February 2005

Security Awareness Management - Konzeption, Methoden und Anwendung

Jan vom Brocke
European Research Center for Information Systems (ERCIS)

Christian Buddendick
European Research Center for Information Systems (ERCIS)

In: Ferstl, Otto K, u.a. (Hg) 2005. *Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety*; 7. Internationale Tagung Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag

ISBN: 3-7908-1574-8

Security Awareness Management – Konzeption, Methoden und Anwendung

Jan vom Brocke, Christian Buddendick
European Research Center for Information Systems (ERCIS)

Zusammenfassung: IT-Sicherheit ist für Unternehmen von elementarer Bedeutung. Im IT-Sicherheitsmanagement werden Techniken entwickelt, mit denen die Sicherheit von Informationssystemen gewährleistet werden soll. Aktuelle Studien zeigen, dass der überwiegende Teil von Betriebsstörungen auf menschliches (Fehl-)Verhalten zurückzuführen ist. Daher erscheint es notwendig, das IT-Sicherheitsmanagement um Teilbereiche zu erweitern, in denen das menschliche Verhalten in den Mittelpunkt der Betrachtung gerückt wird. Mit diesem Beitrag wird hierzu das Security Awareness Management (SAM) vorgestellt. Ausgehend von der Konzeption des SAM wird als zentrale Methode das Security Awareness Training (SAT) eingeführt. Das SAM wird abschließend anhand einer erfolgreichen Anwendung in der unternehmerischen Praxis veranschaulicht.

Schlüsselworte: IT-Sicherheit, IT-Security, Security Awareness, Security Awareness Management, Security Awareness Training, E-Learning, Multi-Channel-Learning

1 Konzeption eines Security Awareness Managements

1.1 Gegenstand des Security Awareness Management

Die Sicherheit unternehmerisch genutzter Informationssysteme zählt zu den führenden Herausforderungen der Zukunft [Erns03]. Das IT-Sicherheitsmanagement umfasst, nach ISO 13335-1 (Guidelines for the Management of IT Security), "all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability" [ISO00]. Diese übergeordneten Ziele der IT-Sicherheit lassen sich in Abhängigkeit der Betrachtungsperspektive durch weitere Ziele konkretisieren [zu einem Überblick vgl. FePf00]. Aus Unternehmenssicht ist neben dem Bedarf nach technischen Lösungen [Ecke03, S. 4ff.; GrJe03; Stelz93, S. 43ff.; PrPe04; MeBe04] verstärkt die Rolle des Menschen in Betracht zu ziehen. So zeigt eine aktuelle Studie von FOX, dass 60 – 80% sämt-

licher Betriebsstörungen auf menschliches Verhalten zurückzuführen sind [Fox03, 678]. Aufgrund dieses erheblichen Einflusses des Menschen auf die Sicherheit von Informationssystemen gewinnt der Aspekt des Sicherheitsbewusstseins – die sog. Security Awareness – zunehmend an Bedeutung [Fox03, 677].

Durch ein Security Awareness Management (SAM) soll die zielgerichtete Entwicklung und Nutzung des Sicherheitsbewusstseins in einem Unternehmen gewährleistet werden. Das SAM umfasst somit Funktionen die der Planung, Durchsetzung und Kontrolle des sicherheitsbewussten Verhaltens von Mitarbeitern dienen. Zur Erfüllung dieser Funktionen werden angemessene Methoden benötigt. Ein Beispiel für die Bedeutung des SAM liefert der Bereich des E-Mailverkehrs: Technische Maßnahmen zur Filterung infizierter E-Mails (z. B. durch Trojanische Pferde) können durch Maßnahmen des SAM begleitet werden, indem Systemnutzer über die Gefahrenquellen (z. B. E-Mails mit Anhängen unbekannter Absender) sowie Möglichkeiten ihrer Abwehr (Löschen der E-Mails) informiert werden. Im Folgenden ist zu untersuchen, wie ein SAM zu konzipieren ist, um einen Beitrag zur Sicherheit des Einsatzes von Informationssystemen in Unternehmen zu leisten. Aufgrund der zentralen Bedeutung des Menschen, sind hierzu zunächst relevante kognitionswissenschaftliche Grundlagen einzuführen.

1.2 Kognitionswissenschaftliche Grundlagen des SAM

Die kognitionswissenschaftliche Forschung beschäftigt sich mit der Erklärung von menschlichen Handlungen, wobei eine Reihe von Theorieansätzen wie z. B. die ACT*-Theorie nach ANDERSON [Ande83, S. 18; Ande88, S. 219ff.] Erklärungen für bestimmte Handlungen liefern. Dem Theorieansatz der Handlungsregulation kommt in der Kognitionsforschung eine zentrale Bedeutung zu [zu einem Überblick vgl. BeRi94]. Handeln wird dort als Resultat von mehreren psychischen Kräften (Motivationen und Emotionen) und Funktionen (Wahrnehmen, Lernen, Denken) erklärt [SeDö96, S. 20f.; Dörn96, S. 100ff.]. Die PSI-Theorie [Dör+88; Scha97], als Teil dieses Theorieansatzes, ist besonders für die Erklärung von menschlichen Handlungen bei denen Informationssysteme genutzt werden, geeignet [EsRu99, S. 101]. Sie wird in Abbildung 1 schematisch dargestellt.

Nach der PSI-Theorie bilden individuelle Bedürfnisse, die sowohl materieller (z. B. Geld, sicherer Arbeitsplatz), als auch immaterieller (z. B. Affiliation, Kompetenz) Art sein können [DöSc98, S. 10], den Ausgangspunkt menschlichen Handelns. Damit diese Bedürfnisse durch Handlungen verwirklicht werden können, sind sie in handhabbaren Zielen zu bündeln und zu konkretisieren. Motive als globale Handlungsanweisungen in denen mögliche Wege der Zielerreichung berücksichtigt werden, ergeben sich aus einzelnen Zielen. Erweist sich ein Motiv in einer bestimmten Situation als durchsetzbar, so wird aus ihm eine Absicht. Die Beurteilung erfolgt hierbei vor dem Hintergrund des vorhandenen Vorwissens und den daraus resultierenden Erwartungen sowie der wahrgenommenen Realität. Eine

Konkretisierung der verfolgten Absichten erfolgt durch die Auswahl bzw. Konstruktion von Handlungen. Die faktische Umsetzung von Handlungen wird als Aktion bezeichnet. Regulierend auf sämtliche Phasen des Prozesses wirken sowohl die Wahrnehmung der aktuellen Situation als auch das Vorwissen über Handlungsstrukturen, die in der Vergangenheit zur Erreichung des Handlungsziels eingesetzt worden sind [DöSc98, S. 24]. Stimmen Ziel und Ergebnis des Prozesses überein, konnte ein vorhandenes Bedürfnis erfolgreich verwirklicht werden. Störfaktoren führen in der Realität häufig dazu, dass vorhandene Bedürfnisse nicht verwirklicht werden können.

