PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

ABSCHNITT 3
TECHNIKEN

Version 2 – 5. Februar 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01 71 75 84 15 - Fax 01 71 75 84 00

Dieses Dokument wurde vom Beratungsbüro der DCSSI
(SGDN / DCSSI / SDO / BCS)
in Zusammenarbeit mit dem EBIOS-Club erstellt.

Kommentare und Vorschläge sind willkommen und können an folgende Adresse geschickt werden
(siehe Kommentarsammelformular am Ende des Leitfadens):

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

Änderungsprotokoll

Version	Gegenstand der Änderung	Stand
02/1997 (1.1)	Veröffentlichung des Leitfadens "Expression des besoins et identification des objectifs de sécurité" (EBIOS).	Genehmigt
23/01/2004	Generalüberarbeitung: - Erläuterungen und Anpassung an die Internationalen Normen über Sicherheit und Risikomanagement - Hervorhebung des Referenzsystems zur Unterscheidung von allen übrigen zu berücksichtigenden Anforderungen. - Integrierung der Konzepte "Hypothese" und "Sicherheitsvorschriften" (ISO/IEC 15408) - Übernahme der ausgewählten wesentlichen Elemente in die Zielsystemstudie - Verbesserungen bei der Festlegung der Bedürfnisskala: Werte, die von der Institution, bezogen auf ihre unmittelbaren Auswirkungen, als akzeptable Grenzen eingestuft werden. - Integrierung der für jedes Element formalisierten Bedürfnisse in die nachfolgende Aktivität. - Integrierung der Bestimmung des Betriebsmodus' in die Hypothesen. - Anpassung der Konzepte an ISO/IEC 15408: Untersucht wird der Ursprung der Bedrohungen, d. h. die Angriffsmethoden und die bedrohenden Elemente, sowie deren Charakterisierung nach Art (natürlich bedingt, menschlich bedingt, umweltbedingt), Ursache (unbeabsichtigt, vorsätzlich bei weiterer Aufsplitterung nach Exposition, verfügbaren Ressourcen, Fachkenntnissen und Motivation) und Angriffspotential. - Hervorhebung der nicht berücksichtigten Angriffsmethoden - Formalisierung der Bedrohungen im Sinne von ISO/IEC 15408 (bedrohendes Element, Angriffe und Wert bezogen auf die Entitäten), bevor diese dem Sicherheitsbedarf gegenübergestellt werden. - Änderung bezüglich der Gegenüberstellung von Bedrohungen und Bedürfnissen zur Identifizierung von Risiken - Hervorhebung der nicht berücksichtigten Risiken - Integrierung der Festlegung minimaler Sicherheitsziele für die Aktivitäten "Formalisierung von Sicherheitszielen" und "Bestimmung von funktionellen Anforderungen" - Änderung bezüglich der Festlegung von Sicherheitszielen, bei der die Hypothesen, die aus der Sicherheits-Policy erwachsenen Vorschriften, die Zwänge, das Referenzsystem und die Risiken berücksichtigt werden - Hinzufügen der Bestimmung von Sicherheitsniveaus, wodurch das Niveau der Sicherheitsziele bestimmt (z. B. unter Berücksichtigung des Angriffspotentials) und ein Gewährleistungsniveau ausgewählt werden kann. - Hinzufügen der Bestimmung funktioneller Sicherheitsanforderungen; dadurch können funktionelle Anforderungen bezogen auf die Sicherheitsziele bestimmt und diese Entsprechung dargestellt werden - Hinzufügen der Bestimmung von Sicherheitsgewährleistungsanforderungen, mit denen eventuelle Gewährleistungsanforderungen festgelegt werden können. Formverbesserungen, Anpassungen und geringfügige Korrekturen (Grammatik, Rechtschreibung, Formulierungen, Gestaltung, Kohärenz usw.)	Vom EBIOS-Club genehmigt
05/02/2004	Veröffentlichung der Version 2 des EBIOS-Leitfadens	Genehmigt

Inhaltsverzeichnis

Einleitung

Die EBIOS[1] –Methode besteht aus fünf sich ergänzenden Abschnitten

- Abschnitt 1 - Einführung
  In diesem Abschnitt werden der Kontext, der Nutzen und der Stellenwert der EBIOS-Methodik vorgestellt. Vervollständigt wird dieser Abschnitt durch ein Literaturverzeichnis, ein Glossar und ein Abkürzungsverzeichnis.

- Abschnitt 2 - Methodik
  Dieser Abschnitt beschreibt den Ablauf der verschiedenen Aktivitäten der Methode.

- Abschnitt 3 - Techniken
  In diesem Abschnitt werden Mittel zur Realisierung der Aktivitäten der Methode angeboten. Es ist ratsam, diese Techniken den Anforderungen und Praktiken der jeweiligen Institution anzupassen.

- Abschnitt 4 – Mittel zur IT-Risikobewertung
  Dieser Abschnitt entspricht dem ersten Teil der Grundkenntnisse der EBIOS-Methode (Entitätstypen, Angriffsmethoden, Schwachstellen)

- Abschnitt 5 – Mittel zur Behandlung von IT-Risiken
  Dieser Abschnitt entspricht dem zweiten Teil der Grundkenntnisse der EBIOS-Methode (Sicherheitsziele, Sicherheitsanforderungen, Tabellen zur Festlegung der funktionellen Sicherheitsziele und –anforderungen).

Das vorliegende Dokument entspricht dem dritten Abschnitt der Methode. Hier werden die Aktivitäten der Methode genauer beschrieben und Lösungen zur Realisierung angeboten.

Die in diesem Abschnitt vorgestellten Techniken sind nur Vorschläge. Jedem bleibt es überlassen, die seinem Kontext, d. h. seiner Geschäftkultur und den Gewohnheiten seiner Institution am ehesten angepassten Techniken und die ihm angenehmsten Tools auszuwählen. Was einzelne Details anbelangt, können auch Anpassungen vorgenommen werden.

[1] EBIOS ist eine Schutzmarke des Generalsekretariats der Nationalen Verteidigung in Frankreich.

Schritt 1 - Kontextstudie

Aktivität 1.1 – Untersuchung der Institution

Die Institution vorstellen

Bei der Vorstellung der Institution können die charakteristischen Elemente, die die Identität einer Institution definieren, kurz in Erinnerung gerufen werden. Es geht hier um die Bestimmung, die Tätigkeit, die Aufgaben, die Werte und die strategischen Achsen dieser Institution. Alle genannten Elemente sowie alle, die an der Sicherstellung dieser Elemente teilhaben, müssen klar identifiziert sein (z. B. bei Vergabe von Unteraufträgen).

Die Schwierigkeit dieser Aktivität liegt im Verständnis der wahren Organisation der Institution. Nur bei klarer Definition der Struktur kann deutlich werden, welche Aufgabe und Bedeutung jeder einzelnen Abteilung beim Erreichen der Ziele der Institution zukommt.
Die Eingliederung des Sicherheitsbeauftragten in die Allgemeine Führungskraft statt in die Direktion Datenverarbeitung kann beispielsweise viel über das Interesse der Führungskraft an der IT-Sicherheit aussagen.

Die hauptsächliche Bestimmung (was die Institution machen möchte)

Die Hauptbestimmung einer Institution lässt sich in etwa mit der Frage nach ihrer Existenzberechtigung umschreiben (ihr Aktivitätsbereich, ihr Marktsegment usw.). Bei der Bestimmung kann es sich z. B. um den öffentlichen Dienst oder die Industrie handeln.

Die Tätigkeit (was die Institution machen kann)

Die Tätigkeit einer Institution, die durch die Gesamtheit der Techniken bzw. das Know-how der Mitarbeiter charakterisiert werden kann, besteht in der Erfüllung der übertragenen Aufgaben. Sie ist dem Aktivitätsbereich der Institution eigen und prägt gewissermaßen ihre "Kultur".

Die Aufgaben (was die Organisation machen muss)

Die Bestimmung einer Institution beruht auf der Erfüllung von Aufgaben. Es geht darum, die erwiesenen Dienste und/oder die erzeugten Produkte unter Angabe der Endabnehmer genau zu definieren.

Die eigenen Werte (was die Organisation gut macht)

Hier geht es um die Grundsätze bzw. eine klar definierte Ethik, die an die Art und Weise geknüpft sind, wie eine Tätigkeit ausgeübt wird. Davon betroffen sein kann das Personal, das Verhältnis zu externen Intervenienten (Kundschaft u. ä.), die Qualität gelieferter Produkte oder Dienstleistungen.
So kann z. B. die Bestimmung einer Institution der öffentliche Dienst sein, ihre Tätigkeit der Transport und die zu erfüllende Aufgabe das Abholen von Schülern mit Schulbussen. Als Werte wären die Pünktlichkeit der Dienstleistung und die Sicherheit bei ihrer Erbringung zu nennen.

Struktur der Institution

Die Struktur der Institution kann verschiedenartig angelegt sein:

- Divisionsstruktur: Jede konstituierte Abteilung untersteht der Autorität eines Abteilungsleiters, der für die strategischen, administrativen und operationellen Entscheidungen innerhalb seiner Entität verantwortlich ist.
- Funktionsstruktur: Die funktionelle Autorität bezieht sich auf die Verfahren und die Beschaffenheit der Arbeit, gelegentlich auch auf die Entscheidungen oder die Planung (z. B.: Produktion, Datenverarbeitung, Personalwesen, Marketing usw.).

Anmerkungen:

- Eine Abteilung innerhalb einer Institution mit Divisionsstruktur kann durchaus funktionell strukturiert sein und gegensätzlich;
- bei einer Institution, bei der die gesamte Organisation auf beiden Strukturtypen basiert, spricht man von einer Matrixstruktur;
- unabhängig von der Struktur einer Institution können folgende Niveaus unterschieden werden:
  - Das Entscheidungsniveau (Definition strategischer Orientierungen);
  - das Steuerungsniveau (Koordination und Management);
  - das operationelle Niveau (Produktion und Unterstützungen).

Organigramm

Ziel ist die schematische Darstellung der Struktur der Institution. Bei dieser Darstellung müssen die Unterordnungs- und Überordnungsverhältnisse der Instanzen, aber auch sonstige Abhängigkeiten deutlich aufgezeigt werden. Selbst zu Instanzen ohne formelle Machtbefugnisse bestehen Verbindungen, nicht zuletzt um den Austausch von Informationen zuzulassen.
So kann beispielsweise ein IT-Korrespondent, der als Nutzer seinem Abteilungsleiter untersteht, auch Anweisungen von der Direktion Datenverarbeitung erhalten.

Die strategischen Achsen (was die Organisation besser machen will).

Hier geht es um die Formalisierung von Richtlinien, die die weitere Entwicklung der Institution bestimmen sollen, um den Belangen sowie den voraussichtlichen weiteren Tendenzen besser Rechnung tragen zu können.

Die auf der Institution lastenden Zwänge auflisten

Es geht darum, alle Zwänge zu berücksichtigen, welche auf der Organisation lasten und welche bei dem Bemühen um Sicherheit die Richtung vorgeben können. Sie können institutionsinternen Ursprungs sein. In diesem Fall kann die Institution sie eventuell anpassen. Wenn sie jedoch institutionsextern sind, sind sie in der Regel unumgänglich. Zwänge bezüglich der Mittel (Budget, Personal) und in Folge von Ausnahmesituationen sind die gewichtigsten.

Die Institution steckt Ziele, die es zu erreichen gilt (die die Tätigkeit an sich, das Verhalten betreffen), und die über einen mehr oder weniger langen Zeitraum die Weichen für die Zukunft stellen. Sie definiert die Entwicklungsrichtung und die Mittel, die es einzusetzen gilt. Zur Festlegung der Hauptachsen berücksichtigt die Institution die Weiterentwicklung der Techniken und des Know-hows, die von Nutzern oder Kunden geäußerten Wünsche usw.. Diese Finalität kann in Form von Funktions- oder Entwicklungsstrategien konkretisiert werden. Dabei kann es sich um eine Senkung der Betriebskosten, die Verbesserung der Serviceleistungen o. ä. handeln.

Diese Strategien werden wohl ein Kapitel dem Informationssystem (IT-System) widmen, das seinerseits dazu beizutragen hat, dass diese Strategien auch angewendet werden. Folglich ist die Berücksichtigung der Eigenschaften, die an die Identität oder die zu erfüllende Aufgabe und die Strategie der Institution gebunden sind, von grundlegender Bedeutung für die Problemanalyse, da die Beeinträchtigung eines Elements des IT-Systems (zumindest was die Sicherheit anbelangt) zur Infragestellung dieser strategischen Ziele beitragen könnte. Es ist auch wichtig, dass die vorgeschlagenen Sicherheitsmaßnahmen in Einklang mit den innerhalb der Institution geltenden Vorschriften, Gebräuchen und Mitteln stehen.

In den folgenden Abschnitten werden ohne Anspruch auf Vollständigkeit verschiedene Arten von Zwängen aufgelistet.

Zwänge politischer Natur

Sie können staatliche Stellen, öffentliche Einrichtungen oder ganz allgemein Institutionen betreffen, die Regierungsentscheidungen anzuwenden haben. Im Allgemeinen handelt es sich um Entscheidungen strategischer oder operationeller Ausrichtung, die von einer Führungskraft oder einer Entscheidungsinstanz ausgehen und die anzuwenden sind.
So wirft beispielsweise die Entmaterialisierung von Rechnungen oder amtlichen Dokumenten Sicherheitsprobleme auf.

Zwänge strategischer Natur

Vorgesehene oder mögliche Weiterentwicklungen der Strukturen oder Orientierungen der Institution können Zwänge hervorrufen. Sie werden in den strategischen oder operationellen Organisationsleitschemen berücksichtigt.
So kann z. B. die internationale Zusammenarbeit zur Koordinierung sensibler Informationen Abkommen über einen gesicherten Informationsaustausch notwendig machen.

Territoriale Zwänge

Die Struktur und/oder die Bestimmung der Institution können spezielle Zwänge zur Folge haben, wie z. B. eine Streuung der Standorte über das gesamte In- oder Ausland.
In diesem Zusammenhang können Postbüros, Botschaften, Banken oder die verschiedenen Filialen eines industriellen Großkonzerns als Beispiel dienen.

Konjunkturbedingte Zwänge

Der geordnete Betrieb einer Institution kann durch außergewöhnliche Situationen wie z. B. Streiks oder nationale bzw. internationale Krisensituationen grundlegend modifiziert werden.
So muss beispielsweise die Kontinuität bestimmter Dienste auch in Perioden schwerer Krisen sichergestellt werden können.

Strukturelle Zwänge

Die Struktur der Institution kann auf Grund ihrer Beschaffenheit (divisionell, funktionell o. a.) zu einer ihr eigenen Sicherheits-Policy führen, wobei die Organisation der Sicherheit genau an diese Strukturen angepasst ist.
So muss eine internationale Struktur in der Lage sein, die verschiedenen Sicherheitsanforderungen der einzelnen Länder in Einklang zu bringen.

Funktionelle Zwänge

Hier geht es um die Zwänge, die unmittelbar aus den generellen oder speziellen Aufgaben der Institution erwachsen.
Eine Institution, deren Aufgabe es ist, rund um die Uhr in Bereitschaft zu sein, muss z. B. eine maximale Verfügbarkeit ihrer Mittel sicherstellen.

Personalbedingte Zwänge

Die personalbedingten Zwänge sind verschiedenster Art und hängen von folgenden Faktoren ab: Grad der Verantwortung, Personalbestand, Qualifikation, Ausbildung, Sensibilisierung im Hinblick auf die Sicherheit, Motivation, Verfügbarkeit usw..
Es kann z. B. notwendig sein, dass das gesamte Personal einer Institution der Verteidigung zum Umgang mit extrem vertraulichen Informationen ermächtigt ist.

Zwänge terminlicher Natur

Sie können durch Neuorganisation von Abteilungen oder durch das Inkrafttreten einer neuen Politik im In- oder Ausland hervorgerufen werden und bestimmte Fälligkeiten zu bestimmten Terminen nach sich ziehen.
Ein Beispiel wäre die erstmalige Einrichtung einer Direktion für die Sicherheit.

Methodenbedingte Zwänge

Unter Berücksichtigung des in der Institution vorhandenen Know-hows (z. B. bei der Projektplanung, den Spezifikationen oder der Entwicklung) werden bestimmte Methoden vorausgesetzt.
Ein solcher Zwang kann z. B. darin bestehen, dass die Sicherheits-Policy mit den innerhalb der Institution geltenden qualitätsspezifischen Aktionen zu vereinbaren ist.

