

SECMAN: Ein innovativer Ansatz für die Integration von Schutzbedarfsanalyse und BSI-Grundschutz

*Christian Friberg
PPI Financial Systems GmbH, Kiel*

*Norbert Luttenberger
Carsten Gerhardt
Christian-Albrechts-Universität zu Kiel*

1	Motivation	1
2	Die BSI-Methodik zur Schutzbedarfsfeststellung	2
	2.1 Risikoanalyse	2
	2.2 Schutzbedarfsfeststellung nach BSI-Methode	3
3	Die SECMAN-Methodik	5
4	Das SECMAN-Tool	7
	4.1 Rollenbasierte Zugriffskontrolle	7
	4.2 Das SECMAN-Programmsystem	9
5	Zusammenfassung und Ausblick	10

1 Motivation

„Aller Anfang ist schwer“ und „Wo beginnen?“, das sind nicht nur die Stoßseufzer von Praktikanten, die ihren Praktikumsbericht schreiben, von Diplomanden, die ihre Diplomarbeit schreiben, von Ingenieuren, die ein Lastenheft schreiben, und von Informatikern, die eine Programmspezifikation schreiben, sondern auch von Netzwerkadministratoren und Security-Spezialisten, die die Aufgabe übertragen bekommen haben, die IT-Infrastruktur eines Betriebes „sicher“ zu machen. Zu unübersehbar die Aufgabe: Soll man zuerst einmal ein Firewall-System installieren, lieber die gelben Klebezettel mit den Paßwörtern von den Bildschirmen der Benutzer reißen oder den studentischen Hilfskräften das Super- User-Paßwort wegnehmen, das diese erhalten haben, „damit sie arbeiten können“. Und zu groß ist der zu erwartende Widerstand der Benutzer: „Produzieren wir hier nur noch Sicherheit, oder sollen wir auch noch produktiv arbeiten?“

Zum Glück gibt es doch eine Lösung, wird mancher sagen: Es gibt doch das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI-GSHB) [1]. In der Tat umfaßt dieses Handbuch nicht nur einer Menge außerordentlich nützlicher und wichtiger Detailangaben (auf die man beim ersten Durchblättern unweigerlich stößt), sondern auch eine gut begründete Systematik, deren Ziel es ist, den Arbeitsaufwand für den Netzwerkadministrator und den Security-Spezialisten für die große Mehrzahl der Anwendungsfälle zu senken. Ein verdienstvoller Schritt in die richtige Richtung also. Man wird am BSI-GSHB nicht vorbeikommen.

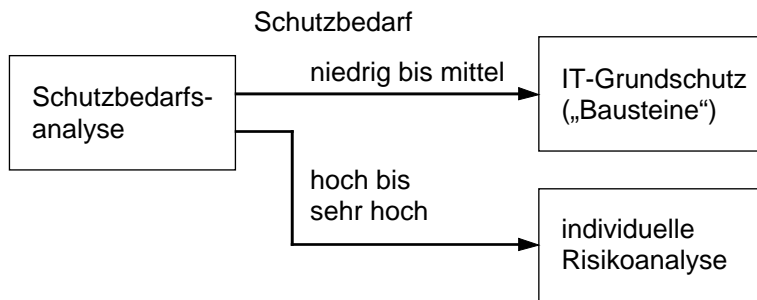


Bild 1: Vorgehensweise nach BSI-Methodik

Und dennoch. Schaut man genauer nach, liest man im Kap. 2.1 des BSI-GSHB ein Caveat: „Für IT-Systeme mit *mittlerem* Schutzbedarf ... ist lediglich die Umsetzung der in diesem Handbuch empfohlenen Maßnahmen erforderlich. Für IT-Systeme mit *hohem* Schutzbedarf bleibt neben dem IT-Grundschutz prinzipiell die Durchführung einer detaillierten Risikoanalyse (z. B. nach dem IT-Sicherheitshandbuch) erforderlich. Für die Unterscheidung zwischen mittlerem und hohem Schutzbedarf wird ... eine diesbezügliche Vorgehensweise (*Schutzbedarfsfeststellung*) vorgestellt.“ (Hervorhebungen durch die Autoren dieses Aufsatzes.) Vor der Durchführung einzelner Sicherheitsmaßnahmen muß also eine sog. Schutzbedarfsfeststellung durchgeführt werden, auf deren Korrektheit größter Wert zu legen ist, denn „*werden bei der Schutzbedarfsfeststellung bereits Fehler gemacht, so pflanzen sich diese im weiteren Verfahren fort und sind kaum noch zu korrigieren*“ (BSI-GSHB, Kap. 2.1).

Aus diesen methodischen Grundlagen ergab sich die Motivation für unsere Arbeit:

- Zum einen ging es darum, ein rechnergestütztes Werkzeug zu entwickeln, mit dem der gesamte Prozeß der Umsetzung von IT-Sicherheitsmaßnahmen – von der Schutzbedarfsfeststellung bis zur Umsetzung von detaillierten Maßnahmen – gesteuert und begleitet werden kann.
- Zum anderen wurde bald klar, daß die vom BSI vorgeschlagene Methodik für die Schutzbedarfsanalyse zu technikzentriert ist. Die von uns vorgenommene methodische Innovation baut – in bewußter Distanz zur BSI-Schutzbedarfsfeststellung – auf Geschäfts- und Projektprozessen auf und ist damit besser an den Zielen von Benutzern und Organisationen orientiert.
- Diese innovierte Methodik prägt selbstverständlich das von uns entwickelte rechnergestützte Werkzeug SECMAN (Security Manager), dessen hervorstechendes Merkmal die rollenbasierte Interaktion mit unterschiedlichen Typen von Benutzern ist.

