SPAM Filter aktivieren?

Die Referenzfragen sollten zeigen, was die Benutzer unter den Optionen verstanden hatten. Die Ergebnisse zeigten neben anderen Daten aus den Fragebögen (Beruf, eigener PC, ...) wie weit sich Benutzer mit der Thematik IT-Sicherheit auskannten. Der Grad der Kenntnis der Thematik wurde dann als Grundlage für die Referenz bezüglich der Sicherheit verwendet.

Die Antworten der einzelnen Fragen konnten mit den Ergebnissen der Mousemaps in Relation gesetzt werden. Dies zeigte, wie sich das Mausverhalten der Benutzer in Abhängigkeit davon, ob sie sich sicher bei der Einstellung waren und ob sie wussten was ihre Einstellung wirklich bedeutete, änderte. Außerdem wurden in dem Fragebogen noch sämtliche Hilfetexte vorgestellt und

die Teilnehmer sollten die Unterstützung durch den Hilfetext auf einer Skala von 1 (sehr gut) bis 5 (sehr schlecht) angeben. Bei obiger Einstellmöglichkeit *„SMPT-Over-Pop aktivieren?“* lautete zum Beispiel der Hilfetext:

- Setzen sie diese Einstellung nur, falls ihr Provider dies erfordert.

Mit diesem Versuch sollten sich die drei oben beschriebenen problematischen Szenarien (unsicheres Verhalten, falsche Erwartungen/Interpretationen oder Benutzer die die Konsequenzen nicht überblicken) bei der Interaktion in Mousemaps untersucht werden. Vor Beginn des Versuches mit realen Teilnehmern wurden einige weitere Experiment-Hypothesen aufgestellt. Diese dienten dazu die zuvor in diesem Abschnitt aufgestellte Hypothesen bewerten zu können.

Experiment-Hypothese 1: Zu Beginn des Versuches soll der Benutzer sein Sicherheitsbedürfnis mit genau einem Wert auswählen. Selektiert der Benutzer bei der Einstellung des Sicherheitsbedürfnisses jedoch mehrere Checkboxen ist er sich an dieser Stelle unsicher[11].

Experiment-Hypothese 2: Fokussiert der Benutzer Konfigurationseinstellungen, wählt sie aber nicht aus, denkt er an dieser Stelle über die Konfigurationseinstellungen nach und ist sich unsicher.

Experiment-Hypothese 3: Unerfahrene unsichere PC-Benutzer wählen mehr Tooltips als erfahrener Benutzer aus.

Experiment-Hypothese 4: Unerfahrene Benutzer benötigen eine längere Wegstrecke mit der Maus.

[11] Es kann nur genau ein Sicherheitsbedürfnis ausgewählt werden. Allerdings kann es der Benutzer vor der Bestätigung mehrfach ändern.

Ergebnisse und Wertung der Hypothesen

Für die Evaluation mit GAMJA wurden die Daten der 35 Versuchsteilnehmer am SUESA Versuch verwendet. Die Stammdaten zu diesen Benutzern befinden sich im Kapitel zu SUESA. Nachdem die Versuchsteilnehmer den Versuch durchgeführt und ihre Fragebögen ausgefüllt hatten, wurden aus den Antworten der Fragebögen zahlreiche Ergebnisse extrahiert. So wurden die Teilnehmer ausgehend von ihren Antworten beispielsweise in Kategorien (erfahren bei der jeweiligen Aktion im Gegensatz zu unerfahren) bei den unterschiedlichen Bereichen eingeteilt. Aus diesen Ergebnissen wurden Überlegungen für mögliche Relationen zu den Mousemaps generiert, die im nächsten Schritt verifiziert werden sollten.

Für die Auswertung der Ergebnisse wurde die Vereinfachung, dass unerfahrene Benutzer auch „unsicher“ im Umgang mit der Software sind, getroffen. Diese Vereinfachung kam durch empirische Beobachtung bei der Durchführung des Versuchs. Unerfahrene Benutzer versuchten sich bei sehr vielen ihrer Handlungen beim Versuchsleiter rückzuversichern, da sie sich unsicher über ihre Handlungen waren. Erfahrene Benutzer hatten einen sicheren Umgang mit dem System.

Experiment-Hypothese 1: Aus der Menge der Teilnehmer wählten drei der 35 Versuchsteilnehmer (das entspricht ca. 8%) ein Bedürfnis aus und veränderten dann ihre Entscheidung. Der Hypothese nach sollten diese drei Versuchsteilnehmer sich bei der Einschätzung ihres Sicherheitsbedürfnisses nicht sicher sein. Ein Vergleich der Eintragungen in den Fragebögen mit der Auswahl in dem System ergab, dass genau diese drei Teilnehmer im Fragebogen angegeben hatten, dass ihnen die Sicherheit des Systems unwichtig sei. Aus diesem Grund wählten diese drei Personen schließlich die Einstellung “Schnell, komfortabel und unsicher“. Einer dieser drei Teilnehmer gab an, gute Kenntnisse im Umgang mit sicherheitsrelevanter Software zu besitzen. Die anderen beiden Teilnehmer bescheinigten sich Grundkenntnisse.

Die Analysedaten aus den Mousemaps zeigen folgende Ergebnisse. Die drei Teilnehmer wählten im Durchschnitt jeden dritten Tooltip aus (das entspricht 6,6 Tooltips). Damit liegen sie über dem Durchschnitt der Versuchsteilnehmer der bei 4.75 Tooltips lag (siehe Anhang D.1). Die zurückgelegte Wegstrecke dieser drei Versuchsteilnehmer beträgt im Durchschnitt 147927 Pixel. Dies liegt über dem Durchschnitt aller Versuchsteilnehmer (131676 Pixel). Dieses Ergebnis würde die Hypothese belegen und ebenfalls die hohe Auswahl an Tooltips erklären.

Für die Überprüfung der weiteren Hypothesen werden nur noch die Interaktionsdaten der Teilnehmer verwendet, die alle Menüs bearbeitet hatten. Die Daten der sieben Teilnehmer, die teilweise Menüs übersehen hatten (vergleiche Abschnitt 4.3 zu SUESA), werden nicht verwendet. Die betrachteten 28 Versuchsteilnehmer hatten die Wahl insgesamt 20 Konfigurationseinstellungen, aufgeteilt auf vier Menüs, auszuwählen. Daraus ergeben sich insgesamt $2^{20} = 1048576$ unterschiedliche Möglichkeiten das Testprogramm zu konfigurieren. Zu jedem der 20 Konfigurationsmöglichkeiten kann genau ein Tooltip ausgewählt werden. Der Button des Tooltips muss aktiviert werden um den Hilfetext anzuzeigen. Die Fokussierung des Tooltips reicht nicht um den Hilfetext anzuzeigen. Im Eventrecordingtool von SUESA wird protokolliert, ob eine Konfigurationscheckbox bzw. Tooltipcheckbox fokussiert und oder aktiviert wird. In GAMJA werden fokussierte Checkboxen durch einen farbigen Kreis umrandet dargestellt. Für jeden Konfigurationsmöglichkeit ergeben sich somit $2^4 = 16$ unterschiedliche Handlungsoptionen durch den Teilnehmer ausgehend von den vier Zuständen: Konfiguration aktiviert, Konfiguration fokussiert, Tooltip aktiviert und Tooltip fokussiert.

Experiment-Hypothese 2: Die zugehörigen Handlungsoptionen sind in der Tabelle 4.9 dargestellt. Die Handlungsoption Nr. 10 wurde dabei von keinem Teilnehmer ausgewählt. Dies kann damit erklärt werden, dass die Auswahl eines Tooltips Unsicherheit zeigt. Das gradlinie Anwählen der Hilfefunktion (Tooltip) ohne Verharren (Fokussierung) würde dagegen Sicherheit zeigen. Die Auswahl der Option elf zeigt, dass der Benutzer bei beiden Checkboxen diese fokussiert, dann aber zögert sie auch zu aktivieren. Dies zeigt ebenfalls Unsicherheit bei der Benutzung. Von neun Versuchsteilnehmern wurde diese Option insgesamt 12 mal ausgewählt (ca. 2%). Die Option neun wurde von 20 Teilnehmern insgesamt 55 ausgewählt. Dies entspricht ungefähr 9,8% der 560 Optionen. Bei dieser Option hat der Benutzer die Konfigurationsmöglichkeit nicht verstanden und zur Hilfe den Tooltip ausgewählt. In 160 der 560 möglichen Fälle wurde nur die Checkbox fokussiert, aber nichts ausgewählt. Dies entspricht ca. 28 %.

Zusammengefasst wurden die vier Fälle 9-12 227 mal ausgewählt. Dies entspricht ca. 40,5 % der Gesamtmöglichkeiten. Diese hohe Zahl lässt sich damit erklären, dass keine der Versuchspersonen das Testprogramm des Versuchsaufbaus vorher kannte. Aus diesem Grund ist zu erklären, dass die Teilnehmer an vielen Stellen zögerten und kurz über die Möglichkeiten des Systems nachdachten. Die Hypothese ist damit in diesem Experiment belegt worden.

Nr.	Konfiguration aktiviert	Konfiguration fokussiert	Tooltip aktiviert	Tooltip fokussiert
8	...			
9	0	1	1	1
10	0	1	1	0
11	0	1	0	1
12	0	1	0	0
13	...			

Tab. 4.9: Handlungsoptionen für fokussierte aber nicht ausgewählte Einstellungen

Experiment-Hypothese 3: Die Tabelle D.1 im Anhang zeigt die Wahl der Tooltips durch die 28 Versuchsteilnehmer in Abhängigkeit ihrer Selbsteinschätzung über ihr Sicherheitsbedürfnis.

Mit Ausnahme der Teilnehmer, die bei sich selbst einen sehr guten Kenntnisstand einschätzten, zeigt die Tabelle, dass Benutzer mit zunehmendem (selbst eingeschätzten) Kenntnisstand der IT-Sicherheit weniger Tooltips auswählten. Dies macht auch Sinn, da sie mehr Einstellungsoptionen kennen sollten je höher ihr Kenntnisstand ist.

Die detaillierte Untersuchung der beiden Teilnehmer, die einen sehr guten Kenntnisstand einschätzten, bringt folgende Ergebnisse:

- Teilnehmer zehn wählte 3 Tooltips (und bestätigt damit die Hypothese)
- Teilnehmer acht wählte dagegen 13 Tooltips aus. Die Auswertung seines Fragebogens erklärt die Diskrepanz bei der Auswahl der Tooltips. Teilnehmer acht vermerkte in seinem Fragebogen, dass ihm unklar sei, wie weitreichend die Einstellungen im Testprogramm gemeint sind. Die häufige Auswahl der Tooltips ist bei Teilnehmer acht nicht darauf zurückzuführen, dass er die Konfigurationsmöglichkeit nicht versteht, sondern dass er weitere Details zur Konfiguration wünscht (z.B. ob durch die Konfigurationsmöglichkeit interne Firewall deaktivieren eine andere frei geschaltet wird.).

Werden der Teilnehmer, der keine Einstufung der Sicherheitskenntnisse abgab, und Teilnehmer acht aus der Tabelle D.1 entfernt, ist zu sehen, dass diese Hypothese durch die Daten in GAMJA belegt wurde.

Experiment-Hypothese 4: Der Grundgedanke bei dieser Hypothese bestand darin, dass unerfahrene Benutzer nicht so zielstrebig wie erfahrene Benutzer Systemeinstellungen auswählen können. Um die Hypothese zu überprüfen wurde die Tabelle D.2 erstellt. In dieser Tabelle sind die Mausstrecken der 27 Benutzer eingetragen, die alle Menüs des Testprogramms bearbeiteten und eine selbst eingeschätzte Aussage über ihren IT-Kenntnisstand tätigten. In der Tabelle ist ersichtlich, welche Benutzer eine längere und welche eine kürzere Wegstrecke als der Durchschnitt zurücklegten. Der Durchschnitt betrug 143787 Pixel. Aus der Gruppe der Teilnehmer, die gute oder sehr gute Kenntnisse angaben, liegen neun von dreizehn Teilnehmern unter dem Durchschnitt. Dies entspricht ca 82%. Der Durchschnitt dieser Gruppe beträgt: ca. 134728 Pixel. Die anderen 14 Teilnehmer gaben an keine oder nur Grundkenntnisse zu haben. Der Durchschnitt dieser Gruppe liegt mit ca. 151703 Pixeln über dem Gesamtdurchschnitt. Auch wenn in dieser Gruppe sieben Teilnehmer über dem Gesamtdurchschnitt von 143787 Pixeln lagen und sieben darunter, belegen die jeweiligen Durchschnittswerte der Gruppen diese Hypothese. Eine Analyse der Mousemaps zeigt zudem, dass (nur) einige Teilnehmer nicht alle Menüs bearbeiteten. Diese gaben an über keine oder Grundkenntnisse zu verfügen. So hatte Versuchsteilnehmer Nr. 24 zum Beispiel das Email-Menü nicht bearbeitet.

In der Tabelle 4.10 sind die Ergebnisse der oben aufgestellten Hypothesen zur besseren Veranschaulichung grafisch dargestellt.

Nr.	Hypothese	Ergebnis
Experiment-Hypothese 1	Selektion Sicherheitsbedürfnis	erfüllt
Experiment-Hypothese 2	Fokussierung Konfigurationseinstellungen	erfüllt
Experiment-Hypothese 3	Anzahl Tooltips	erfüllt
Experiment-Hypothese 4	Länge der Mausstrecke	erfüllt

Tab. 4.10: Ergebnisse der aufgestellten Hypothesen in GAMJA

Die Erkenntnisse aus den oben dargestellten Hypothesen können dazu benutzt werden, Benutzergruppierungen hinsichtlich ihrer Erfahrungen in Mousemaps automatisch zu generieren. Somit kann GAMJA die Ergebnisse automatischer Klassifizierungen um den Aspekt der „unsicheren Verwendung“ erweitern.

4.4.3 Zusammenfassung und Ausblick

Unsichere Benutzer stellen für Systeme eine Bedrohung dar, da sie durch ihr Verhalten falsche Entscheidungen treffen können. Die Evaluation, an welchen Stellen Benutzer bei der Benutzung von Systemen unsicher sind, kann daher zu einer Verbesserung von Systemsicherheit führen. Die zu Beginn aufgestellte Hypothese konnte belegt werden, indem Interaktionsdaten mit Hilfe von Mousemaps so aufbereitet wurden, dass sie Evaluatoren Anhaltspunkte für Unsicherheit zeigten.

Bei der prototypischen Evaluation des Konzepts konnten Benutzer durch die Bereitstellung von Durchschnittsdaten in Gruppen bezüglich ihres Sicherheitsverhaltens gruppiert werden. Ein Kriterium dafür war zum Beispiel die durchschnittliche Wegstrecke innerhalb des System. Es wurden die durchschnittlichen Wegstrecken für die Gruppen „Erfahren in einer Kategorie“ (sicher) und „Unerfahren in einer Kategorie“ (unsicher) gebildet und miteinander verglichen. Dabei zeigte sich, dass Benutzer mit guten Kenntnissen im Durchschnitt kürzere Wegstrecken mit der Maus zurücklegten als Benutzer ohne Erfahrungen in dem jeweiligen Gebiet. Benutzer, die sich bei den Aktionen sicher waren, setzten diese zielstrebig um. Dagegen schweiften unsichere Benutzer mit ihrer Aufmerksamkeit zu anderen Aspekten ab, oder versuchten weitere Informationen zu erhalten bevor sie eine Auswahl trafen. Allerdings reicht dieses Kriterium für sich genommen zur Unterscheidung nicht aus. Einige erfahrene Benutzer legten längere Wegstrecken als der Durchschnitt der unerfahrenen Benutzer zurück. Einige unerfahrene Benutzer wählten dagegen ihre Einstellungen gradlinig aus.