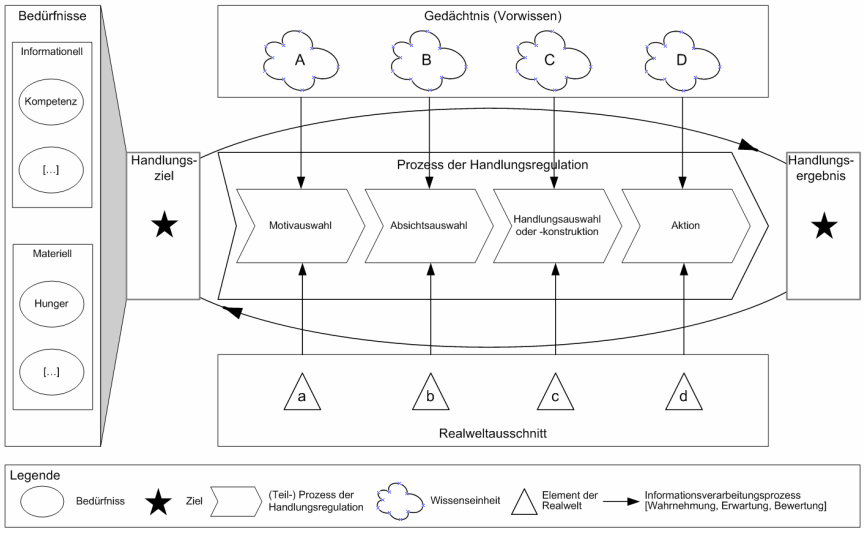

Abbildung 1: Prozess der Handlungsregulation nach der PSI-Theorie

Im Folgenden wird die PSI-Theorie auf Handlungen im unternehmerischen Umgang mit Informationssystemen übertragen. Auf diese Weise können sicherheitskritische Störfaktoren identifiziert werden, die Ansatzpunkte für das SAM liefern.

1.2 Anforderungen an das SAM

1.2.1 Identifikation von Störfaktoren

Bei der Übertragung der PSI-Theorie auf Nutzungsprozesse von Informationssystemen fällt auf, dass eine Vielzahl unterschiedlicher Handlungsprozesse von Bedeutung sind. Das Grundproblem besteht darin, dass individuelle Bedürfnisse mit den Sicherheitsinteressen auf Gesamtunternehmensebene in Konflikt stehen können. Die hieraus resultierenden Störfaktoren sind in Abbildung 2 vor dem Hintergrund der PSI-Theorie systematisiert worden.

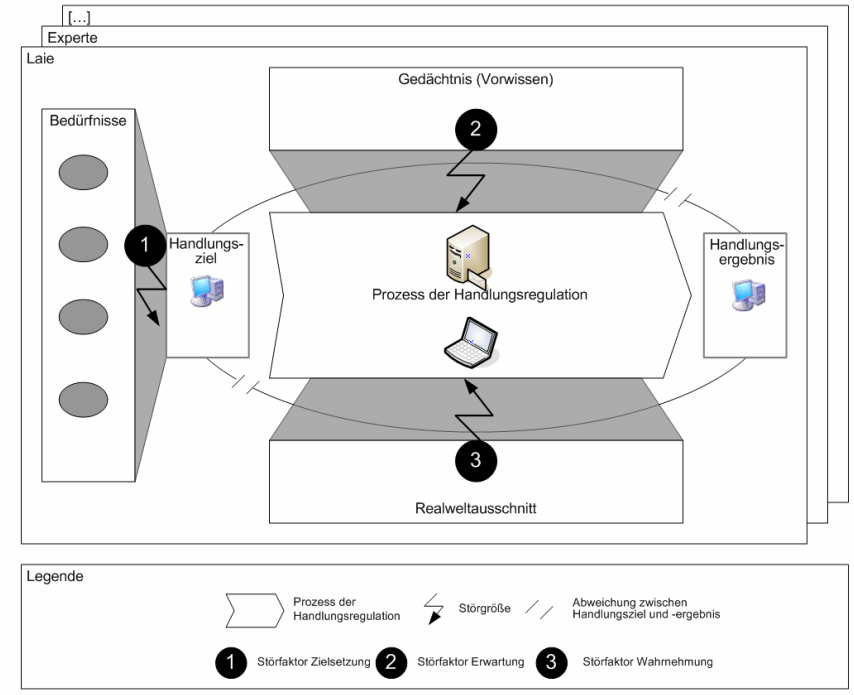

Abbildung 2: Handlungen von Nutzern von Informationssystemen und Störfaktoren

Die in Abbildung 2 verzeichneten Störgrößen werden im Folgenden vorgestellt.

Störfaktor: Zielbildung

Mitarbeiter eines Unternehmens nutzen Informationssysteme zur Ausführung betrieblicher Prozesse. Die Gewährleistung der Systemsicherheit stellt somit i. d. R. nicht das primäre Handlungsbedürfnis der Nutzer dar [EsRu99, S. 97f.; Hölt03, S. 166]. Vielmehr sind sogar Bedürfnisse denkbar, von denen sicherheitsgefährdende Aktionen ausgehen können. Ein Beispiel stellen Geltungsbedürfnisse dar, die einzelne Nutzer dazu verleiten können, zur Signalisierung von IT-Kompetenz z. B. Sicherheitseinstellungen im E-Mail-Client zu modifizieren. Sicherheit stellt somit für Nutzer grundsätzlich ein derivatives Bedürfnis dar, das im störungsfreien Betrieb der genutzten Systeme besteht (z. B. Funktionsfähigkeit des Mailverkehrs). Ein SAM hat somit das Bedürfnis nach Sicherheit bei den individuellen Nutzern zu wecken oder dessen Bedeutung zu verstärken. Auf diese Weise ist zu erreichen, dass Nutzer im Zuge ihrer Zielbildung möglichst nur solche Ziele auswählen, die die Sicherheit nicht gefährden.

Störfaktor: Erwartung

Einen weiteren Störfaktor stellt das individuelle Vorwissen der Nutzer dar, das deren Erwartungen prägt. Selbst wenn der Nutzer bei seinen Handlungen ein sicherheitsförderliches Ziel verfolgt, kann durch fehlendes oder falsches Vorwissen die Erreichung des Ziels gefährdet werden. Nutzer können vor allem zu falschen Erwartungen hinsichtlich der Konsequenzen ihrer Handlungen verleitet werden. So ist z. B. zu beobachten, dass Nutzer aufgrund ihrer Erfahrungen mit dem Briefverkehr ähnliche Erwartungen an Authentizität und Vertraulichkeit des E-Mailverkehrs bilden [Wagn99, S. 58]. Falsche Erwartungen können Nutzer zu Aktionen verleiten, die das Ziel der Sicherheit konterkarieren. Für das SAM stellt sich somit die Herausforderung, die Erwartungsbildung der Nutzer dahingehend zu beeinflussen, dass diese die Konsequenzen ihrer Handlungen auf die Systemsicherheit angemessen einzuschätzen lernen.

Störfaktor: Wahrnehmung

Der Prozess der Handlungsregulation wird auch dadurch beeinflusst, wie Nutzer Informationssysteme wahrnehmen. Ursächlich für eine Verzerrung der Wahrnehmung ist vor allem die geringe Sichtbarkeit von Handlungskonsequenzen [EsRu99, S. 102; EKDB98, S. 66]. Zum einen können die Sicherheitsstörungen in Bereichen des Informationssystems auftreten, die außerhalb des Wahrnehmungsbereichs des Nutzers liegen. Zum anderen tragen zeitliche Verzögerungen der Handlungskonsequenzen zu einer Verzerrung der Wahrnehmung bei [EsRu99, S. 101]. Die fehlerhafte Wahrnehmung von Informationssystemen führt regelmäßig zu einer falschen Beurteilung von Risiken [Gram01, S. 90; Hin+02, S. 1] und somit zu Handlungen, die die Sicherheit gefährden. Ein Nutzer kann z. B. aufgrund eines Berichtes über den umfassenden Schutz durch Virenscanner, die an seinem Arbeitsplatz eingesetzten Informationssysteme als sicher wahrnehmen und dementsprechend sämtliche eingehenden E-Mails ohne weitere Prüfung öffnen. Aufgabe eines SAM sollte es somit sein, eine angemessene Wahrnehmung der Informationssysteme und deren Sicherheit zu bewirken.