Zwänge kultureller Natur

In manchen Institutionen ist auf Grund der bestehenden Arbeitsgewohnheiten oder der Haupttätigkeit so etwas wie eine institutionseigene "Kultur" entstanden, die mit den Sicherheitsmaßnahmen

womöglich nicht vereinbar ist. Diese Kultur bildet den allgemeinen Bezugsrahmen der in dieser Institution tätigen Personen und kann verschiedene Parameter wie z. B. den Charakter, die Erziehung, die Ausbildung, die berufliche bzw. außerberufliche Erfahrung, die Meinungen, die Philosophie, den Glauben, Gefühle, den sozialen Status o. ä. betreffen.

Budget-Zwänge

Die empfohlenen Sicherheitsmaßnahmen können z. T. sehr kostspielig sein. Wenn die Investitionen für die Sicherheit nicht mit den Kriterien der Rentabilität einhergehen, fragen die Finanzabteilungen der Institution i. d. R. nach ihrer wirtschaftlichen Berechtigung.
So dürfen im Privatsektor und in bestimmten öffentlichen Institutionen die Gesamtkosten für die Sicherheitsmaßnahmen die Konsequenzen der gefürchteten Risiken nicht überschreiten. Die Führungskraft muss daher die Risiken beurteilen und ggf. kalkulierte Risiken eingehen, wenn prohibitive Kosten für die Sicherheit vermieden werden sollen.

Die von der Institution anzuwendenden Vorschriftsreferenzen auflisten

Die Berücksichtigung von Gesetzen, Vorschriften oder Regelungen kann Änderungen im Hinblick auf die Umgebung, die Arbeitsgewohnheiten, die Erfüllung von Aufgaben bewirken oder den internen Aufbau beeinflussen.
So wird beispielsweise der Betrieb staatlicher Behörden durch interne Vorschriften geregelt (Zollordnung, Gesetzgebung über das öffentliche Auftragswesen usw.).

Deshalb sollten die von der Institution anzuwendenden Vorschriftsreferenzen erfasst werden, egal ob es sich um Gesetze, Dekrete, speziell für den Bereich der Institution geltende Erlasse oder um interne bzw. externe Regelungen handelt. Dies betrifft auch die Verträge oder Übereinkommen und im weiteren Sinne die Verpflichtungen mit rechtlichem Charakter.

Eine funktionelle Beschreibung des globalen IT-Systems erstellen

Es geht darum, die Funktionsbereiche, welche zum Erreichen der strategischen Ziele beitragen, sowie deren Wechselwirkungen zu identifizieren. Zu diesem Zeitpunkt der Studie ist man bemüht, die existierenden und/oder zukünftigen Wechselwirkungen der Funktionsbereiche zusammen mit dem Bereich, dem das Zielsystem angehört, darzustellen.
Ein solches Vorgehen setzt voraus, dass das Bedürfnis funktionell klar geäußert worden ist.
Da das Ziel dieser Aktivität in der Formalisierung der konzeptuellen Architektur des IT-Systems besteht, damit das Zielsystem im Anschluss eingegrenzt und charakterisiert werden kann, können manchmal die Studien herangezogen werden, mit denen das IT-System erstellt worden ist (z.B. Kommunikations-Konzeptvorlagen und Bearbeitungen gemäß [MERISE]).

Mit einer Gliederung in Funktionsbereiche erhält man eine Funktionsübersicht des IT-Systems und der eventuellen Beziehungen mit externen Akteuren. Durch diese Aufteilung kann das Zielsystem besser im IT-System situiert werden, und die absehbaren Konsequenzen können besser begriffen werden.

Generell kann jedes IT-System in folgende Funktionen untergliedert werden:
- Operationelle Funktionen bzw. Funktionen mit operationellem Schwerpunkt;
- Unterstützungsfunktionen;
- Funktionen zur Kontrolle und Überwachung der Aktivitäten.

Die operationellen Funktionen betreffen die von der Institution zu erfüllenden Aufgaben.
Die Unterstützungsfunktionen betreffen die Verwaltung der Mittel, die zur Durchführung der operationellen Funktionen erforderlich sind.
Die Funktionen zur Kontrolle und Überwachung der Aktivitäten fallen in den Bereich des Managements.

Die Weiterentwicklung einer operationellen Funktion kann unmittelbare Auswirkungen auf alle anderen Funktionen haben, hingegen hat die Änderung einer Unterstützungs- oder Kontrollfunktion i. d. R. keinen direkten Einfluss auf die operationellen Funktionen.

Aktivität 1.2 – Studie des Zielsystems

Das Informationssystem (IT-System) trägt auch zur Realisierung der strategischen Ziele der Institution bei. Das IT-System und die Funktionsweise des Systems müssen ausreichend bekannt sein, um alle zur Ausarbeitung der Sicherheitsbedarfe des Zielsystems notwendigen Elemente herausfiltern zu können. Dazu ist es angebracht, das Zielsystem wieder in das IT-System der Institution zu positionieren.

Das Zielsystem vorstellen

Das Zielsystem muss Gegenstand einer synthetischen Beschreibung sein, die eindeutig den Umfang, die Beziehungen zu anderen Bereichen bzw. externen Akteuren und die Finalitäten innerhalb des globalen IT-Systems aufzeigt.

Die absehbaren Konsequenzen auflisten

In diesem Stadium der Betrachtung wird davon ausgegangen, dass die strategischen Ziele bekannt sind (vgl. Informatik-Strategie, Wahrscheinlichkeitsstudie usw.), die funktionellen Bedürfnisse festgelegt und definiert sind, die Informations- und Organisationszwänge des Zielsystems verzeichnet sind. Deshalb sollten nun die absehbaren Konsequenzen und der Kontext, in dem sich das Zielsystem befindet, analysiert werden.

Diese Analyse identifiziert das strategische Gewicht des Zielsystems für die Institution und bewertet das Wichtigkeitsniveau der Funktionen im Zielsystem. Sie hebt die Auswirkung der Realisierung oder des Betriebs des Systems, die Erwartungen der Nutzer oder ihrer Vorgesetzten, die erwarteten Gewinne usw. hervor. Die absehbaren Konsequenzen können zum Beispiel technischer, finanzieller oder politischer Natur sein.

Die wesentlichen Elemente auflisten

Zur genaueren Beschreibung des Zielsystems besteht die folgende Aktion darin, die wesentlichen Elemente zu identifizieren. Diese Auswahl wird von einer heterogenen und repräsentativen Arbeitsgruppe des IT-Systems getroffen (Verantwortliche, Informatiker und Nutzer).
Die wesentlichen Elemente sind i. d. R. alle Funktionen und Informationen, die im Zentrum der Aktivität des Zielsystems stehen. Es können aber auch andere wesentliche Elemente wie z. B. institutionsspezifische Verfahren berücksichtigt werden. Diese zweite Vorgehensweise eignet sich eher für die Ausarbeitung einer Sicherheits-Policy oder eines Sicherheitsstrategie für das Managements der IT-Systeme oder eines Kontinuitätsplans. Die wesentlichen Elemente stellen den Informationsbestand bzw. die "immateriellen Güter" dar, die man schützen möchte. Je nach Finalität ist es bei manchen Studien nicht nötig, eine vollständige Analyse aller das Zielsystem konstituierenden Elemente durchzuführen. In einem solchen Kontext kann der Studienumfang auf die vitalen Elemente des Zielsystems beschränkt werden.
Die Auswahl der wesentlichen Elemente erfolgt in Absprache mit einem Verantwortlichen, der gleichzeitig Nutzer des (bestehenden oder zukünftigen) Systems ist. Dieser nennt, nach einer ersten Analyse, alle von ihrer Natur her sensiblen Elemente. Die wesentlichen Elemente sind i. d. R. Funktionen oder Informationen, für die bei Nicht-Einhalten der Verfügbarkeit, der Integrität, der Vertraulichkeit oder sonstiger Sicherheitskriterien der Eigentümer oder Hoheitsträger haftbar gemacht werden könnte oder die ihm selbst oder Dritten Schaden zufügen könnten.

Die wesentlichen Funktionen (oder Teilfunktionen) sind vor allem:

- Funktionen, deren Ausfall oder Beeinträchtigung es unmöglich macht, dass das System seine Aufgabe erfüllen kann;
- Funktionen, die geheim eingestufte Verarbeitungen oder hochspezialisierte technologische Verfahren enthalten;
- Funktionen, die bei Änderung die Sicherstellung der Aufgabe durch das System stark in Frage stellen würden.

Die zu berücksichtigende Sensibilität der Informationen kann verschieden gewichtet sein:

- die gemäß [IGI 900] als geheim eingestuften Informationen, deren Sicherheitsanforderungsniveau nicht diskutierbar ist;
- die gemäß [Rec 901] als sensibel, jedoch nicht als geheim eingestuften Informationen, deren Sicherheitsanforderungsniveau in Abhängigkeit von den institutionsspezifischen Umgebungsbedingungen diskutierbar ist.

Allgemeiner ausgedrückt lassen sich folgende wesentliche Informationen unterscheiden:

- Klassifizierte Informationen, egal ob diese als geheim eingestuft sind oder nicht;
- zur Erfüllung der Aufgabe oder der Tätigkeit durch die Institution vitale Informationen;
- persönliche Informationen, beispielsweise personenbezogene Daten im Sinne des französischen Gesetzes über Datenverarbeitung und Freiheiten;
- strategische Informationen, die zur Erreichung der Ziele gemäß den strategischen Orientierungen notwendig sind;
- kostenintensive Informationen, deren Sammlung, Speicherung, Verarbeitung oder Übertragung viel Zeit in Anspruch nehmen und/oder hohe Erwerbskosten verursachen.

Funktionen und Informationen, die bei dieser Auswahl nicht berücksichtigt wurden, werden im weiteren Verlauf der Studie Gegenstand keines weiteren Sicherheitsbedarfes sein. Das bedeutet, dass ihre eventuelle Beeinträchtigung keinen Einfluss auf den geordneten Ablauf der vom System zu erfüllenden Aufgabe haben wird.
Doch werden auch diese Funktionen und Informationen häufig mit Maßnahmen versehen, die zum Schutze der ausgewählten Funktionen und Informationen ergriffen wurden.

Die Blätter zur Sicherheitsbedarfsanalyse werden dem Nutzer die Möglichkeit geben, sich über die Sensibilität wesentlicher Funktionen und Informationen zu äußern.

Eine funktionelle Beschreibung des Zielsystems erstellen

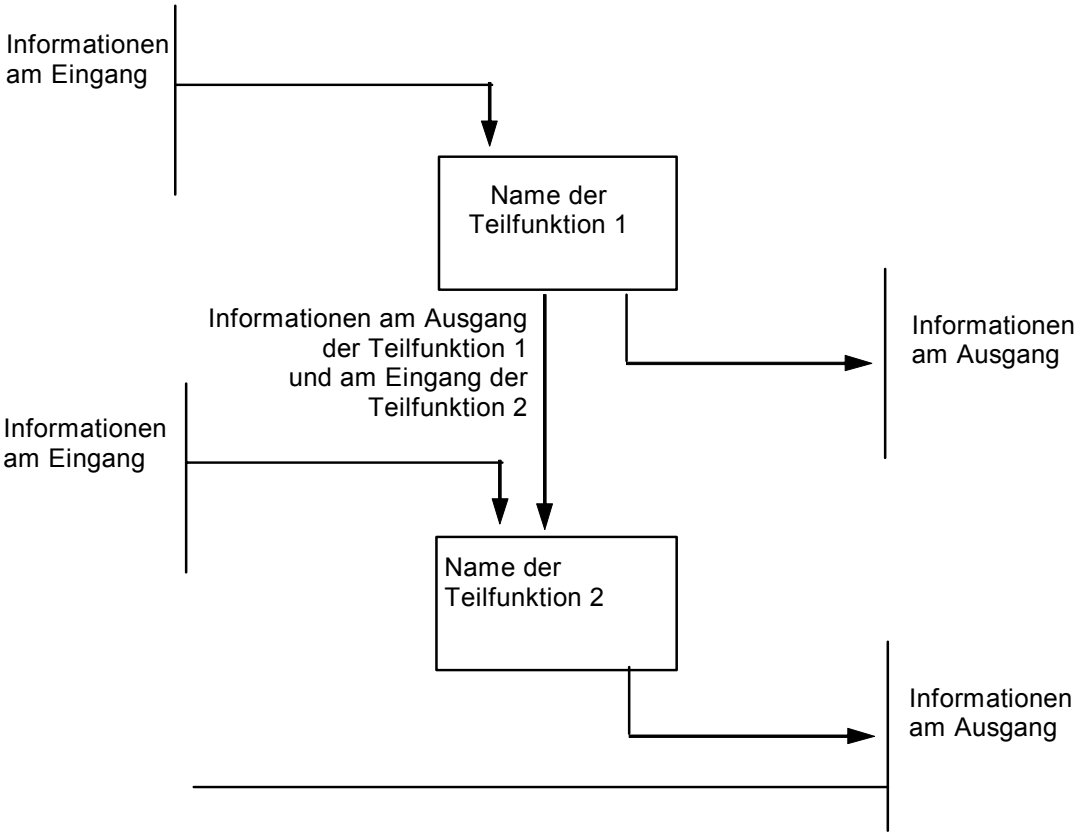
Zu diesem Zeitpunkt sind die Zwecke des Zielsystems klar formuliert, sein Platz in Bezug auf das existierende System ist etabliert. Deshalb sollte für jede identifizierte wesentliche Funktion folgendes angegeben werden:

- Die Informationen am Eingang und am Ausgang (erwartete Ergebnisse);
- Die zu realisierenden Bearbeitungen (wobei auch die Schnittstellen angegeben werden sollten, über die das Zielsystem Informationen mit den anderen IT-System austauscht).

Eine Funktion kann im Allgemeinen in Teilfunktionen gegliedert werden; die Teilfunktion ist ein kohärentes Ganzes aus Bearbeitungen (Gruppe von elementaren Aufgaben) und Informationen.

Bei einem zu entwerfenden System wird zur Modellbildung des Zielsystems die ausgewählte allgemeine Entwurfsmethode verwendet (Beispiele: MERISE, SADT, UML…).

Bei einem existierenden System oder beim Fehlen einer Modellbildung während des Entwurfs sollte die folgende Darstellung verwendet werden: Die Funktionen werden in einem Flussdiagramm dargestellt, in dem die Beziehungen zwischen den Teilfunktionen und die Informationen am Eingang und am Ausgang der Funktionen erscheinen (siehe Beispiel auf der nächsten Seite).



Beispiel: Darstellung einer Funktion des Human-Ressource-Managements

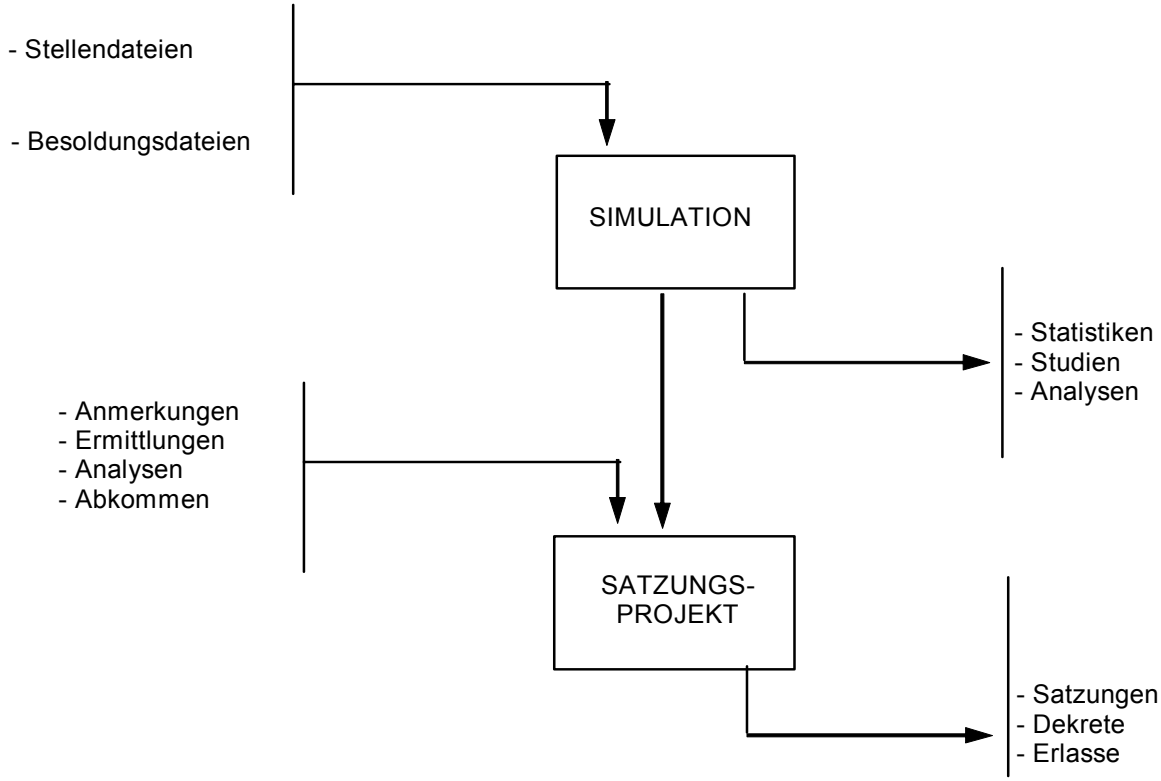


Abbildung 1 – Darstellung der Funktionen und Informationen

Aufteilung des Systems in Teilsysteme

Die Aufteilung des Systems in Teilsysteme kann zur Vereinfachung der weiteren Studie ins Auge gefasst werden.