Ein weiteres Ergebnis lieferte die Untersuchung der zwar fokussierten aber nicht ausgewählten Einstellmöglichkeiten. In diesem Falle überlegten die Benutzer, was die Einstellung auslösen würde. Die Relation zu den Mousemaps ergab, dass erfahrene Benutzer kaum Dinge fokussieren, die sie nicht auswählen. Einen Spezialfall stellten die ausgewählten Hilfetexte des Programms dar. Auch sie wurden durch das implementierte GAMJA System aufbereitet. So zeigte das System, wie viele Hilfetexte ein Benutzer auswählte und bei wie vielen er dann die Einstellung nicht auswählte. Auch die Wahl von Hilfetexten dient als Kriterium für Unsicherheit. Da in vielen Programmen Hilfetexte nicht in dieser Form zur Verfügung stehen, kann dieses Ergebnis nur für Spezialfälle dienen.

Des Weiteren zeigte der Versuch mit GAMJA, dass für einige Bereiche die erstellten Mousemaps der Versuchspersonen sehr unterschiedlich (z.B. anonymen Netzwerkzugriff verhindern) waren. Die Rücksprache mit den Ver-

suchspersonen ergab, dass es dafür zwei Gründe gab. Zum einen waren einige Teilnehmer in dem Bereich unerfahren und wussten nicht was sie einstellen sollten. Zum anderen waren an diesen Stellen die Texte für viele der Benutzer nicht exakt und ließen zu viel Interpretationsspielraum. Dieser ermöglicht fehlerhafte Interpretationen, die dadurch eine Bedrohung des Systems darstellen. Viele Benutzer wussten was ein anonymer Netzwerkzugriff ist aber ihnen war nicht klar, ob es sich um den eigenen oder um einen fremden Netzwerkzugriff handelte. So konnten Bereiche ermittelt werden, in denen die Versuchsteilnehmer unsicher über die Konsequenzen ihres Handelns waren.

Das Ziel, Systeme mit geringem Bedrohungspotential zu entwickeln und bereit zu stellen, muss die Betrachtung der Interaktion der Benutzer mit den Systemen beinhalten. Viele Bedrohungen entstehen erst dadurch, dass Benutzer sich unsicher bei ihren Handlungen sind. Dies kann durch mangelnde Erfahrungen oder falsche Interpretationen zu Stande kommen. Das in diesem Abschnitt vorgestellte Konzept zeigt, dass durch die Untersuchung von Mousemaps Kriterien erzeugt werden können, die eine Evaluation hinsichtlich von Bedrohungen erleichtern. Der Fokus lag dabei in dem ersten Experiment darauf, „Unsicherheit“ der Benutzer mit Hilfe von Mousemaps zu zeigen. Die Untersuchung zeigte noch nicht exakt Bedrohungsfälle, aber sie gab dem Evaluator Ansatzpunkte wo eine vertiefte Betrachtung erfolgen könnte. Das implementierte System GAMJA kann aber dazu eingesetzt werden, verschiedene Darstellungen der gleichen Funktionalität miteinander hinsichtlich der „unsicheren Benutzung“ zu vergleichen. Dann kann die Funktionalität mit dem höchsten Potential zur sicheren Benutzung umgesetzt und so das Bedrohungspotential minimiert werden.

Zukünftige Ergebnisse müssen zeigen, ob durch Umsetzungen des Konzeptes auch weitere Kriterien bereit gestellt werden können. Dies kann zum Beispiel dadurch erfolgen, dass bei der Benutzung von „Experten“ Mousemaps angefertigt werden. Diese könnten als Referenz zur Benutzung durch „normale Benutzer“ dienen und geeignete Abstandsvektoren und Durchschnittswerte zur Verfügung stellen.

4.5 Zusammenfassung der Fallstudienergebnisse

Die Trends bei IT-Systemen führen zu Systemen, bei denen immer mehr unterschiedliche Benutzer immer häufiger mit diesen interagieren. Beispiele für solche Systeme sind ambiente Systeme oder intelligente Umgebungen. Die zuvor beschrieben Experimente zeigen, dass durch die veränderte Rolle der Benutzer auch Sicherheitsprobleme vorliegen, die nicht allein durch herkömmliche technische Gegenmaßnahmen adressiert werden. Eine Lösung dieser Herausforderung besteht in der Umsetzung von benutzerzentrierter IT-Sicherheit bei IT-Systemen bei der verschiedene weitere Aspekte untersucht und bearbeitet werden.

Um den Themenkreis benutzerzentrierter IT-Sicherheit zu untersuchen wurde zunächst eine Vorbetrachtung von heutigen Standards zur Evaluierung und Zertifizierung von IT-Sicherheit durchgeführt die zeigte, dass diese Standards ergänzt werden müssen (siehe Einleitung Kapitel 4). Eine Zertifizierung nach den Common Criteria (CC) zeigte, dass diese Art der Standards auf die technischen Gegenmaßnahmen fokussiert ist. Das Hauptanliegen der Zertifizierung besteht darin, Benutzern und Entwicklern von Systemen Maßstäbe zum Vergleich der IT-Sicherheit zur Verfügung zu stellen. Allerdings werden als Bedrohungen mutwillige Angreifer untersucht. Die CC sollten um einen Bereich erweitert werden, der untersucht, wie Fehleranfällig die Bedienung ist und welche Bedrohunglage aus der falschen Bedienung entsteht.

Nach der Vorbetrachtung der Standards wurden einige Experimenten durchgeführt und folgende Ergebnisse ermittelt.

1. Benutzer sind sich der Bedrohungen bei allgegenwärtigen unterstützenden Systemen nicht bewusst (siehe 4.1) und reagieren auf offensichtliche Bedrohungen nicht ausreichend (siehe 4.2)
2. Benutzergruppierung anhand von Interaktion kann die Sicherheit erhöhen (siehe 4.3)
3. Die Analyse von unsicherem Verhalten kann ebenfalls die Sicherheit erhöhen (siehe 4.4)

Benutzer sind sich nicht bewusst, welchen Bedrohungen sie in allgegenwärtigen Umgebungen ausgesetzt sind. Beim SHA-Experiment gab ein großer Teil

der Benutzer bereitwillig sensible Daten ein. Die Benutzer realisierten in dieser Situation nicht, dass sie einer potentiellen Bedrohung ausgesetzt waren. Das Experiment zeigte, dass sie die Daten als sensibel einstuften aber bereitwillig diese Daten einem unbekannten System aussetzten. Zu einem ähnlichen Ergebnis kam Weiss [125]. Bei der dort geschilderten Untersuchung wurde Managern verschiedene Fragen hinsichtlich ihres Sicherheitsbewusstseins gestellt.

„Auf die Frage, ob sie eine Aktentasche mit zehn Millionen Dollar per Postpaket verschicken würden, sagten alle befragten Manager spontan: „Nein, natürlich nicht!“ Doch bei der Frage, wie man eine CD mit ein paar Millionen Kundendaten verschickt, kommt als Antwort immer noch „im Briefumschlag“, weil der Verlust eines Datenträgers am Wert des Mediums gemessen wird - und nicht an dessen Inhalt.“

Daher müssen Maßnahmen ergriffen werden Benutzern diese Problematik verständlich zu machen. Schulungen können aber wie Nielsen [97] schreibt nicht die einzige Maßnahme sein. Damit wäre seiner Meinung nach die Verantwortung fälschlicherweise alleine den Benutzern übertragen worden. Daher müssen auch Maßnahmen darin bestehen, dass die Systeme so gestaltet werden, dass Benutzer die Gefahren leichter erkennen können. Weil Benutzer sich der Bedrohungen nicht bewusst sind, verhalten sie sich falsch, geben von sich aus zu viele Daten preis und schaffen selbst weitere Bedrohungen. Systeme müssen daher so bedrohungsminimierend wie möglich entwickelt werden. Eine Maßnahme dazu bietet die Entwicklung gemäß Usability-Kriterien. Dadurch wird das Fehlbedienungspotential und somit zugleich das Gefährdungspotential gesenkt.

Auch das Verhalten von Benutzern in Situationen, wo ihre Daten aktiv durch Angreifer angegriffen werden, muss verbessert werden. Wie die Untersuchung im Kapitel 4.2 zeigte, tun Benutzer auch dann nicht das bestmögliche für die Datensicherheit, wenn sie direkt bedroht werden oder die Bedrohung erkennen. Bei der Benutzung von IT-Systemen steht für Benutzer die zu bewältigende Aufgabe im Vordergrund. Solange bei dieser Aufgabe die IT-Sicherheit für den Benutzer keine Bedeutung hat (z.B. Spielen im Vergleich zu Online Banking), kompromittiert er durch sein Verhalten das gesamte System. Daher muss die Bedeutung der Querschnittsfunktion IT-Sicherheit weiter gesteigert werden.

Aber nicht nur das mangelnde Bewusstsein der Benutzer stellt für die IT-Sicherheit eine große Bedrohung dar. Neben dem mangelnden Bewusstsein trägt die schlechte Verständlichkeit der Sicherheitsfunktionen zu einem erhöhtem Bedrohungspotential in Systemen bei. Dieses resultiert aus

dem Fehlverhalten der Benutzer wie das im Kapitel 4.3 aufgestellte Konzept und die damit gemachte Fallstudie zeigte. Das Konzept gruppierte Benutzer um Systeme für Benutzergruppen anpassen zu können und dadurch das Fehlbedienungspotential zu minimieren. Die Ergebnisse zeigen, dass die Interpretationsmöglichkeiten von Systemen dahingehend minimiert werden müssen dass Benutzer sie einheitlich verstehen. Begrifflichkeiten und Optionen, die von Benutzern interpretiert werden können, werden von Benutzern sehr unterschiedlich angewendet, und es ergibt sich so ein hohes Potential an Möglichkeiten und Folgezuständen. Benutzer neigen in dieser Situation nicht dazu, Gefahren minimierend zu verhalten sondern fällen ihre Entscheidungen ohne rationale Grundlage. Dieses Verhalten wird durch häufige Warnmeldungen durch das System weiter gefördert. Je mehr Meldungen erscheinen, desto weniger werden sie durch Benutzer wahrgenommen.

Daher wurde das Konzept um eine Komponente erweitert, die untersuchte, an welchen Stellen Benutzer unsicher bei der Wahl ihrer Entscheidung waren. Diese Untersuchung erfolgte im System GAMJA auf Basis von Mousemaps. Die Analyse von Situationen, in denen sich Benutzer unsicher bei der Wahl ihrer Entscheidung sind, kann ebenfalls dazu benutzt werden Systeme sicherer zu machen, indem genau diese Situationen vermieden werden.

Nachdem in diesem Kapitel einige Herausforderungen benutzerzentrierter IT-Sicherheit und schon Ansätze für Lösungen angesprochen wurden, werden potentielle Lösungen im nachfolgenden Kapitel diskutiert und behandelt.

5
Fazit, Lösungen und Ausblick

Σκοπέειν δὲ χρὴ παντὸς χρήματος τὴν τελευτήν κῆ αποβήσεται

(Überlieferung nach Solon)

Das Fazit am Ende dieser Arbeit lautet:

Sichere IT-Systeme sind nur durch besondere Berücksichtigung seiner Benutzer möglich. Nur die konsequente Umsetzung von benutzerzentrierter IT-Sicherheit kann das Fehlerpotential und somit die Bedrohungen durch Benutzer minimieren.

Dieses Ergebnis kam durch die folgenden Betrachtungen in dieser Arbeit. Basierend auf früheren Ergebnissen als Projektleiter für die Zertifizierung von generischer Sicherheit nach dem weltweiten Standard der Common Criteria wurde analysiert, dass heutige Evaluationsmethoden für IT-Sicherheit die Interaktion des Benutzers mit dem System wenig beachten. Dass dies ein Problem darstellt wurde in einem ersten Experiment gezeigt. Benutzer waren sich des Gefahrenpotentials nicht bewusst und kompromittierten durch allzu „freizügige“ zur Verfügungstellung von Daten ihre Sicherheit.

Ein weiteres Experiment zeigte weiter, dass das Gefahrenpotential durch Benutzer auch dadurch ansteigt, dass sie auf direkt eintreffende Bedrohungen zum Teil mit fehlerhafter Benutzung reagieren. Die Interaktion von Systemen mit Benutzern stellt somit ein umfangreiches Bedrohungspotential dar und muss sowohl in Standards wie den CC stärker gewichtet als auch durch Maßnahmen auf Herstellerseite Gefahren minimierend bereit gestellt werden.

Eine Möglichkeit dazu bietet die einfachere Benutzung durch Verwendung von Maßnahmen der Usability. Ein Maßnahme zur leichteren Benutzung bie-

tet die individuelle zur Verfügungstellung der Systeme für jeden einzelnen Benutzer. Da die individuelle Bereitstellung jedoch sehr kostenintensiv ist wurde untersucht, ob im IT-Sicherheitsumfeld auch eine gruppenspezifische Bereitstellung möglich ist und Gefahren minimierend sein kann.

Es wurde gezeigt, dass dies möglich ist und dass eine Untersuchung der Interaktion eine Gruppierung der Benutzer ermöglichte und zudem Schwachstellen der IT-Sicherheit aufzeigen konnte. In einem letzten Schritt wurde das Konzept zur Untersuchung der Interaktion dahingehend ergänzt, dass sich durch Untersuchung von „unsicherer“ Bedienung Schwachstellen ermitteln ließen.

Nach Betrachtung der Experimente und dort gesammelten Ergebnisse lassen sich die in Kapitel 1 aufgestellten Fragen wie folgt beantworten.

Beantwortung der Fragen aus Kapitel 1.2

Welche neuen Bedrohungen/Herausforderungen gibt es im Kontext zukünftiger Systeme wie zum Beispiel intelligenter Umgebungen oder ambienter Systeme? Welche Bedrohungen stellen Benutzer dar und in welchen Situationen sind sie bedroht?

Eine große Bedrohung stellen Benutzer durch unbewusste Handlungen dar. Zum einen geben sie sehr viele sensible Daten preis, ohne sich deren Bedrohungen bewusst zu sein. Zum anderen stellen sie durch Fehlbedienungen ein erhöhtes Bedrohungspotential dar.

Erkennen Benutzer die Bedrohungen und wie verhalten sie sich in bedrohten Situationen?

Benutzer erkennen noch nicht den Umfang der Bedrohungen, denen sie durch die neuen Systeme und Konzepte ausgesetzt sind. Neben Aufklärungsarbeit bei den Benutzern müssen sie aber auch in die Lage versetzt werden Bedrohungen zu erkennen, Verantwortung zu übernehmen und sich entsprechend zu verhalten.

Anhand welcher Kriterien können zukünftige Systeme (wie z.B. intelligente Umgebungen/ ambiente Systeme) ihre Unterstützung anpassen und optimieren?

Zukünftige Systeme können und müssen ihre Unterstützung dahingehend anpassen, dass sie auch Querschnittsfunktionen wie die IT-Sicherheit in den Fokus des Benutzers rücken und ihn in die Lage versetzen mit seiner Verantwortung umzugehen.

Wird die Problematik der benutzerzentrierten IT-Sicherheit durch heutige Zertifizierungen/Untersuchungsmethoden adressiert?

Heutige Zertifizierungen wie zum Beispiel die Common Criteria fokussieren noch zu sehr auf das Produkt und seine technischen Eigenschaften. Die Benutzung und daraus resultierende Probleme werden noch zu wenig beachtet und evaluiert.

Wie können Lösungen für die Problematik benutzerzentrierter IT-Sicherheit aussehen? Wie können Systeme Benutzer bei der Benutzung von IT-Sicherheit unterstützen? Wie kann durch Gruppen spezifische Betrachtung des Verhaltens eine Minimierung des Bedrohungspotentials erreicht werden?

