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 2
METHODIK

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 Bedarfe 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 den Sicherheitsbedarfen 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 IT-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

Verzeichnis der Abbildungen

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 Wissensdatenbanken der EBIOS-Methode (Entitätstypen, Angriffsmethoden, Schwachstellen)

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

Das vorliegende Dokument entspricht dem zweiten Abschnitt der Methode. Hier wird die methodische Vorgehensweise an Hand von Kurzbeschreibungen vorgestellt.

Die einzelnen Schritte werden zunächst beschrieben, zur Einordnung des jeweiligen Schritts innerhalb der gesamten EBIOS-Methodik kurz schematisiert, und abschließend werden die verschiedenen Aktivitäten eines jeden Schritts synoptisch dargestellt.

Jede Aktivität wird formal nach einem einheitlichen Muster beschrieben.

BESCHREIBUNG
Zusammenfassung der methodischen Vorgehensweise und schematische Darstellung zur Einordnung der Aktivität innerhalb des Schritts.

VORBEDINGUNGEN
Sonstige Aktivitäten, die im Vorfeld der Aktivität sicherzustellen sind.

EINGANGSDATEN
Daten, die zur Realisierung der Aktivität erforderlich sind.

AKTIONEN
Aktionen, die für den Erfolg der Aktivität maßgebend sind.

AUSGANGSDATEN
Daten, die im Anschluss an die Aktionen der Aktivität erstellt werden.

PRAKTISCHE HINWEISE
Anmerkungen und Hinweise zur Durchführung der Aktivität.

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

Vorstellung der Methodik

Die EBIOS-Methode formalisiert eine Methodik zur IT-Risikobewertung und Behandlung von Risiken auf dem Gebiet der IT-Sicherheit.

Sie kann für zukünftige oder bereits bestehende Systeme, für das gesamte IT-System oder nur einen der Teilbereiche angewendet werden.

Die fünf Schritte der Methodik werden in der folgenden Abbildung dargestellt:

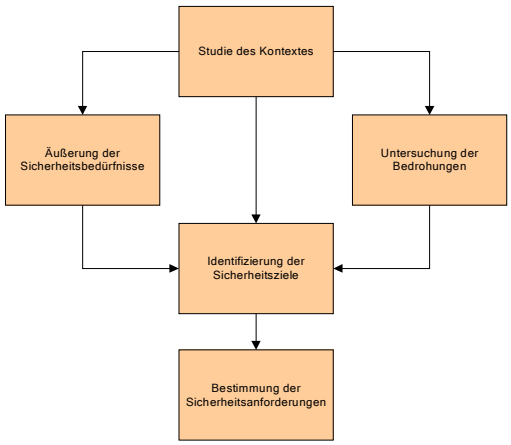
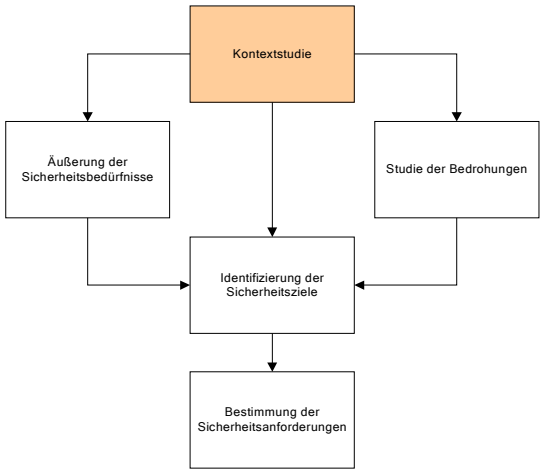


Abbildung 1 – Globale EBIOS-Methodik

- Am Ende des ersten Schritts sind die Umgebung, die Zielsetzung und die Funktionsweise des Zielsystems bekannt, die wesentlichen Elemente und die entsprechenden Entitäten sind eindeutig identifiziert.
- Der zweite Schritt dient der Risikobewertung (Einschätzung der Risiken und Definition der Risikokriterien). Er ermöglicht die Formalisierung von Auswirkungen und die Einschätzung der Sicherheitsbedarfe der wesentlichen Elemente im Hinblick auf Verfügbarkeit, Integrität und Vertraulichkeit.
- Auch der dritte Schritt steht im Zusammenhang mit der Risikobewertung (Risikoanalyse). Hier geht es darum, die auf dem System lastenden Bedrohungen zu erfassen und zu beschreiben. Dazu werden die Angriffsmethoden und die diese Methoden eventuell einsetzenden bedrohenden Elemente sowie die ausnutzbaren Schwachstellen der Entitäten und die gebotenen Wahrscheinlichkeiten untersucht.
- Der vierte Schritt trägt zur Evaluierung und Behandlung der Risiken bei. Er dient der Formalisierung der Risiken, die tatsächlich auf dem System lasten, indem die Bedrohungen (negative Ereignisse) den Sicherheitsbedarfen (Konsequenzen) gegenübergestellt werden. Die Risiken werden durch Sicherheitsziele abgedeckt, die unter Berücksichtigung der Hypothesen, Sicherheitsvorschriften, Vorschriftsreferenzen, des Betriebsmodus und der identifizierten Zwänge definiert wurden; sie bilden das Sicherheitslastenheft.
- Der fünfte und letzte Schritt betrifft die Risikobehandlung. Hier wird erklärt, wie funktionelle Anforderungen festgelegt werden können, mit denen die Sicherheitsziele und Gewährleistungsanforderungen zur Steigerung ihrer Vertrauenswürdigkeit erreicht werden können.

Schritt 1 - Kontextstudie

Ziel dieses entscheidenden Schritts ist die globale Identifikation des Zielsystems und seine Situierung in seiner Umgebung, um das Ziel der Sicherheitsstudie genau zu bestimmen.



Dadurch können die für das System absehbaren Konsequenzen, sein Benutzungskontext, die sicherzustellenden Aufgaben oder Dienstleistungen und die eingesetzten Mittel bestimmt werden. Dieser Schritt dient auch dem Zusammentragen aller Informationen, die zur Planung der Studie erforderlich sind.

Am Ende dieses Schrittes ist das Nachforschungsfeld der Studie klar abgegrenzt, die Hypothesen, Verpflichtungen und Zwänge sind erfasst und die zu behandelnden Themen sind bekannt.

Dieser erste Schritt setzt sich aus drei Aktivitäten zusammen:

- Untersuchung der Institution
- Studie des Zielsystems
- Bestimmung des Ziels der Sicherheitsstudie