In diesem Aufsatz werden wir zunächst den vom BSI vorgeschlagenen methodischen Ansatz für die Schutzbedarfsanalyse darstellen und kritisieren und dann unsere eigenen methodischen Überlegungen erläutern. Wir stellen danach das Werkzeug SECMAN vor und zeigen den darin enthaltenen rollenbasierten Ansatz. Wir schließen mit einem Ausblick auf künftige Entwicklungen.

2 Die BSI-Methodik zur Schutzbedarfsfeststellung

Der klassische Ansatz zur Herstellung eines gewissen Sicherheitsniveaus einer Organisation ist die *Risikoanalyse* [2]. Da mit der Risikoanalyse ein ggf. sehr hoher Aufwand verbunden ist, schlägt das BSI eine vereinfachte Methode vor, die man als eine Untermenge der Risikoanalyse betrachten kann, und die vom BSI mit der Bezeichnung *Schutzbedarfsfeststellung* versehen wurde. Um diesen Begriff besser bestimmen zu können, soll er im folgenden von der Risikoanalyse abgegrenzt werden.

2.1 Risikoanalyse

Die Risikoanalyse setzt sich zusammen aus Risikoidentifikation und der Risikobewertung. Die *Risiko-*

identifikation (die auch in der Schutzbedarfsanalyse der BSI-Methodik auftaucht, und zwar als Aufzählung von *Gefährdungen*) ist auf die spezifische Risikosituation des Unternehmens abgestimmt und erfaßt möglichst alle Risiken, die das Unternehmen treffen können. Die Identifikation technischer Risiken – nur um solche geht es uns hier – basiert z.B. auf Systemanalysen, Fehlerbaumanalysen oder Störfallanalysen. Für die Identifikation von Risiken im IT-Bereich schlägt das BSI eine „Baustein“-orientierte Systematik vor, die grob gesehen folgende Bereiche umfaßt:

- Organisation
- Personal
- Notfallvorsorge-Konzept
- Datensicherungskonzept
- Infrastruktur
- Nicht-vernetzte IT-Systeme
- Vernetzte Systeme
- Datenübertragungseinrichtungen
- Telekommunikation
- Sonstige IT-Komponenten

Bei der *Risikobewertung* geht es darum, einerseits die bei Eintritt des Risikos verursachten finanziellen Auswirkungen (Schadenausmaß) zu quantifizieren und andererseits eine Schadenseintrittswahrscheinlichkeit abzuschätzen. Bei der Abschätzung des Schadensausmaßes bedient man sich verschiedener Instrumente und Methoden. Bei der PML- bzw. MPL-Analyse wird z.B. für die Beurteilung eines Großschadenrisikos der *Maximum Possible Loss* (MPL) oder der *Probable Maximum Loss* (PML) ermittelt. Stoßen die quantitativen Verfahren an ihre Grenzen, so bedient man sich qualitativer Aussagen. Das Schadensausmaß kann bei fehlender Quantifizierbarkeit nach den Kategorien „gering“, „mittel“, „groß“ und „katastrophal“ eingeteilt werden. Die Schadeneintrittswahrscheinlichkeit wird in der Praxis fast immer qualitativ nach den Kategorien „sehr gering“, „gering“, „mittel“, „hoch“ und „sehr hoch“ gewichtet. Vor allem betriebswirtschaftliche Schäden (Marktverlust, Imageverlust etc.) können so besser abgebildet werden.

Die erkannten Risiken werden – gegliedert nach ihren finanziellen Auswirkungen und der Eintrittswahrscheinlichkeit – in einer *Risikomatrix* zusammengestellt. Die Risikomatrix liefert in komprimierter und übersichtlicher Form Informationen über die Risikolage eines Unternehmens, um so die Priorität, mit welcher die Maßnahmen zur Risikobewältigung realisiert werden sollen, festzulegen. In der Risikomatrix kann eine individuelle Akzeptanzlinie angebildet werden, die festlegt, ab welchem Schwellenwert ein Handlungsbedarf ausgelöst wird. Bei der Ermittlung der Gesamtrisikolage müssen auch die Risikointerdependenzen berücksichtigt und aggregiert werden. Insbesondere bei den modernen Produktionsmethoden (Just-in-time, Single-Sourcing etc.) gewinnt die Aggregation der Einzelrisiken an Bedeutung.

Die Durchführung einer organisationsweiten Risikoanalyse ist – wie man sich leicht vorstellen kann – sehr aufwendig und verlangt von den durchführenden Personen große Erfahrung. Insbesondere erfordert die Risikoanalyse einen Überblick sowohl über die Bedeutung einzelner Objekte für die zu untersuchende Organisation als auch über die möglichen Gefahren und entsprechende Maßnahmen zu ihrer Beseitigung. Häufig ist dieser Ansatz daher mit den dafür zur Verfügung stehenden Ressourcen nicht durchführbar.

2.2 Schutzbedarfsfeststellung nach BSI-Methode

Um mit einfacheren Mitteln ein gewisses Schutzniveau herstellen zu können, geht das BSI von einem vereinheitlichten Bedrohungsszenario aus, das aus Risikoanalysen verschiedener Organisationen hervorgegangen ist. Dadurch kann das Expertenwissen über Sicherheitsprobleme in einem Satz von Maßnahmen zusammengeführt und dem Sicherheitslaien zur Verfügung gestellt werden.

Wie in Bild 1 dargestellt ist die *Schutzbedarfsanalyse* der erste Schritt innerhalb der BSI-Methode. Sie umfaßt drei Schritte:

1. Erfassung der zu schützenden IT-Systeme: Rechner, Server, Netze usw.

2. Erfassung der zu diesen IT-Systemen zugehörigen IT-Anwendungen und Informationen und Zuordnung der Wichtigkeit der IT-Schutzziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* zu diesen Anwendungen und Informationen. (Vertraulichkeit soll sicherstellen, daß der Zugriff auf bestimmte Daten und Informationen nur berechtigten Benutzern ermöglicht wird. Integrität bezeichnet die Korrektheit, Manipulationsfreiheit und Unversehrtheit von Daten und Informationen. Unter Verfügbarkeit versteht man die Fähigkeit eines IT-Systems, Daten und Informationen, Prozesse und IT-Anwendungen zur rechten Zeit bereitzustellen.)
3. Schutzbedarfsfeststellung: Der Schutzbedarf richtet sich nach dem Ausmaß der Schäden, die eintreten würden, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Anwendung und/ oder Informationen beeinträchtigt würden.