Die Herausforderungen benutzerzentrierter IT-Sicherheit sind vielschichtig. Sie betreffen sowohl Hersteller, wie Betreiben und Endnutzer und können nur gemeinsam gelöst werden. Es gibt kein Patentrezept, da Benutzer und zu unterstützende Aufgaben zu verschieden sind. Trotzdem können einige Aspekte generell unternommen werden um Systeme, Daten und den Umgang mit ihnen sicherer zu machen. Ein erster Schritt dazu besteht darin, dass Benutzer, Betreiber und Hersteller lernen, in welchem Umfeld sie sich bewegen und wie sie sich verhalten sollten.

Benutzer müssen lernen, dass sie sich in bedrohten Situationen befinden und auch sie persönlich konkreten Bedrohungen ausgesetzt sind. Weiterhin, dass sie eine umfangreiche Verantwortung für die Sicherheit von Daten und Systemen haben. Zusätzlich müssen sie verstehen, dass Hersteller und Betreiber nicht alleine durch Maßnahmen auf Hersteller- und Betreiberseite die Systeme vollständig absichern können.

Aber dem Benutzer kann nicht alleine die Verantwortung für Handlungen an seinem Computer aufgebürdet werden. Auch Nielsen betont in [97], dass Schulungen für Benutzer nicht die alleinige Antwort auf Herausforderungen bei der Benutzbarkeit von Systemen sein können. Der Themenkomplex der IT-Sicherheit ist zu komplex, als dass er von allen Benutzern zufriedenstellend durchdrungen werden kann. Benutzer haben nicht die Zeit und das Wissen, sich ständig die neuesten Entwicklungen im Bereich der IT-Sicherheit und der IT-Bedrohungen zu verfolgen. Außerdem wird dadurch die Verantwortung vom Ersteller an die Benutzer weitergegeben, und der gesamte Nutzen des Internets kann so nicht realisiert werden.

Daher kann mit Schulungen und mit möglichst einfach zu bedienenden Programmen ein gewisses Maß an Sicherheit erreicht werden. Aber als alleinige Maßnahme reicht es nicht aus.

Hersteller und Betreiber müssen lernen, dass sie ihre Systeme Benutzer gerecht erstellen und anbieten müssen. Das heißt, die Benutzer und ihre zu lösenden Aufgaben müssen im Fokus stehen und nicht die eingesetzte Technologie oder implementierte Funktionalitäten. Weiterhin müssen sie berücksichtigen, dass Benutzer verschiedenen sind. Benutzer haben unterschiedliche Wünsche, Ziele, Erwartungen und Fähigkeiten.

Eine weitere Lösung zur Erzielung von höherer Sicherheit in intelligenten Umgebungen muss darin bestehen, dass Benutzer aktiv die Möglichkeit der Verknüpfung ihrer wahren Identität mit der der virtuellen Identität vermeiden müssen. Ebenso müssen Hersteller und Betreiber die Trennung fördern. Dies kann zum Beispiel dadurch geschehen, dass an Stellen, an denen eine Benutzerkennung verlangt wird, eine Benutzerkennung vorgeschlagen wird (z.B. ein Bild) oder Benutzer dazu ermutigt werden ein Synonym zu verwenden.

Systeme müssen so konstruiert werden, dass sie das Lernen des Benutzers in kritischen Situationen dahingehend fördern, dass er fehlerfreier handelt. Ein Schritt in diese Richtung wären Systeme die den Benutzer dazu ermuntern, die Verknüpfung seiner Identität mit seinen Daten zu erschweren. So könnten Systeme bei Eingabe eines Benutzernamens drauf hinweisen, dass keine realen Namen verwendet werden sollten. Zusätzlich könnten die Systeme Namensdatenbanken haben, die die Eingabe von realen Daten unmöglich machen würde.

Die konsequente Einbeziehung und Umsetzung von Usability-Erkenntnissen bei IT-Systemen führt zu weniger Fehlern und Problemen durch den Benutzer und somit zu höherer IT-Sicherheit. Die in dieser Arbeit gezeigten Untersuchungen des Verhaltens von Benutzern sind ein Schritt auf dem Weg zu besserem Verständnis der Systeme durch Benutzer und somit zu besserer IT-Sicherheit. So können Systeme so designt werden, dass sie auf das gemeinsame Verständnis aller Beteiligten referenzieren.

Aber auch die Umsetzung anderer Usability-Aspekte wie zum Beispiel der Feedback-Aspekt erhöht die IT-Sicherheit, da durch ihn Benutzer einen Einblick haben, was ihre Handlungen auslösen und so besser einschätzen können.

Ausblick

Die gezeigten Bedrohungen der Benutzer, ihrer Daten und auch der Systeme können nicht allein durch technische Maßnahmen oder durch die Übernahme der Verantwortung durch Benutzer und Hersteller vereitelt werden. Die vorgestellten Konzepte und insbesondere die Einbeziehung von Usability-Maßnahmen verringert zwar das Bedrohungspotential, aber eine komplette Aufhebung der Bedrohungen kann so nicht erreicht werden.

Dazu sind die Systeme zu komplex und die möglichen Seiteneffekte nicht überschaubar. Zwar versucht die Gesellschaft durch immer weitere Konzepte die Sicherheit der Systeme zu erhöhen, aber woher weiß der Nutzer, was passiert, wenn er mit einem Informationssystem interagiert? Welche Daten werden gesammelt? Wie werden sie ausgewertet? Was passiert, wenn er einen Button betätigt?

Der vorgestellte Ansatz zur Einbeziehung der Benutzer soll es Benutzer erleichtern und ermöglichen, eine ungefähre Vorstellung von dem zu bekommen, was gerade bei dem System passiert. Aber auch ein sensibler, gut ausgebildeter Benutzer kann in den wenigsten Fällen abschätzen, was genau mit seinen Daten gerade passiert oder welche Daten er preisgegeben hat.

Aus diesen Gründen müssen auch gesellschaftliche Veränderungen bei der IT-Sicherheit eintreten. Gesellschaftlich ist es geächtet Daten zu missbrauchen. Aus diesem Grund gibt es den Datenschutz. Aber dies kann und wird nicht bis zur letzten Konsequenz verfolgt und durchgeführt werden. Ein anderer Weg besteht darin, dass ein gesellschaftlicher Rahmen entstehen könnte, in dem offener mit Daten umgegangen wird. Wenn Daten offen für jeden verfügbar sind, sind sie auch nicht mehr so wertvoll. Wenn die Daten keiner mehr unberechtigt will, dann lohnt sich auch ein Stehlen von Daten nicht mehr. Weiterhin könnten eher die Personen bestraft werden die Daten missbräuchlich verwenden, als die Leute, die Daten stehlen. Durch das gleichzeitige Hochsetzen von Strafen für missbräuchliche Nutzung und dem Offenlegen von Daten sinkt der Anreiz für das Stehlen von Daten.

Bevor Daten aber keinen oder sehr geringen Bedrohungen mehr ausgesetzt sind, ist es nötig, diese zu schützen. Beim Schützen der Daten haben sowohl Benutzer als auch Hersteller von Systemen einen Teil der Verantwortung. Damit Benutzer diese Verantwortung übernehmen können, müssen bei der Entwicklung der Systeme Erkenntnisse der Usability angewendet und umgesetzt werden. Das in dieser Arbeit beschriebene Konzept der Untersuchung des Verhaltens und anschließender Gruppierung stellt dazu einen ersten Schritt dar.

Anhang A
Rahmenbedingungen für die verwendeten Fragebogen

1. Zunächst wurden die Hypothesen und Fragestellungen erarbeitet, die bei der Evaluation mit dem Fragebogen überprüft werden sollten.
2. Dann wurden darauf basierend Fragen generiert und eine erster initialer Fragebogen erstellt
3. Mit diesem ersten Fragebogen wurde eine Vorevaluation mit 2-3 Teilnehmern durchgeführt um dessen Gebrauchswert zu überprüfen und gegebenenfalls zu optimieren.
4. Mit dem optimierten Fragebogen (und Testaufbau) wurde dann das Experiment durchgeführt und die Hypothesen überprüft.

Jeder Fragebogen erhielt am Anfang eine Einverständniserklärung der Teilnehmer, dass ihre eingegebenen und Interaktionsdaten für diese Arbeit verwendet werden dürfen. Die Fragebögen wurden allen Teilnehmer der Experimente vom Evaluator ausgehändigt und hatten mehrere Funktionen.

- Der Fragebogen sollte eine gemeinsame Basis für alle Versuchsteilnehmer schaffen. Dazu wurde in jedem Experiment die Aufgabenstellung am Anfang des jeweiligen Fragebogens so vollständig und eindeutig wie möglich beschrieben. Hiermit sollte für alle Teilnehmer die Testumgebung und Testsituation möglichst identisch werden.

  Für die Teilnehmer war es jederzeit möglich weitere Fragen zu stellen. Diese wurden protokolliert und dienten zur Optimierung des Versuchsablaufes bei erneuten Testdurchläufen.
- Mit den jeweiligen Fragebögen sollten zusätzlich zur Datenerfassung der implementierten Systeme weitere Daten für die Auswertung gesammelt werden.

  Um die Ergebnisse der verwendeten „Testprogramme“ mit den Benutzern in Relation setzen zu können, wurden zahlreiche Fragen zu den Teilnehmern und ihrem normalen Umgang mit den Computern gestellt.

Fragebogen für die Benutzung des SHA Fitnessassistenten

Einführung in das Experiment und die Aufgabenstellung

Danke, dass Sie an dem folgenden Experiment zur Bestimmung von Problemen bei der Benutzung eines Fitnessassistenten teilnehmen. Wir möchten mit diesem Experiment sehen, an welchen Stellen beliebige Benutzer mit unserem System Probleme haben. Es werden dabei verschiedene Aspekte der Usability (Gebrauchstauglichkeit) untersucht.

Mit Abgabe des Fragebogens erklären Sie sich bereit, dass diese Daten zu Forschungszwecken verwendet werden können. Die Daten dienen nur als anonymer Testdatensatz für die Evaluation des Fitnesstrainers. Sie werden in keiner Weise weitergegeben. Falls Sie Fragen oder Anregungen haben, stellen Sie diese bitte sofort oder notieren sie diese. Wir sind für alle Anregungen dankbar.

Zunächst erhalten sie den ersten Teil eines Fragebogens. In diesem werden Ihnen einige Fragen zu Ihrer Person gestellt werden. Danach erhalten sie eine Aufgabe und einen Prototypen des Systems. Mit diesem lösen Sie dann bitte die gestellte Aufgabe.

Den Abschluss des Experimentes bildet der zweite kurze Teil des Fragebogens über die von Ihnen gemachten Erfahrungen mit dem System. Sie können jederzeit dem Evaluator Fragen stellen!

Fragen zu Ihrer Person

Die Daten und Eingaben dürfen im Rahmen dieses Versuches anonym erhoben und zur Erstellung einer Studie und zur Verbesserung des bereitgestellten Werkzeugs verwendet werden.

❒ Ich stimme der anonymen Datenerfassung zu
❒ Nein, meine Daten dürfen nicht erhoben werden

`A.1` Ihr Geschlecht:

❒ Weiblich ❒ Männlich

`A.2` Ihr Alter:

❒ jünger als 21 ❒ 21 - 25
❒ 26 - 30 ❒ 31 - 35
❒ 36 - 40 ❒ 41 - 45
❒ 46 - 50 ❒ 51 - 55
❒ 56 - 60 ❒ 61 oder älter

A.3 Welchen Beruf üben Sie aus?

A.4 A4: Besitzen Sie einen eigenen privaten Computer?

❒ Ja ❒ Nein (Weiter bei Frage A 6)

A.5 Administrieren Sie Ihren privaten Computer selbst?

❒ Ja ❒ Nein

A.6 Wie schätzen Sie Ihre Erfahrung bei der Benutzung von Programmen ein?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Große Erfahrungen Kaum Erfahrungen

Aufgabenstellung

Stellen Sie sich für den nachfolgenden Teil des Experimentes bitte folgende Situation vor: Sie sehen das folgende Programm bei Ihrem Arzt. Er erläutert Ihnen, dass Sie mit diesem Programm ihre Fitness steigern könnten. Außerdem bestehe die Möglichkeit durch Benutzung des Programms bei der Krankenkasse Bonuspunkte zu sammeln und eine Beitragsermäßigung zu erhalten. Sie sind neugierig und möchten das Programm ausprobieren.

Aufgabe: Melden Sie sich bitte am System an und führen eine Versuchseinheit damit durch.

Nachdem Sie eine Trainingseinheit absolviert haben, beantworten Sie bitte den Rest des Fragebogens.

Fragen an den Versuchsteilnehmer nach Beendigung der Trainingseinheit.

B.1 Wie komfortabel war die Dateneingabe?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Sehr komfortabel Sehr unkomfortabel

B.2 Waren die Menüs, Buttons und Arbeitsschritte immer logisch vorhersehbar/nachvollziehbar?

❒ Ja ❒ Nein

B.3 Würden Sie das System benutzen?

❒ Ja ❒ Nein

Begründung:

B.4 An welchen Stellen wussten sie nicht die vom System gewünschten realen korrekten Daten?

B.5 An welchen Stellen haben sie reale und korrekte Daten eingegeben?

- ❒ Name
- ❒ Vorname
- ❒ Gewicht
- ❒ Größe
- ❒ Email
- ❒ Telefon
- ❒ Aufenthaltsort

B.6 Finden Sie das System übersichtlich?

❒ Ja ❒ Nein

B.7 War das System überladen oder enthielt es nur die benötigten Informationen/ Funktionen?

❒ Überladen ❒ Nicht Überladen

B.8 Welche sensiblen Daten sind Ihrer Meinung nach im System vorhanden?

B.9 Welche der folgenden Werte sind für Sie sicherheitssensibel?

- ❒ Name
- ❒ Vorname
- ❒ Blutdruck
- ❒ Gewicht
- ❒ Puls
- ❒ Email
- ❒ Telefon
- ❒ Aufenthaltsort

B.10 Welche der folgenden Werte darf Ihr Arbeitgeber erfahren?

- ❒ Name
- ❒ Vorname
- ❒ Blutdruck
- ❒ Gewicht
- ❒ Puls
- ❒ Email
- ❒ Telefon
- ❒ Aufenthaltsort

B.11 Empfanden Sie die Spannung am Sensor als unangenehm?

❒ nicht gespürt ❒ schwache Vibration
❒ starke Vibration ❒ äußerst unangenehm

Fragen zu Ihrem generellen Sicherheitsempfinden

Im Folgenden werden Ihnen noch einige Fragen zu ihren sonstigen Empfinden des Themenkomplexes Sicherheit gestellt.

C.1 Haben Sie Ihre Haustür besonders gesichert?

❒ Ja ❒ Nein

C.2 Haben Sie ein Auto?

❒ Ja ❒ Nein (Weiter bei Frage C 5)

C.3 Halten Sie immer besonderen Sicherheitsabstand zu dem Wagen vor Ihnen?

❒ Ja ❒ Nein

C.4 Schließen Sie Ihr Auto beim Tanken ab?

❒ Ja ❒ Nein

C.5 Fühlen Sie sich an Ihrem Wohnort (Stadt,Land) sicher?:

❒ Ja ❒ Nein (Warum nicht?)

C.6 Zählen Sie Ihr Wechselgeld nach?

❒ Ja ❒ Nein

C.7 Achten Sie beim Geldautomaten darauf, dass niemand Ihre Eingaben sieht?

❒ Ja ❒ Nein

C.8 Nehmen Sie Ihre normale Geldbörse mit an den Strand?

