Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

EBIOS

MÉMENTO

Version vom 4. Februar 2004

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

Warum hat EBIOS einen solchen Erfolg?

Eine Referenzmethode in puncto IT-Risikoanalyse

Die von EBIOS vorgeschlagene methodologische Vorgehensweise ermöglicht **eine globale und kohärente Vision** der IT-Sicherheit. Sie liefert ein einheitliches Vokabular und gemeinsame Konzepte, bildet ein zusammenhängendes Ganzes und ermöglicht es, angepasste Sicherheitsvorgaben und -anforderungen zu bestimmen. Die Methode berücksichtigt alle technischen (Software, Hardware, Netzwerke) und nicht-technischen Entitäten (Organisation, Faktor Mensch, physische Sicherheit). Sie ermöglicht die Einbeziehung aller IT-Sicherheitsakteure in die Sicherheitsproblematik. Zusätzlich schlägt sie eine dynamische Vorgehensweise vor, welche die Interaktionen zwischen den verschiedenen Tätigkeitsbereichen und Funktionen der Organisation begünstigt und den gesamten Lebenszyklus des Systems betrachtet (Entwurf, Realisation, Einsatz, Wartung usw.)

Von der DCSSI gefördert und von **den französischen Behörden anerkannt ist EBIOS auch eine Bezugsgröße im Privatsektor und im Ausland**. In diesem Zusammenhang öffnet ihr die Übersetzung ins Deutsche und ins Englische sowie die Übereinstimmung mit internationalen Normen noch bessere Perspektiven. 2002 stufen internationale Vergleiche EBIOS unter die drei besten IT-Risikoanalysen ein.

Zahlreiche Institutionen des öffentlichen und privaten Sektors nutzen die Methode, **um IT-Risikoanalysen durchzuführen oder durchführen zu lassen**: Die Behörden (in bestimmten Behörden systematisch, in allen übrigen empfohlen), das Nationale Weltraumforschungszentrum CNES (Centre national d'études spatiales), das Atomenergie-Kommissariat CEA (Commissariat à l'énergie atomique), die staatliche Krankenkasse CNAM (Caisse nationale d'assurance maladie), der Kreditkarten-Verband "CB", ALCATEL CIT, Gesundheitsämter, die Pariser Flughafengesellschaft ADP (Aéroports de Paris), der Europarat usw.

Im Übrigen **haben mehrere Beratungsbüros** in ihrer Rolle als Berater der Auftraggeber **die EBIOS-Methode angenommen**.

Es ist darauf hinzuweisen, dass in Frankreich ein Minister oder ein Industrieunternehmer ein FEROS (spezielles Pflichtenheft im Hinblick auf die IT-Sicherheit) erstellen muss; sobald ein System als geheim eingestufte Informationen verarbeitet. EBIOS ist das ideale Mittel für diese Arbeit, da sich die Ergebnisse dieser Methode direkt in ein FEROS einfügen lassen.

Einfache Vorgehensweise und angepasste Ergebnisse

Die EBIOS-Methode **ist leicht zu verstehen und anzuwenden**. Ihre Grundphilosophie ist einfach, intuitiv und ihr Ablauf natürlich. Die Methode besteht darin, Sicherheitsbedarfe und Bedrohungen zu formalisieren und die Risiken zu bestimmen, denen eine Institution ausgesetzt ist.

Jedermann kann sich die Methode aneignen und sein persönliches Vorgehen den jeweils untersuchten Themen anpassen. EBIOS wurde sowohl auf einfache (z. B. Web-Server) als auch auf komplexe Systeme (z. B. Steuerungssysteme für Auswahlverfahren und Personal, die verschiedene Verknüpfungen benötigen), auf noch anzulegenden wie auf bereits bestehende Systeme sowie auf vollständige wie auch auf IT-Teilsysteme angewandt.
Ein einziges Tool ermöglicht die Verwirklichung verschiedener sicherheitsrelevanter Maßnahmen, die mit dem IT-Risikomanagement verbunden sind. EBIOS wird effektiv genutzt,

um zur Erstellung eines IT-Sicherheitsstrategie beizutragen, die ersten Etappen einer IT-Sicherheits-Policy bzw. -Leitlinie und eines IT-Kontrollschemas zu realisieren, zur Ausarbeitung eines Schutzprofils (protection profiles) beizutragen, ein FEROS oder jedes andere IT- Lasten- oder Pflichtenheft abzufassen.

Die EBIOS-Methode hilft bei der Definition von Aufgaben, die der Auftraggeber wahrzunehmen hat. Die Methode ermöglicht es nämlich, den Umfang der Studie unter Bewahrung einer Globalsicht des in seinem Kontext studierten Systems zu bestimmen, die Bedarfe zu analysieren (gebunden an die zu schützenden Güter), die Bedrohungen zu identifizieren und einen Projektplan sowie die Verantwortlichkeiten zu definieren.