Das Hauptziel dieser Aufgliederung in Teilsysteme ist es, die Anwendung der EBIOS-Methode zu vereinfachen. Der Leiter der Studie kann entscheiden, ob das System in mehrere Teilsysteme aufgeteilt werden soll. Er legt damit fest, ob mehrere Teilsysteme zu unterscheiden sind, wobei jedes für sich einfacher zu untersuchen ist, oder ob ein einziges Zielsystem Gegenstand der Studie sein soll.

Die Aufgliederung in Teilsysteme bleibt der Einschätzung des Leiters der Studie vorbehalten. Die Untersuchung mehrerer Teilsysteme ist i. d. R. einfacher als die globale Untersuchung eines vielschichtigen Systems, jedoch sollte die Anzahl der Teilsysteme niedrig sein (weniger als fünf), da jedes Teilsystem Gegenstand einer eigenen Studie sein wird.

Die Aufgliederung in Teilsysteme bringt folgende Vereinfachungen:

- Die Auswahl von Richtungen, in die die Bemühungen gehen sollen: Daraus kann hervor gehen, für welche Teilsysteme eine Studie überflüssig oder zumindest weniger vorrangig ist.
- Die Organisation der Studie: Die Untersuchung eines Teilsystems kann einer geringeren Anzahl Mitarbeiter anvertraut werden.

Es gibt keine Methode im eigentlichen Sinne zur Aufgliederung eines Systems in Teilsysteme, vielmehr gilt es, eine Anzahl von Kriterien zu überprüfen. Folgende Kriterien sind für die Aufteilung relevant:

- Kriterium Nr. 1: Berücksichtigung der HW-Architektur

  Soviel Teilsysteme bilden, wie autonome Rechner (oder Rechnergruppen) vorhanden sind. Wenn, wie allgemein üblich, die einzelnen Rechner miteinander verbunden sind, hängt die Aufgliederung vom Interoperabilitätsniveau der einzelnen Systembereiche (Rechner oder Rechnergruppen) ab.

  Beispiel: Zunehmendes Interoperabilitätsniveau
  - Physisch getrennte Rechner. Datenübertragung über Band oder Diskette.
  - Über eine Datenübertragungsverbindung verbundene Rechner.
  - Autonome Rechner, die über ein lokales Netz kooperieren.
  - Über ein lokales Netz verbundene Rechner, die mit dem gleichen Betriebssystem ausgestattet sind und zentral administriert werden.

- Kriterium Nr. 2: Aufgliederung nach wesentlichen Funktionen oder Informationen.

  Ein physisch abgeschlossenes Teilsystem kann nach Funktionen, die von den jeweiligen Rechnern bzw. Teilsystemen durchgeführt werden, oder nach der Art und Weise, wie die Informationen größter Sensibilität bearbeitet werden, aufgegliedert werden.

- Kriterium Nr. 3: Autonomie der Verantwortung

  Eine Anzahl von Entitäten, die insofern ein Ganzes bilden, als sie in der Praxis dem gleichen Verantwortungsbereich unterstehen (Nutzergruppe, technischer Einsatz o. ä), könnte als getrennt zu untersuchendes Teilsystem benutzt werden. Dabei könnte es sich um einen Systembereich handeln, der der Verantwortung einer auf dem Organigramm der Institution eindeutig identifizierten Abteilung untersteht. Dieses Kriterium kann auch angewendet werden, wenn mehrere separate Dokumentationen vorhanden sind.

- Kriterium Nr. 4: Implementierung in getrennten Teilzonen

  Wenn die einzelnen Bestandteile (Hardware, Unterstützungen, Personal) in unterschiedlichen Teilzonen untergebracht sind (Gebäude, beschränkt zugängliche Teilzonen, Untergeschosse usw.), kann jede Teilzone ein eigenes Teilsystem darstellen (vorausgesetzt, das Interoperabilitätsniveau nach außen ist schwach genug).

- Kriterium Nr. 5: Isolierung "gemeinsamer Teilsysteme"

  Nach Anwendung der vier ersten Kriterien können sich bestimmte Entitäten oder Bestandteile im Überlappungsbereich mehrerer Teilsysteme befinden (z. B gemeinsame Server, gemeinsame Netzwerke, gleiches Personal oder gemeinsame

Teilzonen). Auch sie können Teilsysteme bilden, die getrennt untersucht werden können. Die Ergebnisse dieser Studien werden im Anschluss auf die entsprechenden Teilsysteme übertragen. Es handelt sich gewissermaßen um ein Faktorisieren der Arbeit.

Die Hypothesen auflisten

Es handelt sich um die Formalisierung der auf das Zielsystem bezogenen Hypothesen. Die Hypothesen werden aus Gründen der internen oder externen Politik der Institution, aus finanziellen Gründen oder aus Gründen der zeitlichen Planung meistens von der Institution auferlegt, welche die Studie leitet.
Die Hypothesen können auch ein von vornherein bei einer bestimmten Umgebung akzeptiertes Risiko sein.
Im Falle der Erstellung eines Schutzprofils (protection profile) oder einer Sicherheitsvorgabe, welche die vollständige Erfassung der Bedrohungen durch die Sicherheitsziele nachweisen müssen, kann es sich um Schwachstellen handeln, die in den nachfolgenden Schritten nicht durch ein Sicherheitsziel abgedeckt werden können. In demselben Fall kann es sich um die formalisierte Berücksichtigung von identifizierten Zwängen handeln, während die anderen nur Hilfen für das Verstehen des Kontextes sind.

Es wird empfohlen, die folgende Nomenklatur für die Hypothesen zu verwenden: H.xx (H steht für Hypothese und xx für den Namen der Hypothese).

Der Sonderfall der Auswahl des Sicherheitsbetriebsmodus'

Die Bestimmung des Sicherheitsbetriebsmodus des Systems gibt an, wie das System den Anwendern verschiedener Kategorien die Bearbeitung, Übertragung oder Aufbewahrung von Informationen verschiedener Vertraulichkeitsstufen ermöglicht. Sie sorgt für eine Vergegenwärtigung der allgemeinen Sicherheitsproblematik, weil der Sicherheitsbetriebsmodus den Kontext für die Verwaltung der Informationen eines IT-Systems definiert.

Generell gehört der Sicherheitsbetriebsmodus des Systems einer der folgenden Kategorien an:

- Kategorie 1: Exklusiver Betriebsmodus
  - Alle Personen, die Zugang zum System haben, sind auf höchstem Klassifikationsniveau befugt, und sie müssen bezüglich der vom System verarbeiteten, gespeicherten oder übertragenen Informationen über die gleichen (oder entsprechende) Kenntnisse verfügen können.
- Kategorie 2: Dominierender Betriebsmodus
  - Alle Personen, die Zugang zum System haben, sind auf höchstem Klassifikationsniveau befugt, aber sie müssen bezüglich der vom System verarbeiteten, gespeicherten oder übertragenen Informationen nicht alle über die gleichen (oder entsprechende) Kenntnisse verfügen können.
- Kategorie 3: Vielschichtiger Betriebsmodus
  - Alle Personen, die Zugang zum System haben, sind nicht alle auf höchstem Klassifikationsniveau befugt, und sie müssen bezüglich der vom System verarbeiteten, gespeicherten oder übertragenen Informationen nicht alle über die gleichen (oder entsprechende) Kenntnisse verfügen können.

Zur Auswahl des Betriebssicherheitsmodus des Systems ist es wichtig zu wissen, ob folgende Elemente existieren oder existieren müssen:

- ein hierarchische Klassifizierung der Informationen (z. B. vertraulich, geheim u. ä..) und/oder eine Klassifizierung nach Sparten (medizinisch, gesellschaftlich, atomar usw.),
- Anwenderkategorien,
- ein Konzept, das einen Anspruch auf Kenntnisnahme, Änderungsberechtigung, Verfügung o. ä. vorsieht.

Die Wahl des Sicherheitsbetriebsmodus kann in Anbetracht der während der nachfolgenden Schritte identifizierten Risiken revidiert werden. Es ist jedoch wichtig, diesen Aspekt so früh wie möglich zu erörtern, weil seine Umsetzung bedeutende Konsequenzen für die Architektur des IT-Systems und die IT-Sicherheit hat.

Die Sicherheitsvorschriften auflisten

Es kann sein, dass die Sicherheit der IT-Systeme schon in einem Studien-Bezugssystem und in Dokumenten behandelt worden ist; obwohl eine detaillierte Analyse in diesem Stadium nicht angebracht ist, können Auskünfte eingeholt werden: Prioritäten, Ergebnisse, Anweisungen usw.
Ziel ist die Erfassung der wichtigsten Sicherheitsvorschriften und -maßnahmen, egal ob sie formalisiert sind oder nicht. Folgende Dokumente können für die Sammlung dienen:

- Sicherheits-Policy des IT-Systems;
- Kontinuitätspläne der Anwendungen;
- Sicherheitsanweisungen der Entwicklungen;
- Ergebnisse von Sicherheits-Audits;
- Sicherheitsprojekte usw.

Es wird empfohlen, die folgende Nomenklatur für die Sicherheitsvorschriften zu verwenden: P.xx (P steht für Politik und xx für den Namen der Sicherheitsvorschrift).

Die auf dem Zielsystem lastenden Zwänge auflisten

Durch die Identifizierung der Zwänge können diejenigen bestimmt werden, die eine Auswirkung auf das Zielsystem haben, und diejenigen, die man beeinflussen kann. Sie vervollständigen und komplettieren die bereits erkannten Zwänge der Institution. In den folgenden Abschnitten werden ohne Anspruch auf Vollständigkeit verschiedene Arten von denkbaren Zwängen aufgelistet.

Zwänge der chronologischen Abfolge

Alle Anwendungsprojekte können nicht gleichzeitig entwickelt werden. Einige setzen bestimmte Realisierungen im Vorfeld voraus. Ein System kann Gegenstand einer Aufgliederung in Teilsysteme sein; ein System ist jedoch nicht unbedingt von der Gesamtheit aller Teilsysteme eines anderen Systems abhängig (durch Funktionserweiterung eines Systems).

Technische Zwänge

Die technischen Zwänge, die physischer Natur sind, können durch die Hardware bzw. die installierte Software vorgegeben sein oder durch die Räumlichkeiten bzw. Standorte des IT-Systems verursacht werden:

- Dateien (Anforderungen bezüglich der Organisation, der Verwaltung von Datenträgern, der Verwaltung von Nutzerrechten usw.);
- Allgemeine Architektur (Anforderungen bezüglich der Topologie, unabhängig davon ob diese zentralisiert oder verteilt ist, ob es sich um eine Client-Server-Architektur, eine physische Architektur o ä. handelt);
- Applikative Software (Anforderungen bezüglich der Konzeption spezieller Software, der marktüblichen Standards usw.);
- Programmpakete (Anforderungen bezüglich der Standards, des Evaluierungsniveaus, der Qualität, der Übereinstimmung mit den Normen, der Sicherheit usw.);
- Hardware (Anforderungen bezüglich der Standards, der Qualität, der Übereinstimmung mit den Normen usw.);
- Kommunikationsnetze (Anforderungen bezüglich der Flächendeckung, der Standards; der Kapazität, der Zuverlässigkeit usw.)
- Immobilien-Infrastrukturen (Anforderungen bezüglich des Bauwesens, der Konstruktion der Gebäude, der Starkströme, der Schwachströme usw.).

Finanzielle Zwänge

Die Realisierung von Sicherheitsmaßnahmen ist häufig durch das Budget, das eine Institution bereitstellen kann, eingeschränkt; dennoch ist der finanzielle Zwang als letztes zu berücksichtigen (der Teil des Budgets, der für die Sicherheit gedacht ist, lässt sich in Abhängigkeit von der Sicherheitsstudie aushandeln).

Umgebungsbedingte Zwänge

Die umgebungsbedingten Zwänge sind durch die geografische oder wirtschaftliche Umgebung, in der sich das IT-System befindet, vorgegeben: Land, Klima, natürliche Risiken, geografische Lage, wirtschaftliche Konjunktur usw..

Zeitliche Zwänge

Die Zeit, die zur Realisierung der Sicherheitsmaßnahmen nötig ist, muss mit der Evolutivität des IT-Systems in Einklang gebracht werden; bei ausgesprochen langer Implementierungsdauer besteht die Gefahr, dass die Lösung nicht mehr in Relation mit den Risiken steht, da sich diese bereits weiterentwickelt haben. Die Zeit ist bei der Wahl der Lösungen und Prioritäten ausschlaggebend.

Methodenbedingte Zwänge

Unter Berücksichtigung des Know-hows und der in der Institution üblichen Gewohnheiten (z. B. bei der Projektplanung, den Spezifikationen oder der Entwicklung) werden bestimmte Methoden vorausgesetzt.
Auf Basis der in Erfahrung gebrachten Elemente wird eine Anzahl organisatorischer Hypothesen abgeleitet und registriert.

Organisatorische Zwänge

Folgende Bereiche sind möglicherweise betroffen:

- Der Betrieb (Anforderungen bezüglich der Fristen, des Ergebniszwangs, der Überwachungs- und Kontrollanforderungen, der Ersatzpläne, des Notbetriebs usw.);
- die Wartung (z. B. Anforderungen bezüglich der Aktionen nach Zwischenfalldiagnose, bezüglich der vorbeugenden und instand setzenden Maßnahmen);
- Human-Ressource-Management (Anforderungen bezüglich der Ausbildung der Operatoren und Nutzer, der Qualifikation zur Besetzung bestimmter Stellen wie z. B. Systemadministrator oder Datenadministrator);
- die administrative Verwaltung (Anforderungen bezüglich der Verantwortungen der Akteure u. ä.);
- die Verwaltung von Entwicklungen (Anforderungen bezüglich der Entwicklungstools, der Software-Umgebung, der Abnahmepläne, der einzusetzenden Organisation usw.);
- die Verwaltung externer Beziehungen (Anforderungen bezüglich der Organisation der Beziehungen mit Dritten, bezüglich der Verträge usw.).

Die speziellen Vorschriftsreferenzen des Zielsystems auflisten

Die Beachtung von Gesetzen, Vorschriften oder Regelungen kann die Wahl materieller Lösungen oder Verfahren einschränken und die Umgebung bzw. bestehende Arbeitsgewohnheiten verändern.

Es ist daher empfehlenswert, alle im Zielsystem anzuwendenden Vorschriftsreferenzen zu erfassen.

Aktivität 1.3 – Bestimmung des Ziels der Sicherheitsstudie

Die Entitäten des Systems auflisten und beschreiben

Das Zielsystem besteht aus einem Gefüge technischer und nicht-technischer Entitäten, die es zu identifizieren und zu beschreiben gilt. Diese Entitäten besitzen Schwachstellen, die sich Angriffsmethoden zu Nutze machen könnten und die den immateriellen wesentlichen Elementen des Zielsystems (Funktionen und Informationen) schaden könnten. Daher müssen diese Entitäten gesichert werden. Verschiedene Typen sind zu unterscheiden.

Die verschiedenen Entitätstypen werden in den folgenden Abschnitten vorgestellt (es wird empfohlen, die Entitätstypen und –untertypen des Leitfadens "Mittel zur IT-Risikobewertung" zur Auflistung und Beschreibung zu benutzen).

Die Hardware

Der Typ "Hardware" wird von allen physischen Elementen eines IT-Systems gebildet, egal ob es sich dabei um aktive Datenverarbeitungsmittel oder passive Datenträger handelt.

Die Software

Der Entitätentyp "Software" umfasst alle Programme, die für den Betrieb einer DatenverarbeitungsEntität erforderlich sind.

Die Netzwerke

Der Entitätentyp "Netzwerk" umfasst alle Telekommunikationseinrichtungen, über die mehrere ausgelagerte Rechner oder Teile des IT-Systems untereinander verbunden werden können.

Das Personal

Der Entitätentyp "Personal" umfasst die Gesamtheit aller Personengruppen, die mit dem IT-System in Kontakt stehen.

Die Standorte

Der Entitätentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind.

Die Organisationen

Der Entitätentyp "Organisation" beschreibt den organisatorischen Rahmen. Er umfasst sämtliche Strukturen der Personal-Aufgaben-Zuordnung sowie alle Prozeduren zur Regelung dieser Strukturen.