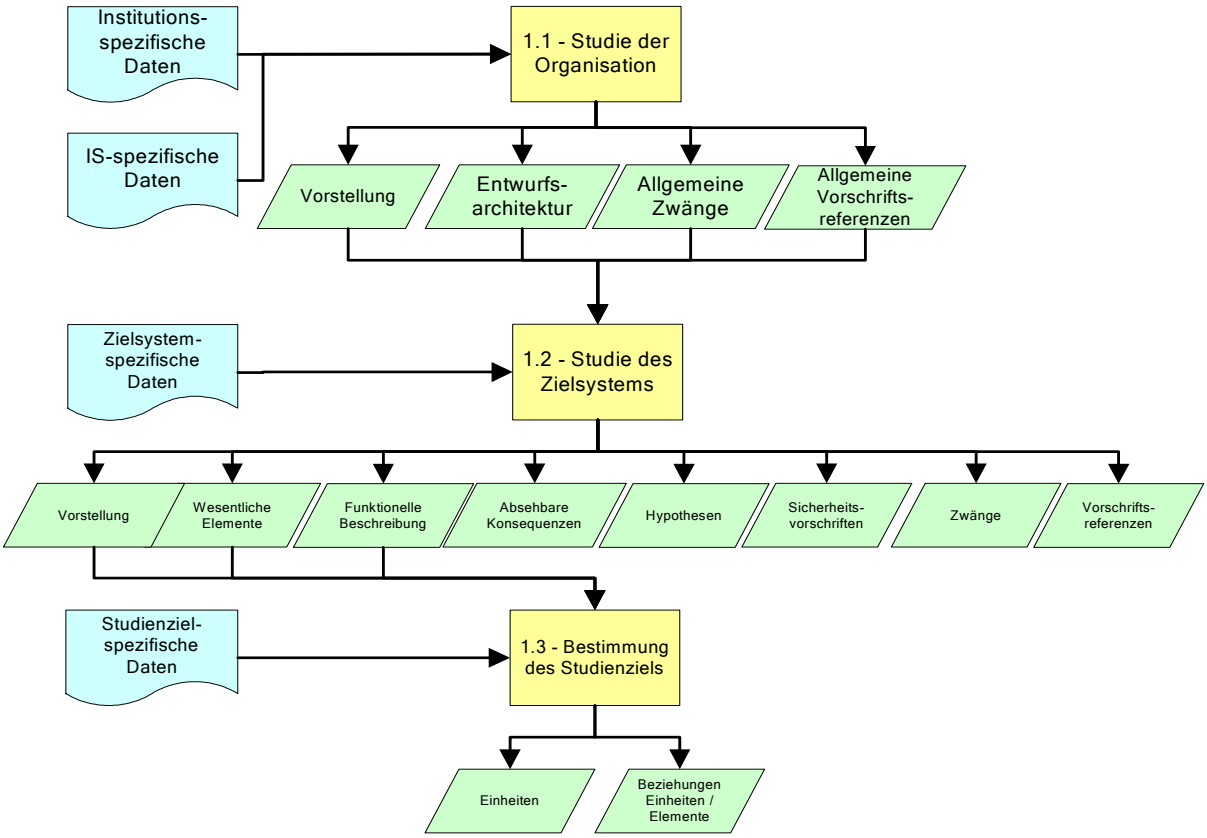
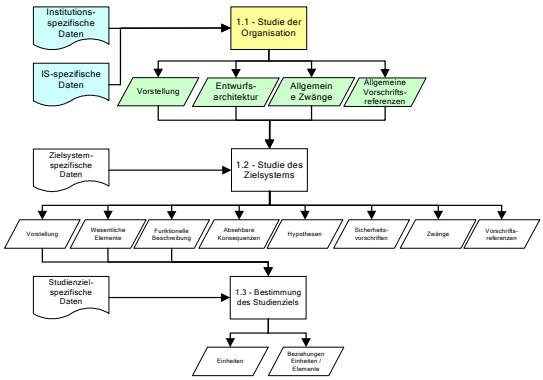


Abbildung 2 – Synoptische Darstellung der Kontextstudie

Aktivität 1.1 – Untersuchung der Institution

BESCHREIBUNG

Mit dieser Aktivität soll der Rahmen der Studie definiert werden. Es geht darum, allgemeine Informationen über die vom Sicherheitsprojekt betroffene Institution zusammenzutragen, um ihre Beschaffenheit, ihren Aufbau und die auf ihr lastenden Zwänge besser bewerten zu können. Es ist auch notwendig, eine umfassende Übersicht über das IT-System der Institution zu bekommen. Mit Hilfe dieser Elemente können in den folgenden Aktivitäten die absehbaren Konsequenzen des Zielsystems auf die Institution aufgezeigt und die Übereinstimmung der Sicherheitsziele und –anforderungen mit den sicherzustellenden Aufgaben kontrolliert werden.



VORBEDINGUNGEN

Gegenstandslos

EINGANGSDATEN

- Daten über die Institution und ihr IT-System (strategische Unterlagen, Unterlagen über die Aufgaben, Zuweisungen und die Organisation, Unterlagen über das IT-System, zusammenfassende Berichte über Gespräche mit den Verantwortlichen der Institution).

AKTIONEN

- Die Institution vorstellen.
- Die auf der Institution lastenden Zwänge auflisten.
- Die von der Institution anzuwendenden Vorschriftsreferenzen auflisten.
- Eine funktionelle Beschreibung des globalen IT-Systems erstellen.

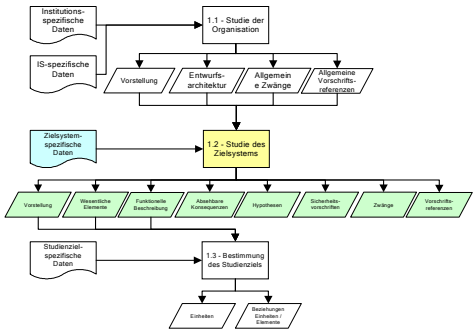
AUSGANGSDATEN

- Vorstellung der Institution
- Auflistung der auf der Institution lastenden Zwänge.
- Auflistung der von der Institution anzuwendenden Vorschriftsreferenzen.
- Konzeptuelle Architektur des IT-Systems

PRAKTISCHE HINWEISE

- Diese erste Aktivität ist für den weiteren Verlauf der Studie entscheidend, sie ermöglicht es, den Kontext der Studie bestmöglich zu verstehen.
- Eine Arbeitsgruppe (oder ein Steuerungskomitee) ist einzurichten, die anzusprechenden Personen müssen eindeutig benannt und die Besprechungen terminlich geplant werden.
- Eine erste Besprechung muss dazu dienen, die Beschaffenheit des ursprünglich aufgeworfenen Problems zu überprüfen und klären, ob dieses Problem in den Zuständigkeitsbereich der Arbeitsgruppe fällt. Bei dieser Besprechung muss ein Maximum an Informationen zusammengetragen werden können.
- Dabei ist auch über die Zweckmäßigkeit zu urteilen, welche der vorgeschlagenen Themen zu behandeln sind, wobei u. a. der Umfang des Projekts, die bereits vor der Besprechung zusammengetragenen ersten Elemente und die Verantwortungen der Ansprechpartner zu berücksichtigen sind.
- Bei der Untersuchung der Institution ist die Entscheidungsinstanz derselben auf höchstem hierarchischem Niveau einzubeziehen.
- Die Informationen sind bei den von der Studie betroffenen operationellen Verantwortlichen einzuholen.
- Fragebögen dienen der Vorbereitung der Besprechungen, die befragten Personen werden mit dem Ziel angeleitet, die Antworten formalisieren zu können.

Aktivität 1.2 – Studie des Zielsystems



BESCHREIBUNG

Ziel dieser Aktivität ist es, den Benutzungskontext des zukünftigen oder bereits bestehenden Systems näher zu beschreiben. Dazu muss die Unter des IT-Systems der Institution, die das Zielsystem der Studie bildet, einschließlich der absehbaren Konsequenzen näher dargelegt werden. Das Zielsystem muss beschrieben und die Hypothesen, Sicherheitsvorschriften und Zwänge müssen erfasst werden.

VORBEDINGUNGEN

- Aktivität 1.1.

EINGANGSDATEN

- Zielsystemspezifische Daten.
- Vorstellung der Institution.
- Auflistung der auf der Institution lastenden allgemeinen Zwänge.
- Auflistung der von der Institution anzuwendenden allgemeinen Vorschriftsreferenzen.
- Konzeptuelle Architektur des IT-Systems.

AKTIONEN

- Das Zielsystem vorstellen.
- Die absehbaren Konsequenzen auflisten.
- Die wesentlichen Elemente auflisten.
- Eine funktionelle Beschreibung des Zielsystems erstellen.
- Die Hypothesen auflisten.
- Die Sicherheitsvorschriften auflisten.
- Die auf dem Zielsystem lastenden Zwänge auflisten.
- Die speziellen Vorschriftsreferenzen des Zielsystems auflisten.