Die EBIOS-Methode ist für die Projektleitung ein hervorragendes Mittel, um die vom Auftraggeber definierten Ziele zu verfolgen, um auf Fragen nach der Durchführbarkeit und den damit verbundenen Kosten und Fristen zu antworten und um schließlich entsprechende Lösungen auszuwählen.

Es handelt sich auch um ein Werkzeug zur Messung der Auswirkungen und als Basis für Verhandlungen zwischen dem Auftraggeber und den Führungskräften (des Projekts, der Institution usw.), welches letzteren die Möglichkeit bietet, die Angemessenheit das IT-System zu kontrollieren und die Untersuchungen sowie die IT-Sicherheit zu zentralisieren.

Die **Kompatibilität mit anderen methodologischen IT-Sicherheits-Tools** ermöglicht die Wahrung einer vollkommenen Kohärenz beim IT-Risikomanagement. So können beispielsweise die Normen ISO/IEC 15408 und ISO/IEC 17799 zur Bestimmung der Sicherheitsvorgabe und –anforderungen herangezogen werden.

Software-Tool mit freier Lizenz

Dieses kostenlose Softwareprogramm ist auf einfache Anfrage bei der DCSSI (conseil.dcssi@sgdn.pm.gouv.fr) erhältlich. Dank einfacher Handhabung wird **die Durchführung von IT-Risikoanalysen erheblich vereinfacht** und die Möglichkeit zur Vorbereitung verschiedener Synthesedokumente geboten (Zusammenstellung aller Daten, FEROS, FEROS-Kurzfassung, Schutzprofil, Zusammenstellen strategischer Elemente, Sicherheits-Policy usw.) Darüber hinaus erlaubt es, Wissensdatenbanken und Studien wieder zu verwenden. Mit Quellcodes und Entwurfsdokumentation geliefert, kann es durch alle Benutzer weiterentwickelt werden. Das Softwareprogramm wird als Freeware herausgegeben, ist in UML entworfen und in Java und XML geschrieben.

Starke Ausbildungsnachfrage

Die EBIOS-Ausbildung erleichtert das Verständnis der Methode und ihrer Anwendung. Sie erlaubt den Kursteilnehmern, die empfohlenen Einsatzpraktiken kennen zu lernen und mit anderen Benutzern der Methode Gedanken auszutauschen. Der zweitägige Schulungskurs wird im IT-Sicherheits-Ausbildungszentrum CFSSI (Centre de Formation en Sécurité des Systèmes d'Information - http://www.ssi.gouv.fr/formation/index.html) angeboten. Das Beratungsbüro der DCSSI conseil.dcssi@sgdn.pm.gouv.fr steht den Kursteilnehmern zur Verfügung, um eine Betreuung ihres Risikoanalyseprojekts zu gewährleisten. Die Ausbildung orientiert sich an einer Fallstudie, anhand derer die Methodik konkret dargestellt wird und Beispiele geliefert werden, auf die man sich bei den ersten Anwendungen der Methode beziehen kann.

Darüber hinaus wurde auch eine Session für EBIOS-Ausbilder zur Sicherstellung der Weitergabe der Methode innerhalb der Behörden eingerichtet.

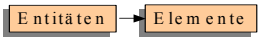
Gründung des EBIOS-Clubs

Zum Austausch von Erfahrungen und zur Verbesserung der Methode und ihrer Arbeitsmittel hat die Zentraldirektion für die IT-Sicherheit (DCSSI) 2003 den EBIOS-Club gegründet.

Hier haben Anwender, die an der Weiterentwicklung der Methode und neuesten Informationen interessiert sind, die Möglichkeit zu regelmäßigen Treffen.

Prinzipien der EBIOS-Methode

Kontextstudie



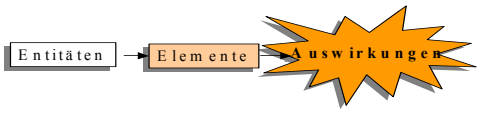
Ein IT-System beruht auf **wesentlichen Elementen,** Funktionen und Informationen, die für die Institution die Wertschöpfung des IT-Systems darstellen.

So beruht z. B ein Flugbahnkontrollsystem für den Abschuss einer Rakete auf verschiedenen Informationen wie Parametern oder Rechenergebnissen sowie diversen Funktionen, mit denen diese Berechnungen durchgeführt werden können.

Die wesentlichen Elemente sind mit einer Gesamtheit von **Entitäten** unterschiedlichster Art verknüpft: Hardware, Software, Netzwerke, Organisationen, Personal und Standorte.