Die Systeme (optional)

Der Entitätentyp "System" umfasst alle klar definierten IT-Installationen einschließlich operationeller Umgebung. Er umfasst verschiedene Entitäten, die anderen zuvor genannten Entitätstypen angehören. Dieser Entitätentyp ist bei einer makroskopischen Analyse von Bedeutung.

Zum besseren Verständnis dieses Entitätentyps soll das Beispiel der Vernetzung von in Fahrzeugen mitgenommenen Terminals herangezogen werden, wobei die Terminals im Rahmen einer Fahrzeugkontrolle die Abfrage von Fahrzeug-Datenbanken ermöglichen.

Hardwaretypen:

- *In einem Landfahrzeug mitgenommenes Terminal, etwa ein PC-kompatibles Laptop, das eine Minidatenbank bearbeiten kann;*
- *ein zentrales Serversystem mit modularen Kommunikationsfronten, das eine nationale Datenbank bearbeitet.*

Softwaretypen:

- *Betriebssystem des zentralen Servers: große Dialogverkehrskapazitäten;*
- *relationales Datenbankverwaltungssystem mit zwei Niveaus im Kooperativmodus, im nationalen Server installiert.*

Netzwerktypen:

- *Nationales Netzwerk mit Paketvermittlung X25 (Zwangsvorgabe);*
- *Funknetz mit nationaler Reichweite zwischen den in den Fahrzeugen befindlichen Terminals und dem nationalen X25-Netzwerk.*

Personaltypen:

- *Personal zur Entwicklung und Wartung der Anwendungen: Internes Personal und externe Assistenz;*
- *befugtes und spezialisiertes Fachpersonal des EDV-Zentrums, auf technischer Plattform tätig;*
- *Nutzer der in den Fahrzeugen befindlichen Terminals: Befugtes Personal.*

Standorttypen:

- *Durch Umzäunung und Videoüberwachung geschütztes EDV-Zentrum in einem nicht klassifizierten geografischen Umfeld an Standorten mit großen Risiken.*
- *Über das ganze Land verteilte Personenkraftfahrzeuge.*

Organisationstypen:

- *Entwicklung und Wartung in der Regie;*
- *Prozeduren zur Aktualisierung der lokalen und zentralen Datenbanken von ortsfesten Spezialabteilungen aus, die direkt an das Landesnetz angeschlossen sind.*

Die Entitätstypen können weiter in Unterentitätstypen aufgegliedert werden, die Beschreibungen sind dann umso detaillierter.

Die wesentlichen Elemente und die Entitäten gegenüberstellen

Mit dieser Task kann folgendes herausgestellt werden:

- Die Verbindungen zwischen den wesentlichen Funktionen und den Entitäten, die zur Realisierung dieser Funktionen im Zielsystem beitragen,
- Die Verbindungen zwischen den wesentlichen Informationen und den Entitäten, die zur Verarbeitung dieser Informationen im Zielsystem beitragen.

Diese Verbindungen sind bei der Gegenüberstellung von Bedrohungen und Bedürfnissen bedeutsam. Sie werden über eine Matrix dargestellt, in der die wesentlichen Elemente und die ausgewählten Entitäten verzeichnet sind. Die Entsprechung wesentliches Element / Entität wird in der Tabelle durch ein oder mehrere Kreuze materialisiert, und zwar genau an der Stelle, an der sich das wesentliche Element und die betroffenen Entitäten kreuzen.

Beispiel einer Matrix wesentliche Elemente / Entitäten

Entitäten / ***Wesentliche Elemente***	***HARDWARE***				***SOFTWARE***				***NETZWERKE***				***PERSONAL***					***ST.ORTE***			***ORGA.***		
	M1	***M2***	***M3***	***M4***	***L1***	***L2***	***L3***	***L4***	***R1***	***R2***	***R3***	***R4***	***P1***	***P2***	***P3***	***P4***	***P5***	***S1***	***S2***	***S4***	***O1***	***O2***	***O3***
Funktion 1	+					+	+	+					+	+	+	+			+			+	+
…	+					+	+	+					+	+	+	+	+	+	+		+		+
Funktion N	+	+			+	+		+	+			+		+	+	+	+	+	+			+	+
Information 1	+		+		+	+		+		+		+		+	+	+	+	+	+			+	+
…	+			+	+	+		+			+	+		+	+	+	+	+	+			+	+
…	+					+	+	+					+	+	+	+			+	+	+	+	+
Information N	+					+	+	+					+	+	+	+	+	+	+	+			+

Schritt 2 - Sicherheitsbedarfsanalyse

Aktivität 2.1 – Realisierung der Bedürfnisblätter

Die zu berücksichtigenden Sicherheitskriterien auswählen

Die den Informationen und Funktionen zugeordneten Sicherheitsbedarfe äußern sich durch Sicherheitskriterien[2]. Drei Sicherheitskriterien sind unumgänglich:

- Verfügbarkeit (D): Eigenschaft der Zugänglichkeit der wesentlichen Elemente durch autorisierte Nutzer zu einem bestimmten Zeitpunkt.
  - Bei einer Funktion: Garantie der Kontinuität der Bearbeitungsdienste, keine Probleme auf Grund von Ansprechzeiten im weitesten Sinne.
  - Bei einer Information: Garantie der vorgesehenen Verfügbarkeit bezüglich des Datenzugriffs (Fristen und Zeiten), kein vollständiger Informationsverlust; solange von der Information eine archivierte Version existiert, gilt die Information als verfügbar; zur Untersuchung der Verfügbarkeit einer Information wird von der Existenz einer archivierten Version ausgegangen und bei Einschätzung der Verfügbarkeit wird die Archivierfunktion dieser Information berücksichtigt.
- Integrität (I): Eigenschaft der Genauigkeit und Vollständigkeit der wesentlichen Elemente.
  - Bei einer Funktion: Gewährleistung der Konformität des Algorithmus oder des Einsatzes automatischer oder nicht automatischer Bearbeitungen bezogen auf ihre Spezifikationen; keine falschen oder unvollständigen Ergebnisse der Funktion.
  - Bei einer Information: Garantie der Exaktheit und Vollständigkeit der Daten im Hinblick auf Bedienungsfehler oder unzulässige Benutzung; keine Verfälschung der Information.
- Vertraulichkeit (C): Eigenschaft der wesentlichen Elemente, nur den autorisierten Nutzern zugänglich zu sein.
  - Bei einer Funktion: Schutz von Algorithmen, die Verwaltungsvorschriften und Ergebnisse beschreiben und deren Verbreitung an unbefugte Dritte Schaden anrichten könnte; keine Weitergabe von vertraulichen Prozessen oder Mechanismen.
  - Bei einer Information: Schutz von Daten, deren Zugriff oder Benutzung durch unbefugte Dritte Schaden anrichten könnte; keine Weitergabe von vertraulichen Daten.

Die geäußerten Bedürfnisse können auch Kriterien wie Beweis (Zurechenbarkeit), Kontrolle (Überprüfbarkeit) und Anonymität oder sonstige Sicherheitskriterien betreffen, deren Beeinträchtigung bei einer Funktion oder einer Information die Belange des Systems gefährden können.

- Beweis, Kontrolle: Die Garantie, das das Senden bzw. der Erhalt einer Information nicht abgestritten werden kann, dabei können die gelieferten Ergebnisse protokolliert werden (Beispiel: Eine Geldüberweisung und die Überprüfung des Buchführungsjournals über die Eingangsdaten).
- Anonymität: Maßnahme, dank der ein Nutzer, der eine Information erzeugt (z. B. Abgabe einer Wahlstimme) oder eine Aktion durchführt (z. B. ein Telefonanruf), die unmittelbar von einem Rechner bearbeitet wird, nicht identifiziert werden kann.
- Zuverlässigkeit: Kohärenzeigenschaft zwischen einem erwarteten Verhalten und einem Ergebnis.
- …

Die Bedürfnisskala festlegen

Die Sicherheitsbedarfe müssen für jedes ausgewählte Sicherheitsgrundwert geäußert werden. Die Graduierung der Sicherheitsbedarfe muss in Form von Bedürfnisniveaus erfolgen. Dazu muss für jedes Bedürfnisniveau jeden Sicherheitsgrundwert eine Definition formuliert werden.
Die Skala reicht in der Regel von 0 (keine Beeinträchtigung) bis 4 (sehr starke Beeinträchtigung). Es ist jedoch durchaus denkbar, Skalen mit einer anderen Anzahl Niveaus zu definieren.
Dabei sollte für jedes Sicherheitsgrundwert die Anzahl Niveaus gleich sein.
Die Referenzwerte sollten so weit wie möglich explizit sein und eine Anzahl Grenzwerte enthalten.

[2] z. T. nach dem weißen Buch über die IT-Sicherheit in Kreditinstituten

Diese Arbeit geschieht meistens mit Hilfe einer Tabelle mit doppelter Eingabe, wobei die Sicherheitskriterien in die Spalten und die Niveaus in die Zeilen eingetragen werden und am Schnittpunkt die Definitionen einzugeben sind.

Die folgende Tabelle dient als Beispiel für eine 5-stufige Skalierung mit den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit.

Sicherheitsbedarfe	***Verfügbarkeit***	***Integrität***	***Vertraulichkeit***
0	*Kein Verfügbarkeitsbedürfnis*	*Kein Integritätsbedürfnis*	*Öffentlich*
1	*Langfristig (näher zu bestimmen)*	*[nicht benutzter Wert]*	*Eingeschränkt*
2	*Mittelfristig (näher zu bestimmen)*	*Mittleres Integritätsbedürfnis*	*Vertraulich (Partner)*
3	*Kurzfristig (näher zu bestimmen)*	*[nicht benutzter Wert]*	*Vertraulich (intern)*
4	*Sehr kurzfristig (näher zu bestimmen)*	*Vollkommene Integrität*	*Geheim*

Diese Skala muss in Zusammenarbeit mit den Personen, die die Bedürfnisse zu bestimmen haben, dem Kontext der Studie angepasst werden. Dadurch ist für sie jeder Wert aussagekräftig, und die Werte sind untereinander kohärent.

Die relevanten Auswirkungen festlegen

Die Konsequenzen eines eingetretenen Schadensfalls können nach verschiedenen Gesichtspunkten eingeschätzt werden. Die für die Institution signifikanten Auswirkungen müssen vom Verantwortlichen der Nutzer identifiziert werden. Verschiedene Bereiche, die von Auswirkungen betroffen werden können, können dadurch offensichtlich werden und Elemente zur Rechtfertigung der Sicherheitsbedarfe liefern.

Die Auswirkungen können unter den im Folgenden angebotenen möglichen Auswirkungen ausgewählt werden, auch wenn diese Liste keinen Anspruch auf Vollständigkeit erhebt und diese auf jeden Fall dem untersuchten Kontext angepasst werden muss:

- Dienstunterbrechung:
  - Unfähigkeit, den Dienst zu erbringen;
- Imageverlust:
  - Verlust der Glaubwürdigkeit in die interne Informatik,
  - Verlust des guten Rufes;
- Störung des internen Betriebs:
  - Beeinträchtigung der Institution selbst;
  - zusätzliche interne Belastungen;
- Störung des geordneten Tätigkeitsablaufs bei Dritten:
  - Störungen bei Dritten, mit denen die Institution in Verbindung steht
  - sonstige Beeinträchtigungen;
- Verstoß gegen Gesetze, gegen Regelungen:
  - Unmöglichkeit, den gesetzlichen Verpflichtungen nachzukommen;
- Vertragsverletzung:
  - Unmöglichkeit, den vertraglichen Verpflichtungen nachzukommen;
- Gefährdung der Sicherheit des Personals, der Nutzer:
  - Gefahr für das Personal und / oder die Nutzer der Institution;
- Verletzung der Privatsphäre der Nutzer;
- Finanzielle Verluste;
- Aufwendungen für Abhilfe und Wiederherstellung:
  - für Personal;
  - für Material;
  - für Studien, Gutachten;
- Verlust von Gütern, von Kapital, von Werten;
- Verlust von Kunden, von Lieferanten;
- Gerichtliche Verfolgung und (Geld-)Strafen;
- Verlust eines Vorteils gegenüber der Konkurrenz;

- Verlust des technologischen, technischen Vorsprungs;
- Leistungsverlust, Vertrauensverlust;
- Verlust des Ansehens auf technischem Gebiet;
- Schwächung der Verhandlungskapazität;
- Soziale Krise (Streiks);
- Regierungskrise;
- Dienstenthebung;
- Materielle Schäden;
- ...

Diese Auswirkungen gelten als Beispiel; die Auswirkungen, die für die Institution am zutreffendsten sind, müssen von der Arbeitsgruppe vorgeschlagen und genau der Institution angepasst werden. Die Ergebnisse der vorhergehenden Aktivitäten, v. a. die, die die Untersuchung der Institution, die Belange und Konsequenzen und den Systemkontext betreffen, können zur Auswahl der Auswirkungen herangezogen werden. Die Infragestellung der Aufgaben, der Tätigkeit oder der Werte der Institution gelten als signifikante Auswirkungen. Um die Auswirkungen objektiver gestalten zu können, ist es angebracht, für jede Auswirkung explizite Beispiele im Hinblick auf die absehbaren Konsequenzen zu liefern.

Nachdem die Sicherheitskriterien und die Auswirkungen bestimmt sind, können für jedes wesentliche Element Blätter für die Sicherheitsbedarfsanalyse erstellt werden.

Äußerungsblatt der Sicherheitsbedarfe:

Name des wesentlichen Elements	***Auswirkung 1***	***…***	***Auswirkung n***	***Sicherheitsbedarfe***	***Zusätzliche Angaben***
Sicherheitsgrundwert 1	*B11*	*…*	*B1n*	*f(B11…B1n)*	
…	*…*	*…*	*…*	*…*	
Sicherheitsgrundwert n	*Bn1*	*…*	*Bnn*	*f(Bn1…Bnn)*	

Die Synthese des Sicherheitsbedarfes für jedes wesentliche Element und jedes Sicherheitsgrundwert (Spalte "Sicherheitsbedarfe) wird unter Berücksichtigung der zu den Auswirkungen geäußerten Werte bestimmt.

Diese Blätter können für jedes Sicherheitsgrundwert um Schadensfälle erweitert werden, um die Sicherheitsbedarfsanalyse durch Annahme verschiedener Standpunkte zu erleichtern.

Im Folgenden sind verschiedene Schadensfälle aufgelistet, die sich auf die wesentlichen Sicherheitskriterien beziehen (Situation und Kontext werden zur Auflistung spezifischer Schadensfälle für jedes einzelne Kriterium führen):

- bezüglich der Verfügbarkeit:
  - Leistungsminderung,
  - Kurzzeitige Unterbrechung,
  - Langfristige Unterbrechung,
  - Unzugänglichkeit,
  - Vollständiger Ausfall (Vernichtung);
- bezüglich der Integrität:
  - Unbeabsichtigte Änderung,
  - Vorsätzliche Änderung,
  - Unkorrekte Ergebnisse,
  - Unvollständige Ergebnisse;
- bezüglich der Vertraulichkeit:
  - Interne Verbreitung,
  - Externe Verbreitung.

Erweitertes Äußerungsblatt der Sicherheitsbedarfe:

Name des sensiblen Elements	***Schadens-fälle***	***Auswirkung 1***	***…***	***Auswirkung n***	***Sicherheitsbedarfe***	***Zusätzliche Angaben***
Sicherheitsgrundwert 1	*Schadens-fall 1*	*B111*	*…*	*B11n*	*f(B111…B1nn)*	
Sicherheitsgrundwert 1	*…*	*…*	*…*	*…*		
Sicherheitsgrundwert 1	*Schadens-fall n*	*B1n1*	*…*	*B1nn*		
…	*…*	*…*	*…*	*…*	*…*	
Sicherheitsgrundwert n	*Schadens-fall 1*	*Bn11*	*…*	*Bn1n*	*f(Bn11…Bnnn)*	
Sicherheitsgrundwert n	*…*	*...*	*…*	*...*		
Sicherheitsgrundwert n	*Schadens-fall n*	*Bnn1*	*…*	*Bnnn*		

In diesem Fall wird die Zusammenfassung des Sicherheitsbedarfes für jedes wesentliche Element und jedes Sicherheitsgrundwert (Spalte "Sicherheitsbedarfe) unter Berücksichtigung aller zu den Auswirkungen und Schadensfällen geäußerten Werte bestimmt.

Aktivität 2.2 - Zusammenfassung der Sicherheitsbedarfe

Jedem wesentlichen Element ein Sicherheitsbedarf pro Sicherheitsgrundwert zuweisen

Um die Studie mit Erfolg durchführen zu können, muss eine heterogene und für das IT-System repräsentative Arbeitsgruppe (Verantwortliche, Informatiker und Nutzer) gebildet werden. Diese muss über die geäußerten Sicherheitsbedarfe und Rechtfertigungen debattieren können.