AUSGANGSDATEN

- Vorstellung des Zielsystems.
- Auswahl der wesentlichen Elemente.
- Funktionelle Beschreibung des Zielsystems.
- Liste der absehbaren Konsequenzen des Zielsystems.
- Liste der Hypothesen.
- Abdeckung der Sicherheitsvorschriften.
- Liste der speziellen Zwänge des Zielsystems.
- Liste der speziellen Vorschriftsreferenzen des Zielsystems.

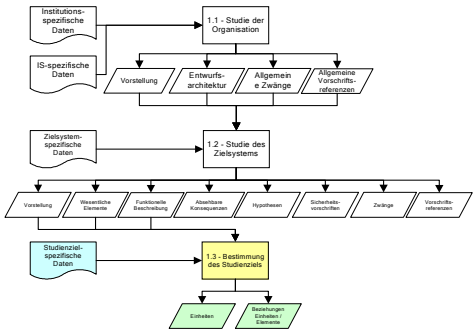
PRAKTISCHE HINWEISE

- Anzahl und Feinheit der wesentlichen Elemente hängen von der Zielsetzung der Studie und der Beschaffenheit des Zielsystems ab. So erfordert eine globale Untersuchung eines IT-Systems, deren Ziel es ist, sich einen allgemeinen Überblick über die Risiken zu verschaffen, nicht die gleiche Feinheit wie die Studie eines konkreten Systems, das formell zugelassen werden soll.
- Fehlende Systemspezifikationen können eine Weiterverfolgung der Sicherheitsstudie in Frage stellen. In der Tat ist es kaum sinnvoll, ein unzureichend bekanntes System absichern zu wollen. Es ist jedoch denkbar, eine rasche, globale Studie weiterzuführen, die dann in dem Maße zu verfeinern ist, wie die Spezifikationen fortschreiten.
- Bei komplexen Systemen ist die Aufteilung in Teilsysteme ins Auge zu fassen. In diesem Fall ist es ratsam, mehrere Studien parallel laufen zu lassen.

Aktivität 1.3 – Bestimmung des Ziels der Sicherheitsstudie

BESCHREIBUNG

Diese Aktivität hat zum Ziel, die Entitäten genau zu bestimmen, auf denen die wesentlichen Elemente des Zielsystems beruhen (Funktionen und Informationen). Die Aktivität besteht darin, die verschiedenen Entitäten zu erfassen und zu beschreiben; dabei ist es unerheblich, ob es sich um den Entitätstyp Hardware, Software, Netzwerk, Personal, Standort oder Organisation handelt. Weiter geht es darum, alle wesentlichen Elemente jeder einzelnen Entität zu verzeichnen.



VORBEDINGUNGEN

- Aktivität 1.2.

EINGANGSDATEN

- Studienzielspezifische Daten.
- Vorstellung des Zielsystems.
- Auswahl der wesentlichen Elemente.
- Funktionelle Beschreibung des Zielsystems.

AKTIONEN

- Die Entitäten des Systems auflisten und beschreiben.
- Die wesentlichen Elemente und die Entitäten gegenüberstellen.

AUSGANGSDATEN

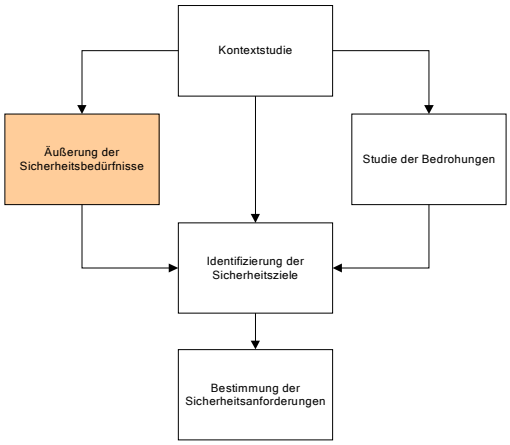
- Liste der Entitäten.
- Beziehungen Entitäten / Elemente.

PRAKTISCHE HINWEISE

- Es ist ratsam, zur Auflistung und Beschreibung der Systementitäten die Entitätstypen und –untertypen zu benutzen, die im Leitfaden "Mittel zur IT-Risikobewertung" beschrieben sind.
- Auch wenn das Zielsystem nur von einer einzigen Organisation (oder einem einzigen Standort) abhängt, darf dennoch nicht vergessen werden, eine Entität des Entitätstyps "Organisation" (oder "Standort") zu identifizieren. Bestimmte Entitäten sind bei vielen Zielsystemen tatsächlich nur einmal vertreten, dennoch müssen sie registriert werden, da sie Schwachstellen besitzen, die im weiteren Verlauf der Studie zu berücksichtigen sind. In der Regel ist von jedem Entitätstyp mindestens eine Entität vertreten.
- Bei der funktionellen Beschreibung können die Entitäten, auf denen das Zielsystem beruht, den Schemen beigeordnet werden. Dadurch kann das System übersichtlicher dargestellt und besser verstanden werden.

Schritt 2 - Sicherheitsbedarfsanalyse

Dieser Schritt trägt zur Einschätzung der Risiken und Definition der Risikokriterien bei. Er bietet den Systemnutzern die Möglichkeit, sich über ihre Sicherheitsbedarfe im Hinblick auf die von ihnen bearbeiteten Funktionen und Informationen zu äußern.



Die Sicherheitsbedarfsanalyse wird durch die operationellen Anforderungen des Systems bedingt, und zwar unabhängig von jedweder technischer Lösung.

Es geht um die Ausarbeitung und Benutzung einer Bedürfnisskala und die Hervorhebung der Auswirkungen, die für die Institution nicht mehr akzeptierbar sind.

Dank der Sicherheitsbedarfsanalyse kann zudem ein System-Betriebsmodus, d. h. eine allgemeine Methodik zur Verwaltung der Systemnutzer, definiert werden.

Dieser zweite Schritt lässt sich in zwei Aktivitäten unterteilen:

- Realisierung der Bedürfnisblätter
- Zusammenfassung der Sicherheitsbedarfe

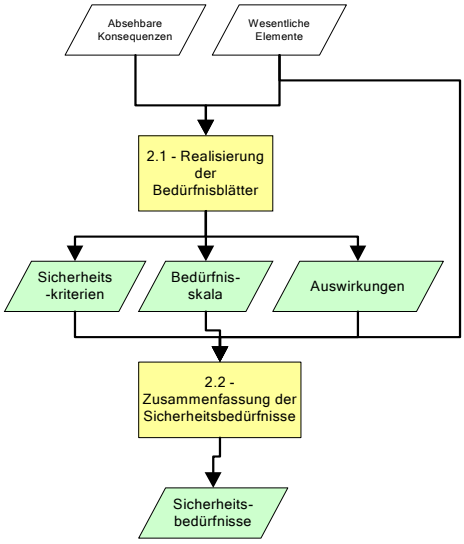
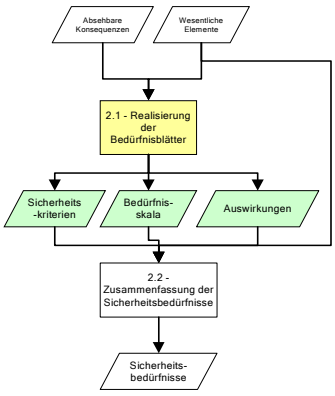


Abbildung 3 – Synoptische Darstellung der Sicherheitsbedarfsanalyse

Aktivität 2.1 – Realisierung der Bedürfnisblätter

BESCHREIBUNG



Ziel dieser Aktivität ist die Erstellung von Tabellen, die für die Sicherheitsbedarfsanalyse durch die Nutzer notwendig sind. Mit Hilfe dieser Tabellen können die Nutzer objektiv und kohärent die Sicherheitsbedarfe der Elemente äußern, mit denen sie im Rahmen der Ausübung ihrer Tätigkeit gewöhnlich zu tun haben. Es handelt sich um eine Aktivität, die zur Einschätzung der Risiken und Definition der Risikokriterien im Rahmen des Risikomanagements beiträgt.