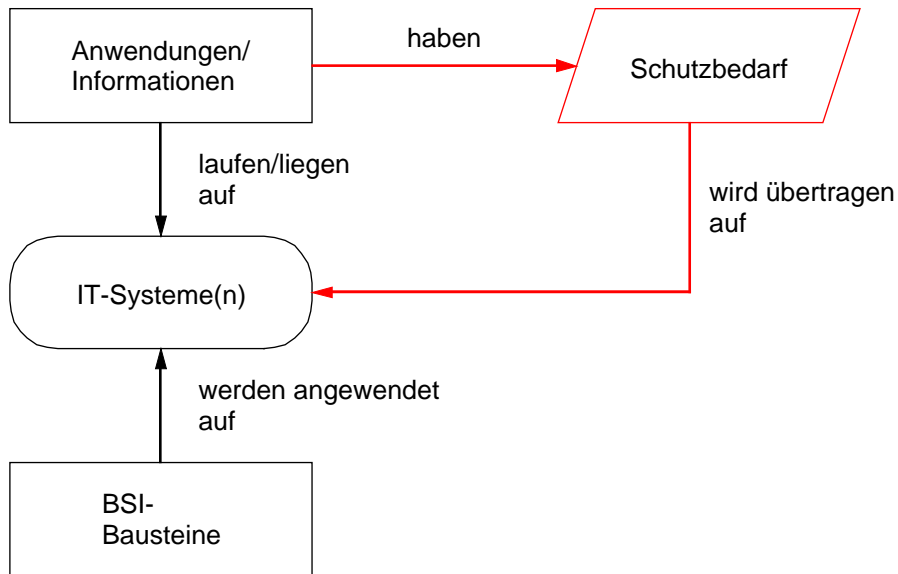


Bild 2: Die BSI-Schutzbedarfsanalyse

Der Schutzbedarf wird in drei Kategorien eingeteilt:

- **niedrig bis mittel:** Die Schadensauswirkungen sind begrenzt und überschaubar. Die vom BSI vorgeschlagenen Grundschutzmaßnahmen sind in der Regel ausreichend.
- **hoch:** Die Schadensauswirkungen können beträchtlich sein, Schutzmaßnahmen sollten auf Basis einer individuellen Risikoanalyse ermittelt werden.
- **sehr hoch:** Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen. Eine individuelle Risikoanalyse ist unbedingt erforderlich.

Die BSI-Schutzbedarfsanalyse läßt sich von der Risikoanalyse in drei Punkten abgrenzen:

1. Im Gegensatz zur Schutzbedarfsanalyse betrachtet die Risikoanalyse nicht nur Schadensauswirkungen, sondern auch Schadenseintrittswahrscheinlichkeit.
2. Im Gegensatz zur Schutzbedarfsanalyse ist die Risikoanalyse nicht nur auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ausgerichtet, sondern kann ggf. weitere Schutzziele betrachten.
3. Die Risikoanalyse versucht, wann immer möglich mit quantitativen Maßen vorzugehen; darauf wird in der Schutzbedarfsanalyse von vornherein verzichtet.

Das Ziel des vom BSI vorgeschlagenen *IT-Grundschutzes*, der auf dieser Schutzbedarfsanalyse aufbaut, ist es, durch die geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den *mittleren Schutzbedarf* angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Anwendungen dienen kann. Für bekannte Gefährdungen und Schwachstellen

hat das BSI überschlägige Risikobetrachtungen vorweggenommen und geeignete Maßnahmenbündel für typische IT-Konfigurationen, Umfeld- und Organisationsbedingungen erarbeitet. Der Anwender des IT-Grundschutzhandbuchs muß diese aufwendigen Analysen nicht wiederholen, er muß lediglich dafür Sorge tragen, daß die empfohlenen Maßnahmen konsequent und vollständig umgesetzt werden.

Vom BSI wird die Durchführung der Schutzbedarfsanalyse (nachdrücklich) empfohlen, um sicherzustellen, daß in der betrachteten Organisation keine IT-Systeme mit hohem oder sehr hohem Schutzbedarf „übersehen“ werden, für die die mehr oder weniger pauschalen IT-Grundschutzmaßnahmen nicht ohne weiteres ausreichend sind. Für solche Systeme werden individuelle Sicherheitsuntersuchungen angemahnt, die unter Beachtung von Kosten- und Wirksamkeitsaspekten geeignete Sicherheitsmaßnahmen zu identifizieren helfen, die über den IT-Grundschutz hinausgehen.

Die SECMAN-Methodik, die im folgenden Abschnitt detailliert dargestellt wird, umfaßt als integralen Bestandteil eine modifizierte Schutzbedarfsanalyse, die – bei aller Verwandtschaft mit der BSI-Methodik – eine bessere Ausrichtung der Schutzmaßnahmen an den Werten und der Struktur des Unternehmens verspricht.