1.2.2 Ableitung von Gestaltungsempfehlungen

Die identifizierten Störfaktoren führen dazu, dass Nutzer entweder nicht das erwünschte Sicherheitsniveau anstreben oder dieses aufgrund unangemessener Erwartungen und Wahrnehmungen nicht erreichen. Für das SAM liefern sie somit konkrete Ansatzpunkte zur Gewährleistung der IT-Sicherheit. Zur Erreichung einer angemessenen Security Awareness sind vor allem Lernprozesse zu realisieren. Als zentrale Methode des SAM ist daher ein sog. Security Awareness Training (SAT) zu konzipieren. Die Zielsetzung des SAT besteht darin, die Systemnutzer derart zu schulen, dass die identifizierten Defekte ex-ante vermieden werden können. Hierzu sind die Systemnutzer für die Bedeutung der Systemsicherheit zu sensibilisieren (Zielsetzungsdefekt) und im sicherheitsbewussten Umgang mit An-

wendungssystemen zu schulen (Erwartungs- und Wahrnehmungsdefekt). Die IT-Sicherheit soll auf diese Weise proaktiv gefördert werden, um Opportunitätskosten reaktiver Maßnahmen zu vermeiden (z. B. Systemstillstand).

Neben den inhaltlichen Anforderungen, abgeleitet aus den Störfaktoren, ist die Präferenzstruktur der avisierten Adressaten des SAT dahingehend zu berücksichtigen, dass durch die einzusetzende Infrastruktur verschiedene Lernkanäle unterstützt werden. Abbildung 3 verdeutlicht den Zusammenhang zwischen den inhaltlichen Anforderungen und den aus der individuellen Präferenzstruktur resultierenden Anforderungen.

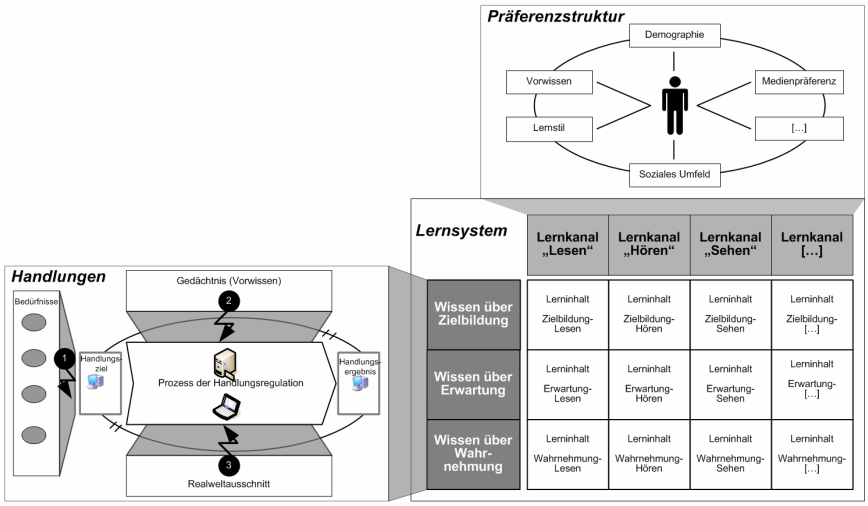

Abbildung 3: Anforderungen an das Security Awareness Training

Die praktische Umsetzung des SAT wird durch die hohe Anzahl an Nutzern und deren individuellen Handlungsregulationsprozessen erschwert. Die einzelnen Nutzer verfügen hierbei über individuelle Bedürfnisse, unterschiedliches Vorwissen und eine spezifische Wahrnehmung der Informationssysteme und Sicherheit [EsRu99, S. 105]. Besonders ausgeprägt ist diese Heterogenität zwischen Laien und Experten in einem Unternehmen. Hieraus ergibt sich die Notwendigkeit der differenzierten Ausgestaltung des SAT in Abhängigkeit von den avisierten Adressaten. Kommunikationsprobleme können dazu führen, dass Experten dazu neigen, den Wissensstand der Laien zu überschätzen und somit relevante Informationen nicht zu vermitteln [Juc+03, S. 129]. Andererseits können Laien die von den Experten im Rahmen des SAT bereitgestellten Informationen für überzogen halten, weil sie vermuten, dass die Experten ihren Wissensvorsprung zum Ausbau ihrer Machtposition ausnutzen wollen [Fox03, S. 678]. Bei der praktischen Umsetzung eines SAT ist diese Problematik zu berücksichtigen und deren Eintritt zu vermeiden.

2 Methoden des Security Awareness Managements

Die aus den Störfaktoren und der individuellen Lernpräferenz der Nutzer abgeleiteten Anforderungen werden im Folgenden hinsichtlich ihrer Konsequenzen für die Gestaltung eines geeigneten Lernsystems untersucht.

2.1 Lerninfrastrukturen für das SAM

Bei der Entwicklung von Infrastrukturen für das SAM stellen sich die Herausforderungen aus lernpsychologischer und wirtschaftlicher Sicht.

- **Lernpsychologische Sicht:** Infrastrukturen für das SAM haben einer Vielzahl unterschiedlicher Lernpräferenzen gerecht zu werden. So ist zu erwarten, dass nicht nur die Präferenzen verschiedener Nutzer sehr weit auseinander liegen, sondern dass letztlich auch die Präferenz eines einzelnen Nutzers situativ variiert. Demnach sind Infrastrukturen zu schaffen, in denen Systemnutzer die Möglichkeit haben, sowohl die Lernziele als auch den Lernprozess autonom zu bestimmen.
- **Wirtschaftliche Sicht:** Um die Kosten der Einrichtung und des Betriebs der Infrastruktur möglichst gering zu halten, empfiehlt sich eine weitgehend standardisierte Infrastruktur.

Einen Lösungsansatz bieten computergestützte Lernplattformen, die aktuell unter dem Begriff des E-Learnings thematisiert werden [Gro+01; Seu+01, S. 25 ff.; DiEr01, S. 10ff.; AdPa02, S. 669; GrBr04, S. 303]. Ein besonderes Potential kommt dabei Plattformen zu, die nach dem Referenzmodell des Multi Channel Learning entwickelt werden [Broc03, S. 34; Broc04, S. 308 ff.; KaRa04, S. 12ff.]. Mit diesem Referenzmodell wird ein Gestaltungsprinzip für Lehr- und Lernsysteme vorgeschlagen, nach dem alternative Lernkanäle entwickelt werden, zwischen denen Lernende während der Nutzung entsprechend ihres situativen Bedarfs frei wählen können. Gegenüber einer eher technik-getriebenen multimedialen Aufbereitung werden mit Lernkanälen didaktisch motivierte Zusammenstellungen von Repräsentationsformen für spezifische Lernziele und -kontexte vorgenommen. Um derartige E-Learning-Systeme für das SAT nutzen zu können, sind vor allem folgende spezifische Anforderungen zu stellen.

Grundlegend sind Lernkanäle vorzusehen, mit denen relevantes Fachwissen über Fragen der IT-Sicherheit vermittelt werden kann. Um eine möglichst breite Anzahl auch fachfremder Systemnutzer erreichen zu können, stellen sich hier besondere Anforderungen an die Anschaulichkeit der Wissensaufbereitung. So bieten sich z. B. Lernkanäle an, in denen eine audio-visuelle Aufbereitung der Lerninhalte möglich ist. Um den Transfer des erworbenen Wissens in den Berufsalltag zu unterstützen, sollten Kanäle vorgesehen werden, in denen praktische Probleme zur IT-Sicherheit zum Gegenstand gemacht werden. Zudem erweist es sich als förder-

lich, Lernende in den Problemlösungsprozess zu involvieren und optional Referenzlösungen zu präsentieren. Um die Selbsteinschätzung der Kompetenz auf dem Gebiet der IT-Sicherheit zu verbessern, dienen Kanäle, in denen Nutzer ihren Wissenstand überprüfen können. Ein wirksames Mittel zur Sensibilisierung der Systemnutzer für sicherheitsbewusstes Handeln, ist in der Bereitstellung von Lernkanälen zu sehen die zielgerichtete Diskursprozesse der Mitarbeiter unterstützen [KaRa04, S. 6]. Diese Kanäle tragen zugleich zur Schaffung eines „Wir-Gefühls“ [Hein00, S. 12] bei und steigern die Verbreiterung der Akzeptanz des SAT.