Nehmen wir das Beispiel eines Parameters zur Flugbahnberechnung für den Raketenabschuss. Er ist verknüpft mit den Kontrollrechnern, der Anwendersoftware, den Operatoren, der Rakete, den geltenden Vorschriften usw.

Sicherheitsbedarfsanalyse



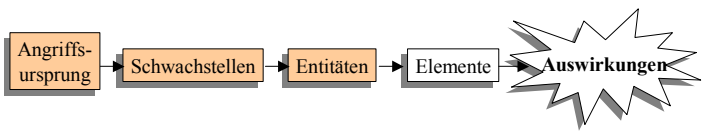
Jedes wesentliche Element hat einen **Sicherheitsbedarf**, damit der Tätigkeitsbereich korrekt funktioniert.

Dieser Sicherheitsbedarf drückt sich in unterschiedlichen Sicherheitsgrundwerten wie Verfügbarkeit, Integrität und Vertraulichkeit aus. Wird dieser Bedarf nicht berücksichtigt, hat dies einen unmittelbaren Einfluss auf die Institution. Die **Auswirkung** kann verschiedene Formen annehmen: finanzielle Verluste, Beeinträchtigung des geordneten Tätigkeitsablauf, Imageverlust, Beeinträchtigung der Sicherheit des Personals, Umweltverschmutzung u. ä.

Nehmen wir das Beispiel des Flugbahnberechnungsparameters für den Raketenabschuss wieder auf. Es handelt sich um eine Information, die einen starken Sicherheitsbedarf in Bezug auf die Verfügbarkeit und die Integrität haben dürfte, um eine Beeinträchtigung der Sicherheit des (Flug-)Personals zu vermeiden.

Bedrohungsanalyse

Im Übrigen ist jede Institution verschiedenen **bedrohenden Elementen** ausgesetzt, und zwar durch sein natürliches Umfeld, seine Kultur, sein Image, seinen Fachbereich usw.



Ein bedrohendes Element ist durch seine **Art** (natürlich bedingt, menschlich bedingt oder umweltbedingt) und seine **Ursache** (unbeabsichtigt oder vorsätzlich) charakterisierbar.

Ihm stehen verschiedene **Angriffsmethoden** zur Wahl, die es zu identifizieren gilt.

Eine Angriffsmethode wird durch die Sicherheitsgrundwerte (Verfügbarkeit, Integrität, Vertraulichkeit...) charakterisiert, die sie beeinträchtigen kann und durch die bedrohenden Elemente, die gewillt sind, diese auch anzuwenden.

Setzen wir unser Beispiel fort. Eine Institution, die Raketen abschießt, muss eine große Zahl von Angriffsmethoden und bedrohenden Elementen berücksichtigen:

- *Physische Unfälle (z. B. Brand),*
- *Natur-Ereignisse (z. B. seismische Phänomene),*
- *Ausfall wesentlicher Dienstleistungen (z. B. Stromausfall),*
- *Infragestellung der Informationen (z. B. durch Ausnutzen einer Software-Schwachstelle),*
- *technische Pannen (z. B. Materialfunktionsstörungen),*
- *physische Aggressionen (z. B. Sabotage),*
- *Fehler (z. B. Interpretationsfehler) usw.*

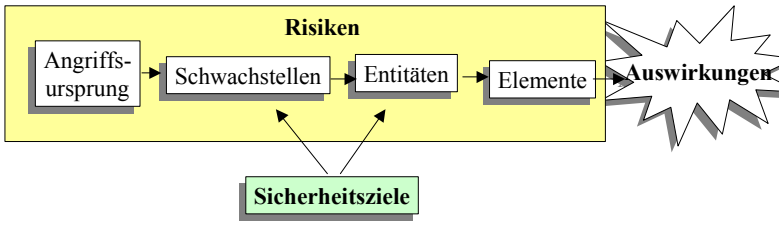
Jede Entität besitzt **Schwachstellen**, die von den bedrohenden Elementen mit der jeweils eigenen Angriffsmethode ausgenutzt werden können.

So kann man mehrere Schwachstellen aufzeigen, die im Zusammenhang mit den Entitäten der Institution stehen, die Raketen abschießt:

- *Möglichkeit des Vorhandenseins versteckter Funktionen, die während der Entwurfs- oder Entwicklungsphase eingeschleust wurden (Software),*
- *Möglichkeit der Verwendung ungeprüften Materials (Hardware),*
- *Möglichkeit der Erzeugung oder Änderung von Systembefehlen (Netzwerke),*
- *Zugriffsmöglichkeit über das Netzwerk auf die Software der Systemressourcen (Netzwerke),*
- *Einfachheit, mit der der Standort durch indirekte Zugänge erreichbar ist (Räumlichkeiten),*
- *Nicht-Einhalten von Vorschriften durch manche Mitarbeiter (Personal),*
- *Fehlende Sicherheitsmaßnahmen während des Entwurfs, der Einrichtung oder der Nutzung des Systems (Organisation) usw.*

Bestimmen der Sicherheitsvorgabe

Es bleibt nur noch zu bestimmen, wie die wesentlichen Elemente von den bedrohenden Elementen und deren Angriffsmethoden in Mitleidenschaft gezogen werden können. Es handelt sich um das **Risiko**.