VORBEDINGUNGEN

- Aktivität 1.2.

EINGANGSDATEN

- Liste der absehbaren Konsequenzen des Zielsystems.
- Liste der wesentlichen Elemente.

AKTIONEN

- Die zu berücksichtigenden Sicherheitskriterien auswählen.
- Die Bedürfnisskala festlegen.
- Die relevanten Auswirkungen festlegen.

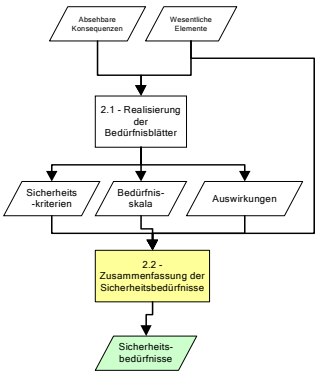
AUSGANGSDATEN

- Liste der Sicherheitskriterien.
- Bedürfnisskala.
- Liste der Auswirkungen.

PRAKTISCHE HINWEISE

- Die Bedürfnisskala ist eines der wichtigsten Diskussionsinstrumente der Studie. Sie ist von der Arbeitsgruppe festzulegen und dient nicht nur den Diskussionen über die Sicherheitsbedarfe sondern auch den Diskussionen über die Sicherheitsziele.
- Die Bedürfnisskala muss objektiv und kohärent sein. Sie enthält Gewichtungen und Referenzwerte und stützt sich auf die Liste mit den zu berücksichtigenden Sicherheitskriterien und eine Liste möglicher Auswirkungen mit repräsentativen Beispielen.
- Bezüglich der Auswirkungen hilft eine Darstellung in Form eines Ursachenbaums, die zu Grunde liegende Idee für die Arbeitsgruppe anschaulicher zu gestalten.
- Zur Ermittlung der Sicherheitsbedarfe wird für jede befragte Person und für jedes wesentliche Element ein Blatt erstellt. Die Erstellung eines Blattes pro Funktion bzw. Teilfunktion rechtfertigt sich dadurch, dass die Sicherheitsbedarfe einer Funktion nicht unmittelbar von den in ihr bearbeiteten Informationen abgeleitet werden können. Beispiele:
  - So kann eine Funktion allein auf Grund der zum Einsatz kommenden Art der Bearbeitung vertraulich sein, und nicht auf Grund der Vertraulichkeit der von ihr bearbeiteten Informationen.
  - Der Zugriff auf eine Dienstleistung kann keine besonders starke Disponibilität erfordern, der geordnete Betrieb dieses Dienstes kann hingegen eine maximale Disponibilität der benötigten Informationen beanspruchen.

Aktivität 2.2 - Zusammenfassung der Sicherheitsbedarfe



BESCHREIBUNG

Ziel dieser Aktivität ist es, den wesentlichen Elementen die entsprechenden Sicherheitsbedarfe zuzuordnen, die aus der Synthese der von den Nutzern vergebenen Werte hervorgegangen sind. Am Ende dieser Aktivität verfügt man über eine objektive und kohärente Vision der Sicherheitsbedarfe des Zielsystems. Es handelt sich um eine Aktivität, die zur Einschätzung der Risiken im Rahmen des Risikomanagements beiträgt.

VORBEDINGUNGEN

- Aktivität 2.1.

EINGANGSDATEN

- Liste der wesentlichen Elemente.
- Liste der Sicherheitskriterien.
- Bedürfnisskala.
- Liste der Auswirkungen.

AKTIONEN

- Jedem wesentlichen Element ein Sicherheitsbedarf pro Sicherheitsgrundwert (Verfügbarkeit, Integrität, Zuverlässigkeit usw.) zuweisen.

AUSGANGSDATEN

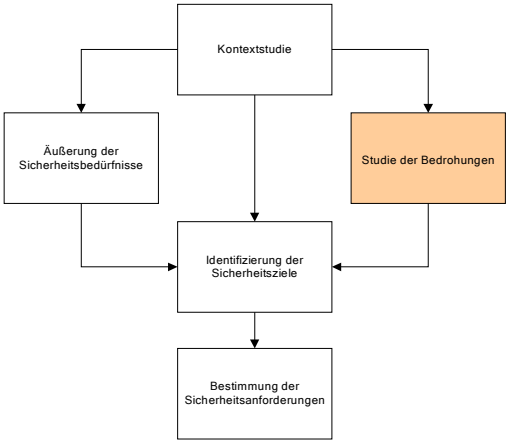
- Syntheseblatt der Sicherheitsbedarfsanalyse.

PRAKTISCHE HINWEISE

- Die Zuweisung der Sicherheitsbedarfe zu den wesentlichen Elementen stellt die für die Institution akzeptierbare Grenze dar.
- Die Einschätzung der Sicherheitsbedarfe entspricht der Vision, die ein Nutzer von dem System haben kann; dieser muss daher extreme Werte seiner Sichtweise rechtfertigen, damit später auf Institutionsebene eine kohärente Zusammenfassung gewährleistet werden kann.
- Alle Sicherheitsbedarfe sind so weit wie möglich zu rechtfertigen.
- Die Nutzer, die für die Einschätzung der Sicherheitsbedarfe ausgewählt wurden, müssen für die Systembenutzung repräsentativ sein. Sie müssen sich zu den Elementen äußern, die sie gewöhnlich benutzen.
- Jedem wesentlichen Element können bei der funktionellen Beschreibung die Sicherheitsbedarfe hinzugefügt und bei der schematischen Darstellung beigeordnet werden. Eventuelle Abhängigkeiten zwischen den Sicherheitsbedarfswerten können dadurch offensichtlicher werden. In der Tat sind die Sicherheitsbedarfe von Funktionen und Informationen gelegentlich miteinander verknüpft, gleiches gilt für mehrere Funktionen oder mehrere Informationen untereinander. Sobald Elemente miteinander verknüpft sind, besteht die Möglichkeit der Weiterverbreitung.

Schritt 3 – Bedrohungsanalyse

Dieser Schritt trägt zur Risikobewertung bei. Er hat zum Ziel, die auf dem System lastenden Bedrohungen zu bestimmen.



Die Formalisierung der Bedrohungen erfolgt durch Identifizierung der einzelnen Komponenten: Die Angriffsmethoden, denen die Institution ausgeliefert ist, die bedrohenden Elemente, die diese Methoden einsetzen können und die Schwachstellen der einzelnen Systemeinheiten einschließlich deren Niveau, die ausgenutzt werden können.

Die im Verlauf dieses Schrittes erkannten Bedrohungen sind für das System spezifisch. Ihre Charakterisierung ist unabhängig von den Sicherheitsbedarfen, den verarbeiteten Informationen und den vom System unterstützten Funktionen.