3 Die SECMAN-Methodik

Zur Definition einer angemessenen Methode für die Schutzbedarfsanalyse ist ein schwieriges Problem zu lösen: Wie wird die Auswirkung von möglicherweise eintretenden Schäden korrekt „bewertet“. Offensichtlich werden die Schadensauswirkungen falsch erfaßt, wenn man sie auf die IT-Systeme selbst bezieht, da *„deren Wert ... meistens nur einen geringen Teil des Gesamtwertes aus[macht], die strategische und operative Bedeutung der IT liegt oft weit höher. Daher ist es wichtig, sich [...] klarzumachen, wie stark die Aufgabenerfüllung innerhalb der Institution von der eingesetzten IT abhängt.“* (BSI-GSHB, Kap. 1.2) Das BSI schlägt – wie Bild 2 zeigt – zur Lösung des angeführten Problems vor, die Bewertung von Schadensauswirkungen anhand der „Anwendungen und Informationen“ vorzunehmen, die auf den IT-Systemen installiert, gespeichert, verarbeitet werden, und dazu deren Schutzbedarf bezüglich Vertraulichkeit, Integrität und Zuverlässigkeit anzugeben. Leider wird jedoch dieser Ansatz in der BSI- Grundschutzanalyse nur halbherzig unterstützt, und darüberhinaus scheint uns dieser Ansatz aus zwei Gründen wenig hilfreich:

- Viele Anwendungen (z.B. Textverarbeitung) tauchen in vielen Kontexten auf. Es ist jedoch stets der betriebliche Kontext von Projekt- und Geschäftsprozessen, der über die Wichtigkeit der Erreichung eines Schutzziels entscheidet. Es können von daher nicht allein „Anwendungen“ sein, denen ein „Wert“ und damit ein Schutzbedarf zukommt.
- Das gleiche trifft für angeführten „Informationen“ zu: Auch diese können nicht isoliert betrachtet werden. In aller Regel ist in einer Organisation oder in einem Projekt nicht nur eine einzelne Information wichtig, sondern ein Verbund aus einer Vielzahl von Informationen, der als ganzer betrachtet werden muß. Es führt zu einem methodisch problematischen Vorgehen, eine technische Zeichnung losgelöst von den zugehörigen textuellen Erläuterungen zu betrachten. Auch hier geht es also wieder um die Einbettung von Informationen in komplexe Geschäfts- und/oder Projektprozesse.

Die SECMAN-Methodik sieht deshalb eine Schutzbedarfsanalyse vor, die auf einer Analyse der organisationsinternen Geschäfts- und Projektprozesse und der von diesen Prozessen benötigten Ressourcen beruht. Geschäftsprozesse sind z.B. die regelmäßige Systemadministration, die Pflege der Internet-Präsenz, aber auch Buchhaltungsverfahren; typische Projektprozesse sind z.B. Entwicklung, Test, Auslieferung usw. Wir werden im folgenden abkürzend nur noch von Prozessen sprechen. Alle Prozesse benötigen Ressourcen, die konkrete IT-Systeme oder aber abstrakte Beschreibungen der benötigten Arbeitsmittel sein können. Diesen Ressourcen werden die o.a. Schutzziele zugeordnet (s. Bild 3).

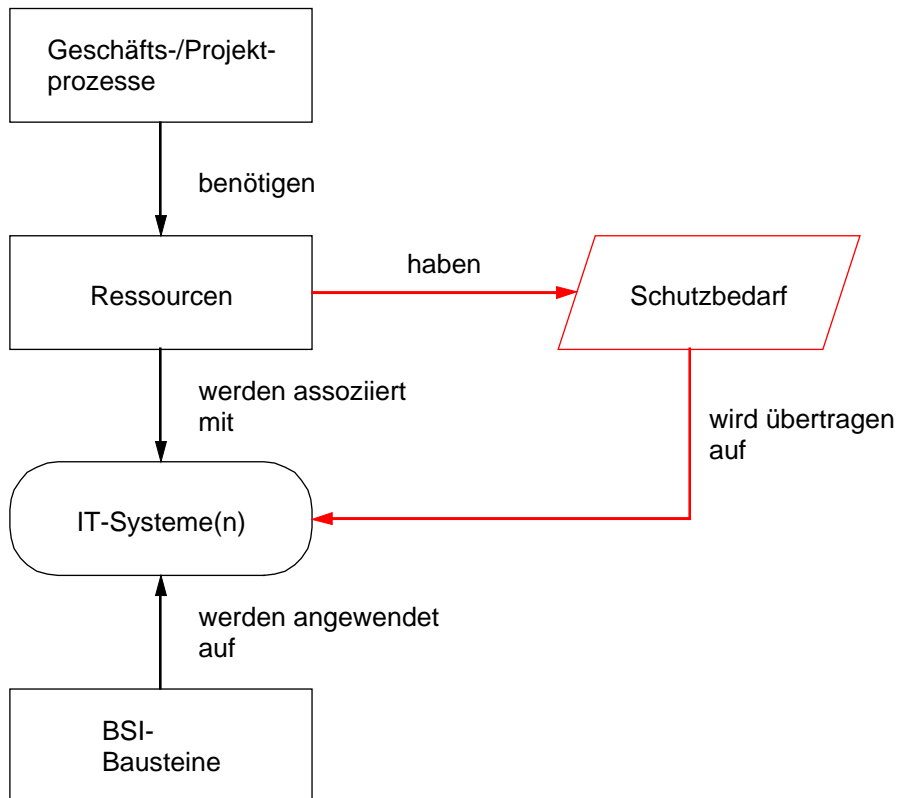


Bild 3: SECMAN-Methodik

Der Ablauf einer Sicherheitsanalyse in SECMAN gliedert sich in die folgenden Schritte:

1. Die von einem Prozeß benötigten Ressourcen werden in einem „Prozeßinventar“ erfaßt.
2. Der Schutzbedarf der Ressourcen wird prozeßspezifisch von den Prozeßbeteiligten bestimmt. Z.B. legt der Leiter eines Entwicklungsprojektes fest, daß die Integrität der Java-Quelldateien besonders schützenswert ist.
3. Die Prozeßressourcen werden mit konkreten Objekten aus dem IT-Verbundes der Organisation assoziiert. Diese Assoziation ist in aller Regel von einem Sicherheitsbeauftragten durchzuführen. Dieser verknüpft z.B. die Java-Quelldateien mit dem Server, auf dem diese Daten mitsamt dem zugehörigen Source Code Control System abgelegt ist. (Ggf. läßt sich aufgrund des unterschiedlichen Charakters von abstrakten Ressourcen und konkreten IT-Objekte nicht immer eine eindeutige Abbildung zwischen den Sichten definieren. Eine nur lose Assoziation reicht für eine algorithmische Auswertung nicht, erleichtert jedoch die manuelle Informationsgewinnung.)
4. Der prozeßspezifisch ermittelte Schutzbedarf wird auf die konkreten Objekte des IT-Verbunds übertragen. Diese Übertragung ist in aller Regel von einem Sicherheitsbeauftragten durchzuführen. Für unser Beispiel bedeutet dies, daß er sämtliche Ressourcen sichtet, die mit dem Server assoziiert sind (also z.B. die Java-Quelldateien, aber ggf. auch Ressourcen aus weiteren Prozessen) und aus deren Schutzbedarf einen Schutzbedarf für den Server ableitet.
5. Die Bewertung des Schutzbedarfes fließt in die Sortierung der Maßnahmen für den Sicherheitsaudit ein. Dem für die Sicherheit des Servers verantwortlichen – also z.B. dem Systemadministrator – würden in unserem Beispiel diejenigen Maßnahmen bevorzugt angezeigt werden, die die Integrität des Servers erhöhen.

Auf dieser Basis können einige wichtige Fragen beantwortet werden:

- Welche Maßnahmen sollen aufgrund der Wertigkeit der exponierten Objekte für das Unterneh-

mens und aufgrund der Unternehmensstruktur *bevorzugt* ausgeführt werden?

- Welche Maßnahmen *passen* besonders gut auf den Schutzbedarf eines Unternehmenswertes? (Ist es z.B. sinnvoller, eine Kundendatei zu verschlüsseln oder den Zugang zu einem Serverraum zu überwachen?)
- Welche Maßnahmen haben *schädliche* „Nebenwirkungen“? (Die Integrität und die Verfügbarkeit von Daten kann z.B. durch Anlegen einer Sicherungskopie erhöht werden, ihre Vertraulichkeit wird dadurch aber möglicherweise in Frage gestellt.)

Für diese Art der Schutzbedarfsanalyse wird offensichtliche Wissen benötigt, welches zwar in der Organisation vorhanden ist, sich aber über mehrere Personen verteilt (z.B. Abteilungsleiter, Projektleiter, Sicherheitsbeauftragter). Die Erstellung und Durchführung von Sicherheitsaudits muß also als kooperativer Prozeß verstanden werden, der Fachwissen auf der einen und Sicherheitswissen auf der anderen Seite benötigt. Besonders wichtig dabei ist, daß der Schutzbedarf aus der Sicht der Prozeßverantwortlichen so formuliert werden kann, daß von konkreten technischen Details, wie dieser Schutz zu erbringen ist, abstrahiert werden kann.