Das Risiko stellt einen möglichen Schaden dar. Das Risiko ist die Tatsache, dass ein bedrohendes Element wesentliche Elemente mit einer speziellen Angriffsmethode beeinträchtigen kann, indem es die Schwachstellen der auf den wesentlichen Elementen beruhenden Entitäten ausnutzt.

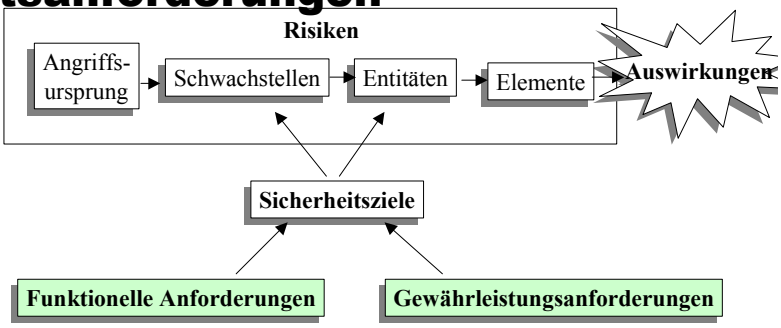
In unserem Beispiel besteht das Risiko in der Infragestellung sensibler Informationen durch Einrichtung von Software-Schwachstellen auf Grund der bestehenden Möglichkeit, netzwerkgebunden Systembefehle zu erzeugen oder zu ändern, was Auswirkungen auf die Sicherheit des Personals und das Image der Institution haben könnte.

Die **Sicherheitsvorgaben** bestehen darin, die Schwachstellen der Einheiten, welche den erkannten Risiken tatsächlich ausgesetzt sind, umfassend abzudecken.

Es ist in der Tat unnütz, etwas zu schützen, was keinem Risiko unterliegt. Es ist auch festzuhalten, dass je bedeutsamer das Angriffspotential ist, desto bedeutsamer ist auch das Niveau der Sicherheitsvorgaben. Die somit identifizierten Ziele bilden somit ein optimal angepasstes Lastenheft.

Eines der Sicherheitsvorgaben für die Raketenabschuss-Institution wäre, die an das Netzwerk gebundene Erzeugung und Änderung von Systembefehlen abzusichern.

Festlegen der Sicherheitsanforderungen



Diejenigen, die damit beauftragt sind, die Methode vor Ort anzuwenden, müssen die im Zusammenhang mit der Sicherheit erwarteten Funktionalitäten genau definieren. Sie müssen zudem die vollständige Abdeckung der Sicherheitsvorgaben durch diese **funktionellen Anforderungen** nachweisen.

In unserem Beispiel wäre folgende funktionelle Anforderung hinsichtlich der Absicherung der netzwerkgebundenen Erzeugung und Änderung von Systembefehlen denkbar: Das System muss während des Normalbetriebs in regelmäßigen Abständen eine Reihe von Selbsttests durchführen, um den korrekten Betrieb nachzuweisen.

Schließlich müssen die Beauftragten **Gewährleistungsanforderungen** definieren, mit denen das geforderte und später nachzuweisende Stufe der Vertrauenswürdigkeit (EAL-Stufe gemäß Common Criteria) erreicht werden kann.

Eine der Gewährleistungsanforderungen ist folgende: Der Entwickler muss unter Beachtung des geforderten Widerstandsniveaus eine Widerstandsanalyse der Systemsicherheitsfunktionen durchführen.

Zusammenfassung

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

Dank einfacher Handhabung und modularem Konzept lässt sich die Methode allen Kontexten und verschiedenen Sicherheitsaktivitäten anpassen. Darüber hinaus erweist sich EBIOS als ein hervorragendes Verhandlungs-, Schieds- und Sensibilisierungsinstrument.

Die Übereinstimmung mit den internationalen Normen, das freie Softwareprogramm, die Ausbildung und der Club der Anwender machen EBIOS zu einer wertvollen Methode, die von Experten der IT-Sicherheit auf höchstem Niveau eingestuft wird.

Weitere Informationen sind erhältlich über:

- die Website der DCSSI http://www.ssi.gouv.fr
- die EBIOS-Mailbox ebios.dcssi@sgdn.pm.gouv.fr
- die Mailbox des Beratungsbüros conseil.dcssi@sgdn.pm.gouv.fr