❒ Ja ❒ Nein

`C.9` Der Komfort von IT-Systemen wird häufig in Bereichen mit hoher Sicherheitsanforderungen zugunsten der Sicherheit eingeschränkt. Aus diesem Grund würden wir gerne ihre Einschätzung über die notwendige Einstufung der folgenden Bereiche kennen. In welchen der folgenden Domänen empfinden sie die Daten als besonders kritisch?

- Reiseauskunft der Bahn

  ❒ kritische Daten ❒ unkritische Daten

- Bankenwesen

  ❒ kritische Daten ❒ unkritische Daten

- Gesundheitswesen

  ❒ kritische Daten ❒ unkritische Daten

- Transfer von Bargeld

  ❒ kritische Daten ❒ unkritische Daten

`C.10` Wie schätzen Sie Ihr Interesse bezüglich der Sicherheit von Computern und Ihrer Daten ein?

❒ Großes Interesse ❒ Wichtig
❒ Nicht so wichtig ❒ Ist mir egal

`C.11` Hatten Sie schon einmal ein Problem mit sensiblen Daten von Ihnen?

❒ Ja (Wenn ja, welche(s)?) ❒ Nein

Sonstige Anmerkungen: Vielen Dank für Ihre Teilnahme am Test und notieren Sie bitte hier Ihre weiteren Anmerkungen zum Fragebogen.

Im Folgenden werden nur noch die abweichenden Daten der weiteren erstellten und verwendeten Fragebögen beschrieben.

Abweichende Daten des Fragebogens für das Experiment mit MEGSA

Einführung in das Experiment und die Aufgabenstellung

Danke, dass Du an dem folgenden Experiment zur Bestimmung von Benutzergruppen bei Programmen teilnimmst. Das Experiment wird im Rahmen einer Lehrveranstaltung durchgeführt und soll dazu dienen, Computer leichter benutzbar zu gestalten. Es werden verschiedene Aspekte der Usability (Gebrauchstauglichkeit) untersucht. Du erhälst gleich eine Aufgabenstellung, die Du bitte ausführst. Das Experiment besteht aus zwei Teilen. Zuerst führst Du bitte ein Programm aus und löst die unten beschriebene Aufgabe. Danach füllst Du bitte den Rest dieses Fragebogens aus. Mit Abgabe des Fragebogens erklärst Du Dich bereit, dass diese Daten zu Forschungszwecken verwendet werden können. Die Daten dienen nur als anonymer Testdatensatz für eine Studie bei einem mobilen Lernwerkzeug im Hochschulbereich. Die Daten werden in keiner Weise weitergegeben. Falls Du Fragen oder Anregungen hast, stelle diese bitte sofort oder notiere sie. Wir sind für alle Anregungen dankbar.

Aufgabe: Stelle Dir vor, Du nimmst an einer Lehrveranstaltung teil. In dieser Lehrveranstaltung wird das folgende Lernspiel angeboten. Mit einem mobilen Endgerät kannst Du Fragen zu der Lehrveranstaltung stellen und die Fragen anderer Teilnehmer lösen. In beiden Fällen kannst Du Punkte erhalten. Am Ende des Semesters kann man durch seine Punkte einen Bonus bei der Klausur erhalten. Falls Du nicht das eigene Handy verwendest, bist Du für das von der Universität bereitgestellte Handy verantwortlich!

Stelle nun bitte zu der Lehrveranstaltung Informatik beliebige Fragen und beantworte einen Teil der bereits eingegebenen Fragen. (Wenn Du kein Informatiker bist, stelle beliebige andere Fragen und notiere am Ende des Fragebogens bitte die Lehrveranstaltung)

Deine konkreten Aufgaben lauten:

1. erstelle einen Benutzer
2. Führe die Aufgaben 2a und 2b im Wechsel solange aus bis die Zeit zur Erledigung der Aufgabe erreicht ist. Versuche dabei möglichst viele Punkte zu erreichen.
   (a) erstelle eine Frage im MEGSA System
   (b) löse zwei Fragen die von anderen Teilnehmern ins MEGSA System eingegeben wurden.

Wichtig: Lies Dir bitte immer alles genau durch! Wenn Du nicht genau weisst, was zu tun ist, frage bitte einfach.

Fragebogenergänzungen

Die Fragen aus dem Fragebogen A zur Person wurden um die folgenden Fragen ergänzt:

A.7 Hast Du schon einmal selbst ein Computerprogramm erstellt?

❒ Ja ❒ Nein

A.7 Welche der folgenden Programme nutzt Du? (Mehrfachnennungen sind möglich)

❒ Onlinebanking
❒ E-Mail Verschlüsselung
❒ abgesicherte Chatprogramme

Die Fragen zur Programmbenutzung des SHA Experimentes wurden komplett durch die Folgenden ersetzt. Die Fragen C.1 bis C.11 blieben identisch.

Fragen zur Programmbenutzung

D.1 Wie würdest Du die Bezeichnungen der Einstellungen bewerten?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Eindeutig Verwirrend

Anmerkungen:

D.2 Wie würdest Du die Eingabe der Fragen und Antworten bewerten?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Intuitiv Sehr schlecht

Anmerkungen:

D.3 Wie beurteilest Du die allgemeine Übersichtlichkeit der Anwendung?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Sehr gut Sehr schlecht

Anmerkungen:

D.4 Gab es bei der Benutzung Probleme?

❒ Ja ❒ Nein

Wenn ja, welche?

D.5 Würdest Du das Werkzeug in einer Lehrveranstaltung benutzen?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Ja auf jeden Fall Nein auf keinen Fall

Anmerkungen:

D.6 Was würdest Du an dem Programm verbessern?

D.7 Würde Dir ein solches Spiel zur Unterstützung in der Lehrveranstaltung Spass machen?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Nein Es würde mir Spass machen!

Anmerkungen:

D.8 Wie würdest Du die Nutzung des soeben getesteten Systems beschreiben? (Mehrfachnennungen sind möglich)

❒ spannend
❒ frustrierend
❒ sinnvoll
❒ sicher

Anmerkungen:

D.9 Wie schätzt Du Dein Wissen bezüglich der Nutzung eines Computers ein?

❒ Sehr gute Kenntnisse ❒ Gute Kenntnisse
❒ Grundkenntnisse ❒ Keine Kenntnisse

D.10 Fühlst Du Dich bei der Nutzung des gerade benutzten Systems mit Deinen Daten sicher?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Sehr sicher Sehr unsicher

Anmerkungen:

Änderungen des Fragebogens bei den Experimenten mit SUESA und GAMJA

Bei den Experimenten SUESA und GAMJA war der Fragebogen identisch, unterschied sich aber zu dem Fragebogen im MEGSA Experiment in den folgenden Details.

Einführung und die Aufgabenstellung beim SUESA und GAMJA Experiment

Danke, dass Sie an dem folgenden Experiment zur Bestimmung von Benutzergruppen bei Programmen teilnehmen. Das Experiment wird im Rahmen einer Dissertation durchgeführt und soll dazu dienen, Computer leichter benutzbar zu gestalten. Es werden dabei verschiedene Aspekte der Usability (Gebrauchstauglichkeit) untersucht. Sie erhalten gleich eine Aufgabenstellung, die Sie bitte ausführen. Das Experiment besteht aus zwei Teilen. Zuerst führen Sie bitte ein Programm aus und lösen die unten beschriebene Aufgabe. Danach füllen Sie bitte den Rest dieses Fragebogens aus. Mit Abgabe des Fragebogens erklären Sie sich bereit, dass diese Daten zu Forschungszwecken verwendet werden können. Die Daten dienen nur als anonymer Testdatensatz für die Überprüfung einer Methode zur Gruppenbildung bei Computerbenutzern. Sie werden in keiner Weise weitergegeben. Falls Sie Fragen oder Anregungen haben, stellen Sie diese bitte sofort oder notieren sie diese. Wir sind für alle Anregungen dankbar.

Aufgabe: Stellen Sie sich vor, Sie haben einen neuen PC erworben. Diesen möchten Sie mit dem Internet verbinden und über ihn Ihre normale Korrespondenz über das Internet (z.B. E-Mail, Chat oder Online Banking) erledigen. Beim ersten Start des Computers erscheint das folgende Programm und soll Ihnen helfen, die Kommunikation über das Internet sicher zu erledigen.

Wichtig: Lesen Sie bitte immer alles genau durch! Wenn Sie nicht genau wissen, was eine Einstellung bedeutet, können Sie sich immer einen Hilfetext anzeigen lassen, indem Sie das Fragezeichen hinter der jeweiligen Einstellungsmöglichkeit betätigen.

Starten Sie bitte jetzt das Programm:

Wenn Sie die Aufgabe mit dem Programm erledigt haben, füllen Sie bitte den Rest des Fragebogens aus.

Aus dem Fragebogen für das MEGSA Experiment wurden die Fragen 2, 5, 7 und gestrichen.

Zusätzlich waren die folgenden Fragen integriert:

`E.1` Wie würden Sie die Unterstützung durch die Hilfetexte zu den Einstellungen bewerten?

❒ 1 ❒ 2 ❒ 3 ❒ 4 ❒ 5
Sehr gut Sehr schlecht

Anmerkungen:

`E.2` Hatten Sie während des Konfigurationsvorgangs an einer oder mehrerer Stellen besondere Probleme? Wenn ja, beschreiben Sie bitte, an welcher Stelle und warum das Problem auftrat.

❒ Ja ❒ Nein

Anmerkungen:

`E.3` Wie schätzen Sie Ihr Interesse bezüglich der Sicherheit Ihres Computers und Ihrer Daten ein?

❒ Sehr wichtig ❒ Wichtig
❒ Nicht so wichtig ❒ Unwichtig

E.4 Welche der folgenden Komponenten sind auf Ihrem Computer installiert? (Mehrfachnennungen sind möglich)

❒ Firewall
❒ Virenscanner
❒ IDS-Systeme
❒ Tools zur E-Mail-Verschlüsselung
❒ Tools zur Festplattenverschlüsselung

E.5 Hatten Sie auf Ihren Computer schon einmal ein Sicherheitsproblem?

❒ Ja ❒ Nein

E.6 Wenn ja, welche(s)?

E.7 Welche der folgenden Programme nutzen Sie? (Mehrfachnennungen sind möglich)

❒ Onlinebanking
❒ E-Mail Verschlüsselung
❒ abgesicherte Chatprogramme

E.8 Wie schätzen Sie Ihr Wissen bezüglich der möglichen Absicherung eines (Ihres) Computers ein?

❒ Sehr gute Kenntnisse ❒ Gute Kenntnisse
❒ Grundkenntnisse ❒ Keine Kenntnisse

E.9 Welche Bedrohungen, speziell bezogen auf die Informationstechnologie, kennen Sie?

E.10 Wer sollte für die Sicherheit von Computerprogrammen sorgen? (Mehrfachnennungen sind möglich)

❒ Hersteller von Programmen
❒ Hersteller von Hardware
❒ Benutzer

Zur Untersuchung der Hilfetexte waren im letzten Teil des Fragebogens zunächst sämtliche Konfigurationsoptionen und danach alle Hilfetexte aufgeführt. Dort sollten die Versuchsteilnehmer beschreiben, welche Effekte sie hinter den Optionen vermuteten und ob sie die Hilfetexte als hilfreich empfanden. Im Folgenden ist ein Beispiel von 20 genannt.

F.1 Option: Welche Auswirkungen hat die Einstellung: SMPT-Over-Pop aktivieren?

F.2 Hilfetext: Setzen sie diese Einstellung nur, falls ihr Provider dies erfordert!

Anhang B
Anhang zu MEGSA

Warnmeldungen

Für die Experimente wurden neun verschiedene Warnmeldungen in MEGSA erstellt, welche in vier verschiedene Meldungsarten unterteilt werden können. Jede Meldung beinhaltete 3 bis 5 Buttons. Die Betätigung eines Buttons sorgte dafür, dass die Meldung verschwand. Diese Betätigungen wurden von MEGSA mitprotokolliert.

Bei jeder Meldung waren die Buttons „Continue“, „Reboot Mobile“ und „Inform Support“ integriert. Die „Continue“ Option stand dabei dafür, dass der Benutzer einfach über die Fehlermeldung hinweggehen konnte und die Aufgabe weiter bearbeiten konnte ohne sich über die Meldungsursache zu kümmern. Bei Wahl der „Reboot Mobile“ Option sollte der Benutzer die Meldung ernst nehmen und durch seine Wahl mögliche Seiteneffekte einschätzen können. Die „Inform Support“ sollte dagegen von Benutzern gewählt werden, die die Meldungsursache ernst nahmen, aber den Hintergrund der eingeblendeten Meldung nicht komplett überblicken konnten. Zusätzlich gab es bei einigen Meldungstypen noch Buttons, die das Bedrohungspotential erhöhten, indem unsichere Aktionen (z.B. unbekannter Download) gestartet wurden. Und andere Buttons, die das Bedrohungspotential durch das Lernspiel minimierten, indem sie es beendeten.

Warnmeldungstyp 1 - Standard: In der Abbildung B.1 sind die Warnmeldungen des Typs Standard dargestellt. Diese Meldungen kennen Benutzer bereits von ihren eigenen Systemen in ähnlicher Form. Für das Erscheinen dieser Meldungen ist es nicht notwendig, dass gerade eine Aktion ausgeführt wurde. Sie können während des gesamten Experimentes an jeder Stelle zu jeder beliebigen Zeit erscheinen.

Mit diesen Meldungen wird das Verhalten beim Umgang mit bereits bekannten Fehlermeldungen bei der Verwendung eines mobilen Systems untersucht. Die Wahl des „Continue“ Buttons zeigte die Benutzer mit dem geringsten Sicherheitsbewusstsein, da sie die Aufgabe trotz Meldung einfach weiter bearbeiten wollten.

Warnmeldungstyp 2 - aktive Interaktion des Benutzers: Abbildung B.2 zeigt die Meldungen des Typs 2 in MEGSA. Die Meldungen dieses Typs können nur dann auftreten, wenn die Lernanwendung gestartet wird, oder eine Aktion durch den Benutzer

Abb. B.1: MEGSA-Meldungen Typ 1 – Standard-Warnmeldungen

ausgelöst wird (z.B. Senden einer Frage oder Antwort). Dieser Meldungstyp ist den meisten Benutzern ebenfalls von den eignen Systemen bekannt.

Mit diesen Meldungen wird untersucht, ob den Versuchsteilnehmern ein Sicherheitsrisiko, welches durch eigene Handlungen verursacht wird, bewusst ist.

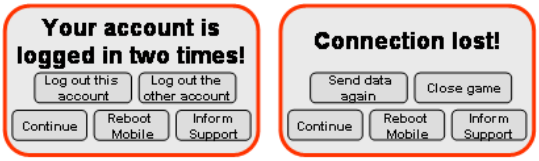


Abb. B.2: MEGSA-Warnmeldungen Typ 2 - aktive Benutzeraktion

Warnmeldungstyp 3 - Aktivierung: Die Meldungen des Typs drei sind in Abbildung B.3 abgebildet. Warnmeldungen des Typs drei können ebenfalls während der gesamten Nutzung des Lernprogramms auftreten. Bereits Grundkenntnisse im Umgang mit Computersystemen sollten ausreichen um zu erkennen, dass hier Angriffe durch Schadprogramme angezeigt werden.

Mit diesen Meldungen wird untersucht, wie Benutzer mit der allgemeinen Bedrohung durch Schadprogramme umgehen und ob sie anderen (Benutzern oder Angreifern) leichtfertig den Zugang zu ihrem System gestatten.