4 Das SECMAN-Tool

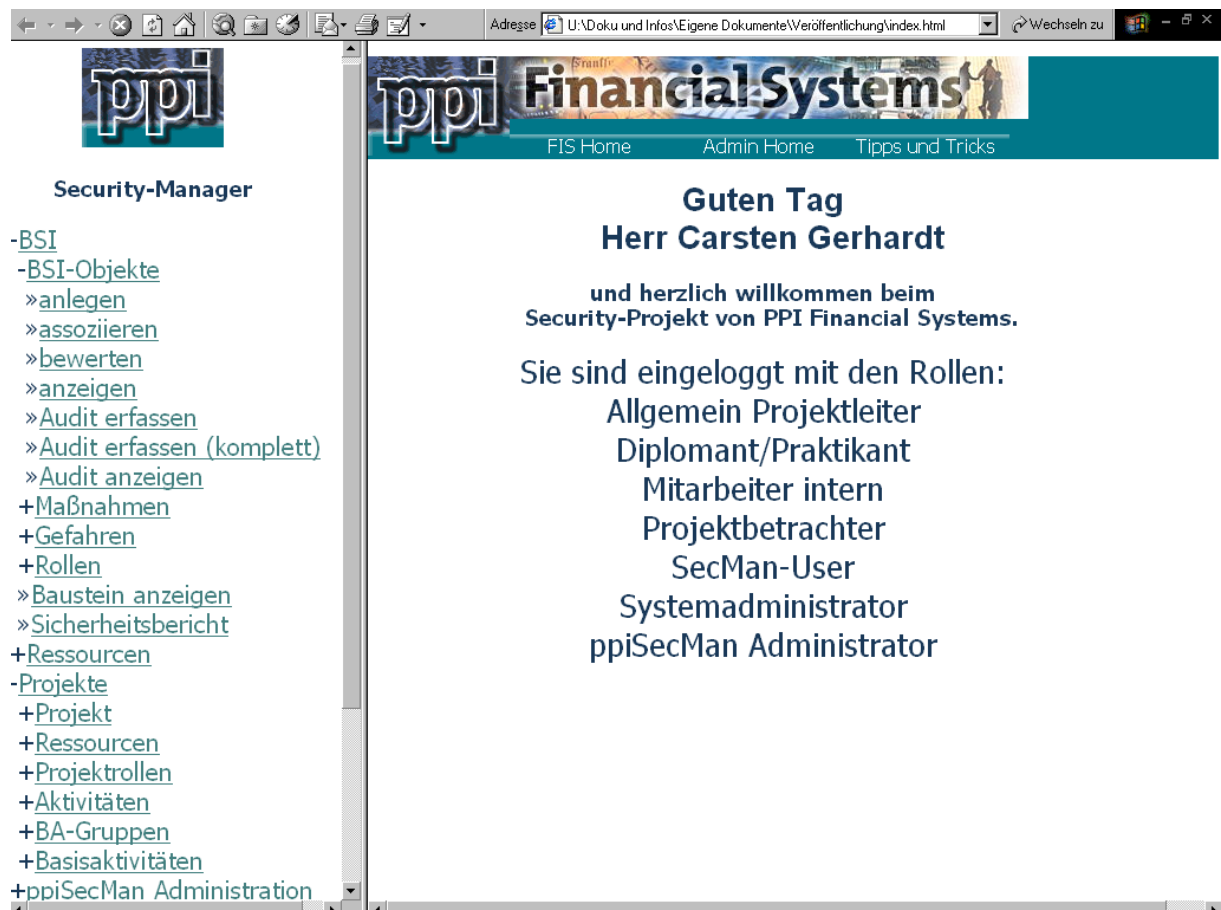


Bild 4: Das SECMAN-Tool

4.1 Rollenbasierte Zugriffskontrolle

Die dargestellte SECMAN-Methodik erfordert, daß bei der Erfassung und Verarbeitung eines Sicherheitsaudits zwischen Personen mit Projektwissen und solchen mit Sicherheitswissen differenziert wer-

den kann. Konsequenterweise ist für das SECMAN-Tool ein Rollenmodell entwickelt worden, das diese Differenzierung berücksichtigt. Dabei werden die jeweiligen Wissenskomponenten nicht direkt Benutzern, sondern bestimmten Rollen (Aufgabenbeschreibungen) zugeordnet. Auf diesem Rollenmodell baut eine rollenbasierte Zugriffskontrolle (*Role Based Access Control*, RBAC) auf.

Rollenbasierte Zugriffskontrolle ist ein Konzept, welches schon lange in der Informationsverarbeitung verwendet wird, aber erst Anfang der 90er Jahre formal definiert wurde [3] [4]. Mit RBAC wird eine möglichst flexible Verwaltung von Zugriffsrechten, aber auch von Aufgaben und Pflichten angestrebt. Rechte, Aufgaben und Pflichten werden dabei nicht direkt an einzelne Personen gebunden, sondern an Rollen, die diese Benutzer einnehmen können. Die jeweiligen Rechte, Aufgaben und Pflichten werden damit Personen nur indirekt zugeordnet. Eine wichtige Frage bei der Generierung von RBAC-Regulativen ist damit die Definition von Rollen, die geeignet sind, die Aufgabenverteilung in der zu modellierenden Organisation angemessen wiederzugeben. Diese Rollen lassen sich oft aus den Aufgabenbeschreibungen entnehmen (top down) oder aber aus den aktuell vorhandenen Benutzerrechten ableiten (bottom up). Es sind einige erfolgversprechende Ansätze entwickelt worden, um Rollen direkt aus *Use Cases* [5] oder anderen formalen Betrachtungen der Organisation zu gewinnen [6] [7] [8]. Der Vorteil der rollenbasierten Vorgehensweise besteht darin, daß bei einer Veränderung der Zuordnung von Rechten, Aufgaben und Pflichten zu bestimmten Personen einfach nur die Rollenzuordnung für diese Personen angepasst werden muß.

In der SECMAN-Methodik wird die Struktur der Aufgabenverteilung durch Rollen modelliert. Diese Rollen dienen im ersten Schritt zur Modellierung der Aufgabenbereiche und der damit zusammenhängenden Arbeitsprozesse, Ressourcen und Bewertungen.

Diese Rollen werden darüberhinaus zur Zugriffskontrolle in SECMAN-Tool genutzt (RBAC). Eine Rolle, die in der Prozeßmodellierung als Projektleiter definiert ist, darf entsprechend in SECMAN diejenigen Einträge bearbeiten, die zur Erfassung der projektbezogenen Daten und Bewertungen dienen. Analog gilt dies für permanente Funktionsbeschreibungen wie z.B. Ressortleiter (Administrator oder Leiter innerer Dienst). Diese Zugriffskontrolldefinitionen werden auch auf Rollen ausgedehnt, die in der Modellierung der Organisation u.U. nicht zu finden sind und eine nur interne Bedeutung haben. Dies kann z.B. ein Sicherheitsexperte sein, der die Abbildung zwischen Projektwissen und BSI-Objekten herstellen soll. In der SECMAN-Methodik bieten es sich an, für folgende drei Aufgaben verschiedene Rollen mit der Durchführung zu betreiben:

1. Erfassung von Projektwissen, insbesondere von Ressourcen und ihrer Bewertung – hier sind z.B. Projektleiter gefragt.
2. Erfassung von realen Objekten und Durchführung von Audits nach BSI-Grundschriftbuch – viele dieser Aufgaben werden z.B. vom Systemadministrator wahrgenommen.
3. Assoziation zwischen Projektressourcen und BSI-Objekten und Bewertung dieser Objekte anhand der Projektinformation – diese Rolle sollten Personen mit Einblick in Firmeninterne und Sicherheitsfragen einnehmen.

Dieses Beispiel zeigt, wie inhaltlich unterschiedliche Aufgaben, die auch unterschiedlich erfahrenes und qualifiziertes Personal zur Durchführung benötigen, durch eine Modellierung mit einem Rollenmodell abgebildet werden können.