Zusammenstellung der Sicherheitsbedarfe

Die Zusammenstellung der Sicherheitsbedarfe erfolgt unter Zuhilfenahme der Äußerungsblätter der Sicherheitsbedarfe und der Bedürfnisskala, die den betroffenen Nutzern zuvor ausgehändigt wurden. Die angegebenen Werte spiegeln den Standpunkt der Nutzer gegenüber ihrem persönlichen Sicherheitsbedarf wider. Dabei kann der jeweilige Standpunkt durch einen zusätzlichen Kommentar gerechtfertigt werden (insbesondere bei extremen Werten). Jedes Blatt muss synthetisch zusammengefasst werden, um für jedes wesentliche Element einen Sicherheitsbedarfvektor ermitteln zu können.

Diese Evaluierung ist von den Nutzern selbst vorzunehmen, indem akzeptable Werte geäußert werden, deren Überschreiten als nicht akzeptabel anzusehen ist. An jedem Zeilen-Spalten-Schnittpunkt der Bedürfnis-Äußerungsblätter ist eine Note einzutragen, wodurch ein Verfügbarkeits-Integritäts-Vertraulichkeitsvektor ermittelt werden kann. Hingegen sind die Nutzer des Systems nicht unbedingt Experten auf dem Gebiet der Sicherheit des IT-Systems, noch sind sie für die IT-Sicherheit sensibilisiert. Die Arbeitsgruppe bzw. die Personen, die die Interviews unter den Nutzern durchführen, sind dafür verantwortlich sich zu vergewissern, ob die Bedürfnisskala richtig verstanden wurde und sie müssen die Homogenität der erzielten Ergebnisse sicherstellen.

Die Sicherheitsbedarfe sind unabhängig von den eventuellen Risiken und den eingesetzten Mitteln zur Sicherung. Sie stellen somit einen intrinsischen Wert der Sensibilität der Informationen, Funktionen oder Teilfunktionen dar. Sollte beispielsweise auf dem Gebiet der Verteidigung Dokumenten ein Wert der Vertraulichkeit zugewiesen werden, hieße es, diese Dokumente (als geheim, vertraulich o. ä.) einzustufen.

Unterliegt ein wesentliches Element Bedürfnissen, die im Laufe der Zeit variieren, ist es ratsam, diese verschiedenen Zustände getrennt zu untersuchen, so als handele es sich um entsprechend viele verschiedene wesentliche Elemente.

Wenn man im Hinblick auf die Auswirkungen klar formulierte Risiken ermitteln will, sollten alle Äußerungsblätter der Sicherheitsbedarfe ausgefüllt werden.

Zusammenfassung der Sicherheitsbedarfe

Die Arbeitsgruppe trägt die durch die Nutzer ermittelten Ergebnisse auf dem Syntheseblatt der geäußerten Sicherheitsbedarfe ein und ermittelt den als Synthese erachteten Wert. Diese Synthese, bei der die verschiedenen Standpunkte harmonisiert werden, wird anschließend validiert. Die Person, durch die die Genehmigung erteilt wird, muss über eine globale Vision der wesentlichen Elemente verfügen (z. B. kann es sich um den Verantwortlichen der Nutzer oder allgemein um den Eigentümer der wesentlichen Elemente handeln). Ein Konsens kann durch die Äußerung der einzelnen Argumentierungen und durch Schiedssprechung erreicht werden. Als letztes Mittel kann davon ausgegangen werden, dass die Synthese des Sicherheitsbedarfes nach Sicherheitskriterien eines wesentlichen Elementes dem Höchstwert der von den Nutzern auf jedem der Blätter zugewiesenen Werte entspricht.

Sollten zu große Abweichungen festgestellt werden, kann es notwendig werden, die Nutzer zu bitten, ihre Werte noch einmal zu überdenken oder sie näher zu begründen. Auf jeden Fall muss die Synthese in Bezug auf die wesentlichen Elemente der Institution, die bei der Kontextstudie herausgestellt wurden, gerechtfertigt sein.

Beispiel eines Syntheseblatts geäußerter Sicherheitsbedarfe:

Liste der wesentlichen Elemente.	***Zusammenfassung der Sicherheitsbedarfe***		
	Vertraulichkeit	***Integrität***	***Verfügbarkeit***
Funktion 1	*0*	*3*	*3*
Funktion 2	*1*	*3*	*2*
…	*…*	*…*	*…*
Funktion n	*0*	*4*	*2*
Information 1	*2*	*1*	*1*
…	*…*	*…*	*…*
Information n	*4*	*3*	*0*

Schritt 3 – Bedrohungsanalyse

Aktivität 3.1 – Untersuchung der Ursprünge der Bedrohungen

Relevante Angriffsmethoden auflisten

Die Auswahl der Angriffsmethoden besteht unter Zuhilfenahme der Liste mit den allgemeinen Angriffsmethoden und bedrohenden Elementen des Leitfadens "Mittel zur IT-Risikobewertung" darin, jene Methoden und Elemente zu berücksichtigen, die einem im Hinblick auf den Kontext, die zu bewältigenden Aufgaben und die das Zielsystem bildenden Entitäten als relevant erscheinen. Die Auswahl wird zusammen mit der Arbeitsgruppe auf Grundlage einer Liste themenspezifischer Angriffsmethoden getroffen. Folgende Themen werden angeboten:

- physische Schadensfälle
- Naturereignisse
- Verlust wesentlicher Dienste
- Störungen durch Strahlung
- Verletzung bzw. Infragestellung von Informationen
- Technische Störungen
- Unzulässige Aktionen
- Verletzung bzw. Infragestellung von Funktionen.

Diese Auflistung erleichtert die Auswahl der relevanten Angriffsmethoden. Bestimmte Themen (physische Schadensfälle, Naturereignisse, Verlust wesentlicher Dienste) können ausgeschlossen werden, ein solcher Ausschluss muss jedoch begründet werden. Es ist z. B denkbar, dass bestimmte Themen bereits früher untersucht wurden.

Eine Angriffsmethode ist zu berücksichtigen, wenn ihre Durchführung realistisch erscheint und davon auszugehen ist, dass sie eine Auswirkung haben wird.

Die Nicht-Berücksichtigung einer Angriffsmethode oder eines Themas sollte begründet werden, damit die getroffene Auswahl auch später noch nachvollzogen werden kann. Damit die Verfolgbarkeit der getroffenen Auswahl so eindeutig wie möglich ist, besteht die Möglichkeit, alle nicht berücksichtigten Angriffsmethoden in Hypothesen umzuwandeln (wobei alle nicht berücksichtigten Angriffsmethoden in eine einzige Hypothese zusammengefasst werden können).

Die in den Wissensdatenbanken vorgeschlagenen Angriffsmethoden sind so genannte Allgemeine Methoden, da sie Kategorien definieren, in die mit weitaus größerem Feinheitsgrad beschriebene Angriffsmethoden fallen können. Die vorgeschlagene Liste kann insofern als vollständig angesehen werden, als immer die Möglichkeit besteht, eine bestimmte Angriffsmethode in eine angebotenen Kategorie zu integrieren. Nichtsdestotrotz kann diese Liste dem Kontext der Institution und dem Benutzungskontext des Zielsystems angepasst werden.

Die Angriffsmethoden können auch von Sicherheitsstudien stammen, die an benachbarten Systemen durchgeführt werden oder Unterlagen mit allgemeingültigem Charakter entnommen werden (Sicherheits-Policy, Sicherheitscharta).

Die Angriffsmethoden durch Sicherheitskriterien charakterisieren, die sie beeinträchtigen können

Jede Angriffsmethode kann mindestens ein Sicherheitsgrundwert treffen (Verfügbarkeit, Integrität, Vertraulichkeit usw.).
Es ist daher angebracht, alle berücksichtigten Angriffsmethoden durch die Sicherheitskriterien zu charakterisieren, die sie treffen können. Eine solche Charakterisierung besteht darin, nicht alle denkbaren Eventualitäten, sondern nur die unmittelbaren Auswirkungen auf die Sicherheitskriterien zu bestimmen.
Beispiel: Ein Brand wird in erster Linie das Kriterium der Verfügbarkeit beeinträchtigen, obwohl infolgedessen auch die Integrität und Vertraulichkeit betroffen sein können; demzufolge wird ein Brand generell durch eine Beeinträchtigung der Verfügbarkeit charakterisiert.
Die Charakterisierung jeder Angriffsmethode durch die Sicherheitskriterien (die gleichen wie bei der Sicherheitsbedarfsanalyse) ermöglicht es in einem der nächsten Schritte, zur Bestimmung der tatsächlichen Risiken die Sicherheitsbedarfe bequem den Bedrohungen gegenüberzustellen.

Die zugeordneten bedrohenden Elemente durch ihre Art und ihre Ursachen charakterisieren

Die Angriffsmethoden werden von bedrohenden Elementen eingesetzt, die am besten für jede Angriffsmethode einzeln charakterisiert werden. Zu beschreiben sind:

- die Art des bedrohenden Elementes (natürlich bedingt, menschlich bedingt oder umgebungsbedingt, d. h. zielsystemextern).
- die Ursachen eines jeden bedrohenden Elementes (unbeabsichtigt, vorsätzlich); diese können weiter verfeinert werden nach Exposition und verfügbaren Ressourcen bei unbeabsichtigen Ursachen und nach Fachkenntnissen, verfügbaren Ressourcen und Motivation bei vorsätzlichen Ursachen.

Es ist ratsam, zur Charakterisierung der bedrohenden Elemente den Abschnitt über die Allgemeinen Angriffsmethoden und bedrohenden Elemente des Leitfadens "Mittel zur IT-Risikobewertung" anzuwenden.

Auch die Typologie der Bedrohungen nach [IGI 900] und [Rec 901] kann angewendet werden. Danach kann der Ursprung weiter nach Spielerei, Habgier, strategischem oder terroristischem Zweck aufgeschlüsselt werden.

Einen dem Angriffspotential des bedrohenden Elementes entsprechenden Wert zuweisen

Die Charakterisierung der bedrohenden Elemente kann für jede berücksichtigte Angriffsmethode in einem einzigen Wert zusammengefasst werden. Es handelt sich dabei um das Angriffspotential, das im Allgemeinen einem der folgenden Werte entspricht:

- 1 (unbeabsichtigt und zufällig),
- 2 (begrenzte Wahrscheinlichkeiten oder begrenzt verfügbare Ressourcen),
- 3 (hoher Grad an Fachkenntnis, an Wahrscheinlichkeiten oder an verfügbaren Ressourcen)

Durch dieses Angriffspotential lässt sich ein adäquates Widerstandsniveau für die Sicherheitsziele bestimmen.

In der folgenden Tabelle werden die Auswahl und Charakterisierung von Angriffsmethoden beispielhaft dargestellt:

		Bedrohende Elemente						***Betroffene Sicherheits-kriterien***		
		Typ			***Ursache***					
	Angriffsmethoden	***Natürlich bedingt***	***Menschlich bedingt***	***Umgebungs-bedingt***	***Unbeabsichtigt***	***Vorsätzlich***	***Angriffspotenzial***	***Verfügbarkeit***	***Integrität***	***Vertraulichkeit***
1	*Brand*	+	+	+	+	+	*2*	+	+	
13	*Verlust von Telekommunikationsmitteln*			+	+	+	*1*	+		
19	*Passives Mithören*		+	+		+	*2*			+
20	*Diebstahl von Datenträgern oder Unterlagen*			+		+	*2*			+
21	*Diebstahl von Betriebsmitteln*			+		+	*1*	+		+
23	*Verbreitung*		+	+	+	+	*1*			+
26	*Einrichten von Sofware-Schwachstellen*			+		+	*1*	+	+	+
42	*Beeinträchtigung der Personalverfügbarkeit*	+	+	+	+	+	*1*	+		

Die nicht berücksichtigten Angriffsmethoden einschließlich Begründung hervorheben

Ein Nicht-Beachten einer Angriffsmethode sollte ausreichend begründet werden. Egal ob eine Angriffsmethode als unwahrscheinlich oder ohne Auswirkungen bewertet wird, ob sie an anderer Stelle berücksichtigt oder vorsätzlich zurückgewiesen wird, ist es wichtig zu begründen, warum sie ausgegliedert wurde, denn sie wird im weiteren Verlauf der Studie nicht mehr untersucht, obwohl sie für die Institution der Ursprung eines Risikos sein kann.

Aktivität 3.2 – Studie der Schwachstellen

Die Schwachstellen der Entitäten nach Angriffsmethoden identifizieren

Für jede berücksichtigte Angriffsmethode sollten die Schwachstellen des Zielsystems festgestellt werden, durch die eine Realisierung erst möglich wird (es ist ratsam, zur Identifizierung der Schwachstellen nach Entitäten- bzw. Unterentitätstypen und Angriffsmethoden die Allgemeinen Schwachstellen des Leitfadens "Mittel zur IT-Risikobewertung" zu Rate zu ziehen).

Eine Schwachstelle ist ein Systemmerkmal, das durch ein bedrohendes Element ausgenutzt werden könnte und somit die Realisierung einer Angriffsmethode ermöglichen könnte. Dieses den Systemeen anhaftende Merkmal kann eine Schwäche oder eine Verwundbarkeit in den Augen der Sicherheit sein.
Beispiele:

- *Für eine Entität des Typs "Hardware" stellt die Fähigkeit, Strahlungen zu erzeugen oder der Reiz bestimmter Betriebsmittel (z. B Laptops) ein Merkmal dar;*
- *für eine Entität des Typs "Standort" stellt die Leichtigkeit, mit der man in den Standort gelangen kann, ebenfalls ein Merkmal dar.*

Diese Merkmale werden zu Schwachstellen, wenn sie durch Angriffsmethoden ausgenutzt werden können:

- *Die Benutzung von Laptops stellt eine Schwachstelle für die Angriffsmethode Diebstahl von Betriebsmitteln dar;*
- *Die Fähigkeit, Strahlungen auszusenden stellt eine Schwachstelle für die Angriffsmethode Abfangen kompromittierender Störsignale dar.*

Dabei kann eine Angriffsmethode zu ihrer Realisierung mehrere Schwachstellen ausnutzen.
Beispiel: Die Angriffsmethode Sabotieren der Hardware kann verwirklicht werden, wenn:

- *man sich leicht Zugang zum Standort verschaffen kann (Schwachstelle des Entitätentyps Standort);*
- *die Hardware ein Hinzufügen zusätzlicher Komponenten ermöglicht (Schwachstelle der Entitätstypen Hardware und Software);*
- *kein Plan zur Überwachung der Betriebsmittel vorliegt (Entitätentyp Organisation).*

Die Wissensdatenbanken bieten eine Liste mit allgemeingültigen Schwachstellen an, die den einzelnen Angriffsmethoden und Unterentitätstypen zugeordnet sind. Die Auswahl wird mit Hilfe dieser Liste getroffen, kann aber systemspezifischen Besonderheiten angepasst werden. Wichtig ist festzuhalten, dass die angebotene Liste eine personalisierbare Kenntnisdatenbank darstellt, die dem untersuchten Kontext anzupassen ist. Diese Liste ist naturgemäß ständig entwicklungsfähig.

Eventuell das Niveau der Schwachstellen einschätzen

Die Schwachstellen können durch ihr Niveau charakterisiert werden, das die Möglichkeit zur Realisierung der sie ausnutzenden Angriffsmethoden darstellt.

Dieses Niveau ist von mehreren Kriterien abhängig:

- vom systemeigenen Kontext;
- vom Kenntnisstand im betrachteten Bereich.

In vielen Fällen gibt es keine statistischen Daten, die es erlauben, Verhaltensmuster des IT-Systems zu erstellen. Nur die naturbedingten und technologischen Risiken verfügen über Zahlen, die eine Evaluierung mit Hilfe quantitativer Techniken möglich machen, aber es muss darauf hingewiesen werden, dass solche Analysen von Natur her subjektiv sind.

Ziel der Einschätzung des Schwachstellenniveaus ist es, nur die relevanten Schwachstellen zu berücksichtigen und diese zu hierarchisieren. Man könnte sich mit der Auswahl begnügen, aber durch Einschätzung dieses Wertes kann ein weiterer Grad an Feinheit gewonnen werden.

Dazu kann folgende Skala zu Hilfe genommen werden:

0	*Völlig unwahrscheinlich oder nicht durchführbar*
1	*Kaum wahrscheinlich oder nur mit sehr aufwendigen Mitteln und/oder sehr guten Fachkenntnissen durchführbar*
2	*Mäßig wahrscheinlich oder nur mit gewissen Kenntnissen und/oder spezieller Ausrüstung durchführbar*
3	*Sehr wahrscheinlich oder mit Standardausrüstung und/oder Wissensdatenbanken durchführbar*
4	*Sicher oder von jedermann durchführbar*

Bei natürlich oder menschlich bedingten Angriffsmethoden beruht die Einschätzung des Schwachstellenniveaus auf der tatsächlich beobachteten Durchführbarkeit. Bei böswilliger Absicht beruht die Einschätzung des Schwachstellenniveaus vielmehr auf der Durchführbarkeit im Hinblick auf die notwendigen Mittel, Sachverstanden und Fachkenntnisse.