Ergänzend zu den spezifischen Lernkanälen sollte ein E-Learning-System das im Rahmen des SAT eingesetzt wird, Möglichkeiten der Individualisierung der Lerninhalte bieten. Darunter ist z. B. zu verstehen, dass Nutzer die Lerninhalte in den einzelnen Kanälen um eigene Anmerkungen ergänzen können. Neben persönlichen Erfahrungen können hier auch Fragen dokumentiert werden. Die Infrastruktur sollte darüber hinaus als offenes System realisiert sein. Neben Vernetzungen zu anderen Wissensquellen ist auch die Integration des Lernsystems für das SAT in die bestehende Arbeitsumgebung wünschenswert. Anzustreben ist eine weitgehende Konvergenz von Arbeit und Lernen.

Die Bereitstellung einer Infrastruktur, die die dargestellten Anforderungen erfüllt, ist eine Vorraussetzung für ein wirksames SAM. Sie bildet die Grundlage um Lerninhalte des SAM zu vermitteln. Die an diese Inhalte zu stellenden Anforderungen sind Gegenstand des folgenden Abschnitts.

2.2 Lerninhalte für das SAM

Aus den sicherheitsgefährdenden Störfaktoren im Handlungsprozess lassen sich Anforderungen an die Lerninhalte eines SAT ableiten. Zielbildung, Erwartungen und Wahrnehmung stellen somit drei zentrale Themenkomplexe dar, die in einzelnen Lerninhalten umzusetzen sind.

Wissensgebiet: Zielbildung

Eine wesentliche Grundlage bildet die Schaffung eines gemeinsamen Verständnisses von IT-Sicherheit. Zusätzlich zu einer klaren Definition sind Beispiele zur Veranschaulichung sicherheitsrelevanter Fragestellungen bereit zu stellen [Voss99, S. 149ff.]. Darauf aufbauend ist dem Nutzer die unternehmerische Tragweite der IT-Sicherheit zu verdeutlichen. Hierbei sind auch die Risiken aufzuzeigen, die durch sicherheitsgefährdendes Verhalten entstehen.

Wissensgebiet: Erwartung

Gegenstand des Wissensgebiets Erwartungen sind Lerninhalte, die der Bildung von unangemessenen Erwartungen im Bezug auf die individuellen Handlungen in Informationssystemen vorbeugen. Wesentliche Ursachen für die Bildung von fal-

schen Erwartungen sind die fehlende Transparenz und die zeitliche Verzögerung der Wirkung von Handlungen, die die Sicherheit gefährden. Die Darstellung von eindeutigen Handlungsanweisungen, z. B. in Form von Sicherheitsrichtlinien einer IT-Security Policy [Voss99, S. 190] oder Faustregeln [EsRu99, S. 104], mindern die Bildung von unangemessenen Erwartungen. Die dargestellten Handlungsanweisungen sollten leicht verständlich und für sämtliche Nutzer nachvollziehbar sein [Wagn01, S. 13]. Um die Anschaulichkeit zu erhöhen, können Beispiele zu möglichen Sicherheitsvorfällen geschildert werden [Wagn01, S. 9f.]. Die Darstellung sollte aus einer Perspektive erfolgen, die die Systemnutzer an ihrem Arbeitsplatz gut nachvollziehen können. Oftmals ist hierzu die Darstellung von betrieblichen Handlungen von größerer Bedeutung als die Erörterungen der ihnen zugrunde liegenden technischen Details.

Wissensgebiet: Wahrnehmung

Das Wissensgebiet Wahrnehmung umfasst Lerninhalte, die eine interpretationsfreie Wahrnehmung von Anwendungssystemen ermöglichen. Hierzu sind Lerninhalte bereit zu stellen, in denen die Beherrschung der relevanten Informationssysteme erläutert werden [EsRu99, S. 104; Wagn99, S. 7f.]. Bei der inhaltlichen Ausgestaltung ist zu beachten, dass nur die aus Nutzersicht relevanten Grundlagen und Dienste von Informationssystemen thematisiert werden [EsRu99, S. 106; Wagn99, S. 57f.]. Dem Nutzer sollte vor allem ein systematisches Wissen über das Problemfeld vermittelt werden, das ihn dazu befähigt, auch zukünftige Situationen angemessen zu beurteilen [Wagn99, S. 66].

Um die Individualisierung des Lernsystems auch im Hinblick auf die Inhalte zu gewährleisten, sollten für das SAT möglichst klar abgegrenzte Wissenseinheiten gebildet werden, die miteinander zu vernetzen sind. Um die Wiederverwendbarkeit sowie die Kompositionsmöglichkeit zu steigern, bietet es sich an, dabei tendenziell kleine Wissenseinheiten zu definieren.

Bei der Anwendung des SAM sind weitere Anforderungen aus Sicht der spezifischen Unternehmung zu berücksichtigen. Um diese Anforderungen zu veranschaulichen, aber auch um die Machbarkeit des SAM zu demonstrieren, wird im Folgenden ein Anwendungsbeispiel vorgestellt.

3 Anwendung des Security Awareness Management

3.1 Vorstellung des Anwendungsbeispiels

Am European Research Center for Information Systems (ERCIS) ist ein Projekt zur Entwicklung und Umsetzung des SAM für ein IT-Dienstleistungsunternehmen eines Handelskonzerns durchgeführt worden. Das Dienstleistungsunternehmen

bündelt sämtliche Aufgaben, die zur Bereitstellung von Informationssystemen für die weltweit verteilten Unternehmenseinheiten des Konzerns notwendig sind. Die projektspezifischen Angaben wurden für die Publikation anonymisiert.

Zur Gewährleistung des angestrebten Sicherheitsniveaus der Informationssysteme wurde ein einheitliches Sicherheitskonzept in Form einer IT-Security Policy erstellt, in der die Sicherheitsziele, die Organisation des Sicherheitsmanagements und die notwendige Maßnamen expliziert worden sind. Zur Umsetzung der IT-Security Policy in einem SAT wurde in Zusammenarbeit mit dem ERCIS eine Security Awareness Campaign initiiert. Zentraler Bestandteil dieser Kampagne ist die Ausgestaltung des unternehmensspezifischen SAT auf Basis des E-Learning-Systems Freestyle Learning (FSL). Im Folgenden wird zunächst die aufgebaute Infrastruktur vorgestellt, der sich die Präsentation der Lerninhalte anschließt. Die mediendidaktische Aufbereitung der Inhalte unter Nutzung der Infrastruktur wird anhand ausgewählter Lerneinheiten veranschaulicht.

3.2 Vorstellung der Infrastruktur für das SAM

Als Infrastruktur wurde im Rahmen des Projekts das E-Learning-System Freestyle Learning [Gro+01; Broc01] eingesetzt. Dieses System erlaubt die multiperspektive Aufbereitung der Lerninhalte des SAM nach dem Mehrkanalprinzip [Broc04; GrBr04]. Durch das Mehrkanalprinzip ermöglicht das System individuelle Lernprozesse auf einer einheitlichen softwaretechnischen Plattform. Die Implementierung der Plattform ist als OpenSource Software unter SourceForge verfügbar [http://sourceforge.net]. Der Ordnungsrahmen der Freestyle Learning-Plattform ist in Abbildung 4 dargestellt worden.