Auch die BSI-Grundschriftmethodik arbeitet mit einem Rollenkonzept. Für die Erfassung und Verarbeitung von Sicherheitsaudits definiert sie zwei Typen von Rollen, die sich durch die Verantwortlichkeit für die Durchführung von Maßnahmen unterscheiden:

1. Initiieren von Maßnahmen
2. Durchführen von Maßnahmen

Die Integration dieses Rollenkonzepts in das Rollenkonzept von SECMAN erfolgt durch ein Mapping von SECMAN-Rollen auf BSI-Rollen. Diese Abbildung von Rollen erfolgt frei definierbar. Ist ein Benutzer von SECMAN für eine SECMAN-Rolle zugelassen, die mit einer BSI-Rolle assoziiert ist, so ist er damit indirekt für die Initiierung oder Durchführung einer Maßnahme zuständig. Die Verwendung der Rollen wird durch ein Konzept von persönlicher Verantwortlichkeit für die Durchführung von BSI-Maßnahmen erweitert. Die Möglichkeit, Mitarbeiter persönlich für die Durchführung von Maßnahmen verantwortlich zu machen, ist schon in der Definition des Grundschriftbuches

enthalten. Ist nun ein Benutzer über die Rollenzuordnungen für die Initiierung einer Maßnahme zugelassen, so kann er einer anderen Person diese Verantwortung aufbürden. Diese Vorgehensweise erweitert das Rollenkonzept, welches Rollen Rechten zuordnet, auf die Zuteilung von Pflichten. Mit SECMAN kann so z.B. die Verantwortung für die Maßnahme M 1.15 („Geschlossene Fenster und Türen“) für ein Objekt an einen bestimmten Mitarbeiter vergeben werden.

4.2 Das SECMAN-Programmsystem

Bei der Implementation von SECMAN wurde auf größtmögliche Flexibilität geachtet. Daher wurde SECMAN als 3-Tier-Web-Application implementiert (Bild 5). Somit sind die Anforderungen auf Client- Seite minimal; jeder Rechner mit einem Web-Browser und Netzzugang kann als Client dienen. Die von SECMAN verwalteten Daten werden in einer Datenbank gespeichert. Die Web-Application setzt sich aus mehreren Scripten zusammen, welche die HTML-Seiten für das Web-Frontend erzeugen.

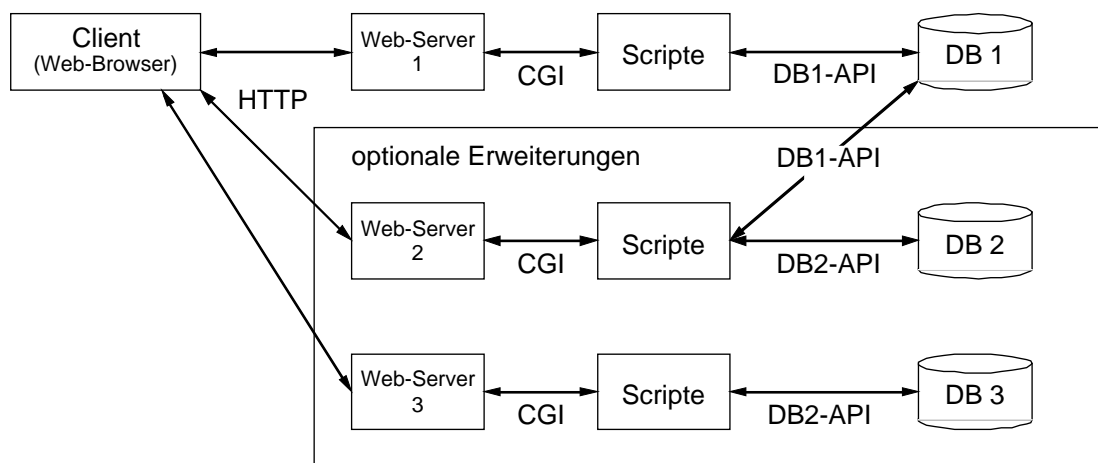


Bild 5: Struktur des SECMAN -Programmsystems

SECMAN ist so konzipiert, dass mehrere Scriptsprachen und mehrere Datenbanken nebeneinander verwendet werden können. Somit können Informationen, die u.U. bereits in anderen vorhandenen Datenbanken vorliegen, relativ einfach in SECMAN integriert werden. Zudem ist es möglich, Teile von SECMAN auf verschiedene Server zu verteilen.

Auf der Server-Seite setzt sich SECMAN aus mehreren Modulen zusammen. Die wichtigsten sind:

- das Basismodul,
- das Prozeßerfassungsmodul, und
- das BSI-Grundschutzmodul

Die Objekte dieser Modulen können miteinander assoziiert werden.

Das *Basismodul* überprüft die Autorisation für den Zugriff auf die angeforderte Funktion der Module und stellt diesen Informationen über den Benutzer und seinen aktiven Rollen zur Verfügung. Damit kann innerhalb der Funktionen eine weitere Einschränkung der angezeigten Informationen oder der Funktionalität selbst erreicht werden. Zum Beispiel kann sich ein Benutzer bei der Funktion „Anzeige eines BSI-Audits“ lediglich die Maßnahmen anzeigen lassen, für die er durch seine Rollen verantwortlich ist, oder die Funktion „Passwort ändern“ erlaubt einem Benutzer, nur sein eigenes Passwort zu ändern.

Die Identifikation der Benutzer wird mit Hilfe von nicht-permanenten Cookies realisiert. Wenn ein Benutzer eine Anfrage ohne einen gültigen Cookie an das System stellt, wird die Anfrage vom Basis-Sicherheits-Modul nicht an die entsprechende Funktion weitergeleitet, sondern zunächst eine Authentifizierung mit Benutzername und Passwort verlangt. Bei einer erfolgreichen Authentifizierung wird für den Benutzer ein Session eingerichtet. Zu der Session werden der Benutzer, die Zeit der

letzten Aktivität und die aktiven Rollen gespeichert und eine eindeutige Identifikation der Session wird beim Client als Cookie gespeichert.

Im *Projekterfassungsmodul* werden folgende Daten erfasst und verwaltet:

- beteiligte Rollen,
- beteiligte Mitarbeiter und ihre Rollen im Projekt,
- verwendete Ressourcen,
- Aktivitäten der Rollen und der dafür benötigten Ressourcen,
- Bewertungen zum Schutzbedarf der Ressourcen,
- Bedeutung der Aktivitäten zur erfolgreichen Durchführung der Projektarbeit.