Die Bedrohungsanalyse besteht aus drei Aktivitäten:

- Untersuchung der Ursprünge der Bedrohungen
- Studie der Schwachstellen
- Formalisierung der Bedrohungen

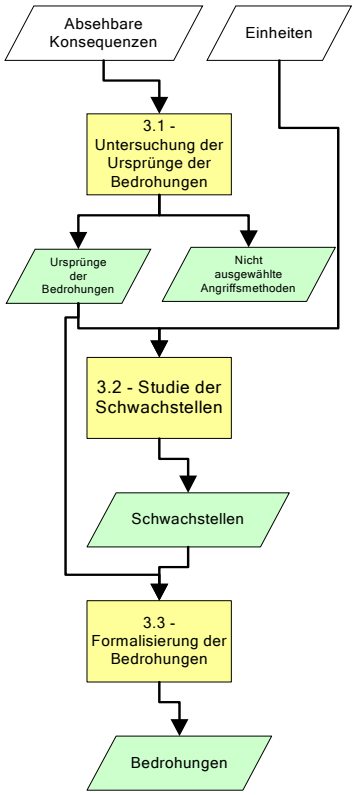
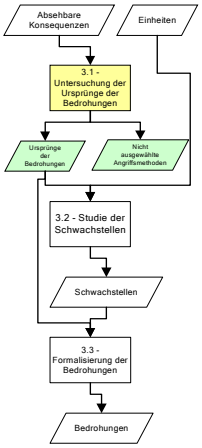


Abbildung 4 – Synoptische Darstellung der Bedrohungsanalyse

Aktivität 3.1 – Untersuchung der Ursprünge der Bedrohungen



BESCHREIBUNG

Ziel dieser Aktivität ist es, die für das Zielsystem relevanten Angriffsmethoden herauszustellen. Jede Angriffsmethode wird durch die Sicherheitskriterien charakterisiert, die sie beeinträchtigen kann (Verfügbarkeit, Integrität, Vertraulichkeit usw.). Jeder Methode werden bedrohende Elemente zugeordnet. Die bedrohenden Elemente sind durch ihre Art (natürlich bedingt, menschlich bedingt oder umgebungsbedingt) und ihre mögliche Ursache (unbeabsichtigt, vorsätzlich) charakterisierbar. Aus dieser Charakterisierung lässt sich ein Angriffspotential ableiten. Wenn die Angriffsmethoden tatsächliche Risiken für das Zielsystem darstellen, muss das Niveau der Sicherheitsmaßnahmen diesem Angriffspotential entsprechen. Diese Aktivität dient der Identifikation von Quellen im Rahmen des Risikomanagements.

VORBEDINGUNGEN

- Aktivität 1.2.

EINGANGSDATEN

- Liste der absehbaren Konsequenzen für das Zielsystem.

AKTIONEN

- Relevante Angriffsmethoden auflisten.
- Die Angriffsmethoden durch Sicherheitskriterien charakterisieren, die sie beeinträchtigen können.
- Für jede festgestellte Angriffsmethode die entsprechenden bedrohenden Elemente durch ihre Art (natürlich beding, menschlich bedingt, umgebungsbedingt) und ihre Ursache (unbeabsichtigt, vorsätzlich) charakterisieren.
- Einen dem Angriffspotential des bedrohenden Elementes entsprechenden Wert zuweisen.
- Die nicht berücksichtigten Angriffsmethoden einschließlich Begründung hervorheben.

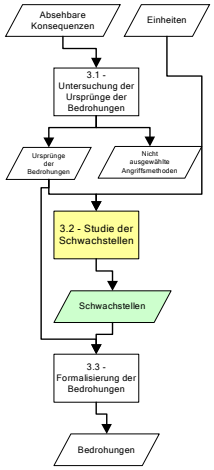
AUSGANGSDATEN

- Liste mit den Ursprüngen der Bedrohungen (bedrohende Elemente und Angriffsmethoden).
- Liste der nicht berücksichtigten Angriffsmethoden einschließlich Begründung.

PRAKTISCHE HINWEISE

- Es ist ratsam, zur Auflistung und Charakterisierung der relevanten Angriffsmethoden und bedrohenden Elemente die allgemeinen Angriffsmethoden und bedrohenden Elemente zu Grunde zu legen, die im Leitfaden "Mittel zur IT-Risikobewertung" beschrieben sind.
- Die Angriffsmethoden werden von einem Sicherheitsbeauftragten in Zusammenarbeit mit dem Verantwortlichen des betroffenen Systems bzw. der untersuchten Aufgaben erfasst
- Die Begründungen, warum bestimmte Methoden berücksichtigt wurden und andere nicht, sind eindeutig zu formulieren.
- Die Charakterisierung bedrohender Elemente sollte zudem in Form eines Wertes ausgedrückt werden, der dem Angriffspotential entspricht, umso leichter lässt sich die Widerständigkeit der Mechanismen bezüglich der Sicherheitsziele und –anforderungen bestimmen.

Aktivität 3.2 – Studie der Schwachstellen



BESCHREIBUNG

Ziel dieser Aktivität ist es, die spezifischen Schwachstellen des Zielsystems zu bestimmen und eventuell nach Niveaus zu charakterisieren. Diese tatsächlichen Schwachstellen des Zielsystems resultieren aus den jeweiligen Eigenschaften der einzelnen Systemeinheiten. Da Schwachstellen ausgenutzt werden, um die Sicherheit des Systems zu beeinträchtigen, muss es bei den Sicherheitszielen darum gehen, diese spürbar einzuschränken. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivitäten 1.3 und 3.1.

EINGANGSDATEN

- Liste der Entitäten.
- Liste mit den Ursprüngen der Bedrohungen (bedrohende Elemente und Angriffsmethoden).

AKTIONEN

- Die Schwachstellen der Entitäten nach Angriffsmethoden identifizieren.
- Eventuell das Niveau der Schwachstellen einschätzen.

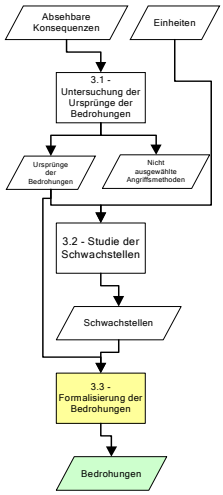
AUSGANGSDATEN

- Liste der berücksichtigten Schwachstellen und deren Niveau.

PRAKTISCHE HINWEISE

- Es ist ratsam, zur Identifizierung der Schwachstellen der Entitäten nach Angriffsmethoden die allgemeinen Schwachstellen zu Grunde zu legen, die im Leitfaden "Mittel zur IT-Risikobewertung" beschrieben sind.
- Die Studie der Schwachstellen wird mit den gleichen Verantwortlichen durchgeführt, die auch bei der Untersuchung der Ursprünge der Bedrohungen zu Rate gezogen wurden.
- Wenn die Liste der vorgestellten Angriffsmethoden dank ihres allgemeinen Charakters Anspruch auf Vollständigkeit erheben kann, so ist die Liste der Schwachstellen von Natur aus variabel und muss dementsprechend individuell angepasst werden.

Aktivität 3.3 – Formalisierung der Bedrohungen



BESCHREIBUNG

Ziel dieser Aktivität ist es, die Bedrohungen festzustellen, die das Zielsystem angreifen können. Die Bedrohungen ergeben sich aus einer Verknüpfung der Angriffsmethoden (die von identifizierten bedrohenden Elementen benutzt werden) mit den berücksichtigten Schwachstellen (die auf den identifizierten Entitäten lasten). Am Ende dieser Aktivität verfügt man über eine objektive und vollständige Vision der tatsächlich auf dem Zielsystem lastenden Bedrohungen. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivitäten 3.1 und 3.2.

EINGANGSDATEN

- Liste mit den Ursprüngen der Bedrohungen (bedrohende Elemente und Angriffsmethoden).
- Liste der berücksichtigten Schwachstellen und deren Niveau.

AKTIONEN

- Die Bedrohungen formell äußern.
- Die Bedrohungen eventuell nach den möglichen Wahrscheinlichkeiten hierarchisieren.

AUSGANGSDATEN

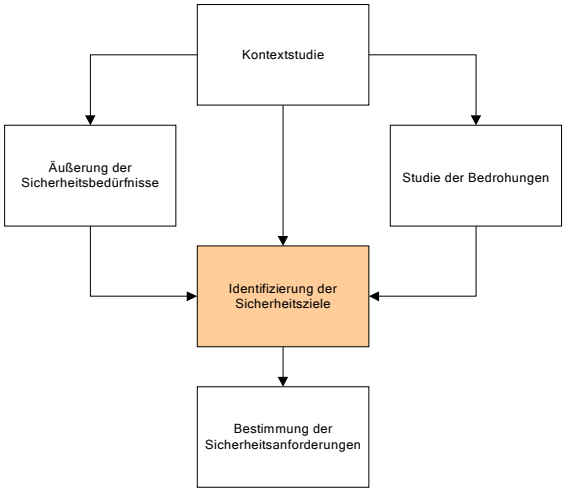
- Liste der berücksichtigten Bedrohungen.