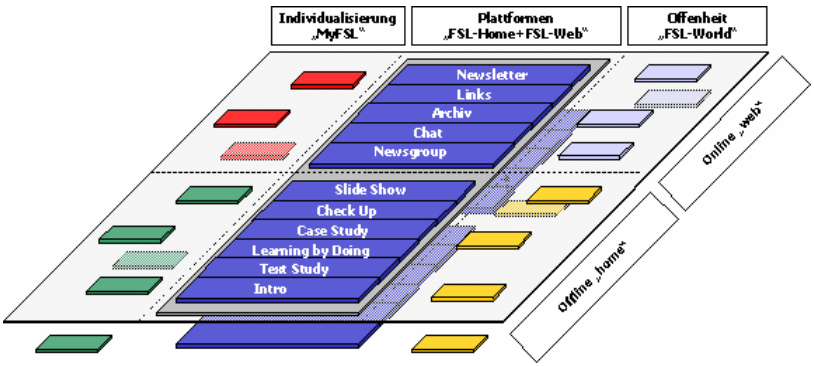

Abbildung 4: Ordnungsrahmen der Freestyle-Plattform [vgl. auch Broc01, S. 149]

Die Freestyle-Plattform eröffnet den Akteuren eine strukturierte Sicht auf die Inhalte des SAM. Die Basis bilden die Lerneinheiten der ausgewählten Learning Channels und Tools. Technisch besteht die Möglichkeit, die in einer Lehr

/Lerneinheit zu realisierenden Kombinationen sind bedarfsgerecht (per „plug in“) zu konfigurieren. Unterschieden werden Learning Channels und Tools auf dem Freestyle Home und Web. Typisch für das Home sind Channels, die in hohem Maße interaktiv sind (z. B. Learning by Doing), intensive multimediale Visualisierung nutzen (z. B. Slideshow) oder in einem persönlich geschützten Bereich zu realisieren sind (z. B. Check Up). Demgegenüber werden im Web Möglichkeiten geboten, in denen eine gemeinschaftliche Auseinandersetzung zu Themenbereichen des SAM erfolgt (z. B. Newsgroup) sowie informationslogistische Prozesse zu unterstützen sind (z. B. Archiv). Sowohl im Freestyle Home als auch im Web sind darüber hinaus Komponenten zur Individualisierung („My FSL“) sowie zur Vernetzung mit anderen Wissensressourcen („FSL World“) vorgesehen.

In dem Anwendungsfall wurden für das SAM spezifische Dienste des Freestyle Learning Home und des Freestyle Learning Web vorgesehen. In Channels des Freestyle Learning Home werden die zu vermittelnden Lerninhalte eines Themas für eine spezifische Lernform repräsentiert. Diese werden durch weitere Tools unterstützt, die zusätzliche Lernfunktionalitäten bieten (z. B. Logbuch). Mit dem Freestyle Learning Web wurde ein Internetportal mit weiteren Diensten eingerichtet. Ein Überblick über die Dienste ist in Abbildung 5 dargestellt.

Dienst	**Beschreibung**
Freestyle Home	
Learning Channels	
Text Study	Detaillierte Darstellung der Lerninhalte als Hypertext, in dem sowohl zu anderen Begriffen der Text Study als auch an referenzierte Stellen anderer Perspektiven navigiert werden kann. Sie hat den Charakter eines besonderen Lehrbuchs, das durch die digitale Repräsentationsform einen erheblichen Mehrwert hinsichtlich der Navigation und Suche (aber auch der Strukturierung) bietet.
Slideshow	Präsentation der Lerninhalte im Stil einer multimedialen Vorlesung. Sie adressiert den audiovisuellen Lernkanal und kann vom Lernenden im Selbststudium interaktiv gesteuert werden.
Learning by Doing	Dient der experimentellen und spielerischen Anwendung des Wissens und ermöglicht somit handelndes Lernen.
Case Study	Schult die praxisorientierte Anwendung von Wissen. Lernzielorientierte Problemstellungen werden in einer motivierenden Problemstellung dargestellt. Zu den Aufgabenstellungen werden mehrere Best-Practice-Lösungen (Referenzlösungen) präsentiert. Die Darstellung erfolgt als Hypertext.
Check Up	Automatisierte Wissenskontrolle anhand standardisierter Abfragemethoden, zu denen Multiple Choice-Fragen und Relator-Darstellungen gehören. Das Faktenwissen („key facts“) kann unter Mitwirkung eines Avatars trainiert werden. Der Lernende erhält entweder eine unmittelbare Rückmeldung nach jeder Check up-Frage, oder aber er stellt sich einer Prüfungssituation und erhält erst am Ende des Tests eine Auswertung seiner Antworten. Auf Wunsch werden persönliche Leistungsstatistiken geführt.
Learning Tools	
Medien Pool	Sammlung von Audio-, Video-, Bild-, PDF- und Powerpoint-Dateien, die einen Zusatznutzen ermöglichen.
Glossar	Definition und Erläuterung der wesentlichen Fachbegriffe. Zusätzlich sind zu jedem Eintrag Querverweise zu verwandten Fachbegriffen möglich.
Notizmanager	Möglichkeit, individuelle Anmerkungen zu jedem Element einer beliebigen Perspektive anzufertigen und zu verwalten.

Freestyle Web	
Learning Channels	
Materialien	Bereitstellung von Dokumenten und anderen Dateien, die nicht in der Learning Unit beinhaltet sind. Zusätzlich kann von hier aus eine Online-Installation der Freestyle Learning Home Software durchgeführt werden.
Diskussion	Ermöglicht die zeitlich asynchrone Kommunikation zwischen Lernenden und Lehrenden. Sie veröffentlichen Artikel mit Fragen bzw. Antworten, Meinungen und Kommentaren. Beiträge, die sich aufeinander beziehen, können vom Nutzer in eine hierarchische Struktur gebracht werden.
Chat-Bereich	Ermöglicht die zeitlich synchrone Kommunikation. Nutzer erhalten einen persönlichen Zugang mit Namen und Kennwort und können Kommentare schreiben, die direkt allen Teilnehmern auf dem Bildschirm angezeigt werden.
Learning Tools	
Mailingliste	Eingetragene Nutzer erhalten persönliche Nachrichten des Lehrers (Dozenten der MGI) per E-Mail. So kann z. B. der Dozent Einladungen zu einem Chat aussprechen.
Nachrichten	Bereitstellung aktueller Informationen zu den Inhalten über Newsletter.

Abbildung 5: Dienste der Freestyle Learning-Plattform

Die auf dieser Infrastruktur umgesetzten Inhalte werden im Folgenden vorgestellt.

3.3 Vorstellung der Inhalte des SAM

Die Inhalte des in dem Projekt entwickelten SAM, richten sich an sämtliche Mitarbeiter des Unternehmens. Grundlage der Inhalte ist eine, als Gesamtbetriebsvereinbarung für jeden Mitarbeiter bindende IT-Security Policy. Sie besteht aus einem allgemeinen und einem speziellen Teil. Im allgemeinen Teil werden die Sicherheitsziele, die Organisation des Sicherheitsmanagements im Unternehmen und die Verantwortungsbereiche der einzelnen Mitarbeiter dargestellt. Der spezielle Teil enthält Verhaltensrichtlinien, die die Mitarbeiter im Umgang mit den Informationssystemen einzuhalten haben. Dieser Teil basiert auf dem Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [BSI02]. Die grundsätzlichen Wissensgebiete, die im Rahmen des SAM thematisiert werden, wurden anhand der drei Störgrößen Zielbildung, Erwartungen und Wahrnehmung strukturiert. Innerhalb dieser drei Gebiete erfolgte eine tiefergehende Gliederung anhand des Aufbaus der unternehmensspezifischen IT-Security Policy. Die Elemente auf unterster Gliederungsebene umfassen klar abgegrenzte Inhalte und bilden somit eigenständige Lerneinheiten. Somit können einzelne Mitarbeiter diejenigen Lerninhalte überspringen, die für ihre Aufgabenerfüllung nicht relevant sind. In Abbildung 6 sind sämtliche Lerninhalte dargestellt, die in dem Projekt durch das SAM umgesetzt worden sind.