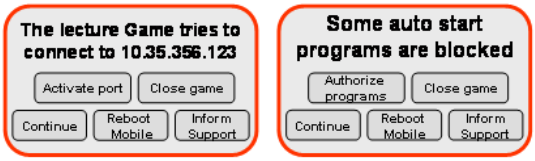


Abb. B.3: MEGSA-Warnmeldungen Typ 3 - Aktivierung

Warnmeldungstyp 4 - externer Download: Der letzte Typ an Warnmeldungen ist in Abbildung B.4 illustriert. Diese Warnmeldungen können ebenfalls jederzeit erscheinen. Auch mit diesen Meldungen wird der potentielle Angriff durch Schadprogramme suggeriert. Im Gegensatz zu Meldungen des Typs drei sind hier in den Texten allerdings umfangreiche Informationen für Gegenmaßnahmen enthalten.

Mit Meldungen dieses Typs wird untersucht, wie genau sich die Teilnehmer die Meldungen durchlesen und ob sie sinnvoll reagieren.

Diese Meldungen wurden in das zuvor beschriebene Spiel integriert und dienten als Grundlage für die nun vorgestellte Untersuchung.

Abb. B.4: MEGSA-Warnmeldungen Typ 4 - externer Download

Stammdaten zu den Experimenten mit MEGSA

Im folgenden werden einige der Stammdaten der Versuchsteilnehmer tabellarisch aufgelistet. Diese Werte wurden aus den Angaben im Fragebogen A erhoben.

Stammdaten zu Experiment 1

Die Tabellen B.1 und B.2 zeigen die Stammdaten der 66 Teilnehmer des ersten Versuches.

Beruf	männlich	weiblich
Firmenmitarbeiter	11	4
Studierende der...		
Informatik	27	2
Chemie	2	2
Elektrotechnik	7	0
Jura	1	2
BWL/VWL	1	0
Hausfrau/-mann	1	4
Keine Angabe	2	0

Tab. B.1: Berufe Experiment 1

Alter	Anzahl
bis 21	9
21 - 25	38
26 - 30	12
31 oder älter	6
Keine Angabe	1

Tab. B.2: Alter Experiment 1

Stammdaten zu Experiment 2, 3 und 4

An den Experimenten zwei (36 Versuchspersonen), drei (27) und vier (17) nahmen ausschließlich Studierende verschiedener Fachrichtungen teil. Das Alter der Teilnehmer lag jeweils zwischen 21 und 32 Jahren.

Stammdaten zu Experiment 5

In den Tabellen B.3 und B.4 werden die Stammdaten der 19 Teilnehmer des fünften Experimentes gezeigt.

Stammdaten zu Experiment 6

Die Stammdaten der 22 Teilnehmer des sechsten Experimentes sind in den Tabellen B.5 und B.6 ersichtlich.

Gesamtheit der Teilnehmer

Insgesamt haben 187 Teilnehmer an den Experimenten und Befragungen mit MEGSA teilgenommen. Die Tabellen B.7 und B.8 stellen die Daten aller Teilnehmer dar.

Beruf	**männlich**	**weiblich**
Firmenmitarbeiter	4	1
Studierende der...		
Chemie	1	2
Elektrotechnik	4	0
Jura	0	2
BWL/VWL	1	1
Hausfrau/-mann	0	2
Keine Angabe	1	0

Tab. B.3: Berufe Experiment 5

Alter	**Anzahl**
bis 21	3
21 - 25	6
26 - 30	3
31 oder älter	5
Keine Angabe	2

Tab. B.4: Alter Experiment 5

Beruf	**männlich**	**weiblich**
Firmenmitarbeiter	7	4
Studierende der...		
Chemie	1	1
Elektrotechnik	3	0
Jura	0	1
BWL/VWL	1	0
Hausfrau/-mann	0	1
Keine Angabe	2	1

Tab. B.5: Berufe Experiment 6

Alter	Anzahl
bis 21	3
21 - 25	6
26 - 30	3
31 oder älter	5
Keine Angabe	2

Tab. B.6: Alter Experiment 6

Beruf	**männlich**	**weiblich**
Firmenmitarbeiter	22	9
Studierende der...		
Informatik	48	4
Chemie	10	7
Elektrotechnik	34	2
Jura	4	6
BWL/VWL	15	7
Hausfrau/-mann	1	7
Keine Angabe	5	6

Tab. B.7: Berufe der Teilnehmer

Alter	**Anzahl**
bis 20	13
21 - 25	87
26 - 30	58
31 oder älter	20
Keine Angabe	9

Tab. B.8: Alter der Teilnehmer

Anhang C
Anhänge zu SUESA

C.1 Konfigurationsoberflächen des Absicherungsprogramms für SUESA

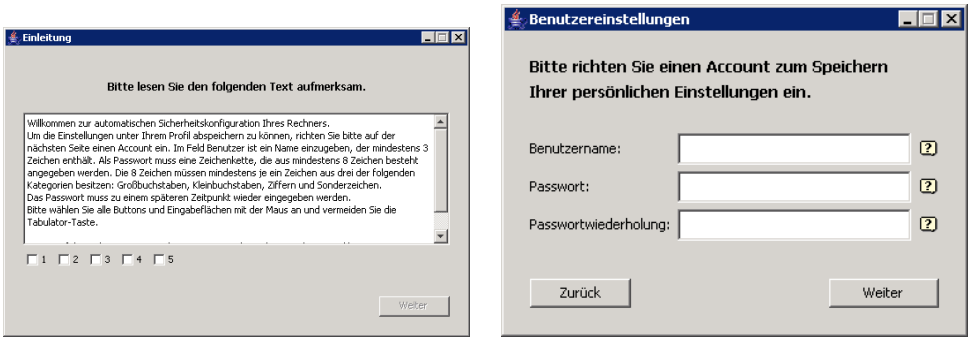
Im Folgenden werden sämtliche grafischen Oberflächen des Absicherungsprogramms, welches für SUESA entwickelt wurde, vorgestellt. Für das Absicherungsprogramm wurden nur die grafischen Oberflächen implementiert und nicht die dahinter liegende Funktionalität. Als Grundlage für das Evaluationsprogramm diente das Sicherheits-Werkzeug XP-AntiSpy [7].

Zu Beginn des Versuches erhielten die Versuchsteilnehmer einen Einleitungstext C.1(a). In diesem war das Ziel des Programms und Regeln zu seiner Benutzung und zur Erstellung des Passwortes beschrieben. Diesen Text mussten die Benutzer bis zum Ende lesen. Am Ende verbarg sich eine variierende Zahl. Nur wenn die korrekte Zahl bei den Checkboxen angewählt wurde, erreichte die Versuchsperson die nächste Seite.

Nun musste die Versuchsperson gemäß den Vorgaben des Einleitungstextes eine regelkonforme Benutzerkennung mit Passwort erstellen C.1(b). Um eine rudimentäre Klassifizierungen in Abhängigkeit vom selbsteingeschätzten Sicherheitsbedürfnis der Versuchsteilnehmer durchführen zu können mussten die Benutzer jetzt ihr Sicherheitsbedürfnis einschätzen C.2.

Nach der Selbsteinschätzung gelangten die Benutzer zu den vier Konfigurationsmenüs des Evaluationsprogramms C.3 und C.4. Insgesamt konnte jeder Benutzer 20 verschiedene Konfigurationseinstellungen in diesen vier Menüs tätigen. Um von diesen Konfigrurationsmenüs zum abschließenden *Speichern* zu gelangen, mussten die Benutzer nur den *Weiter*-Button betätigen. Es wurde an dieser Stelle keinerlei Plausibilität überprüft. Benutzer konnten somit auch ohne Eintragungen bei den Konfigurationsmenüs zum Ende der Aufgabe gelangen.

Zur Beendigung der Aufgabe mussten die Benutzer ihre Konfigurationseinstellungen unter Verwendung ihres Passwortes abspeichern C.5.



(a) Einleitungstext mit Anweisungen (b) Anmeldedialog

Abb. C.1: Einleitungstext und Anmeldedialog

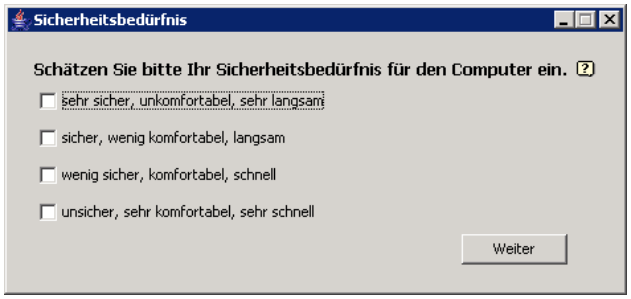
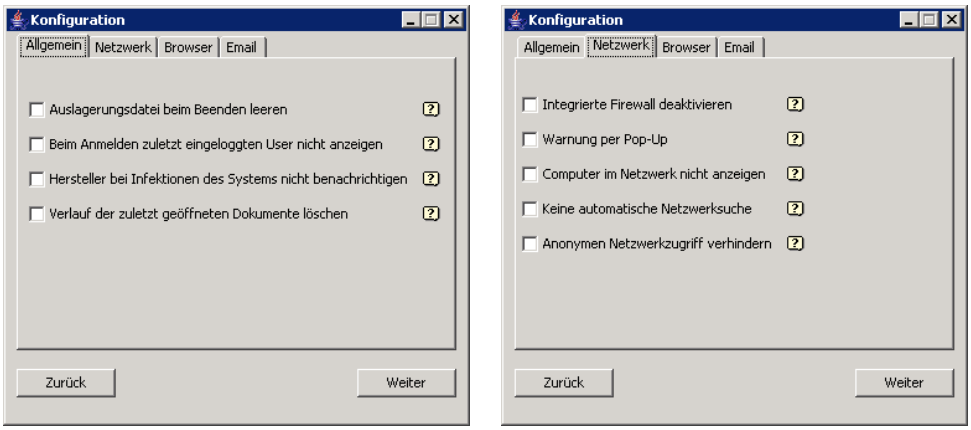
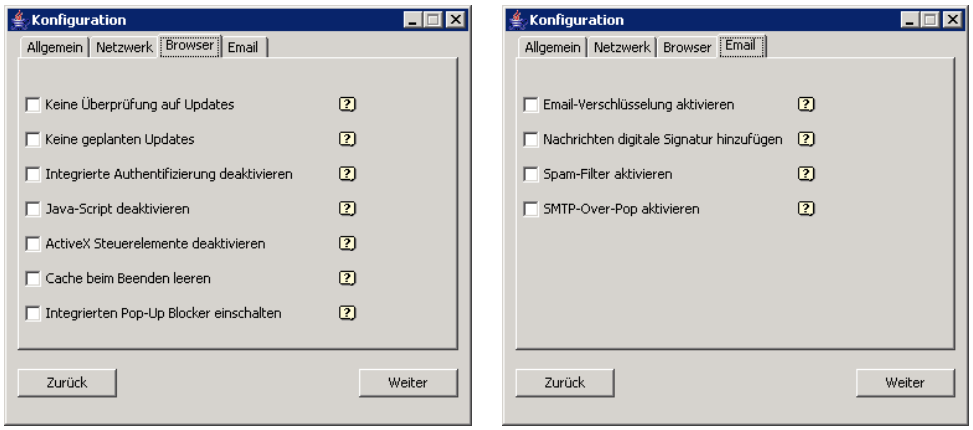


Abb. C.2: Eingabe des Sicherheitsbedürfnisses



(a) Allgemein (b) Netzwerkeinstellungen

Abb. C.3: Konfigurationsmenüs Allgemein und Netzwerkeinstellungen



(a) Browser (b) Email-Einstellungen

Abb. C.4: Konfigurationsmenüs Browser und Email-Einstellungen

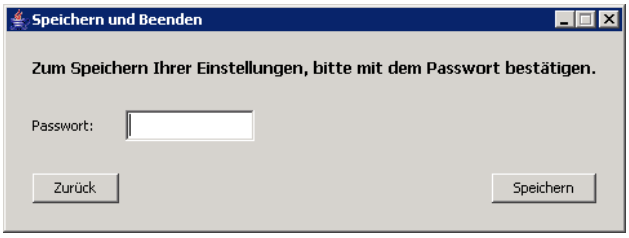


Abb. C.5: Passwortabfrage zum Speichern der gemachten Einstellungen

C.2 SUESA - weitere Funktionalitäten

Neben der beschriebenen Möglichkeit zur Gruppierung in SUESA wurden zwei weitere Funktionalitäten implementiert. Die erste Funktionalität bietet eine erste Auswertung der gefundenen Gruppen. Mit Hilfe der Checkboxen in Abbildung C.6 kann der Evaluator die Gruppen anzeigen, die gewisse Attribute beinhalten. So kann er zum Beispiel alle Gruppen sichtbar machen, bei denen die ersten zwei Attribute ausgewählt wurden und die dritte nicht ausgewählt wurde.

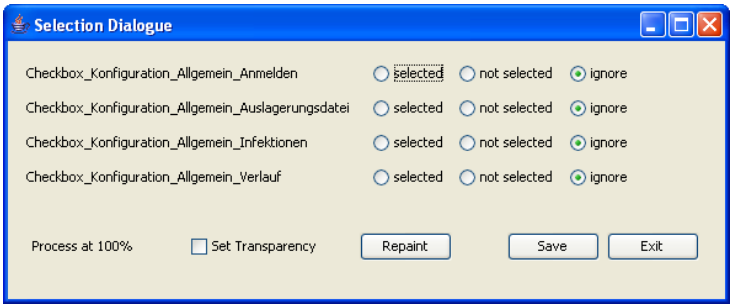


Abb. C.6: Analysemöglichkeiten für die gefundenen Gruppen

Die Ergebnisse seiner Gruppierungen kann der Evaluator für spätere weitere Analysen mit den Funktionen aus Abbildung C.2 abspeichern.

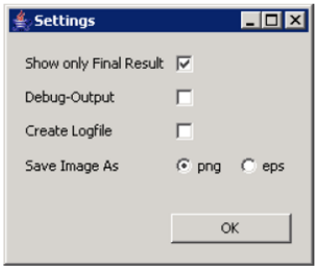


Abb. C.7: Speichermöglichkeiten für die gefundenen Ergebnisse

C.3 Mathematische Rahmenbedingungen und Phasen des SOM-Algorithmus in SUESA

Mathematische Rahmenbedingungen

Die einzelnen Neuronen sind gemäß Formel C.1 aufgebaut. Zusammen ergeben sie das Kohonennetz C.2.

$$\overrightarrow{\omega_i} = (\omega_{i1}, \omega_{i2}, ..., \omega_{im})^T \tag{C.1}$$

$$Kohonennetz = (\omega_i, ...\omega_m) \tag{C.2}$$

Die Neuronen werden in dem Netz durch ihre Gewichtsvektoren $\overrightarrow{\omega_1}, ...\overrightarrow{\omega_m}$ repräsentiert. Daher kann das Netz auch geschrieben werden als:

$$Kohonennetz_{in\_Abhängigkeit\_der\_Gewichtsvektoren} = (\overrightarrow{\omega_1}, ...\overrightarrow{\omega_m}) \tag{C.3}$$

Die Gewichtsvektoren bestehen dabei aus m Elementen:

$$Gewichtsvektoren = \overrightarrow{\omega_1}, ...\overrightarrow{\omega_m} \tag{C.4}$$

Diesem Netz werden im Verlauf der Gruppierung die Eingangsvektoren $\overrightarrow{x}$ präsentiert.

$$\overrightarrow{x} = (x_1, x_2, ..., x_n)^T \tag{C.5}$$

Zusätzlich muss gelten, dass die Neuronen auf der Karte genau so viele Elemente enthalten wie die Eingangsvektoren. Dies ist notwendig damit alle Vektoroperationen durchgeführt werden können. Konkret kann man sich die Elemente der Gewichtsvektoren oder aber auch die Elemente der Eingangsvektoren als die unterschiedlichen Handlungsoptionen der Benutzer und ihr an dieser Stelle getätigtes Verhalten vorstellen. Bei den Eingangsvektoren handelt es sich dann um die realen getätigten Handlungen der Benutzer. Bei den Gewichtsvektoren um jeweils einen Platzhalter für diese Handlungen. Dieser Platzhalter wird dann durch das Lernverfahren so mit Werten belegt, dass die jeweiligen Gruppenmitglieder eine minimale Abweichung zu ihm haben. Ein mögliches Beispiel wäre daher zum Beispiel:

$$\overrightarrow{Gewichtsvektor_{Beispiel}} = \overrightarrow{\omega_{checkbox1}}, ...\overrightarrow{\omega_{hilfefunktion1}}, ...\overrightarrow{\omega_{button_n}} \tag{C.6}$$

Aufbauend auf diesen Grundlagen werden in SUESA die folgenden Schritte zu der Gruppierung der Benutzer bei Verwendung einer SOM durchgeführt.