Die Liste mit den eingeschätzten Schwachstellen bezogen auf die berücksichtigten Angriffsmethoden wird nach Entitäten- bzw. Unterentitätstypen angefertigt.

In der folgenden Tabelle wird ein beispielhaftes Ergebnis vorgestellt.

	Angriffsmethoden	*Schwachstellen*	*Hardware und Software*	*Interne Netze*	*Externe Netze*	*Standort*	*Personal*	*Organisation*
1	*Brand*	*Mangelnde Kohärenz zwischen Brandschutzmaßnahmen und IT-System*				*2*		
		Fehlende Anweisungen (Alarmierung, Vorbeugung, Ausbildung usw.)						*2*
		Fehlende Brandschutzorganisation						*3*
13	*Verlust von Telekommunikationsmitteln*	*Unsachgemäßer Betrieb des internen Telefonnetzes*				*1*		
		Störung externer Netze (Fernmeldenetz)			*1*			
		Störung externer Netze (Netzwerkdienste)			*1*			
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Aktivität 3.3 – Formalisierung der Bedrohungen

Die Bedrohungen formell äußern

Die Formulierung der Bedrohungen kann mehr oder weniger reichhaltig sein. Es geht vor allem darum, explizit ein Angriffsszenario zu äußern, dabei kann das Niveau der Detaillierung je nach Finalität der Studie variieren.

Im günstigsten Fall umfasst die Formulierung einer Bedrohungen folgendes:
- Das bedrohende Element mit seinen Merkmalen, insbesondere seinem Angriffspotenzial,
- die vom bedrohenden Element benutzte Angriffsmethode und die betroffenen Sicherheitskriterien,
- die ausgenutzten Schwachstellen und ihr Niveau,
- die Entitäten, welche diese Schwachstellen aufweisen.

Die Bedrohungen sind durch einen Wahrscheinlichkeitswert charakterisierbar, der nach dem Niveau der ausgenutzten Schwachstellen bestimmt wird.
Obwohl die Wahrscheinlichkeitswerte subjektiv erscheinen, beruht ihre Bedeutung auf der Tatsache, dass diese Werte untereinander in Relation stehen.
Wenn eine Bedrohung die Ausnutzung einer einzigen Schwachstelle beinhaltet, entspricht die Wahrscheinlichkeit der Bedrohung eben diesem Schwachstellenniveau.
Wenn eine Bedrohung die Ausnutzung mehrerer Schwachstellen beinhaltet, sollte die Wahrscheinlichkeit der Bedrohung unter Berücksichtigung der jeweiligen Schwachstellenniveaus ermittelt werden:
- generell indem die Bedrohungswahrscheinlichkeit erneut untersucht wird,
- indem das niedrigste Schwachstellenniveau berücksichtigt wird, wenn die Bedrohung nur unter Ausnutzung aller Schwachstellen realisiert werden kann,
- indem das höchste Schwachstellenniveau berücksichtigt wird, wenn die Bedrohung bereits unter Ausnutzung einer einzigen Schwachstellen realisiert werden kann.

Beispiel:

Bedrohungen		*Angriffsmethode*	*Angriffspotenzial*	*D*	*I*	*C*	*Wahrscheinlichkeit*
M.INCENDIE	*Verschlimmerung der Konsequenzen eines Brandes auf Grund mangelnder Kohärenz zwischen Brandschutzmaßnahmen und IT-System (Standort des Studienbüros), fehlender Anweisungen oder fehlender Brandschutzmaßnahmen (Organisation des Studienbüros)*	*1*	*2*	*+*			*2*
M.TELECOM	*Verlust der Telekommunikationsmittel auf Grund einer Störung externer Netze (Internet)*	*12*	*1*	*+*			*1*
M.VOL-DOC	*Diebstahl von Informationsträgern oder Unterlagen durch einen Besucher oder Reinigungspersonal auf Grund der Leichtigkeit, mit der man sich während der Öffnungszeiten Zugang zu den Räumlichkeiten verschaffen kann (Standort des Studienbüros)*	*19*	*2*			*+*	*3*
…	…	…	…	…	…	…	…

Die Bedrohungen eventuell nach den möglichen Wahrscheinlichkeiten hierarchisieren

Die Liste der resultierenden Bedrohungen kann in absteigender Reihenfolge der Bedrohungswahrscheinlichkeiten sortiert werden. Diese Liste ist ein Kommunikations-Tool, welches große Aufmerksamkeit verdient. Sie bringt die Bedrohungen, denen die Organisation ausgesetzt ist, so explizit wie möglich zum Ausdruck. Bedrohungen mit einem großen Wahrscheinlichkeitspotenzial sollten deshalb ganz oben in der Liste erscheinen, um die Akteure wirksam zu sensibilisieren.

Schritt 4 - Identifizierung der Sicherheitsziele

Aktivität 4.1 – Gegenüberstellung von Bedrohungen und Bedürfnissen

Die Risiken durch Gegenüberstellung von Bedrohungen und Sicherheitsbedarfen festlegen

Die Bestimmung der Risiken, denen die Institution ausgesetzt ist, besteht darin, deutlich zu machen, auf welche Art und Weise die wesentlichen Elemente getroffen werden können, d. h. zu bestimmen, wie das, was der Institution von Bedeutung ist, durch das beeinträchtigt werden kann, was auf sie zukommen kann.

Dieser Zusammenhang wird durch die Gegenüberstellung von Bedrohungen und Bedürfnissen realisiert. Einerseits wurden die Sicherheitsbedarfe der wesentlichen Elemente nach verschiedenen Sicherheitskriterien geäußert (Verfügbarkeit, Integrität, Vertraulichkeit usw.). Andererseits wurden die Bedrohungen durch die Sicherheitskriterien charakterisiert, die sie beeinträchtigen können (nach Charakterisierung der Angriffsmethoden und gemäß den gleichen Sicherheitskriterien). Daher kann jedes wesentliche Element jeder Bedrohung gemäß den Sicherheitskriterien gegenübergestellt werden, um die möglichen Konsequenzen einer Realisierung von Bedrohungen bestimmen zu können.

Für jedes wesentliche Element wird eine Tabelle mit den Angriffsmethoden erstellt. Zu diesem Zeitpunkt der Studie werden nur die Angriffsmethoden berücksichtigt, von denen anzunehmen ist, dass sie die Schwachstellen eines wesentlichen Elementes auszunutzen gewillt sind (die Überprüfung erfolgt an Hand von Entitäten-/Elemente-Tabellen, die bei der Kontextstudie angefertigt wurden). Die Sicherheitsbedarfe des untersuchten wesentlichen Elementes und die Sicherheitskriterien, die von jeder berücksichtigten Angriffsmethode beeinträchtigt werden können, werden daraufhin übertragen.

Die Blätter können nach Angriffsmethoden oder verfeinert nach Bedrohungen abgefasst werden, die Informationen, auf die es ankommt, sind jedoch die Sicherheitskriterien, die durch die Angriffsmethoden beeinträchtigt werden können. Und die werden, wie gesagt, für jede entsprechende Bedrohung eingetragen. Anstelle der Angriffsmethoden können auch die Bedrohungen berücksichtigt werden, da jedoch die Angriffsmethoden den Bedürfnissen gegenübergestellt werden, wird diese Operation im Allgemeinen mit den Angriffsmethoden faktorisiert.

Für jedes Sicherheitsgrundwert werden folgende Regeln angewendet:

- Wenn ein Sicherheitsgrundwert nicht zugeordnet werden kann, sind die betroffenen Sicherheitsbedarfe gleich Null;
- kann ein Sicherheitsgrundwert zugeordnet werden, sind die betroffenen Sicherheitsbedarfe die gleichen wie die Sicherheitsbedarfe des entsprechenden Elementes.

Beispiel:

I.VISU (Visualisierung)		*Sicherheitsbedarfe*			*D*	*I*	*C*
					2	*2*	*0*
Angriffsmethoden		*Verletzung*			***Betroffene Sicherheitsbedarfe***		
		D	*I*	*C*	***D***	***I***	***C***
1	*Brand*	+	+		*2*	*2*	
13	*Verlust von Telekommunikationsmitteln*	+			*2*		
19	*Passives Mithören*			+			
20	*Diebstahl von Datenträgern oder Unterlagen*			+			
21	*Diebstahl von Betriebsmitteln*	+		+	*2*		
23	*Externe Verbreitung*			+			
26	*Einrichten von Sofware-Schwachstellen*	+	+	+	*2*	*2*	
42	*Beeinträchtigung der Personalverfügbarkeit*	+			*2*		
…	…	…	…	…	…	…	…

Die ermittelten Werte stellen das Risiko für die Institution dar, da der Bedürfniswert berücksichtigt wurde.

In der Tat geht es darum, die Risiken der Verletzung der Sicherheitsbedarfe der wesentlichen Elemente zu bestimmen. Nimmt eine Bedrohung Gestalt an, ist sie in der Lage, diese Bedürfnisse und die identifizierten wichtigsten Auswirkungen zu beeinträchtigen.

Alle Tabellen können daraufhin zusammengefasst werden, um eine globale Vision der Risiken zu erhalten. Diese Zusammenfassung kann mit Hilfe der Angriffsmethoden oder der Bedrohungen geschehen. Mit dieser Zusammenfassung wird die Überlegung auf die tatsächliche Auswirkung von Bedrohungen auf die wesentlichen Elemente und somit auf die Institution gelenkt.

Beispielhafte Zusammenfassung von Risiken gemäß den Angriffsmethoden:

Zusammenfassung von Risiken				*Element 1*			…			*Element N*		
				D	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
				3	*2*	*0*	*…*	*…*	*…*	*0*	*1*	*0*
				Betroffene Sicherheitsbedarfe								
Angriffsmethoden	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
Passives Mithören			*X*	*0*	*0*	*0*	*…*	*…*	*…*	*0*	*0*	*0*
Diebstahl von Betriebsmitteln	*X*		*X*	*3*	*0*	*0*	*…*	*…*	*…*	*0*	*0*	*0*
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Die Höchstwerte der betroffenen Sicherheitsbedarfe können nach Bedrohung oder nach Angriffsmethode bestimmt werden. Hierbei handelt es sich um ein Element zur Hierarchisierung der Risiken.

Die Risiken formell äußern

Die Risikobezeichnung sollte unter Verwendung der Risikosynthesetabelle, der Bedrohungsformulierung und eventuell der Bedürfnisskala so explizit wie möglich verfasst werden. Die Feinheit der Formulierung hängt von der gewünschten Präzision ab.

Im günstigsten Fall umfasst die Formulierung eines Risikos folgendes:

- Das bedrohende Element mit seinen Merkmalen, insbesondere seinem Angriffspotenzial,
- die vom bedrohenden Element verwendete Angriffsmethode,
- die ausgenutzten Schwachstellen,
- die Entitäten, welche diese Schwachstellen aufweisen,
- die Bedrohungswahrscheinlichkeit,
- die wichtigsten betroffenen Sicherheitsbedarfe,
- die Auswirkungen auf die Organisation (gemäß der Bedürfnisskala).

Beispiel:

Risiken		*Max. der betroffenen Sicherheitsbedarfse*	*Bedrohungs-Wahrscheinlichkeit*	*Angriffspotenzial*
R.PIEGEAGE	*Ein Eindringling manipuliert die Software durch Änderung von Systembefehlen, Implementierung von Piratenprogrammen, Änderung eines Anwendungsprogramms (Hardware, Software und Internet) oder Einwirken auf die Software der Systemressourcen (Internet), wodurch die Vertraulichkeit sensibler Informationen (Kostenvoranschläge, Akten über Rechststreitigkeiten u. ä.) und die Integrität wesentlicher Elemente (Strukturberechnungen, Kostenvoranschläge, technische Pläne, technische Parameter, Akten über Rechtsstreitigkeiten usw.) beeinträchtigt werden.*	*4*	*3*	*1*
R.VOL-VISITEUR	*Aufgrund der leichten Zugänglichkeit der Räumlichkeiten (Standort des Studienbüros) entwendet ein Besucher oder jemand vom Reinigungspersonal ein als besonders attraktiv geltendes Betriebsmittel (Marktwert, technologischer Wert der meisten Hardware-, Software- und Netzwerkkomponenten), wodurch die Verfügbarkeit mehrerer wesentlicher Elemente und die Vertraulichkeit sensibler Informationen (Kostenvoranschläge, Akten mit Rechtsstreitigkeiten u. ä.) beeinträchtigt wird.*	*2*	*1*	*1*
…	…	…	…	…

Die Risiken nach Auswirkung auf die wesentlichen Elemente und Wahrscheinlichkeit der Bedrohungen hierarchisieren

Die erstellte Risikoliste kann beginnend mit den Höchstwerten in absteigender Reihenfolge der betreffenden Sicherheitsbedarfe und in absteigender Reihenfolge der betreffenden Bedrohungswahrscheinlichkeiten sortiert werden. Diese Liste ist ein Kommunikations-Tool, welches große Aufmerksamkeit verdient. Sie bringt die tatsächlichen Risiken für die Organisation so explizit wie möglich zum Ausdruck. Die Risiken, welche die größten Sicherheitsbedarfe notwendig machen und die eine große Bedrohungswahrscheinlichkeit besitzen, sollten deshalb ganz oben in der Liste erscheinen, um die Akteure wirksam zu sensibilisieren. Auf diese Weise können sie prioritär behandelt werden.

Ein weiteres Mittel zur Hierarchisierung der Risiken bei gleichzeitiger Einbindung der Akteure ist es, die Teilnehmer die Risiken hierarchisieren zu lassen. In der Tat sind sie es, die zu entscheiden haben, ob ein Risiko zu berücksichtigen und dann auch zu behandeln ist oder nicht. Daher ist es wichtig, dass sie bei diesem Stand der Studie einbezogen werden.

Es ist auch denkbar, eine Hierarchisierung der Risiken gemäß der ersten Methode vorzuschlagen und sie gemäß der zweiten Methode zu überarbeiten.

Die nicht berücksichtigten Risiken einschließlich Begründung hervorheben

Die Arbeitsgruppe kann vorschlagen, Risiken, die die Sicherheitsbedarfe nur geringfügig berühren und deren Bedrohungswahrscheinlichkeit gering ist, fallen zu lassen. Solche Risiken sollten deutlich gemacht und der Grund ihrer Nichtberücksichtigung ausreichend begründet werden, da sie für die Institution Restrisiken darstellen.

Aktivität 4.2 - Formalisierung der Sicherheitsziele

Die Sicherheitsziele auflisten

Die Sicherheitsziele müssen sämtliche Risiken abdecken, deren Abdeckung bestimmt wurde, wobei die Hypothesen, die Sicherheitsvorschriften sowie die verschiedenen Kontextelemente (insbesondere die Zwänge und Belange / absehbaren Konsequenzen) zu berücksichtigen sind. Sie müssen mit dem operationellen Ziel bzw. dem erklärten "Produkt"-Ziel des Zielsystems und allen bekannten Daten über die physische Umgebung kohärent sein.

Die Sicherheitsziele entsprechen im Allgemeinen der Äußerung der Absicht durch den Auftraggeber, die Risiken abzudecken, ohne Lösungen zum Erreichen dieser Ziele anzubieten.
In diesem Sinne stellen sie ein umfassendes, offenes (ohne Vorgabe von Lösungen) Lastenheft dar, das bestens der Institutionsproblematik angepasst ist.

Das Sicherheitsziel kann folgende Risikobestandteile behandeln:

- Den Ursprung der Bedrohungen (bedrohende Elemente und Angriffsmethoden),
- die ausgenutzten Schwachstellen (zur Auflistung der die Schwachstellen abdeckenden Sicherheitsziele können die Allgemeinen Sicherheitsziele und die Tabelle zur Festlegung der Sicherheitsziele und –anforderungen des Leitfadens "Mittel zur Behandlung von IT-Risiken" herangezogen werden),
- die Konsequenzen (betroffene wesentliche Elemente und Auswirkungen auf die Institution).

Es wird empfohlen, die folgende Nomenklatur für die Sicherheitsziele zu verwenden: O.xx (O steht für technisches Ziel und xx für den Namen des Sicherheitsziels).