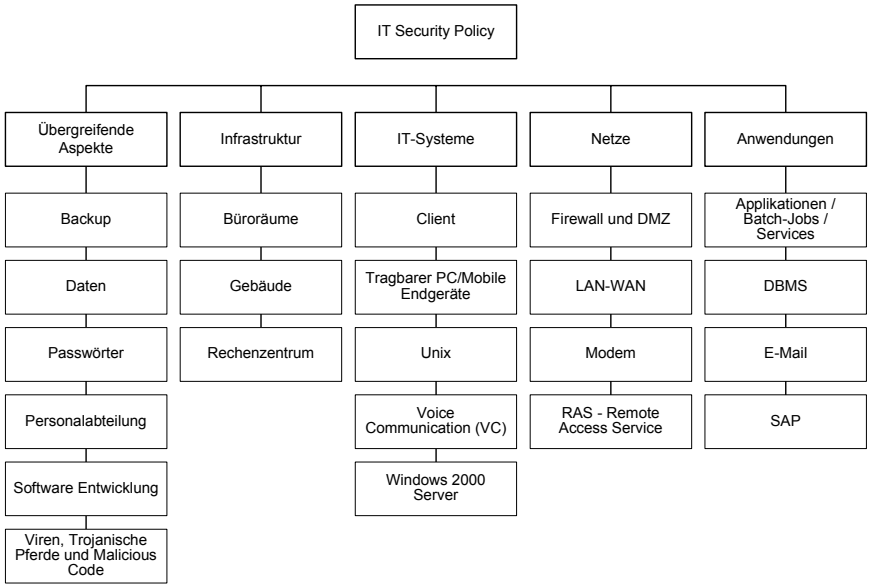

Abbildung 6: Lerninhalte des in dem Projekt umgesetzten SAM

Die einzelnen Lerninhalte sollen das gesamte Spektrum des für eine bestimmte Rolle relevanten Wissens zum Thema IT-Sicherheit abdecken. Im Folgenden wird exemplarisch gezeigt, wie die Inhalte als Lerninhalte auf der Freestyle Learning-Plattform für das SAT in dem Anwendungsfall umgesetzt worden sind.

3.4 Vorstellung der Lerneinheit für das SAM

3.4.1 Dienste des Freestyle Learning Home

Im Freestyle Learning Home sind die Lerneinheiten für das SAM durch Learning Channels und Tools aufbereitet worden. Sie werden im Folgenden vorgestellt.

Intro

Der Inhalt des Learning Channels Intro besteht aus einem Video, in dem der Sicherheitskoordinator des Unternehmens den Anwender in das Thema Informationssystemsicherheit einführt. Hierbei werden kurz die Ziele und die Entstehung der Security Policy dargestellt, sowie in den Inhalt und die Struktur der Lernumgebung eingeführt. Die Bedeutung des Themas IT-Sicherheit wird durch die Darstellung der Abhängigkeit des gesamten Unternehmens von den eingesetzten Informationssystemen herausgestellt. Im Intro werden Informationen geliefert, die Lerninhalte der anderen Perspektiven motivieren und den Umgang mit der Software erleichtern sollen.

Text Study

In dem Learning Channel Text Study sind neben einer allgemeinen Einführung in die Lernumgebung, Informationen über die IT-Security Policy und deren zugrunde liegenden Konzepte umgesetzt worden. Eine wesentliche Grundlage bildet z. B. eine auf das Unternehmen zugeschnittene Definition von IT-Sicherheit. Die umgesetzten textuellen Lerninhalte werden um aussagekräftige Grafiken sowie Faustregeln angereichert. Abbildung 7 zeigt einen Ausschnitt aus der Text Study.

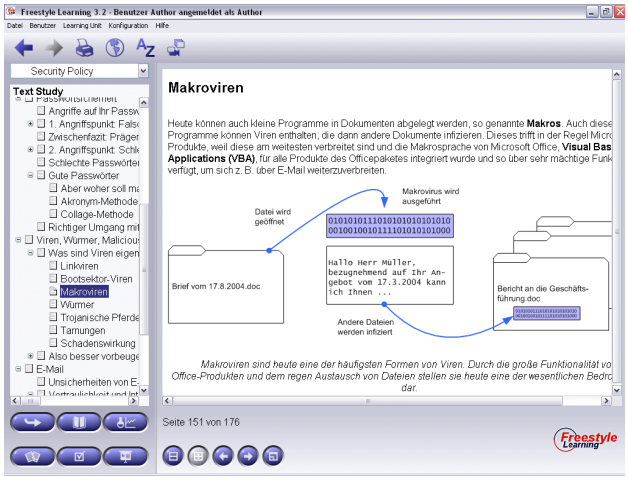

Abbildung 7: Text Study der Lerneinheit für das SAT

In der Text Study werden sämtliche Lerninhalte umgesetzt, so dass sie als gemeinsame Basis individueller Lernprozesse dient. Den einzelnen Mitarbeitern des Unternehmens ist es möglich, für sie nicht relevante Lerninhalte zu überspringen.

Slideshow

Strukturgleich zu dem Learning Channel Text-Study werden die Lerninhalte in dem Learning Channel Slide Show durch vertonte Präsentationsfolien umgesetzt. Die Steuerung der Slideshow kann anhand eines Navigationsbaumes erfolgen. Die einzelnen Folien der Slideshow beinhalten hauptsächlich grafische Darstellungen, die anhand relevanter Schlagworte illustriert werden. Die inhaltliche Erläuterung erfolgt durch die zugehörigen Audiokommentare. Indem die gleichen Folien verwendet werden, die auch in Präsenzschulungen der Security Awareness Campaign eingesetzt werden, werden Wiedererkennungseffekte realisiert.

Learning by Doing

Die Anwendung der Lerninhalte auf praktische Alltagssituationen wird im Learning Channel Learning by Doing durch Präsentation von Anwendungsbeispielen

veranschaulicht. Zusätzlich zu textuellen Beschreibungen werden Schulungsvideos bereitgestellt, in denen sicherheitskritische Fehler im Umgang mit Informationssystemen vorgeführt werden. Um die Anschaulichkeit zu erhöhen, wird richtiges und falsches Verhalten in der gewohnten Arbeitsumgebung der Mitarbeiter demonstriert.

Case Study

In dem Learning Channel Case Study werden die relevanten Inhalte durch die Konfrontation der Lerner mit alltagstypischen Problemen vermittelt. Die aktuellen Beispiele betreffen praktische Sicherheitsvorfälle und deren Folgen. Anhand dieser Fallstudien werden die Mitarbeiter für die Bedeutung von IT-Sicherheit sensibilisiert. Die dargestellten Sicherheitsvorfälle betreffen in der Regel Lerninhalte verschiedener Teilbereiche. Zur Lösung werden mehrere mögliche Szenarien vorgestellt, die von den Anwendern in dem unternehmensspezifischen IT-Security Portal diskutiert werden können. Durch die themenübergreifenden Fallstudien werden bestehende Verbindungen zwischen einzelnen Lerninhalten aufgezeigt und das Systemdenken gefördert.

Check up

Zur eigenständigen Überprüfung des Lernfortschritts kann der Learning Channel Check up genutzt werden. Hier kann das nötige Faktenwissen ebenso trainiert werden, wie die Einschätzung sicherheitskritischer Situationen. Abbildung 8 zeigt stellvertretend eine der Fragen des Check up.