Allgemeine Phasen des SOM Gruppierungsalgoritmus in SUESA

1. *Wahl der Größe des Ergebnisnetzes und seiner Dimensionalität*[1]

   Die Dimensionalität legt fest, auf welche Dimensionalität die hochdimensionalen Eingangsvektoren reduziert werden sollen. Im Verlauf dieser Arbeit wurde als Dimensionalität fast ausschließlich zwei gewählt. So ließen sich die Ergebnisse am besten visuell darstellen. Der Evaluator sah so auf einen Blick, welche Benutzer sich jeweils in der gleichen Gruppen befanden.

   Die Größe des Ergebnisnetzes wird in Abhängigkeit zur Anzahl der jeweils zur Verfügung stehenden Eingangsvektoren bestimmt. Dabei legt die Anzahl der Eingangsvektoren das Minimum für die Kartengröße fest. Wenn es 100 Eingangsvektoren gibt, sollte als minimale Größe eine 10×10 Matrix gewählt werden, da diese auch 100 mögliche Ergebnisvektoren enthält. So könnten alle Eingangsvektoren in unterschiedliche Gruppen gruppiert werden, falls der Kohonenalgorithmus keinerlei Ähnlichkeit feststellen sollte.

   Ausgehend von dieser minimalen Größe sind weitere Größen für das Ergebnisnetz möglich[2]. Bei steigender Größe der Karte kann eine bessere Granularität der Ergebnisse erzielt werden. Allerdings steigt dadurch auch der Aufwand zur Berechnung an. Die Neuronen müssen für die visuelle Ausgabe nicht in quadratischen Netzen angeordnet werden. Kohonen schlägt dagegen vor, dass rechteckige Ergebnisnetze gewählt werden sollten da sie bessere Ergebnisse liefern. In diesem Falle hat das Ergebnisnetz die Breite b und die Höhe h.

2. *Initialisieren der Karte* Die Gewichtsvektoren der Neuronen werden mit zufälligen Werten initialisiert. Dabei ist darauf zu achten, dass diese Werte im gleichen Wertebereich (z.B. nach Normierung), wie die Werte der Testvektoren liegen.

3. *Initialisieren einer Lernrate η und einer Nachbarschaftsgröße σ*

   Die Lernrate muss nun festgelegt werden. Sie bestimmt, wie stark das Gewicht des zu verändernden Neurons durch den Testvektor geändert wird. Im Allgemeinen gilt

   $$1 > \eta_{start} > 0 \tag{C.7}$$

   und

   $$max(b, h) >= \sigma_{start} >= 0 \tag{C.8}$$

4. *Auswahl eines beliebigen Testvektors*

   Bei diesem Schritt wird ein zufälliger Testvektor aus der Menge der Eingabevektoren ausgewählt. Durch die zufällige Auswahl ist es natürlich möglich, dass mehrfach der selbe Vektor ausgewählt wird. Daher sollte die Lernphase so groß sein, dass sich diese Effekte vernachlässigen lassen.

[1] Um ein schnelles Ablesen zu ermöglichen, sollte die Dimensionalität nicht größer als zwei gewählt werden, auch wenn andere Werte als 0 oder 1 möglich sind.

[2] Kohonen empfiehlt in [71], dass man die Größe der Karte durch Ausprobieren festlegt

5. *Bestimmung des „gewinnenden Neurons“ auf der Karte*

   Nun wird das Neuron ermittelt, welches den geringsten Abstand zum Testvektor aufweist. Dieses Neuron ist das BMU (best matching unit). Der Abstand d_j wird dabei mit folgender Formel berechnet.

$$d_j = \sum_{i=0}^{N-1} (x_i(t) - \omega_{ij}(t))^2 \tag{C.9}$$

   Diese Abstandsberechnung basiert auf der allgemeinen Berechnung des Euklidischen Abstands (siehe Formel C.10).

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{C.10}$$

6. *Anpassen der Gewichtsvektoren* Die Gewichtsvektoren in der Nachbarschaft des BMU werden nun nach folgender Formel erneut berechnet und dann angepasst.

$$\overrightarrow{\omega_j^{neu}} = \overrightarrow{\omega_j^{alt}} + \eta(\overrightarrow{x^p} - \overrightarrow{\omega_j^{alt}}) \tag{C.11}$$

7. *Verringerung der Lernrate und der Nachbarschaftsgröße* Nun wird die Lernrate η und die Nachbarschaftsgröße σ verringert. Dies erfolgt meistens linear, kann aber auch exponentiell durchgeführt werden, um schneller zu Ergebnissen zu gelangen.

8. *Abbruchkriterium überprüfen und ggf. die Schritte 4-7 erneut durchführen*
   Der letzte Schritt sorgt für die Iteration der Schritte 4-7. Diese werden solange wiederholt, bis ein Abbruchkriterium erreicht wurde. Bei diesem Abbruchkriterium kann es sich beispielsweise um eine festgelegte Anzahl von Iterationen oder aber auch um dass Erreichen von η_{min} oder σ_{min} handeln.

Dieses beschriebene Konzept einer automatischen Gruppierung von Benutzern wurde in dem Prototypen von SUESA implementiert und in der Praxis umgesetzt und evaluiert.

Modifikationen bei der SOM Implementierung Im Folgenden werden die Änderungen bei der realen Implementation zum beschriebenen theoretischen SOM-Konzept aufgezeigt. Die in C.3 beschriebenen Phasen 1-5 werden wie oben beschrieben durchgeführt. Um schneller Ergebnisse für den Evaluator zu erhalten wurde Phase 7 allerdings modifiziert. Es wurde eine exponentielle Verringerung der Lernrate η und der Nachbarschaftsgröße σ implementiert. Diese Möglichkeit und seine Auswirkungen wurden bereits durch Kohonen beschrieben [71]. Die Formeln C.12 und C.13 zeigen die Änderungen dieser beiden Parameter in Abhängigkeit von der Zeit.

$$\eta(t+1) = \eta_{max} \left(\frac{\eta_{min}}{\eta_{max}} \right)^{\frac{t}{t_{max}}} \tag{C.12}$$

$$\sigma(t+1) = \sigma_{max} \left(\frac{\sigma_{min}}{\sigma_{max}} \right)^{\frac{t}{t_{max}}} \tag{C.13}$$

Durch diese Anpassung sind wesentlich schneller Ergebnisse für den Evaluator sichtbar. Die Abbildung C.8 illustriert dies grafisch. Dort ist die Veränderung der Lernrate in Abhängigkeit der Iterationsschritte aufgetragen. Zu sehen ist, dass eine exponentielle Verminderung der Lernrate ihren Einfluss auf Änderungen schnell dämpft. Das Gleiche gilt für eine exponentielle Verminderung der Nachbarschaftsgröße, da ihr Änderungseinfluss analog zur Lernrate aufgebaut ist.

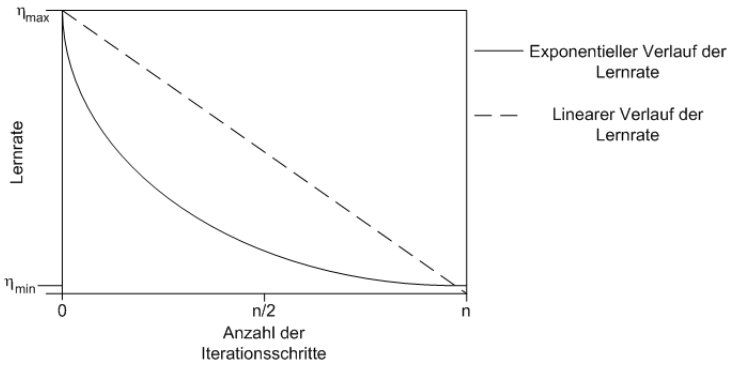


Abb. C.8: Änderung der Lernrate in Abhängigkeit von der gewählten Verringerung

Die oben beschriebene Phase der Anpassung des Gewichtsvektors (Phase 6) wurde in SUESA in Abhängigkeit unterschiedlicher Hauptkriterien zur Gruppierung beim verwendeten Testprogramm ebenfalls verändert. Die Gruppierung kann nach zwei verschiedenen Hauptkriterien durchgeführt werden.

Zum einen kann nach der benötigten Zeit für jeden Dialogschritt gruppiert werden, zum anderen nach dem Verhalten des Benutzers bei den Einstellungen (z.B. Checkboxen oder Hilfeaufrufe). Aus diesem Grunde wurde die oben beschriebene Phase zur Berechnung des Gewichtsvektors in Abhängigkeit dieser zwei Parameter in SUESA wie folgt modifiziert.

Modifikationen bei der Verwendung des Hamming-Abstandes Das Neuron der Karte mit dem geringsten Hamming-Abstand wird als BMU verwendet. In ersten Testversuchen zeigte sich allerdings häufiger, dass verschiedene Neuronen den gleichen Hamming Abstand zum Eingabevektor aufwiesen. Dies führte dazu, dass sich die Eingabewerte nur minimal in der Karte entfalteten. Die jeweils ersten Neuronen passten sich dabei an die Eingabevektoren an und konnten dann nicht mehr durch andere Neuronen verdrängt werden. Aus diesem Grunde wurde eine weitere Modifikation implementiert.

Zu jedem Neuron wurde eine Zufallszahl erstellt. Wenn der Hamming-Abstand zweier Neuronen zum Eingabevektor gleich war, wurden diese Zufallszahlen mit in die Berechnung einbezogen. Dadurch konnten auch die ersten Neuronen als BMU verdrängt werden. Somit wurde eine erheblich bessere Entfaltung der Karte erzielt.

Bei Verwendung des Hamming Abstandes musste die Anpassung der Neuronen in der Nachbarschaft der BMU ebenfalls modifiziert werden. Die Werte der Neuronen beinhalten nur ganzzahlige Werte aus der Menge $\{0, 1\}$. Somit können die Bitvektoren in der Nachbarschaft der BMU ebenfalls nur ganzzahlig geändert werden.

C.4 Weitere SUESA Ergebnisse

Die Tabellen C.1, C.2 und C.3 zeigen die Stammdaten der 35 Versuchsteilnehmer (basierend auf den Ergebnissen der Fragen 1, 2 und 3)

Geschlecht	Anzahl
männlich	26
weiblich	9

Tab. C.1: Geschlecht

Alter	Anzahl
≤ 25	15
26-30	12
31-40	5
41-50	1
51-60	1
≥ 61	1

Tab. C.2: Alter

Beruf	Anzahl
Student (Info.)	16
Angestellte(r)	9
sonstiger Student	4
Auszubildende(r)	2
Hausfrau	1
Pfarrer	1
arbeitssuchend	1
keine Angabe	1

Tab. C.3: Tätigkeit

Die Werte in den Tabellen C.1, C.2 und C.3 sind nicht verwunderlich. Da die Untersuchung hauptsächlich während Veranstaltungen an der Universität im Fachbereich Informatik durchgeführt wurde, sind die meisten Teilnehmer männlich und im Alter zwischen 20 und 30.

Im Fragebogen wurde die Versuchsteilnehmer gefragt, ob sie das Testprogramm problemlos benutzen konnten. Die gegebenen Antworten zeigen die Tabellen C.4, C.5 und C.6.

Wie würden Sie die Bezeichnungen der Einstellungen bewerten?	Anzahl
1 Eindeutig	10
2	10
3	6
4	1
5 Verwirrend	3
Keine Angabe	1

Tab. C.4: Bewertung der Bezeichnungen

Wie bewerten Sie die allgemeine Übersichtlichkeit der Anwendung?	Anzahl
1 Sehr gut	14
2	11
3	5
4	2
5 Sehr schlecht	1
Keine Angabe	2

Tab. C.5: Bewertung der Übersichtlichkeit

Wie würden Sie die Unterstützung durch die Hilfe zu den Einstellungen bezeichnen?	Anzahl
1 Sehr gut	7
2	11
3	9
4	3
5 Sehr schlecht	1
Keine Angabe	4

Tab. C.6: Bewertung der Hilfefunktion

Anhang D
Anhang zu GAMJA

D.1 Daten aus den Mousemaps

Anzahl benutzter Tooltips

Kenntnisse im Bereich Sicherheit	**Anzahl an Tooltips**	**Anzahl an Testpersonen**	**Durchschnitt**
Sehr gute Kenntnisse	16	2	8
gute Kenntnisse	44	11	4
Grundkenntnisse	47	10	4.7
keine Kenntnisse	23	4	5.75
keine Angabe	5	1	5

Tab. D.1: Anzahl an benutzten Tooltips

In dieser Tabelle wurden nur die 28 Versuchsteilnehmer berücksichtigt die alle Menüs bearbeitet hatten. Im Durchschnitt wurden somit 4.75 Tooltips von jedem Benutzer ausgewählt.

Die folgende Tabelle zeigt die Selbsteinschätzung der Teilnehmer in Bezug auf ihre IT-Sicherheitskenntnisse, welche in Beziehung gesetzt wurden zur zurückgelegten Wegstrecke mit der Maus.