PRAKTISCHE HINWEISE

- Die Formalisierung der Bedrohungen muss so genau wie möglich sein und die Angriffsmethode, das bedrohende Element, die ausgenutzte(n) Schwachstelle(n) und die betroffenen Entitäten deutlich machen.
- Die Bedrohungen sind nach Wahrscheinlichkeiten charakterisierbar. Dabei hängt die Bestimmung einer Wahrscheinlichkeit vom Niveau der Schwachstellen ab, die von den bedrohenden Elementen ausgenutzt werden.

Schritt 4 - Identifizierung der Sicherheitsziele

Ziel dieses Schrittes ist es, die auf dem System lastenden Risiken einzuschätzen und zu behandeln.



Durch Gegenüberstellung von Bedrohungen und Sicherheitsbedarfen können die Risiken, die durch die Sicherheitsziele abgedeckt werden sollen, deutlich gemacht werden. Diese Sicherheitsziele stellen das Sicherheitslastenheft für das Zielsystems und seine Umgebung dar. Sie müssen mit der Gesamtheit aller Hypothesen, Zwänge, Vorschriftsreferenzen und Sicherheitsvorschriften kohärent sein, die im Laufe der Studie identifiziert wurden.

Während dieses Schrittes müssen auch das Niveau der Sicherheitsziele und das Gewährleistungsniveau festgelegt werden.

Dieser Schritt besteht aus drei Aktivitäten:

- Gegenüberstellung von Bedrohungen und Bedürfnissen
- Formalisierung der Sicherheitsziele
- Bestimmung der Sicherheitsniveaus

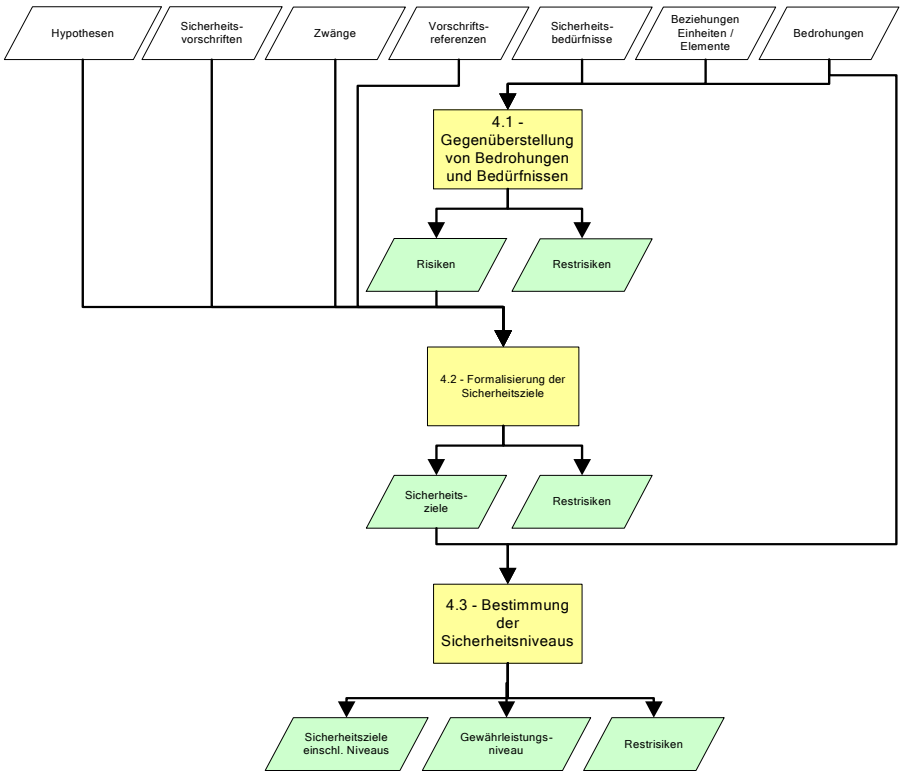
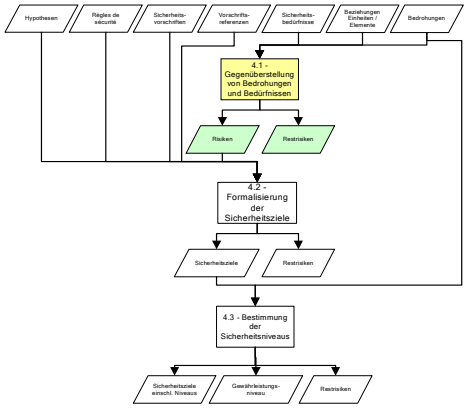


Abbildung 5 – Synoptische Darstellung der Identifizierung der Sicherheitsziele

Aktivität 4.1 – Gegenüberstellung von Bedrohungen und Bedürfnissen



BESCHREIBUNG

Ziel dieser Aktivität ist es, die Risiken festzustellen, die tatsächlich auf dem Zielsystem lasten. Durch die Gegenüberstellung von Bedrohungen und Sicherheitsbedarfen können die Risiken festgestellt und hierarchisiert werden, die wirklich imstande sind, die wesentlichen Elemente anzugreifen. Alle erkannten Risiken müssen eingeschätzt, und die meisten von ihnen müssen durch Sicherheitsziele abgedeckt werden. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivitäten 1.3, 2.2 und 3.3.

EINGANGSDATEN

- Beziehungen Entitäten / Elemente.
- Syntheseblatt der Sicherheitsbedarfsanalyse.
- Liste der berücksichtigten Bedrohungen.

AKTIONEN

- Die Risiken durch Gegenüberstellung von Bedrohungen und Sicherheitsbedarfen festlegen.
- Die Risiken formell äußern.
- Die Risiken nach Auswirkung auf die wesentlichen Elemente und Wahrscheinlichkeit der Bedrohungen hierarchisieren.
- Die nicht berücksichtigten Risiken (Restrisiken) einschließlich Begründung hervorheben.

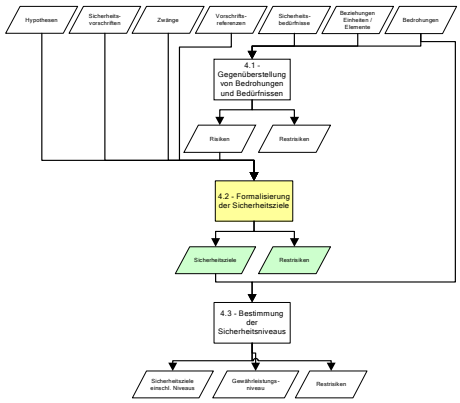
AUSGANGSDATEN

- Hierarchisierte Risikoliste.
- Liste der Restrisiken (fehlende Risikoabdeckung) einschließlich Begründungen.

PRAKTISCHE HINWEISE

- Je genauer ein Risiko formuliert wurde, umso einfacher ist es für den Leser, das Risiko nachzuvollziehen und für diejenigen, die die Studie durchführen, präzise und konkrete Sicherheitsziele zu identifizieren. Tatsächlich hat das Risiko einen besonderen Stellenwert im Zielsystem. Die Bezeichnung eines Risikos kann das bedrohende Element, die ausgenutzten Schwachstellen, die Entitäten, auf denen diese beruhen, die eventuell betroffenen wesentlichen Elemente und die möglichen Konsequenzen im Hinblick auf die Sicherheitsbedarfe und Auswirkungen umfassen.
- Nicht die Personen, die die Studie durchführen, sollen die Risiken hierarchisieren, sondern die Nutzer und die Verantwortlichen des Systems. Dennoch kann die Studie bei der Bewerkstelligung dieser Aufgabe helfen. Höchstwerte bei den Sicherheitsbedarfen, die von den Risiken getroffen werden können und bei den Bedrohungswahrscheinlichkeiten helfen beispielsweise, die Bedeutung von Risiken richtig einzuschätzen.
- Durch die Klassifizierung der Risiken können Prioritäten bei der Auswahl und Realisierung von Gegenmaßnahmen festgelegt werden.