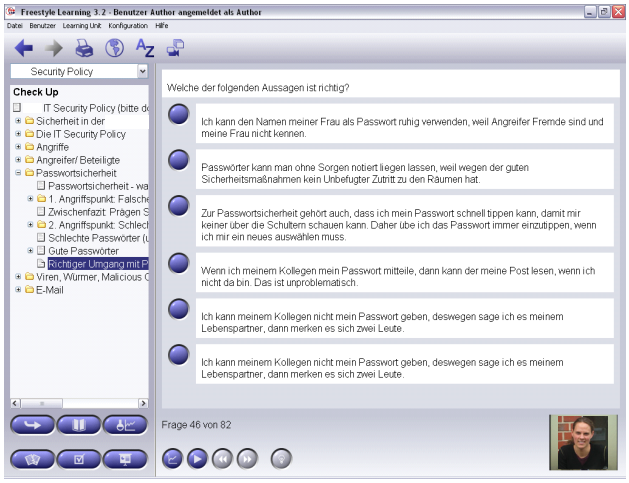

Abbildung 8: Check up Learning Channel der FSL-Unit für das SAT

Zusätzlich wurde ein Avatar implementiert, der durch Videoaufnahmen von Nutzern des Systems realisiert wird. Durch den Aufruf einer Statistik ist es dem Nut-

zer möglich, aus der Anzahl der richtigen und falschen Antworten, Rückschlüsse auf seinen aktuellen Wissensstand zu ziehen.

Zusätzlich zu den Learning Channels sind auf der Plattform Freestyle Learning Home folgende Learning Tools realisiert werden.

Media Pool

Im Media Pool werden ergänzende Informationen verschiedener Medientypen bereitgestellt. Beispiele sind Videos, in denen sich die Security Koordinatoren vorstellen. Ebenfalls werden in dem Media Pool sämtliche relevanten Gesetzestexte in elektronischer Form bereitgestellt, damit der Anwender diese bei Bedarf einsehen kann.

Glossar

Im Glossar wird die Terminologie der IT-Security Policy dokumentiert. Der Nutzer kann zentrale Begriffe nachschlagen, zu denen er eine kurze textuelle Erläuterung erhält. Die Vernetzung des Glossars mit den einzelnen Learning Channels erfolgt durch eine Verlinkung auf die Begriffe des Glossars.

Notes Manager

Durch den Notes Manager wird es Anwendern möglich, individuelle Anmerkungen zu Elementen sämtlicher Learning Channels vorzunehmen. Sie können z. B. Fragen notieren, die sich im Verlauf des Lernprozesses oder an ihrem Arbeitsplatz ergeben. In dem Notes Manager werden sämtliche Notizen, die ein Nutzer im Laufe der Zeit angelegt hat, verwaltet, wobei diese jederzeit editiert werden können.

3.4.2 Dienste des Freestyle Learning Web

Für die Entwicklung einer unternehmensweiten Security Awareness werden im Unternehmen Online Channels und Tools von Freestyle Learning Web eingerichtet worden. Abbildung 9 zeigt die anonymisierte Startseite der Freestyle Web Lösung für das SAM.

In den Newsgroups können Mitarbeiter des Unternehmens zu einzelnen Aspekten der IT-Sicherheit diskutieren. Der kontinuierliche Dialog dient nicht nur dem Gedanken- und Erfahrungsaustausch, sondern auch der kontinuierlichen Weiterentwicklung des SAM. In dem Chat-Room finden regelmäßig Treffen der Anwender mit Experten zu einzelnen Themen des SAM statt. Aktuelle Dokumente für das SAM, die bisher noch nicht in dem Media Pool eingebunden sind, können in einem Archiv bereitgestellt werden. Beispiele sind Gesetzesänderungen auf dem Gebiet der IT-Sicherheit. Externe Informationsquellen werden in einer Link-List thematisch organisiert und bieten Einstiegspunkte für vertiefende Recherchen und Diskussionen.

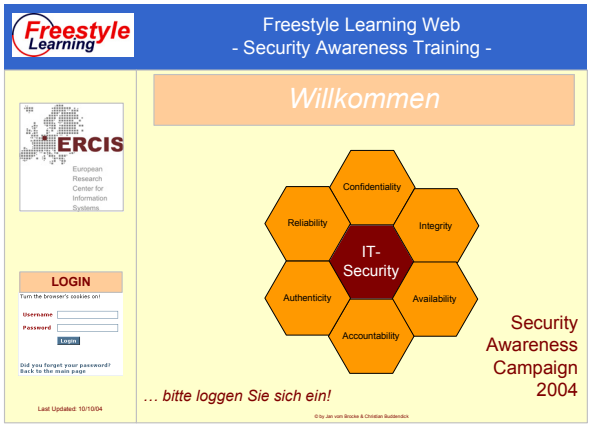

Abbildung 9: Startseite des in FSL-Web umgesetzten SAT

Anhand eines E-Mail-Verteilers werden permanente Impulse gesetzt, die das Sicherheitsbewusstsein der Mitarbeiter fördern.

4 Resümee

Mit dem vorliegenden Beitrag wurde das Konzept des Security Awareness Managements vorgestellt. Hierdurch können die Risiken, die durch Handlungen der Nutzer der Informationssysteme entstehen, verringert werden. Auf der Grundlage kognitionswissenschaftlicher Erkenntisse konnten Anforderungen an die Gestaltung des SAM gewonnen werden. Als zentrale Methode des SAM wurde das Security Awareness Training eingeführt. Für dieses wurde auf Basis des Referenzmodells für das Multi Channel Learning eine Ausgestaltung eines Security Awareness Trainings entwickelt. Die praktische Anwendung des SAM veranschaulicht das Potenzial dieses Ansatzes für ein IT-Sicherheitsmanagements in der Unternehmenspraxis.

Zukünftig sollten vor allem weitere empirische Untersuchungen durchgeführt werden, die das Potenzial des SAM, sowie kritische Erfolgsfaktoren der Umsetzung entsprechender Systeme aufzeigen. In die Untersuchungen sind auch andere Maßnahmen des IT-Sicherheitsmanagements einzubeziehen, um Erkenntnisse über situationsgerechte Maßnahmenbündel zu gewinnen. Diese Erkentnisse können die Grundlage zur Erarbeitung von Referenzmodellen für das SAM liefern, die in einer Vielzahl verschiedener Anwendungsfälle genutzt werden können.

Literatur

[AdPa02] Adelsberger, H. H., Pawlowski, J. M., Electronic Business and Education. In: Handbook on Information Technologies for Education & Training, International Handbook on Information Systems, Hrsg.: H. H. Adelsberger, B. Collis, J. M. Pawlowski, Berlin 2002, S. 653-671.

[Ande83] Anderson, J. R.: The architecture of cognition. Cambridge, MA 1983.

[Ande88] Anderson, J. R.: Kognitive Psychologie. Eine Einführung. Heidelberg 1988.

[BeRi94] Bergmann, B.; Richter, P. (Hrsg.): Die Handlungsregulationstheorie. Von der Praxis einer Theorie. Göttingen 1994.

[Broc01] Brocke, J. vom: Freestyle Learning, Concept, Platforms and Applications for Individual Learning Scenarios. In: Kern, H. (Hrsg.): Proceedings 46th International Scientific Colloquium. Ilmenau 2001, S. 149-151.

[Broc03] Brocke, J. vom: Referenzmodellierung. Gestaltung und Verteilung von Konstruktionsprozessen. Berlin 2003.

[Broc04] Brocke, J. vom: Multi Channel Learning, Ein Referenzmodell zur Entwicklung individueller E-Learning-Systeme. In: Proceedings der 12. Leipziger Informatik-Tage, Von e-Learning bis e-Payment 2004, Hrsg.: K.-P. Fähnrich, K. P. Jantke, W. S. Wittig, Berlin 2004, S. 245-254.

[BSI02] BSI (Hrsg.): IT-Grundschutzhandbuch. Bonn 2002. http://www.bsi.de/gshb/, Abruf am 2004-04-10.