Teilnehmer Nummer:	Kenntnisse im Bereich Sicherheit	Mausstrecke in Pixeln	größer(>) oder kleiner(<) als der Durchschnitt
2	Gute Kenntnisse	88877	<
3	Gute Kenntnisse	109656	<
4	Grundkenntnisse	250451	>
6	Gute Kenntnisse	117773	<
7	Gute Kenntnisse	135011	<
8	Sehr gute Kenntnisse	218674	>
9	Grundkenntnisse	99346	<
10	Sehr gute Kenntnisse	82878	<
11	Gute Kenntnisse	116476	<
12	Gute Kenntnisse	104504	<
13	Grundkenntnisse	217202	>
14	Gute Kenntnisse	154937	>
15	Grundkenntnisse	171614	>
16	Grundkenntnisse	94138	<
17	Keine Kenntnisse	109569	<
18	Grundkenntnisse	127052	<
22	Gute Kenntnisse	244472	>
23	Keine Angabe	150727	>
24	Keine Kenntnisse	85278	<
27	Grundkenntnisse	146003	>
28	Grundkenntnisse	120971	<
29	Keine Kenntnisse	184568	>
30	Keine Kenntnisse	130200	<
31	Gute Kenntnisse	103366	<
32	Gute Kenntnisse	154119	>
33	Gute Kenntnisse	120724	<
34	Grundkenntnisse	222800	>
35	Grundkenntnisse	164650	>

Tab. D.2: Selbsteinschätzung IT-Sicherheitskenntnisse

Anhang E
Die Einleitungs-Zitate

- „πάντα ῥει“
  (Heraklit)
  Alles fliesst
- *Η αυτόγνωσια ειναὶ ῆ πρώτη όλων τών γνωσέων*
  (Aristoteles)
  Das Ganze ist mehr als die Summe seiner Teile
- χαλεπὰ τὰ καλά
  (Überlieferung nach Plutarch)
  Das Gute ist schwer zu erreichen
- *„Bei einem Spiel kann man einen Menschen in einer Stunde besser kennen lernen als im Gespräch in einem ganzen Jahr“*
  (Überlieferung nach Platon)
  Das Zitat ist eine sehr freie Interpretation des Endes vom ersten Buch der *νόμοι*
- „Σκοπέειν δὲ χρὴ παντὸς χρήματος τὴν τελευτήν κῆ αποβήσεται“
  (Überlieferung nach Solon)
  Auf das Ende einer jeden Sache muss man schauen, wie sie einmal ausgehen wird

Anhang F
Abkürzungsverzeichnis

AAL **A**mbient **A**ssisted **L**iving

ACM **A**ssurance **C**onfiguration **M**anagement

ADO **A**ssurance **D**elivery and **O**peration

ADV **A**ssurance **D**evelopment **V**erification

AE **A**gent **E**ntity

AGD **A**ssurance **G**uidance **D**ocumentation

ALC **A**ssurance **L**ife **C**ycle

AMS **A**gent **M**anagement **S**ystem

ATE **A**ssurance **TE**sting

AVA **A**ssurance **V**ulnerability **A**nalysis

AUE **A**utomatisierte **U**sability **E**valuierungsverfahren

BMU **B**est **M**atching **U**nit

BSI **B**undesamt für **S**icherheit in der **I**nformationstechnik

BWL **B**etriebs**w**irtschafts**l**ehre

CA **C**ertification **A**utority

CC **C**ommon **C**riteria

CWT **C**ognitive **W**alk**t**hrough

DB **D**aten**b**ank

EAL **E**valuation **A**ssurance **L**evel

EM **E**xpectation **M**aximization

ET **E**lektro**t**echnik

EVG **EV**aluierungs **G**egenstand

FSP	**F**unctional **Sp**ecifications
HE	**H**euristische **E**valuation
HLD	**H**igh **L**evel **D**esign
IDS	**I**ntrusion **D**etection **S**ystem
IT	**I**nformations- **T**echnik
IU	**I**ntelligente **U**mgebungen
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
PUW	**P**luralistischer **U**sability-**W**alkthrough
SA	**S**ecurity **A**gent
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
SPAM	**SP**iced h**AM**
ST	**S**ecurity **T**arget
StW	**S**ozio**t**echnischer **W**alkthrough
TOE	**T**arget**o**f **E**valuation
WWW	**W**orld **W**ide **W**eb
XML	e**X**tensible **M**arkup **L**anguage

Literaturverzeichnis

[1] *DIN EN ISO 13407. Benutzer-orientierte Gestaltung interaktiver Systeme. Deutsche Fassung der EN ISO 13407.* Beuth, Berlin, 1997.

[2] *DIN EN ISO 9241. Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten. Deutsche Fassung der EN ISO 9241.* Beuth, Berlin, 1997.

[3] *ISO/IEC 17799:2005 Information Technology-Security Techniques-Code of Practice for Information Security Management.* International Standards Organization, Genf, 2005.

[4] *ISO/IEC 27001:2005 International Standard, First Edition.* International Standards Organization, Genf, 2005.

[5] *ISO/IEC 27002:2005 International Standard, Second Edition Renumbered 07/2007.* International Standards Organization, Genf, 2005.

[6] *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model September 2006 Version 3.1 Revision.* 2006.

[7] *XP-Antispy.* `http://www.xp-antispy.org`, 2007. Zugriff 16.05.2007.

[8] *Ambient Assisted Living Deutschland Homepage.* 2008. Zugriff 30.09.2008.

[9] *RFID-Chips stecken bald überall drin - Funkende Kleidung.* http://www.taz.de/1/archiv/dossiers/dossier-ueberwachung/rfid/artikel/1/funkende-kleidung/?src=SZ, 2008, Zugriff 17.06.2008.

[10] *Jacareto.* `http://jacareto.sourceforge.net/.`, 2008, Zugriff 22.05.2008.

[11] Alahuhta, Petteri, Paul De Hert, Sabine Delaitre, Michael Friedewald, Serge Gutwirth, Ralf Lindner, Ioannis Maghiros, Anna Moscibroda, Yves Punie, Wim Schreurs, Michiel Verlinden, Elena Vildjiounaite und David Wright: *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities.* Technischer Bericht ‚Deliverable D2, SWAMI: Safeguards in a World of Ambient Intelligence, Januar 2006.

[12] Albayrak, Sahin: *Introduction to Agent Oriented Technology for Telecommunications.* In: Albayrak, Sahin (Herausgeber): *Intelligent Agents for Telecommunications Applications*, Seiten 1–18. IOS Press, Basel, 1998.

[13] Albayrak, Sahin, Achim Müller, Christian Scheel und Dragan Milosevic: *Combining Self-Organizing Map Algorithms for Robust and Scalable Intrusion Detection.* In: Mohammadian, M. (Herausgeber): *Proceedings of International Conference on Computational Intelligence for Modelling Control and Automation (CIMCA 2005 Book 2)*, Seiten 123–130, Vienna, Austria, 2005.

[14] Arthur Dempster, Nan Laird und Donald Rubin: *Maximum likelihood from incomplete data via the EM algorithm.* In: *Journal of the Royal Statistical Society*, Band Series B, Seiten 1–38, 1977.

[15] Balfanz, Dirk, Glenn Durfee, Rebecca E. Grinter und D. K. Smetters: *In Search of Usable Security: Five Lessons from the Field.* In: *IEEE Security and Privacy*, Band 2, Seiten 19–24, Piscataway, NJ, USA, September 2004. IEEE Educational Activities Department.

[16] Bertelsmann Stiftung: *Aktion Demografischer Wandel.* `http://www.bertelsmann-stiftung.de/cps/rde/xchg/SID-E019EEDE-1C5254C5/bst/hs.xsl/73550.htm`, 2008, Zugriff 10.11.2008.

[17] Beywl, Wolfgang: *Standards für Evaluation.* Deutsche Gesellschaft für Evaluation e.V. Zimmermann-Medien, Köln, 2002.

[18] Bias, Randolph G.: *The pluralistic usability walkthrough: coordinated empathies.* In: *Usability inspection methods*, Seiten 63–76. John Wiley & Sons, Inc., New York, NY, USA, 1994.

[19] Bitkom, (Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V.): *Notebooks ziehen an Tisch-PCs vorbei.* http://www.bitkom.de/49665_46602.aspx, 2007. Zugriff 17.12.2008.

[20] Bortz, Jürgen: *Statistik für Sozialwissenschaftler.* Springer, Berlin [u.a.], 4. vollst. überarb. Auflage, 1993.

[21] Bsufka, Karsten: *Public Key Infrastrukturen in Agentenarchitekturen zur Realisierung dienstbasierter Anwendungen.* Doktorarbeit, Technische Universität Berlin, 2006.

[22] Bundesamt für Sicherheit in der Informationstechnik (BSI): *7138 - BSI-Zertifizierung - Hinweise für Hersteller und Vertreiber.* `http://www.bsi.de/zertifiz/zert/7138.pdf`, 2005, Zugriff: 02.10.2008.

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Certification Report BSI-DSZ-CC-0248-2005 for Java Intelligent Agent Componentware IV Version 4.3.11 from DAI- Labor Technische Universität Berlin.* `http://www.bsi.de/zertifiz/zert/reporte/0248a.pdf`, 2005, Zugriff: 10.11.2007.

[24] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Risiken und Chancen des Einsatzes von RFID-Systemen.* http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf, 2004, Zugriff 11.12.2008.

[25] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Leitfaden IT-Sicherheit.* http://www.bsi.bund.de/gshb/Leitfaden/GS-Leitfaden.pdf, 2007, Zugriff 10.03.2009.

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Die Lage der IT-Sicherheit in Deutschland 2007.* http://www.bsi.bund.de/literat/lagebericht/lagebericht2007.pdf, 2007, Zugriff 11.11.2008.

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kataloge - Stand 10. Ergänzungslieferung.* http://www.bsi.bund.de/gshb/deutsch/index.htm, Februar 2009, Zugriff 01.05.2009.

[28] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Glossar.* http://www.bsi-fuer-buerger.de/glossar/glo_ij.htm, Zugriff 10.03.2009.

[29] Burmester, M.: *Ist das wirklich gut? Bedeutung der Evaluation für benutzerzentrierte Gestaltung.* In: (Hrsg.), J. Machate; M. Burmester (Herausgeber): *User Interface Tuning. Benutzerschnittstellen menschlich gestalten*, Seiten 97–119. Software & SupportVerlag., Frankfurt/Main, 2003.

[30] Capgemini: *Studie IT-Trends 2007.* http://www.de.capgemini.com/m/de/tl/IT-Trends_2007.pdf, Februar 2007, Zugriff 19.02.2009.

[31] Clearswift: *Spyware: Eine Bedrohung mit vielen Gesichtern.* http://www.zdnet.de/i/wp/whitepaper_spyware_a_%20multi_faceted_threa_germ.pdf, 2006, Zugriff 01.02.2009.

[32] Cranor, Lorrie und Simson Garfinkel: *Security and Usability.* O'Reilly Media, Inc., Gravenstein Highway North - Sebastopol, 1. Auflage, August 2005.

[33] Dahm, Markus: *Grundlagen der Mensch-Computer-Interaktion.* Pearson Studium, München [u.a.], 2006.

[34] DAI-Labor: *JIAC IV.* http://www.jiac.de, 2008. Zugriff 22.08.2008.

[35] Dammann, U. und S. Simitis: *Bundesdatenschutzgesetz (BDSG) mit Materialien.* Namos-Verlag, Baden Baden, 1977.

[36] Dhamija, Rachna, J. D. Tygar und Marti Hearst: *Why phishing works.* In: *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, Seiten 581–590. ACM Press, New York, NY, USA, 2006.

[37] Eckert, Claudia: *Zur Sicherheit mobiler persönlicher Endgeräte - Eine Bestandsaufnahme.* In: *Arbeitskonferenz Kommunikationssicherheit*, SAP University Rot, März 2001.

[38] Eckert, Claudia: *IT-Sicherheit.* Oldenbourg Wissenschaftsverlag GmbH, München Wien, 2006.

[39] Encarnacão, José Luis: *Ambient mobility: human environment interface and interaction challenges.* In: *AVI '08: Proceedings of the working conference on Advanced visual interfaces*, Seiten 3–3. ACM, New York, NY, USA, 2008.

[40] Espey, Jürgen, Hartmut Neuf, Cornelius Dufft, Georg Rudinger und Kurt-Hermann Stapf: *Wie alarmiert sind die Nutzer?* In: Müller, G. & Stapf, K. H. (Herausgeber): *Mehrseitige Sicherheit in der Kommunikationstechnik.*, Seiten 233–248. Addison-Wesley-Longmann, Bonn, 1998.

[41] F-Secure: *Bedrohen Spartaner die Sicherheit unserer PCs?* http://www.f-secure.com/de_DE, Februar 2009. Zugriff 01.05.2009.

[42] Focus online: *Datenmissbrauch - Telekom will Strafanzeige erstatten.* `http://www.focus.de/finanzen/news/datenmissbrauch-telekom-will-strafanzeige-erstatten_aid_352246.html`, 2008, Zugriff 30.11.2008.

[43] Friedewald, Michael und Ralf Lindner: *Gesellschaftliche Herausforderungen durch „intelligente Umgebungen“.* In: *Technikfolgenabschätzung, Theorie und Praxis. Technology assessment 17*, Seiten 78–83. Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Mai 2008, Zugriff 17.5.2009.

[44] Frommann, Uwe: *Die Methode Lautes Denken.* `http://www.e-teaching.org/didaktik/qualitaet/usability/Lautes%20Denken_e-teaching_org.pdf`, August 2005, Zugriff 01.03.2008.

[45] Gediga, G., K. Hamborg und I. Duntsch: *Evaluation of Software Systems.* In: Kent, A. und J.G. Williams (Herausgeber): *Encyclopedia of Library and Information Science Vol. 72.*, Seiten 166–192. Marcel Dekker, Inc., New York, 2002.

[46] Gediga, G. und K. C. Hamborg: *Evaluation in der Software-Ergonomie: Methoden und Modelle im Softwareentwicklungsprozess.* In: *Zeitschrift für Psychologie, 210 (1)*, Seiten 40–57, 2002.

[47] Geissler, Tim und Olaf Kroll-Peters: *Applying Security Standards to Multi Agent Systems.* In: *The First International Workshop on Safety and Security in Multiagent Systems (SASEMAS) Part of AAMAS held at Columbia University New York City*, 2004.

[48] Gellner, Michael: *Mousemaps – ein Ansatz für eine Technik zur Visualisierung der Nutzung von Software und zur Automation der Entdeckung von Bedienungsfehlern.* In: G. Szwillus, J. Ziegler (Herausgeber): *Mensch & Computer - Interaktion in Bewegung*, Seiten 197–206. B. G. Teubner, Stuttgart, 2003.

[49] Gellner, Michael, Peter Forbrig und Manja Nelius: *Results of Mousemap-based Usability Evaluations - Towards Automating Analyses of Bahavioural Aspects.* In: *Proceedings of the 8th ERCIM Workshop „User Interfaces for All“*, 2007.

[50] Grünwied, Gertrud: *Psychophysiologische Parameter der Software-Usability: Experimentelle Studie zur Korrelation zwischen Eye-Tracking-Parametern und Software-Designdomänen.* Doktorarbeit, Universität Ulm, 2007.

[51] Gutmann, Peter und Ian Grigg: *Security Usability.* In: *IEEE Security and Privacy*, Band Volume 3, Number 4, Seiten 56–58, 2005.

[52] Harris, Jensen: *The Expert Mode Misadventure.* `http://blogs.msdn.com/jensenh/archive/2006/02/07/526635.aspx`, Februar 2006, Zugriff 10.11.2008.

[53] Hegner, Marcus: *Methoden zur Evaluation von Software.* In: *IZ-Arbeitsbericht Nr. 29.* Informationszentrum Sozialwissenschaften der Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e.V. (ASI), Bonn, 2003.

[54] Hensel, Martin: *Bluetooth-fähige mobile Geräte als Security-Risiko und Angriffspunkt.* http://www.searchsecurity.de/themenbereiche/netzwerksicherheit/wireless-security/articles/88783/, 2007, Zugriff 01.03.2009.

[55] Herrmann, Thomas, Gabriele Kunau und Kai-Uwe Loser: *Sociotechnical Walkthrough - ein methodischer Beitrag zur Gestaltung soziotechnischer Systeme.* In: M. Herczeg, W. Prinz, H. Oberquelle (Herausgeber): *Mensch & Computer - 2002: Vom interaktiven Werkzeug zu kooperativen Arbeits- und Lernwelten*, Seiten 323–332. B. G. Teubner, Stuttgart, 2002.

[56] Hirsch, Benjamin, Stefan Fricke, Olaf Kroll-Peters und Thomas Konnerth: *Agent Programming in Practise, Experiences with the JIAC IV Agent Framework.* In: *Proceedings of the AT2AI 2008*, 2008.

[57] HTW Chur, Hochschule für Technik und Wirtschaft: *3.2 Bedrohungen.* `http://www.tlab.ch/praktika/serieIII/c15/theorie/sicherheit/bedrohungen.html`, Version: 3.0, 15. December 2005, Zugriff: 26.09.2008.

[58] Ivory, Melody Y. und Marti A Hearst: *The state of the art in automating usability evaluation of user interfaces.* In: *ACM Comput. Surv.*, Band 33, Seiten 470–516. ACM Press, New York, NY, USA, 2001.