Aktivität 4.2 - Formalisierung der Sicherheitsziele



BESCHREIBUNG

Ziel dieser Aktivität ist es, Sicherheitsziele festzulegen, mit denen die Risiken entsprechend den festgelegten Sicherheitsniveaus abgedeckt werden können. Dabei ist nachzuweisen, dass alle Risiken durch die Sicherheitsziele unter Berücksichtigung der Hypothesen, Sicherheitsvorschriften und Zwänge vollständig abgedeckt sind. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivitäten 1.1, 1.2, 2.4 und 4.1.

EINGANGSDATEN

- Liste der Hypothesen.
- Liste der Sicherheitsvorschriften.
- Liste der Zwänge.
- Liste der Vorschriftsreferenzen.
- Wahl des Sicherheitsbetriebsmodus.
- Hierarchisierte Risikoliste.

AKTIONEN

- Die Sicherheitsziele auflisten.
- Die vollständige Abdeckung nachweisen, wobei die Kompatibilität der auf der Institution und dem Zielsystem lastenden Zwänge mit:
  - den Risiken,
  - den Hypothesen (und den absehbaren Konsequenzen),
  - den Sicherheitsvorschriften (und den Vorschriftsreferenzen) zu überprüfen ist.
- Die Sicherheitsziele eventuell in zwei Kategorien einstufen:
  - Sicherheitsziele, die das Zielsystem betreffen,
  - Sicherheitsziele, die die Umgebung des Zielsystems betreffen.
- Die fehlenden Abdeckungen (Restrisiken) einschließlich Begründung hervorheben.

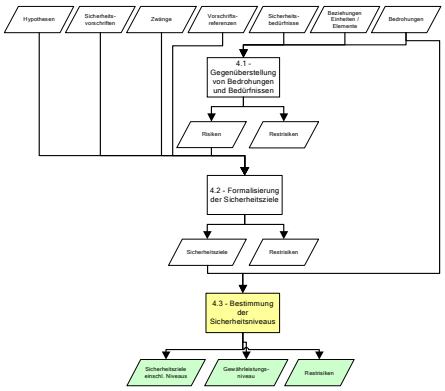
AUSGANGSDATEN

- Liste der Sicherheitsziele.
- Liste der Restrisiken (fehlende Abdeckung durch die Sicherheitsziele) einschließlich Begründungen.

PRAKTISCHE HINWEISE

- 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 Sicherheitsziele können, was die Sicherheitslösungen zur Abdeckung der Risiken anbelangt, als offenes Sicherheitslastenheft dienen.

Aktivität 4.3 - Bestimmung der Sicherheitsniveaus



BESCHREIBUNG

Ziel dieser Aktivität ist es, für die Sicherheitsziele ein angemessenes Widerstandsniveau festzulegen. Zudem kann das Niveau der Anforderungen zur Gewährleistung der Sicherheit bestimmt werden. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivitäten 3.3 und 4.2.

EINGANGSDATEN

- Liste der Sicherheitsziele.
- Liste der berücksichtigten Bedrohungen.

AKTIONEN

- Für jedes Sicherheitsziel das angemessene Widerstandsniveau festlegen.
- Das Niveau der Gewährleistungsanforderungen auswählen.

AUSGANGSDATEN

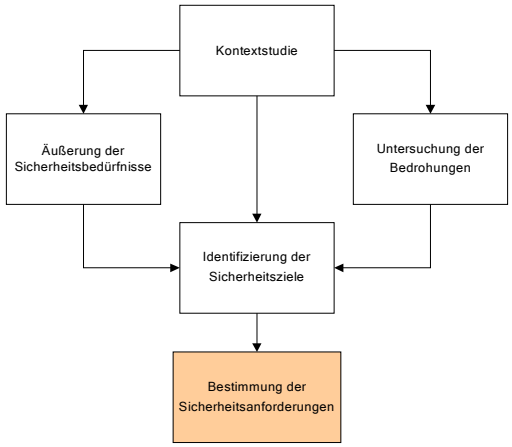
- Liste der Sicherheitsziele mit Widerstandsniveau.
- Liste der Restrisiken (fehlende Abdeckung des Widerstandsniveaus durch die Sicherheitsziele) einschließlich Begründungen.
- Auswahl des Niveaus der Gewährleistungsanforderungen.

PRAKTISCHE HINWEISE

- Mit Hilfe des Angriffspotentials der bedrohenden Elemente kann ein angemessenes Widerstandsniveau der Sicherheitsziele bestimmt werden. Dabei hängt dieses Niveau neben dem Angriffspotential von weiteren Faktoren wie z. B. den Zwängen, den Sicherheitsbedarfen oder der Bedrohungswahrscheinlichkeit ab.

Schritt 5 - Bestimmung der Sicherheitsanforderungen

Ziel dieses Schritts ist es zu bestimmen, wie die Sicherheitsziele erreicht werden können, d. h. wie die das System bedrohenden Risiken behandelt werden können.



Dazu werden folgende Bestimmungen festgelegt:

- Die funktionellen Sicherheitsanforderungen, die das erwartete Sicherheitsverhalten beschreiben und die dazu bestimmt sind, den im vorhergehenden Schritt formulierten Sicherheitsanforderungen zu genügen,
- die Sicherheitsgewährleistungsanforderungen, die insofern die Basis der Vertrauenswürdigkeit bilden, als dass das Produkt oder System ihren Sicherheitszielen genügt.

Diese Anforderungen können beispielsweise ausgehend von funktionellen und Gewährleistungskomponenten erstellt werden, wie sie in den common criteria [ISO 15408] angeboten werden.

Die Abdeckung der Sicherheitsziele durch funktionelle Anforderungen oder Gewährleistungsanforderungen muss in Form einer Auflistung von Argumenten nachgewiesen werden, wobei deren Notwendigkeit und Hinlänglichkeit anzugeben ist.

Dieser Schritt umfasst zwei Hauptaktivitäten:

- Bestimmung der funktionellen Sicherheitsanforderungen
- Bestimmung der Sicherheitsgewährleistungsanforderungen

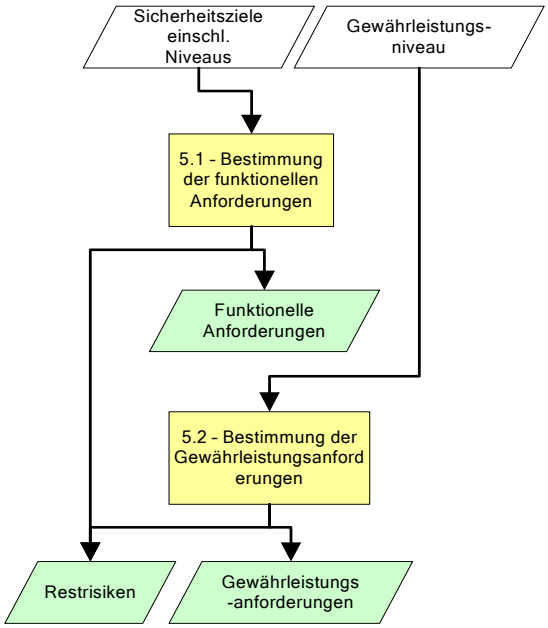
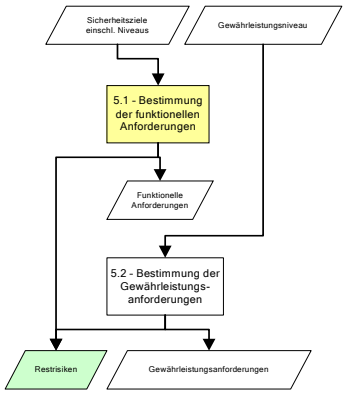


Abbildung 6 – Synoptische Darstellung der Bestimmung der Sicherheitsanforderungen

Aktivität 5.1 - Bestimmung der funktionellen Sicherheitsanforderungen



BESCHREIBUNG

Ziel dieser Aktivität ist es, die funktionellen Sicherheitsanforderungen zu bestimmen, mit denen die für das Zielsystem identifizierten Sicherheitsziele abgedeckt werden können. Danach kann entschieden werden, wie jedes identifizierte Risiko zu behandeln ist. Die Risiken können verweigert, optimiert übertragen oder angenommen werden, das Restrisiko muss eindeutig identifiziert und akzeptiert werden. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivität 4.3.