Beispiele:

O.INC-ORIG	*Maßnahmen sind zu ergreifen, um die Entstehung eines Brandes zu vermeiden*
O.INC-CSQ	*Maßnahmen sind zu ergreifen, um die Auswirkungen eines Brandes auf die wesentlichen Elemente und die finanziellen Verluste einzuschränken*
O.INC-COHERENCE	*Der Standort des Studienbüros muss über Brandschutzmaßnahmen verfügen, die mit dem IT-System kohärent sind*
O.INC-ORGA	*Die Organisation des Studienbüros muss Anweisungen und Brandschutzmaßnahmen vorsehen*
O.TELECOM-ORIGINE	*Maßnahmen sind zu ergreifen, um eine Störungen der externen Netze zu vermeiden*
O.TELECOM-CSQ	*Maßnahmen sind zu ergreifen, um die Auswirkungen von Störungen externer Netze auf die wesentlichen Elemente und damit Störungen des internen Betriebs einzuschränken*
O.TELECOM	*Störungen externer Netze dürfen die Benutzung des Internets durch die Nutzer des Studienbüros nicht behindern.*

Die Vollständigkeit der Abdeckung nachweisen

Die zuvor bestimmten Sicherheitsziele haben zum Ziel, die auf dem Zielsystem lastenden Risiken auszuschalten bzw. zu minimieren und dabei die Hypothesen und Sicherheitsvorschriften zu berücksichtigen.
Die mit der Durchführung der Studie beauftragten Personen müssen sich nun vergewissern, dass diese Ziele zur Abdeckung aller identifizierten Risiken, Hypothesen und Sicherheitsvorschriften notwendig und ausreichend sind.

Ein erster Nachweis besteht darin aufzuzeigen, dass die Sicherheitsziele:
- alle Risiken ausreichend abdecken,
- die Sicherheitsvorschriften (und die Vorschriftsreferenzen) abdecken,
- für die Hypothesen (und eventuell für die Belange / absehbaren Konsequenzen des Zielsystems) relevant sein.

Für jedes Sicherheitsziel sollte die Kompatibilität mit den auf der Institution und dem Zielsystem lastenden Zwängen überprüft werden.

Dabei kann die Abdeckung durch einen Wert der folgenden Skala synthetisiert werden:

0	Keine Abdeckung
1	Teilweise Abdeckung
2	Vollständige Abdeckung

Beispiel:

Risiken	*Sicherheitsziele*	*Nachweis der Abdeckung*	*Abdeckung*	*Angriffspotenzial*
R.PIEGEAGE	*O.SYS-COMMANDES* *O.SYS-ACTIONS*	*Die beiden Sicherheitsziele decken alle vom Risiko ausgenutzten Schwachstellen ab:* *- Möglichkeit zur Änderung von Systembefehlen via Internet,* *- Möglichkeit zur Installation von Piratenprogrammen via Internet,* *- Möglichkeit zur Änderung einer Softwareanwendung via Internet,* *- Möglichkeit zur Einwirkung auf die Software der Systemressourcen via Internet.*	*2*	*1*
R.VOL-VISITEUR	*O.LOCAUX* *O.VOL-PROTECTION* *O.PRISE-EN-CHARGE* *O.AUTH-DOC*	*Die beiden ersten Sicherheitsziele decken alle vom Risiko ausgenutzten Schwachstellen ab:* *- Ungehinderter Zugang zum Studienbüro,* *- als besonders attraktiv geltende Betriebsmittel (Marktwert und technologischer Wert).* *Das dritte Sicherheitsziel verbessert die Risikominderung durch Förderung der Eigenverantwortung der Nutzer.* *Das letzte Sicherheitsziel bietet eine Authentifizierungsgarantie des Autors der Dokumente.*	*2*	*1*
…	…	…	…	…

Eine zweite Rechtfertigung besteht darin nachzuweisen, dass jedes Sicherheitsziel mindestens einem Risiko, einer Sicherheitsvorschrift (oder Vorschriftsreferenz) oder einer Hypothese (oder einer absehbaren Konsequenz des Zielsystems bzw. des Sicherheitsbetriebsmodus) entspricht.

Beispiel:

Sicherheitsziele	*R.SABOTAGE*	*R.DIEBSTAHL-BESUCHER*	*R.DIEBSTAHL-STRENG.*	*R.DIEBSTAHL-BENUTZ.*	*R.VIRUS-ÜBERPRÜF.*	*R.BRAND*	*R.VIRUS-MAIL*	*R.PABX*	*R.TELEKOM*	*R.KRANKHEIT*	*B.DIEBSTAHL-DOK.*	*R.MITHÖREN*	*R.VERLUST-DOK.*	*R.VERBREITUNG*
O.INC-COHERENCE						+								
O.INC-ORGA						+								
O.TELECOM									+					
O.ECOUTE												+		
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Die Sicherheitsziele eventuell in zwei Kategorien einstufen

Ziel der Bestimmung von Sicherheitszielen ist es, alle die Sicherheit betreffenden Besorgnisse zu behandeln und Sicherheitsaspekte zu erklären, die:

- entweder direkt durch das Zielsystem berücksichtigt werden (Sicherheitsziele, die das Zielsystem betreffen),
- oder durch seine Umgebung berücksichtigt werden (Sicherheitsziele, die die Umgebung des Zielsystems betreffen).

Dabei basiert die Bestimmung auf einer Analyse der Auswirkungen auf die Entwicklung (technische, terminliche Glaubwürdigkeit o. ä.), die Sicherheits-Policy (Übereinstimmung mit den Elementen der Allgemeinen Politik), die wirtschaftlichen Faktoren (durch die Berücksichtigung technischer oder organisatorischer Maßnahmen verursachte Kosten) und die Entscheidung Risiken zu akzeptieren (Risiken, deren Bedrohungswahrscheinlichkeit vernachlässigbar ist oder Risiken für die externe Maßnahmen wie z. B. der Abschluss einer Versicherung, ergriffen werden können).

Die fehlenden Abdeckungen einschließlich Begründung hervorheben

Die Arbeitsgruppe kann entscheiden, die Risiken, Sicherheitsvorschriften oder Hypothesen nicht vollständig durch die Sicherheitsziele abzudecken. Solche Risiken sollten deutlich gemacht und der Grund der Unvollständigkeit ausreichend begründet werden, da sie für die Institution Restrisiken bedeuten.

Beispiele:

- *Ein Mitarbeiter gibt infolge des problemlosen Datenaustauschs über Hardware, Software und Netzwerke des Studienbüros Informationen über ein Projekt an einen Konkurrenten weiter und beeinträchtigt somit die Vertraulichkeit sensibler Information (Kostenvoranschläge, Akten mit Rechtsstreitigkeiten u. ä.).*
- *Ein Mitarbeiter gibt infolge fehlender Zugriffskontrollprozeduren zu den Kommunikationstools Informationen über ein Projekt an einen Konkurrenten weiter und beeinträchtigt somit die Vertraulichkeit sensibler Information (Kostenvoranschläge, Akten mit Rechtsstreitigkeiten u. ä.).*

Aktivität 4.3 - Bestimmung der Sicherheitsniveaus

Für jedes Sicherheitsziel das angemessene Widerstandsniveau festlegen

Das von den Sicherheitsmaßnahmen erwartete und die Sicherheitsziele erfüllende Widerstandsniveau wird im Wesentlichen in Abhängigkeit vom Angriffspotenzial der bedrohenden Elemente bestimmt, welche die Risiken für die Institution hervorrufen. Das angemessene Schutzniveau hängt vom Niveau des Angreifers ab.

Es hängt aber auch von weiteren Faktoren wie z. B. den Sicherheitsbedarfen der eventuell betroffenen wesentlichen Elemente, der Bedrohungswahrscheinlichkeit oder dem allgemeinen Kontext ab.

Wir unterscheiden drei Widerstandsniveaus, die die wohl mindestens notwendigen Anstrengungen zur Durchkreuzung des erwarteten Sicherheitsverhaltens durch direkten Angriff der vorhandenen Sicherheitsmechanismen ausdrücken.

1 - Elementar	Ein Widerstandsniveau wie z.B. die Analyse zeigt, dass die betroffene Funktion einen angemessenen Schutz gegen eine zufällige Verletzung der Systemsicherheit durch Angreifer mit geringem Angriffspotenzial bietet.
2 - Mittel	Ein Widerstandsniveau wie z.B. die Analyse zeigt, dass die betroffene Funktion einen angemessenen Schutz gegen eine leicht durchzuführende Verletzung oder eine vorsätzliche Verletzung der Systemsicherheit durch Angreifer mit mittlerem Angriffspotenzial bietet.
3 - Hoch	Ein Widerstandsniveau wie z.B. die Analyse zeigt, dass die betroffene Funktion einen angemessenen Schutz gegen eine willentlich geplante oder organisierte Verletzung der Systemsicherheit durch Angreifer mit hohem Angriffspotenzial bietet.

Was die Risiken abdeckenden Sicherheitsziele anbelangt, hängt das erforderliche Niveau vom Angriffspotential ab. Wenn ein Sicherheitsziel mehrere Risiken mit verschiedenen Angriffspotenzialen abdeckt, zählt das höchste Niveau. Dieser Wert muss unter Berücksichtigung der Sicherheitsbedarfe der eventuell betroffenen wesentlichen Elemente, der Bedrohungswahrscheinlichkeit oder des allgemeinen Kontextes angepasst werden.
Was die Sicherheitsziele zur Abdeckung der Sicherheitsvorschriften (oder der Vorschriftsreferenzen) betrifft, so wird ihr Niveau von der Institution in Abhängigkeit von der Wichtigkeit gewählt, die sie ihnen beimisst, und von den Anstrengungen, die sie zu ihrer Einhaltung unternehmen will.

Das Widerstandsniveau der einzelnen Sicherheitsziele muss begründet werden.

Das Niveau der Gewährleistungsanforderungen auswählen

Es sind 7 vordefinierte Gewährleistungsniveaus[3] (sog. EALs - *Evaluation Assurance Level)* zu unterscheiden:

EAL 1	Funktionell getestet
EAL 2	Strukturell getestet
EAL 3	Methodisch getestet und überprüft
EAL 4	Methodisch entworfen, getestet und nachkontrolliert
EAL 5	Mit Hilfe von halb-formellen Methoden entworfen sowie getestet
EAL 6	Entwurf mit Hilfe von halb-formellen Methoden überprüft sowie getestet
EAL 7	Entwurf mit Hilfe von formellen Methoden überprüft sowie getestet

Diese Niveaus besitzen verschiedene Bestandteile mit ansteigender Strenge, mit denen die angewandte Sicherheit bewertet werden kann.

Das Gewährleistungsniveau EAL ist das Niveau der Vertraulichkeit, das man den Sicherheitszielen zuweisen kann. Genauer gesagt bezieht sich das Gewährleistungsniveau auf die Realisierung funktionaler Sicherheitsanforderungen, die eine Verfeinerung der Sicherheitsziele darstellen. Je höher es ist, umso mehr Garantien besitzt die Institution. Es ist aber wichtig, die Kosten für die Umsetzung der Gewährleistungsanforderungen sowie die Machbarkeit für die Institution oder ihre Zulieferer zu berücksichtigen.

Es gibt keine universelle Methode zur Bestimmung des Gewährleistungsniveaus, dies ist eher eine Frage des Budgets oder des Marketings.

Das gewählte EAL-Niveau kann eventuell durch andere Gewährleistungskomponenten erhöht werden.

Man muss nicht unbedingt die EALs zu Rate ziehen. Die Institution kann auch ihre eigenen Gewährleistungsanforderungen definieren, indem sie Anforderungen aus den bestehenden Komponenten auswählt oder sogar neue definiert.

Die Anforderungen zur Gewährleistung der Sicherheit enthalten in der Regel Anforderungen über das Annehmen gewünschter Verhaltensweisen und das Unterlassen unerwünschter Verhaltensweisen. Gewöhnlich kann bei Benutzung oder durch einen Test nachgewiesen werden, ob eine gewünschte Verhaltensweise auch wirklich Anwendung findet.
Dagegen ist es nicht immer möglich, das Unterlassen einer nicht gewünschten Verhaltensweise schlüssig nachzuweisen. Daher tragen die Tests und Überprüfungen des Entwurfs und der Implementierung deutlich dazu bei, das Risiko des Vorhandenseins einer solchen Verhaltensweise einzuschränken. Die genannten Argumente müssen die Aussage bekräftigen, nach der ein solches unerwünschtes Verhalten nicht vorhanden ist.

[3] Das Gewährleistungsniveau stellt ein Paket von Gewährleistungskomponenten dar, die aus Teil 3 der Norm ISO/IEC 15408 hervorgehen, was einem Niveau der vordefinierten Gewährleistungsskala entspricht.

Schritt 5 - Bestimmung der Sicherheitsanforderungen

Aktivität 5.1 - Bestimmung der funktionellen Sicherheitsanforderungen

Die funktionellen Sicherheitsanforderungen auflisten

Die funktionellen Sicherheitsanforderungen stellen ein Mittel dar, die Sicherheitsziele zu erreichen und damit die innewohnenden IT-Risiken zu behandeln. Sie sind durch oder mit der Projektleitung zu bestimmen (zur Auflistung der funktionellen Sicherheitsanforderungen, die angemessen erscheinen, um den die Schwachstellen abdeckenden Sicherheitszielen zu genügen, können die Allgemeinen funktionellen Sicherheitsanforderungen und die Tabelle zur Festlegung der Sicherheitsziele und –anforderungen des Leitfadens "Mittel für die Behandlung von IT-Risiken" herangezogen werden).

Zur Einschränkung der IT-Risiken werden in der nachstehenden Tabelle beispielhaft die wichtigsten Arten von Sicherheitsmaßnahmen vorgestellt, die durch die funktionellen Sicherheitsanforderungen in Abhängigkeit von den Risikokomponenten spezifiziert wurden.

	Die wichtigsten Komponenten eines Risikos		
Wichtigste Maßnahmearten	Schwachstellen	Ursprung der Bedrohungen (Angriffsmethoden und bedrohende Elemente).	Konsequenzen (wesentliche Elemente und Auswirkungen)
Vorhersage und Vorbereitung	X	X	X
Abschreckung		X	
Schutz	X		
Erkennung	X	X	
Abschirmung		X	X
Bekämpfung	X		X
Wiederverwendung			X
Aufbereitung			X
Kompensierung			X

Diese Tabelle soll bei der Bestimmung der funktionellen Sicherheitsanforderungen helfen. Sie stellt sicher, dass einzelne mögliche Maßnahmearten nicht vergessen werden.

Die funktionellen Sicherheitsanforderungen tragen zur IT-Sicherheits-Risikobehandlung bei, und zwar insofern als die Risiken nicht nur eingeschränkt, sondern auch verweigert, übertragen oder angenommen werden können.
Die Verweigerung eines Risikos wird durch funktionelle Sicherheitsanforderungen materialisiert, die auf eine strukturelle Änderung der Situation des Zielsystems abzielen, so dass das System dem Risiko nicht mehr ausgesetzt ist.
Die Übertragung eines Risikos wird durch spezifische funktionelle Sicherheitsanforderungen materialisiert, wie z. B. ein Zurückgreifen auf Versicherungsverträge oder Vergabe von Unteraufträgen.
Die Annahme eines Risikos wird durch ein Fehlen funktioneller Sicherheitsanforderungen d. h. eine unvollständige Zufriedenstellung der Sicherheitsziele materialisiert. Restrisiken können identifiziert werden.

Die Funktionen des Zielsystems und dessen Umgebung, die insbesondere die Sicherheit der Informationstechnologien sicherstellen und die das gewünschte Sicherheitsverhalten bestimmen, werden mit den funktionellen Vorschriften belegt.
Diese funktionellen Anforderungen können aus ISO/IEC 15408 (Gemeinsame Kriterien) hervorgehen oder vollständig neu erzeugt werden. Es wird dringend empfohlen, eine funktionelle Anforderung nur dann neu zu erzeugen, wenn sie einen funktionellen Aspekt behandelt, der nicht in den Bestandteilen der ISO/IEC 15408 existiert.

Die Liste der funktionellen Sicherheitsanforderungen, die aus den Gemeinsamen Kriterien hervorgehen, besteht aus funktionellen Klassen, Familien und Komponenten. Zwischen den Komponenten kann eine Abhängigkeit bestehen. Die Abhängigkeiten treten auf, wenn sich eine Komponente nicht selbst genügt, sondern vom Vorhandensein einer anderen Komponente abhängt. Dabei können die Abhängigkeiten unter den funktionellen Komponenten untereinander und unter funktionellen Komponenten und Gewährleistungskomponenten vorkommen. Je nach Kenntnisstand in Bezug auf das System und fachlichem Niveau der Akteure der Arbeitsgruppe können die Komponenten im Rohzustand belassen werden, wobei jedoch darauf hinzuweisen ist, dass Verfeinerungen der Komponenten durch den Auftragnehmer vorzunehmen sind.