Bei SECMAN liegt die Konzentration bei der Analyse der Geschäftsprozesse auf der Erfassung einzelner Handlungen innerhalb der Prozesse. Eine mögliche Beschreibung einer solchen Handlung ist z.B.: „Ein Entwickler bearbeitet C-Quellcode mit einem Editor“. Dabei wird ermittelt, welche Rolle (Entwickler) eine Handlung (C-Quellcode editieren) durchführt, welche Ressourcen zur Durchführung als Hilfsmittel benötigt werden (Editor) und welche Ressourcen durch die Handlung beeinflusst werden (C-Quellcode).

Sicherheitsanforderungen für diese Handlungen werden durch die Bewertung der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der beteiligten Ressourcen und Bedeutung der Handlung zur Realisierung der Unternehmensziele berücksichtigt.

Das *BSI-Grundschutzmodul* bietet folgende Funktionen:

- Erfassung der Objekte aus der Strukturanalyse
- Festlegung und Erfassung von Audits für die Objekte
- Bewertung von Maßnahmen bzgl. ihrer Wirksamkeit
- Berichte über den Umsetzungsgrad der Maßnahmen
- Kostenverfolgung von Maßnahmen
- Übersichten über die Abhängigkeiten von Maßnahmen und Gefahren

Dabei erlaubt das BSI-Modul an vielen Stellen einen einfachen Zugriff auf die originalen Beschreibungen des BSI im aktuellen Kontext. Dadurch wird die Arbeit mit dem Modul erleichtert und eine Sensibilisierung für sicherheitsrelevante Aspekte gefördert.

In SECMAN werden z.T. Daten aus verschiedenen Bereichen und Sichtweisen erfasst und verwaltet, welche untereinander eine logische Verbindung besitzen, jedoch nicht eindeutig zusammen gehören. Dies sind zum einen Rollen aus der Prozessanalyse und Rollen aus dem Grundschutzhandbuch, zum anderen sind es Ressourcen aus den Prozessanalysen und Objekte aus der BSI-Strukturanalyse.

Diese Anhängigkeiten können in SECMAN als m:n-Assoziationen erfasst werden. Somit können von jeder Seite zu einem Objekt die damit assoziierten Objekte der anderen Seite erfragt werden. Mit Hilfe der Assoziationen wird der manuelle Informationstransfer zwischen Sicherheitsanforderungen aus den Projektinformationen und den BSI-Analysen erleichtert.

5 Zusammenfassung und Ausblick

Mit SECMAN haben wir ein Instrument vorgestellt, um eine Sicherheitsanalyse nach dem BSI Grundschutzhandbuch mit einer Schutzbedarfsanalyse zu erweitern, die firmeninternes Knowhow in die Analyse integriert. Die ersten Anwendungen verliefen erfolgreich und haben sowohl bei Administratoren, wie auch im Management einen sehr positiven Eindruck hinterlassen. Die Bewertung der Sicherheitsanforderungen für die in den Projekten eingesetzten Ressourcen führten zudem zu einer Sensibilisierung der beteiligten Mitarbeiter.

In Zukunft könnte eine Verbesserung der Handhabbarkeit der Datenerhebung, insbesondere im Bereich der Projekterfassung, den Nutzwert des Programmsystems erhöhen. Geplant hierfür sind generische Projektdefinitionen oder die Übernahmen von Daten aus anderen Programmsystemen und Datenbanken (z.B. einer Mitarbeiter-DB), was durch das offene Konzept der Implementation (sowohl bei der Plattform wie auch der Sprache) erleichtert wird.

Der Bereich der Schutzbedarfsanalyse und der Bewertung der BSI-Objekte mit Hilfe der Assoziationen erfordert noch viel Überblick über technische und organisatorische Zusammenhänge. Hier könnte ein System zur Erkennung von Abhängigkeiten den Benutzer unterstützen. Hierzu wurde z.B. in [9] ein Fuzzy-Ableitungssystem zur Risikoanalyse unter Verwendung unscharfer Daten vorgestellt, dessen Integration gerade untersucht wird.

Literatur

- [1] Bundesamt für Sicherheit in der Informationstechnik:
IT-Grundschutzhandbuch.
Köln (Bundesanzeiger-Verlag) 2001, ISBN 3-88784-915-9
<http://www.bsi.bund.de/gshb/deutsch/menue.htm>
- [2] Philip E. Fites, Martin P.J. Kratz, Alan F. Brebner:
Control and Security of Computer Information Systems.
Rockville u.a. (Computer Science Press, Inc.) 1989, ISBN 0-7167-8191-3
- [3] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman:
Role-Based Access Control Models.
IEEE Computer 29, 2, 38-47 (Feb 1996)
- [4] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli:
Proposed NIST Standard for Role-Based Access Control.
ACM Transactions on Information and System Security 4, 3, 224-274 (Aug. 2001)
- [5] E. B. Fernandez and J. C. Hawkins:
Determining Role Rights from Use Cases.
presented at 2nd Workshop on Role-Based Access Control, Fairfax, VA, USA, 1997
- [6] Gerhard Schimpf:
Role-Engineering Critical Success Factors for Enterprise Security Administration.
Position Paper for the 16th Annual Computer Security Application Conference, New Orleans, 12/2000
- [7] Haio Röckle:
Rollenbasierter Zugriffsschutz.
IT-Sicherheit – Praxis der Daten und Netzsicherheit 1/99, Datakontext-Fachverlag GmbH, Frechen
- [8] Steffen E. Seufert:
Der Entwurf strukturierter rollenbasierter Zugriffskontrollmodelle.
Informatik Forschung und Entwicklung (2002) 17: 1-11 Springer-Verlag
- [9] Arndt Schönberg, Wilfried Thoben:
Ein unscharfes Bewertungskonzept für die Bedrohungs- und Risikoanalyse Workflow-basierter Anwendungen.
In "Sicherheit und Electronic Commerce (WS SEC '98)", Essen, Oktober 1998