[DiEr01] Dichanz, H.; Ernst, A.: E-Learning. Begriffliche, psychologische und didaktische Überlegungen zum „electronic learning“. In: Medienpädagogik, http://www.medienpaed.com/00-2/dichanz_ernst1.pdf Abruf am 2004-04-10.

[Dör+88] Dörner, D.; Schaub, H.; Stäubel, T.; Strohschneider, S.: Ein System zur Handlungsregulation oder – Das Zusammenwirken von Emotion, Kognition und Motivation. In: Sprache & Kognition, 7 (1988) 4, S. 212-232.

[Dörn96] Dörner, D.: Verhalten und Handeln. In: Selg, H.; Dörner, D. (Hrsg.), Psychologie. Eine Einführung in ihre Grundlagen und Anwendungsfelder, Stuttgart 1996, S. 100-114.

[Dörn98] Dörner, D.: Ein Bauplan für eine Seele. Reinbeck 1998.

[DöSc98] Dörner, D.; Schaub. H.: Das Leben von PSI. Über das Zusammenspiel von Kognition, Emotion und Motivation - oder: Eine einfache Theorie für komplizierte Verhaltensweisen. Memorandum Lst Psychologie II Universität Bamberg, 2,27.

[Ecke03] Eckert, C.: IT-Sicherheit. Konzepte – Verfahren – Protokolle. München 2003.

[EKDB98] Enquete Kommission Zukunft der Medien in Wirtschaft und Gesellschaft Deutschlands Weg in die Informationsgesellschaft Deutscher Bundestag (Hrsg.) (Enquete Kommission Deutscher Bundestag): Sicherheit und Schutz im Netz. Bonn 1998.

[Erns03] Ernst & Young LLP.: Global Information Security Survey 2003, http://www.ey.com/global/download.nsf/International/TSRS_-_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf, Abruf am 2004-07-12

[EsRu99] Espey, J.; Rudinger, G.: Der überforderte Techniknutzer – Didaktik der IT-Sicherheit aus psychologischer Sicht. In: BSI (Hrsg.), Zur Didaktik der IT-Sicherheit. Der Boppard-Diskurs zur Technikfolgen-Abschätzung in Querschnittlichen Fragen der IT-Sicherheit. Bonn 1999, S. 97-120.

[FePf00] Federrath, H.; Pfitzmann, A.: Gliederung und Systematisierung von Schutzzielen in IT-Systemen. In: DuD, 24 (2000) 12, S. 704-710.

[Fox03] Fox, D.: Security Awareness. Oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit. In: DuD, 27 (2003) 11, S. 676-680.

[Gram01] Grams, T.: Grundlagen des Qualitäts- und Risikomanagements. Braunschweig 2001.

[GrBr04] Grob, H. L., Brocke, J. vom: Referenzmodelle für E-Learning-Systeme. Konzeption und Anwendung für die Produktionswirtschaft. In: Corsten, H.; Brassler A. (Hrsg.): Entwicklungen im Produktionsmanagement. München 2004, S. 43-62.

[GrJe03] Grimm, R.; Jeckle, M.: XML-Signaturen: Grundlagen, Technik und Profile. In: DuD, 27 (2003) 12, S. 729-733.

[Gro+01] Grob, H. L.; Brocke, J. vom; Lahme, N.: Freestyle Learning. Das mediendidaktische Konzept. In: Grob, H. L. (Hrsg.), Arbeitsberichte „CAL+CAT“, Nr. 20. Münster 2001.

[Hein00] Heinbrink, H.: Virtuelle Seminare: Erfahrungen, Probleme, Forschungsfragen. In: Medienpädagogik, http://www.medienpaed.com/00-2/heidbrink1.pdf, Abruf am 2004-04-10.

[Hin+02] Hinrichs, S.; Wormuth, L.; Musahl, H.-P.: Gefährdungsbeurteilung - Objektive Analyse oder subjektive Gefährdungseinschätzung? In: Trimpop, R.; Zimolong, B.; Kalveram, A. (Hrsg.): Psychologie der Arbeitssicherheit und Gesundheit. Neue Welten - Alte Welten. 11. Workshop 2001, Heidelberg 2002. http://fogs.uni-duisburg.de/texte/gef%E4hrdungsbeurteilung.pdf, Abruf am 2004-04-24.

[Hölt03] Höltkemeier, H.: IT-Sicherheit aus Nutzersicht – Strategien für Sicherheit und Akzeptanz. In: Gora, W.; Krampert, T. (Hrsg.): Handbuch IT-Sicherheit, Stategien, Grundlagen und Projekte. München 2003, S.163-180.

[ISO00] ISO/IEC. TR 13335-1: Guidelines for the Management of IT Security (GMITS): Part 1— Concepts and Models for IT Security, 2000.

[Juc+03] Jucks, R.; Paechter, M. R.; Tatar, D. G.: Learning and Collaboration in Online Discourses. In: International Journal of Educational Policy, Research & Practice, 4 (2003) 1, S. 117-142.

[KaRa04] Kaminski, H.; Raabe, R.: Wissensnetzwerk Controlling - Evaluationsergebnis der didaktisch-pädagogischen Begleitergruppe. In: Grob, H. L. (Hrsg.), Arbeitsberichte „CAL+CAT“, Nr. 27. Münster 2004.

[MeBe04] Mehlau, J. I.; Berger, S.: Konzeption einer mobilen Wissensmanagementlösung und deren Absicherung durch ausgewählte Sicherheitsmuster. In: Bartmann et al. (Hrsg.): Überbetriebliche Integration von Anwendungssystemen - FORWIN-Tagung 2004. Aachen 2004, S. 305-319.

[PrPe04] Priebe, T., Pernul, G.: Sicherheit in Data-Warehouse- und OLAP-Systemen. In: Informationssystem-Architekturen: Rundbrief der Fachgruppe Modellierung betrieblicher Informationssysteme (WI-MobIS) der Gesellschaft für Informatik e.V. (GI), Bamberg, Januar 2004, S. 45-63.

[Scha97] Schaub, H.: Modelling Action Regulation. In: Brezinski, J.; Krause, B.; Maruszewski, T. (Hrsg.): Idealization VIII: Modelling in Psychology. Amsterdam 1997, Rodopi, S. 97-136.

[SeDö96] Selg, H., Dörner, D.: Psychologie als Wissenschaft – Ihre Aufgaben und Ziele. In: Selg, H.; Dörner, D. (Hrsg.): Psychologie. Eine Einführung in ihre Grundlagen und Anwendungsfelder, 2. Auf. Stuttgart 1996, S. 17-33.

[Seu+01] Seufert, S., Back, A., Häusler, M., E-Learning, Weiterbildung im Internet. Das „Plato-Cookbook“ für internetbasiertes Lernen, Kilchberg 2001.

[Stelz93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung. Ein wissenbasiertes, objektorientiertes System für die Risikoanalyse. Wiesbaden 1993.

[Voss99] Vossbein, J.: Integrierte Sicherheitskonzeptionen für Unternehmen. Stand und Perspektiven, Ingelheim 1999.

[Wagn01] Wagner, W.-R.: Datenschutz – Selbstschutz – Medienkompetenz. Wie viel informationstechnische Grundbildung braucht der kompetente Mediennutzer? In: Medienpädagogik. http://www.medienpaed.com/01-2/wagner1.pdf, Abruf am 2004-04-10.

[Wagn99] Wagner, W.-R.: Zur Didaktik der IT-Sicherheit – hat die Didaktik Antworten auf die technische Herausforderung? In: BSI (Hrsg.), Zur Didaktik der IT-Sicherheit. Der Boppard-Diskurs zur Technikfolgen-Abschätzung in Querschnittlichen Fragen der IT-Sicherheit, Bonn 1999, S. 55-70.