[59] Janson, Andre: *Usability-Engineering als Instrument des Managements informationstechnologischer Veränderungsprozesse in Unternehmen.* Doktorarbeit, Otto-Friedrich-Universität Bamberg, 2001.

[60] Jendricke, Uwe: *Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement.* Rhombos-Verlag, Berlin, Januar 2003.

[61] Jennings, Nicholas R. und Michael Wooldridge: *Agent-Oriented Software Engineering.* In: *ARTIFICIAL INTELLIGENCE*, Band 117, Seiten 277–296. 2000.

[62] Jokela, Timo, Netta Iivari, Juha Matero und Minna Karukka: *The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11.* In: *CLIHC '03: Proceedings of the Latin American conference on Human-computer interaction*, Seiten 53–60. ACM Press, New York, NY, USA, 2003.

[63] Kalbach, James: *Von Usability überzeugen.* In: Heinsen, Sven und Petra Vogt (Herausgeber): *Usability praktisch umsetzen*, Seiten 7–21. Hanser, Berlin, 2003.

[64] Karat, Claire-Marie, Robert Campbell und Tarra Fiegel: *Comparison of empirical testing and walkthrough methods in user interface evaluation.* In: *CHI '92: Proceedings of the SIGCHI conference on Human factors in computing systems*, Seiten 397–404. ACM, New York, NY, USA, 1992.

[65] Kemp, J.A.M. und T. van Gelderen: *Co-discovery exploration: an informal method for the iterative design of consumer products.* In: Jordan, B.Thomas, A. Weerdmeester und McClelland (ed.) (Herausgeber): *Usability evaluation in industry*, Seiten 139–146. Taylor and Francis Ltd, London, 1996.

[66] Kersten, Heinrich, Jürgen Reuter und Klaus-Werner Schröder: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung.* Vieweg+Teubner, Wiesbaden, 1 Auflage, Oktober 2007.

[67] Kirste, Thomas: *Intelligente Umgebungen.* `http://www.iuk-verbund.uni-rostock.de/downloads/Kirste-Intelligente_Umgebungen-07-06-22.pdf`, 2007, Zugriff 01.03.2009.

[68] Kleinz, Torsten: *Sicherheit im Internet: Auf dem Weg zum aufgeklärten Anwender.* http://www.heise.de/newsticker/Sicherheit-im-Internet-Auf-dem-Weg-zum-aufgeklaerten-Anwender–/meldung/103329, Februar 2008, Zugriff: 06.05.2008.

[69] Klinke, A.; Renn, O.: *Precautionary principle and discursive strategies: classifying and managing risks.* In: *Journal of Risk Research*, Seiten 159–173, 2001.

[70] Kohonen, Teuvo: *Self-organized formation of topologically correct feature maps.* In: *Neurocomputing: foundations of research*, Seiten 509–521. MIT Press, Cambridge, MA, USA, 1982.

[71] Kohonen, Teuvo: *Self-Organizing Maps.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2001.

[72] Krause, Brian R.: *Usability Vs Security.* http://tech.suramya.com/usability/ Zugriff 10.11.2008.

[73] Kroll-Peters, Olaf: *Werkzeuge zur Unterstützung in der Hochschullehre.* In: *Proceedings of the 4 Academic Days.* Berlin, 2008.

[74] Kroll-Peters, Olaf, Benjamin Hirsch und Natascha Jasmin Tiotuico: *Learning through enthusiasm - how more interaction and relation to real life lead to a better understanding and less learning effort.* In: *Proceedings of the INTED 2008*, Valencia, 2008.

[75] Kroll-Peters, Olaf und Michael Quade: *Herausforderungen der heutigen IT-Systeme.* In: *Jahrbuch öffentliche Sicherheit*, Seiten 587–594. Verlag für Polizeiwissenschaften, Frankfurt a. Main, 2007.

[76] Kroll-Peters, Olaf und Mathias Wilhelm: *Should Entertainment robots use emotional speech.* In: *Proceedings of the IROS 2008*, Nizza, 2008.

[77] Krug, Steve: *Don't make me think! Web Usability: Das intuitive Web*, Band 201. Mitp-Verlag, Heidelberg, 2. Auflage, Juli 2006.

[78] Kujala, Sari und Marjo Kauppinen: *Identifying and selecting users for user-centered design.* In: *NordiCHI '04: Proceedings of the third Nordic conference on Human-computer interaction*, Seiten 297–303. ACM, New York, NY, USA, 2004.

[79] Lavery, Darryn, Gilbert Cockton und Malcolm P. Atklnson: *Comparison of Evaluation Methods Using Structured Usability Problem Reports.* In: *In Behaviour and Information Technology*, Seiten 246–266. Taylor and Francis Ltd, 1997.

[80] Lewis, Clayton und Cathleen Wharton: *Cognitive Walkthroughs.* In: *Handbook of Human-Computer Interaction.* Elsevier Science Inc., New York, NY, USA, 1997.

[81] Markotten, Daniela Gerd tom: *Benutzbare Sicherheit in informationstechnischen Systemen.* Doktorarbeit, Albert-Ludwigs-Fakultät Freiburg i.Brsg., 2003.

[82] Markotten, Daniela Gerd tom, Uwe Jendricke und Günter Müller: *Benutzbare Sicherheit – Der Identitätsmanager als universelles Sicherheitswerkzeug.* In: Müller, Günter und Martin Reichenbach (Herausgeber): *Sicherheitskonzepte für das Internet*, Kapitel 7, Seiten 135–146. Springer-Verlag Berlin, 2001.

[83] Markotten, Daniela Gerd tom und Johannes Kaiser: *Benutzbare Sicherheit - Herausforderungen und Modell für E-Commerce-Systeme.* In: *Wirtschaftsinformatik*, Band 42, Seiten 531–538, 2000.

[84] Meissner, Klaus: *Evaluation intelligenter Benutzerschnittstellen.* `http://chili.ssji.net/utc/IMUI/vorl_10.pdf`, 2005. Zugriff 09.09.2008.

[85] Meyers: *Informationstechnologie.* `http://lexikon.meyers.de/wissen/\discretionary{-}{}{}Informationstechnologie`, Version: 1.1.11 Build: 22 Revision: 5785, 2008, Zugriff: 26.09.3008.

[86] Mitchell, Tom M.: *Machine Learning.* McGraw-Hill, New York, 1997.

[87] Mitnick, Kevin und William Simon: *Die Kunst der Täuschung, Risikofaktor Mensch.* Mitp-Verlag, Heidelberg, 2006.

[88] Müller, Günter, Thorsten Eymann und Michael Kreutzer: *Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft.* Oldenbourg, 2002.

[89] Müller, Günter und Daniela Gerd tom Markotten: *Sicherheit in der Kommunikations- und Informationstechnik.* In: *Wirtschaftsinformatik*, Band 42, Seiten 487–488, 2000.

[90] Müller, Günther und Andreas Pfitzmann: *Mehrseitige Sicherheit in der Kommunikationstechnik.* Addison Wesley, Bonn, 1997.

[91] Nelius, Manja: *Mousemap-basierte Erkennung der Problemfelder von Anwendern bei der Bedienung von Software.* `http://wwwswt.informatik.uni-rostock.de/deutsch/Mitarbeiter/michael/obsys/Obsys_Studie_Nelius_Obsys_Fehlererkennung.pdf`, November 2003, Zugriff 21.09.2008.

[92] Neuf, Hartmut und Jürgen Espey: *Gefahren der Telekommunikation: Welche Risiken beachtet der Verbraucher?* In: Müller, G. & Stapf, K. H. (Herausgeber): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Seiten 199–218. Addison-Wesley-Longmann, Bonn, 1998.

[93] Nielsen, Jakob: *Finding usability problems through heuristic evaluation.* In: *CHI '92: Proceedings of the SIGCHI conference on Human factors in computing systems*, Seiten 373–380. ACM Press, New York, NY, USA, 1992.

[94] Nielsen, Jakob: *Usability Engineering.* AP Professional, New York, 1993.

[95] Nielsen, Jakob: *Heuristic evaluation.* In: *Usability inspection methods*, Seiten 25–62. John Wiley & Sons, Inc., New York, NY, USA, 1994.

[96] Nielsen, Jakob: *Usability 101: Introduction to Usability.* http://www.useit.com/alertbox/20030825.html, 2003, Zugriff: 20.09.2008.

[97] Nielsen, Jakob: *User Education Is Not the Answer to Security Problems.* http://www.useit.com/alertbox/20041025.html, 2004, Zugriff: 22.10.2008.

[98] Nielsen, Jakob und Rolf Molich: *Heuristic evaluation of user interfaces.* In: *CHI '90: Proceedings of the SIGCHI conference on Human factors in computing systems*, Seiten 249–256. ACM Press, New York, NY, USA, 1990.

[99] Pohlmann, Norbert und Hartmut Blumberg: *Der IT-Sicherheitsleitfaden.* Redline GmbH, Heidelberg, 2. aktualisierte Auflage, 2006.

[100] Rannenberg, Kai: *Multilateral security a concept and examples for balanced security.* In: *NSPW '00: Proceedings of the 2000 workshop on New security paradigms*, Seiten 151–162. ACM, New York, NY, USA, 2000.

[101] Rannenberg, Kai, Andreas Pfitzmann und Günter Müller: *Sicherheit, insbesondere mehrseitige Sicherheit.* In: Günter Müller, Andreas Pfitzmann (Herausgeber): *Mehrseitige Sicherheit in der Kommunikationstechnik, Band 1, Verfahren, Komponenten,Integration*, Seiten 21–30. Addison-Wesley, Bonn, 1997.

[102] Reder, Bernd: *Monitoring-Systeme - Nagios wacht für Wilken.* `http://www.networkcomputing.de/frauen-verkaufen-passwoerter-fuer-schokolade/`, 2008, Zugriff 24.11.2008.

[103] Reisse, Christiane und Thomas Kirste: *A distributed mechanism for device cooperation in Smart Environments.* In: *Proceedings of Pervasive 2008 conference*, Sydney, Australia, May 19-22, 2008.

[104] Reiterer, Harald und Reinhard Oppermann: *Evaluation of user interfaces, EVADIS II - a comprehensive evaluation approach.* In: *Behavior & Information Technology*, Band 12, Seiten 137–148, 1993.

[105] Renn, O. und M.M. Zwick: *Risiko- und Technikakzeptanz.* Deutscher Bundestag, Enquete-Kommission, Schutz der Menschen und der Umwelt, Berlin, 1997.

[106] Richter, Michael und Markus Fläckiger: *Usability Engineering kompakt - Benutzbare Software gezielt entwickeln.* Elsevier, Spektrum Akademischer Verlag, erste Auflage, 2007.

[107] Rudolph, K., Gale Warshawsky und Louis Numkin: *Security Awareness.* In: Kabay, M. E. (Herausgeber): *Computer Security Handbook*, Kapitel 29. John Wiley & Sons, Inc., Basel, 4. Auflage, 2002.

[108] Sabine Kirchhoff, Sonja Kuhnt, Peter Lipp Siegfried Schlawin: *Der Fragebogen - Datenbasis, Konstruktion und Auswertung.* Leske + Budrich, Opladen, 2. Auflage, 2001.

[109] Saltzer, J. H. ; Schroeder, M. D.: *The Protection of Information in Computer System.* In: *Proceedings of the IEEE 63*, Seiten 1278 – 1308, 1975.

[110] Sarodnick, Florian und Henning Brau: *Methoden der Usability Evaluation.* Verlag Hans Huber, Bern, 2006.

[111] Schmidt, Jürgen: *Schutzbehauptung - Antivirenprogramme auf dem Prüfstand.* In: *CT Magazin für Computer Technik*, 2009.

[112] Schneier, Bruce: *Applied Cryptography.* John Wiley & Sons, Inc., New York, NY, USA, 2. Auflage, 1996.

[113] Schneier, Bruce: *Secrets and Lies. IT-Sicherheit in einer vernetzten Welt.* Dpunkt Verlag, Heidelberg, 2004.

[114] Schoder, Detlef und Günter Müller: *Potentiale und Hürden des Electronic Commerce: Eine Momentaufnahme.* In: *Informatik Spektrum*, Band 22, Seiten 252–260, 1999.

[115] Singh, Simon: *Geheime Botschaften.* Carl Hanser Verlag München Wien, 2000.

[116] Someren, Maarten W. van, Yvonne F. Barnard und Jacobijn A.C. Sandberg: *THE THINK ALOUD METHOD, A practical guide to modelling cognitive processes.* Academic Press, London, 1994.

[117] Staatskanzlei, Landesregierung Brandenburg: *Demografischer Wandel in Brandenburg.* `http://www.lda.brandenburg.de/cms/media.php/1168/db_end.pdf`, 2005, Zugriff 09.11.2008.

[118] Stapelkamp, Torsten: *Zielgruppenanalyse und -ansprache in Screen- und Interfacedesign.* X.media.press. Springer, Berlin - Heidelberg, 2007.

[119] Stary, Christian: *Interaktive Systeme - Software-Entwicklung und Software-Ergonomie (Interactive systems - software development and ergonomics).* Vieweg, Braunschweig Wiesbaden, Januar 1996.

[120] Technischer Überwachungs Verein Informationstechnik (TÜVIT): *Certification Report TUVIT-DSZ-CC-9222 for function library IAIK-JCE CC Core, Version 3.1.* https://www.secure.trusted-site.de/certuvit/pdf/9222BE.pdf, 2005.

[121] Thome, Günter und Wolfgang Sollbach: *Grundlagen und Modelle des Information Lifecycle Management.* Springer, Berlin Heidelberg, 2007.

[122] Tiotuico, Natascha Jasmin, Olaf Kroll-Peters, Benjamin Hirsch und Paul Zernicke: *Ambient learning perspectives in the context of modern information and communication technology.* In: *Proceedings of the INTED 2008*, Valencia, 2008.

[123] Uehling, Dana L. und Karl Wolf: *User action graphing effort (UsAGE).* In: *CHI '95: Conference companion on Human factors in computing systems*, Seiten 290–291. ACM Press, New York, NY, USA, 1995.

[124] Weidenmann, B. Andreas Krapp und: *Pädagogische Psychologie.* Beltz, Psychologie-Verl.-Union, München, 4. vollst. überarb. Auflage, 2001.

[125] Weiss, Harald: *Mitarbeiter sind weiterhin das größte Sicherheitsrisiko.* `http://microsite.computerzeitung.de/awareness-cz/index.html?pid=ee54f3c7-0de1-40f5-bb23-2cfdf022aee5&page=2`, Dezember 2007, Zugriff: 23.02.2009.

[126] West, Ryan: *The psychology of security.* In: *Commun. ACM*, Band 51, Seiten 34–40. ACM, New York, NY, USA, 2008.

[127] Wharton, Cathleen, Janice Bradford, Robin Jeffries und Marita Franzke: *Applying cognitive walkthroughs to more complex user interfaces: experiences, issues, and recommendations.* In: *CHI '92: Proceedings of the SIGCHI conference on Human factors in computing systems*, Seiten 381–388. ACM Press, New York, NY, USA, 1992.

[128] Wharton, Cathleen, John Rieman, Clayton Lewis und Peter Polson: *The cognitive walkthrough method: a practitioner's guide.* In: *Usability inspection methods*, Seiten 105–140. John Wiley & Sons, Inc., New York, NY, USA, 1994.

[129] Wirtschaftsprüfungsgesellschaft Ernst und Young: *Wireless Lan: Ein Paradies für Hacker?* http://www.ecin.de/mobilebusinesscenter/swlan/index.html, 2003, Zugriff 01.03.2009.

[130] Witten, Ian H. und Eibe Frank: *Data Mining: Practical machine learning tools and techniques.* Diane Cerra, San Francisco, zweite Auflage, 2005.