ISO/IEC 15408 lässt die Möglichkeit offen, auf funktionelle Anforderungen zurückzugreifen, die nicht auf der angebotenen Liste vermerkt sind, um alle Sicherheitsanforderungen der Informationstechnologien darstellen zu können. Folgende Anweisungen sind bei der Eingliederung dieser erweiterten funktionellen Anforderungen zu berücksichtigen:

- Alle funktionellen Sicherheitsanforderungen müssen unter Bezugnahme auf die funktionellen Anforderungskomponenten formuliert werden. Sollte keine der Sicherheitskomponenten zumindest teilweise auf die Sicherheitsanforderungen angewendet werden können, kann die Arbeitsgruppe diese Anforderungen explizit ohne Bezugnahme auf ISO/IEC 15408 formulieren.
- Jede erweiterte funktionelle Anforderung muss klar und eindeutig geäußert werden, damit die Evaluierung realisierbar ist, wobei der Grad der Detaillierung und die Ausdrucksweise der funktionellen Komponenten, so wie sie in ISO/IEC 15408 vorhanden sind, als Modell heranzuziehen sind.
- Die Ergebnisse der Evaluierung, die unter Zuhilfenahme erweiterter funktioneller Anforderungen erzielt wurden, müssen durch einen Hinweis kenntlich gemacht werden.
- Die Eingliederung erweiterter funktioneller Sicherheitsanforderungen muss gemäß den Klassen APE oder ASE des Teils 3 von ISO/IEC 15408 erfolgen, soweit dies angemessen ist.

Bestenfalls muss die Formulierung einer funktionellen Sicherheitsanforderung:

- S – spezifisch sein (nur ein Akteur, ein Bereich gleichzeitig),
- M – messbar sein (Definition des Prüfmittels),
- A – erreichbar sein (ggf. in mehreren Schritten unter Bereitstellung der notwendigen Ressourcen),
- R – realistisch sein (in Abhängigkeit der Akteure, ihrer Fähigkeiten),
- T – zeitlich bestimmt sein (es gibt ein Zieldatum, eine Frist, einen festgelegten Zeitabschnitt).

Für die Bestimmung der funktionellen Sicherheitsanforderungen müssen alle Elemente des Kontextes berücksichtigt werden, und zwar vor allem die Budget- und Technikeinschränkungen.

Beispiele:

EF.INC-DETECT	*Die Räumlichkeiten eines Architektenbüros müssen mit einem Brandschutzsystem mit Alarmweitergabe an einen Kontrollposten ausgestattet sein, der ruhig außerhalb liegen darf. Diese Maßnahmen müssen von Fachleuten geprüft und eingerichtet werden. Sie sind mindestens ein Mal im Jahr zu überprüfen.*
EF.FOURN-ACCES	*Das Studienbüro muss bei mindestens zwei verschiedenen Internet-Providern abonniert sein.*
EF.MAINTENANCE	*Ein Wartungsvertrag muss die Verfügbarkeit der internen und externen Kommunikationsmittel garantieren, wobei die Frist in Relation zu den tätigkeitsspezifischen Belangen des Studienbüros steht (12 Stunden Nicht-Verfügbarkeit).*
EF.CHIFFREMENT	*Der elektronische Nachrichtenverkehr muss durch ein marktübliches Verschlüsselungssystem im Hinblick auf die Vertraulichkeit geschützt werden. Die Tools, die diese Chiffrierschlüssel benutzen, müssen Gegenstand einer Schlüsselmanagementpolitik sein.*

EF.LOCAUX	*Fremdpersonen, die in den "Arbeits"-Bereich des Studienbüros eindringen, müssen begleitet sein.* *Wartungspersonal, Reinigungspersonal oder sonstige Fremdpersonen dürfen sich bei Abwesenheit der Mitarbeiter des Studienbüros nicht in den Räumlichkeiten aufhalten.* *Die Räumlichkeiten müssen durch Sicherheitsschlösser gesichert sein, nur der Direktor und sein Stellvertreten besitzen die Schlüssel dafür.*
…	…

Die Vollständigkeit der Abdeckung der Sicherheitsziele nachweisen

Die Erstellung einer Abdeckungsmatrix soll sicherstellen, dass alle Sicherheitsziele bezüglich des Zielsystems und seiner Umgebung durch mindestens eine funktionelle Sicherheitsanforderung abgedeckt werden. Genauso muss jede funktionelle Sicherheitsanforderung mindestens eines der Sicherheitsziele abdecken.

Der die Sicherheitsanforderungen betreffende Argumentenkatalog muss beweisen, dass die Gesamtheit aller Sicherheitsanforderungen angemessen ist, um den Sicherheitszielen zu genügen, und dass Anforderungen und Ziele in Relation zueinander stehen. Es muss nachgewiesen werden können,:

- dass die Kombination der individuellen funktionellen Sicherheitskomponenten den erklärten Sicherheitszielen genügt,
- dass die Gesamtheit aller Sicherheitsanforderungen ein kohärentes Ganzes bildet, bei dem sich die einzelnen Elemente gegenseitig unterstützen,
- dass das Widerstandsniveau der gewählten Funktionen sowie jede sonstige Widerständigkeit explizit angekündigter Funktionen mit den Sicherheitszielen in Einklang stehen.

Ein erster Nachweis besteht demnach darin, die Abdeckung der Sicherheitsziele nachzuweisen.

Dabei kann die Abdeckung durch einen Wert der folgenden Skala synthetisiert werden:

0	Keine Abdeckung
1	Teilweise Abdeckung
2	Vollständige Abdeckung

Beispiel:

Sicherheitsziele	*Widerstandsniveaus*	*Funktionelle Sicherheitsanforderungen*	*Nachweis der Abdeckung*	*Abdeckung*
O.INC-COHERENCE	*2*	*EF.INC-LUTTE*	*Die Kohärenz der Brandschutzmaßnahmen mit dem IT-System wird durch die Sicherheitsanforderung, die die Brandbekämpfung betrifft, vollständig berücksichtigt.*	*2*

Sicherheitsziele	*Widerstandsniveaus*	*Funktionelle Sicherheitsanforderungen*	*Nachweis der Abdeckung*	*Abdeckung*
O.PABX	*1*	*EF.MAINTENANCE EF.REPRISE*	***Die durch einen Betriebsfehler des internen Telefonnetzes (PABX am Standort des Studienbüros defekt) verursachte Störung wird durch diese Sicherheitsanforderungen eingeschränkt, dennoch kann der Schadensfall eintreten.***	***1***
O.TELECOM	*1*	*EF.FOURN-ACCES EF.MISES-A-JOUR EF.REPRISE*	*Den Störungen der externen Netze wird durch die erste Sicherheitsanforderung vorgebeugt. Die beiden folgenden tragen dazu bei, die Nicht-Verfügbarkeit einzuschränken.*	*2*
O.ECOUTE	*2*	*EF.CHIFFREMENT*	*Die Verschlüsselung genügt dem Ziel, die Vertraulichkeit zu schützen. Die Definition einer Schlüsselmanagementpolitik macht es möglich, das geforderte Widerstandsniveau zu erreichen.*	*2*
…	…	…	…	…

Ein zweiter Nachweis besteht darin aufzuzeigen, dass jede funktionelle Sicherheitsanforderung mindestens ein Sicherheitsziel abdeckt.

Beispiel:

Sicherheitsanforderungen	*O.BRAND-KOHÄRENZ*	*O.BRAND-ORGA*	*O.PABX*	*O.TELEKOM*	*O.MITHÖREN*	*O.RÄUMLICHKEITEN*	*O.SENSIT-PERS*	*O.DIEBSTAHLSCHUTZ*	*O-ÜBERNAHME*	*O.MANIPULATION*	*O.SENSIT-ORGA*	*O.BÖSWILLIG*	*O.ÜBERWACHUNG*	*O.SYS-BEFEHLE*	*O.SYS-AKTIONEN*	*O.KRANKHEIT*	*O.PSSI*	*O.VORSCHRIFT*	*O.AUTH-DOK*
EF.INC-DETECT		+																	
EF.INC-LUTTE	+	+																	
EF.INC-CONSIGNES		+																	
EF.INC-ORGA		+																	
EF.MAINTENANCE			+																
EF.FOURN-ACCES				+															
EF.CHIFFREMENT					+														
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Die fehlenden Abdeckungen einschließlich Begründung hervorheben

Es ist notwendig, über die Mittel, mit denen die Sicherheitsziele realisiert werden können, einen Konsens zu erzielen. Dieser Konsens kann nur erreicht werden, indem die Risiken mit den Kosten für die Sicherheitsmaßnahmen der funktionellen Sicherheitsanforderungen verglichen werden.
Es ist vernünftig, zunächst die wichtigsten und wahrscheinlichsten Risiken zu betrachten, da bei deren Bearbeitung gelegentlich weniger wichtige gleich mit bearbeitet werden können.

Die Arbeitsgruppe kann entscheiden, die Sicherheitsvorschriften nicht vollständig durch die Sicherheitsziele abzudecken. Solche Risiken sollten deutlich gemacht und der Grund der Unvollständigkeit ausreichend begründet werden, da sie für die Institution Restrisiken bedeuten.

Beispiele:

- *Verlust der Telekommunikationsmittel auf Grund einer Betriebsstörung des internen Telefonnetzes (PABX am Standort des Studienbüros defekt); ein Rücknahmeplan und eine Instandsetzungsgarantie innerhalb von 12 Stunden schränken die Nicht-Verfügbarkeit dieser Mittel ein.*
- *Ein Mitarbeiter lässt sich trotz Sensibilisierung manipulieren und verbreitet Informationen über ein Projekt an einen Konkurrenten, wodurch die Vertraulichkeit sensibler Informationen (Kostenvoranschläge, Akten mit Rechtsstreitigkeiten u. ä.) verletzt wird.*
- *Ein Eindringling sabotiert die Software durch Manipulation der Software der Systemressourcen via Internet, und zwar trotz eingeschränkter Zugriffsrechte auf die angeschlossenen Rechner, den Einsatz von Firewalls und regelmäßige Updates der Software; dadurch kann die Vertraulichkeit sensibler Informationen (Kostenvoranschläge, Akten mit Rechtsstreitigkeiten u. ä.) und die Integrität wesentlicher Elemente (Strukturberechnungen, Kostenvoranschläge, technische Pläne, technische Parameter, Akten über Rechtsstreitigkeiten usw.) verletzt werden.*

Die funktionalen Sicherheitsanforderungen in zwei Kategorien einstufen

Die Sicherheitsanforderungen ergeben sich aus der Verfeinerung der Sicherheitsziele :

- zu Sicherheitsanforderungen für das Zielsystem,
- zu Sicherheitsanforderungen für die Umgebung.

Wenn diesen Anforderungen genügt wird, können sie garantieren, dass das Zielsystem der Sicherheitsstudie seinen Sicherheitszielen genügen wird.

Eventuell die Abdeckung der Abhängigkeiten der funktionalen Sicherheitsanforderungen nachweisen

Allen Abhängigkeiten zwischen den Sicherheitsanforderungen untereinander muss Rechnung getragen werden. So gibt es Sicherheitsanforderungen, die aus Gründen der Kohärenz das Vorhandensein anderer Sicherheitsanforderungen benötigen. Den Abhängigkeiten kann Rechnung getragen werden, indem die betroffene funktionelle Komponente in die funktionellen Sicherheitsanforderungen des Zielsystems oder als Anforderung an die Umgebung integriert wird.
Die Nichtberücksichtigung einer Abhängigkeit muss formell gerechtfertigt werden.

Aktivität 5.2 - Bestimmung der Sicherheitsgewährleistungs-anforderungen

Die Sicherheitsgewährleistungsanforderungen auflisten

Die Anforderungen zur Gewährleistung der Sicherheit nach ISO/IEC 15408 gelten für die Arbeiten des Entwicklers, für die gelieferten Beweiselemente und für die Aktionen des Bewerters (Beispiel: Zwänge bezüglich der Genauigkeit beim Entwicklungsprozess und Anforderungen zur Auffindung und Analyse der Auswirkung potentieller Sicherheitslücken).

Die Gewährleistung, dass die Sicherheitsziele dank der gewählten Sicherheitsfunktionen erreicht werden, beruht auf den beiden nachstehenden Faktoren:

- Das Vertrauen in die Konformität der Implementierung der Sicherheitsfunktionen, d. h. dass die Funktionen korrekt implementiert wurden,
- das Vertrauen in die Effizienz der Sicherheitsfunktionen, d. h. die Annahme, dass die Funktionen tatsächlich den geäußerten Sicherheitszielen genügen.

Die Sicherheitsgewährleistungsanforderungen können je nach Finalität der Studie neu formuliert werden, damit die Abfassung den Akteuren der Studie leichter zugänglich wird.

Beispiel einer Rohfassung:

ACM_CAP.1 Versionsnummern

Ziele:

Es ist eine eindeutige Referenz erforderlich, um zu garantieren, dass es keine Mehrdeutigkeiten bei dem TOE-Exemplar gibt, das bewertet wird. Die Identifizierung der TOE durch ihre Referenz gewährleistet, dass die TOE-Nutzer wissen, welches TOE-Exemplar sie benutzen.

Verwandte Themen:

Keine verwandten Themen.

Aufgaben des Entwicklers:

ACM_CAP.1.1D Der Entwickler muss eine Referenz für die TOE liefern.

Inhalt und Darstellung der Beweiselemente:

ACM_CAP.1.1C Die Referenz der TOE muss für jede Version der TOE eindeutig sein.

ACM_CAP.1.2C Die TOE muss durch ihre Referenz gekennzeichnet sein.

Aufgaben des Bewerters:

ACM_CAP.1.1E Der Bewerter muss bestätigen, dass die gelieferten Informationen alle Anforderungen an den Inhalt und die Darstellung der Beweiselemente erfüllen.

Beispiel einer neu formulierten Fassung:

EA.NUM-VERSION	*Das Studienbüro muss für jede Entitätenversion des Zielsystems über eine eindeutige Referenz (oder ähnliches wie z. B. Versionsnummer) verfügen. Über diese Referenz sind sie identifizierbar.*

Eventuell die Sicherheitsgewährleistungsanforderungen in zwei Kategorien einstufen

Die Anforderungen zur Gewährleistung der Sicherheit können einer der beiden folgenden Kategorien angehören:

- Sicherheitsgewährleistungsanforderungen, die das Zielsystem betreffen,
- Sicherheitsgewährleistungsanforderungen, die die Umgebung des Zielsystems betreffen.

Eventuell die Abdeckung der Abhängigkeiten der Gewährleistungsanforderungen nachweisen

Die Anforderungen zur Gewährleistung der Sicherheit können von weiteren Anforderungen abhängen, die es zu berücksichtigen gilt, damit ein kohärentes Ganzes sichergestellt ist.
Die Vollständigkeit der Abdeckung muss nachgewiesen werden.
Die Nichtberücksichtigung einer Abhängigkeit muss formell gerechtfertigt werden.

Kommentarsammelformular

Dieses Formular kann an folgende Adresse gesendet werden:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identifizierung des Beitrags
Name und Institution (fakultativ): .....
Elektronische Adresse: .....
Datum: .....

Allgemeine Bemerkungen zu diesem Dokument
Entspricht das Dokument Ihren Bedürfnissen? Ja ☐ Nein ☐

Wenn ja:

Glauben Sie, dass es vom Inhalt her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

Was haben Sie vermisst?
.....
.....

Welche Teile des Dokuments erscheinen Ihnen überflüssig oder unangemessen?
.....
.....

Glauben Sie, dass es von der Form her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

In welchem Bereich ist es verbesserungsfähig?
- Leserlichkeit, Verständnis ☐
- Aufmachung ☐
- Sonstiges ☐

Formulieren Sie Ihre Wünsche bezüglich der Form:
.....
.....

Wenn nein:

Geben Sie den Bereich an, der Ihnen nicht gefällt und umschreiben Sie, was Ihnen gefallen hätte:
.....
.....

Welche weiteren Themen hätten Sie gerne vorgefunden?
.....
.....

Spezielle Bemerkungen zu diesem Dokument

In nachstehender Tabelle können Sie detailliert Stellung nehmen.

Unter Nr. ist die Laufnummer einzutragen.

In die Spalte "Typ" sind zwei Buchstaben einzutragen:

Mit dem ersten Buchstaben wird die Kategorie der Bemerkung umschrieben:

- R Rechtschreib- oder Grammatikfehler
- E Mangelnde Erläuterung oder Erklärung des behandelten Punktes
- I Text unvollständig oder nicht vorhanden
- I Irrtum

Der zweite Buchstabe beschreibt den Bedeutungsgrad:

- g geringfügig
- G Gravierend

Unter "Referenz" ist die genaue Lokalisierung im Text anzugeben (Kapitelnummer, Zeile...).

Unter "Wortlaut der Bemerkung" kann ein Kommentar abgegeben werden.

Unter "vorgeschlagene Lösung" können Mittel zur Lösung des aufgeworfenen Problems angegeben werden.

Nr.	Typ	Referenz	Wortlaut der Bemerkung	Vorgeschlagene Lösung
1				
2				
3				
4				
5				

Vielen Dank für Ihre Teilnahme