EINGANGSDATEN

- Liste der Sicherheitsziele mit Widerstandsniveau.

AKTIONEN

- Die funktionellen Sicherheitsanforderungen auflisten.
- Die Vollständigkeit der Abdeckung der Sicherheitsziele nachweisen.
- Eventuell fehlende Abdeckungen (Restrisiken) einschließlich Begründung hervorheben.
- Die funktionellen Sicherheitsanforderungen in zwei Kategorien einstufen:
  - funktionelle Sicherheitsanforderungen, die das Zielsystem betreffen,
  - funktionelle Sicherheitsanforderungen, die die Umgebung des Zielsystems betreffen.
- Eventuell die Abdeckung der Abhängigkeiten der funktionellen Sicherheitsanforderungen nachweisen.

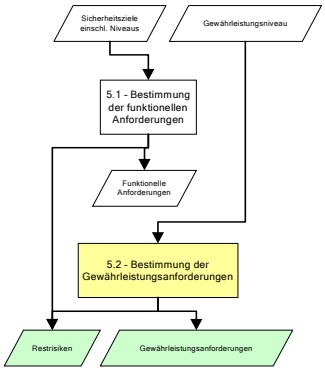
AUSGANGSDATEN

- Liste der nachgewiesenen funktionellen Sicherheitsanforderungen.
- Liste der Restrisiken (fehlende Abdeckung durch die funktionellen Sicherheitsanforderungen) einschließlich Begründungen.

PRAKTISCHE HINWEISE

- Zur Auflistung der funktionellen Sicherheitsanforderungen, die den die Schwachstellen abdeckenden Sicherheitszielen genügen sollen, können die allgemeinen funktionellen Sicherheitsanforderungen und die Tabelle zur Festlegung der Sicherheitsziele und –anforderungen des Leitfadens "Mittel zur Behandlung von IT-Risiken" herangezogen werden.
- Die funktionellen Sicherheitsanforderungen können unter den funktionellen Komponenten der Wissensdatenbank ausgewählt oder aus freien Stücken abgefasst werden. Jedes Sicherheitsziel muss durch mindestens eine Sicherheitsanforderung abgedeckt und die komplette Abdeckung muss ordnungsgemäß nachgewiesen werden. Die Anforderungen werden anschließend so weit wie möglich verfeinert und Abhängigkeiten zwischen Komponenten müssen untersucht und begründet werden.
- Je nach Niveau der Systemuntersuchung müssen die Komponenten nicht unbedingt verfeinert werden, es ist dann jedoch darauf hinzuweisen, dass die Verfeinerung durch den Auftragnehmer im Rahmen dessen Antwort zu erfolgen hat.

Aktivität 5.2 - Bestimmung der Sicherheitsgewährleistungs-anforderungen



BESCHREIBUNG

Ziel dieser Aktivität ist es, alle Anforderungen, die an die Gewährleistung der Sicherheit des Zielobjekts der Sicherheitsstudie gestellt werden, lückenlos zu bestimmen. Die Auswahl der Anforderungen erfolgt in Abhängigkeit des Gewährleistungsniveaus, das bei Bestimmung der Sicherheitsniveaus gewählt wurde. Sie bilden insofern die Basis der Vertrauenswürdigkeit, als das Zielsystem seinen Sicherheitszielen genügt. Diese Aktivität trägt zur Einschätzung der Risiken im Rahmen des Risikomanagements bei.

VORBEDINGUNGEN

- Aktivität 4.3.

EINGANGSDATEN

- Auswahl des Niveaus der Gewährleistungsanforderungen.

AKTIONEN

- Die Sicherheitsgewährleistungsanforderungen auflisten.
- Eventuell die Sicherheitsgewährleistungsanforderungen in zwei Kategorien einstufen:
  - Sicherheitsgewährleistungsanforderungen, die das Zielsystem betreffen,
  - Sicherheitsgewährleistungsanforderungen, die die Umgebung des Zielsystems betreffen.
- Eventuell die Abdeckung der Abhängigkeiten der Sicherheitsgewährleistungsanforderungen nachweisen.

AUSGANGSDATEN

- Liste der nachgewiesenen Sicherheitsgewährleistungsanforderungen.
- Liste der Restrisiken (fehlende Abdeckung durch die Sicherheitsgewährleistungsanforderungen) einschließlich Begründungen.

PRAKTISCHE HINWEISE

- Die Sicherheitsgewährleistungsanforderungen können unter den funktionellen Komponenten der Wissensdatenbank ausgewählt oder aus freien Stücken abgefasst werden.

Anhang – Erstellte Daten

- Vorstellung der Institution.
- Auflistung der auf der Institution lastenden allgemeinen Zwänge.
- Auflistung der von der Institution anzuwendenden Vorschriftsreferenzen.
- Konzeptuelle Architektur des IT-Systems.
- Vorstellung des Zielsystems.
- Liste der wesentlichen Elemente.
- Funktionelle Beschreibung des Zielsystems.
- Liste der absehbaren Konsequenzen des Zielsystems.
- Liste der Hypothesen.
- Liste der Sicherheitsvorschriften.
- Liste der speziellen Zwänge des Zielsystems.
- Liste der speziellen Vorschriftsreferenzen des Zielsystems.
- Liste der Entitäten.
- Beziehungen Entitäten / Elemente.
- Liste der Sicherheitskriterien.
- Bedürfnisskala.
- Liste der Auswirkungen.
- Syntheseblatt der Sicherheitsbedarfsanalyse.
- Wahl des Sicherheitsbetriebsmodus.
- Liste mit den Ursprüngen der Bedrohungen (bedrohende Elemente und Angriffsmethoden).
- Liste der nicht berücksichtigten Angriffsmethoden einschließlich Begründung.
- Liste der berücksichtigten Schwachstellen und deren Niveau.
- Liste der berücksichtigten Bedrohungen.
- Hierarchisierte Risikoliste.
- Liste mit Restrisiken (fehlende Risikoabdeckung) einschließlich Begründungen.
- Liste der Sicherheitsziele.
- Liste der Restrisiken (fehlende Abdeckung durch die Sicherheitsziele) einschließlich Begründungen.
- Liste der Sicherheitsziele mit Widerstandsniveau.
- Liste mit Restrisiken (fehlende Abdeckung des Widerstandsniveaus durch die Sicherheitsziele) einschließlich Begründungen.
- Auswahl des Niveaus der Gewährleistungsanforderungen.
- Liste der nachgewiesenen funktionellen Sicherheitsanforderungen.
- Liste der Restrisiken (fehlende Abdeckung durch die funktionellen Sicherheitsanforderungen) einschließlich Begründungen.
- Liste der nachgewiesenen Sicherheitsgewährleistungsanforderungen.
- Liste der Restrisiken (fehlende Abdeckung durch die Sicherheitsgewährleistungs-anforderungen) einschließlich Begründungen.

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
- U 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