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

EMPFOHLENE PRAKTIKEN ZUM IT-SICHERHEITS-RISIKOMANAGEMENT

Anwendung der EBIOS®-Methode zur Ausarbeitung einer Produkt-Sicherheitsvorgabe

Version vom 10.11.04

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

Was ist eine Produkt-Sicherheitsvorgabe?

Eine Sicherheitsvorgabe (ST *Security Target)* im Sinne der Norm ISO 15408 – common criteria zur Evaluierung der IT-Sicherheit – ist "eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen TOE dienen" *(*TOE – *Target Of Evaluation* ist der Evaluationsgegenstand, d. h. das untersuchte Produkt).

Es handelt sich um ein Dokument mit genormtem Inhalt, das als Lastenheft dienen kann, in dem der Inhalt eines Schutzprofils (PP) weiter verfeinert wurde, und das auch evaluiert werden kann. Dieses ST bietet insbesondere eine berechtigte Verfeinerung der im Schutzprofil (protection profile) formalisierten Sicherheitsanforderungen an. Es bietet dem Nutzer des TOE die Möglichkeit, sich von der Entsprechung zwischen TOE und seinen Bedürfnissen zu überzeugen.

Außerhalb des technischen Bewertungskontextes (durch die DCSSI zertifizierte Produktevaluation) besteht die Möglichkeit zur Abfassung von IT-Sicherheits-Lastenheften in Form von ST, insbesondere in der Absicht, eine anerkannte Struktur und Terminologie zu benutzen.

Welche Vorteile bietet die EBIOS-Methode zur Ausarbeitung eines Produkt-ST?

Ein Produkt-ST muss vollständig und kohärent sein. Seine Abfassung erfordert eine gewissenhafte Ausarbeitung, doch schlägt die Norm keine Methode zu seiner Realisierung vor. EBIOS ermöglicht die Bereitstellung aller zur Ausarbeitung eines ST notwendigen Elemente und garantiert darüber hinaus deren Kohärenz. Als weitere Vorteile hervorzuheben sind:

- Die Relevanz der die Bedrohungen, Hypothesen, Vorschriften zur Sicherheits-Policy und Sicherheitsanforderungen abdeckenden Sicherheitsziele,
- die Rechtfertigung der Ziele und Anforderungen durch die IT-Risikobewertung,
- die Vollständigkeit der Studie dank ihrer strukturierten Methodik,
- die Einbindung der Beteiligten (Führungskraft, Auftraggeber, Auftragnehmer, Nutzer usw.).

Wie arbeitet man ein Produkt-ST unter Verwendung von EBIOS aus?

Eine effiziente Lösung für das Ausarbeiten eines ST besteht in:

- Der Realisierung einer EBIOS-Studie (über einen dem ST entsprechenden Perimeter) bei gleichzeitiger Verfeinerung der Sicherheitsanforderungen,
- der Abfassung eines Schutzprofil (protection profile) und dessen Validierung im Rahmen der Studie,
- der Entnahme der erforderlichen Daten aus der Studie (ein Großteil der Studie),

- der Abfassung einer Einführung (Identifizierung des ST und Gesamtübersicht),
- einer Neuorganisation der Sicherheitsziele (Einstufung je nach Tragweite),
- einer Neuorganisation der Sicherheitsanforderungen (Einstufung je nach Tragweite),
- der Abfassung der Konformitätsankündigungen mit dem Schutzprofil (protection profile).

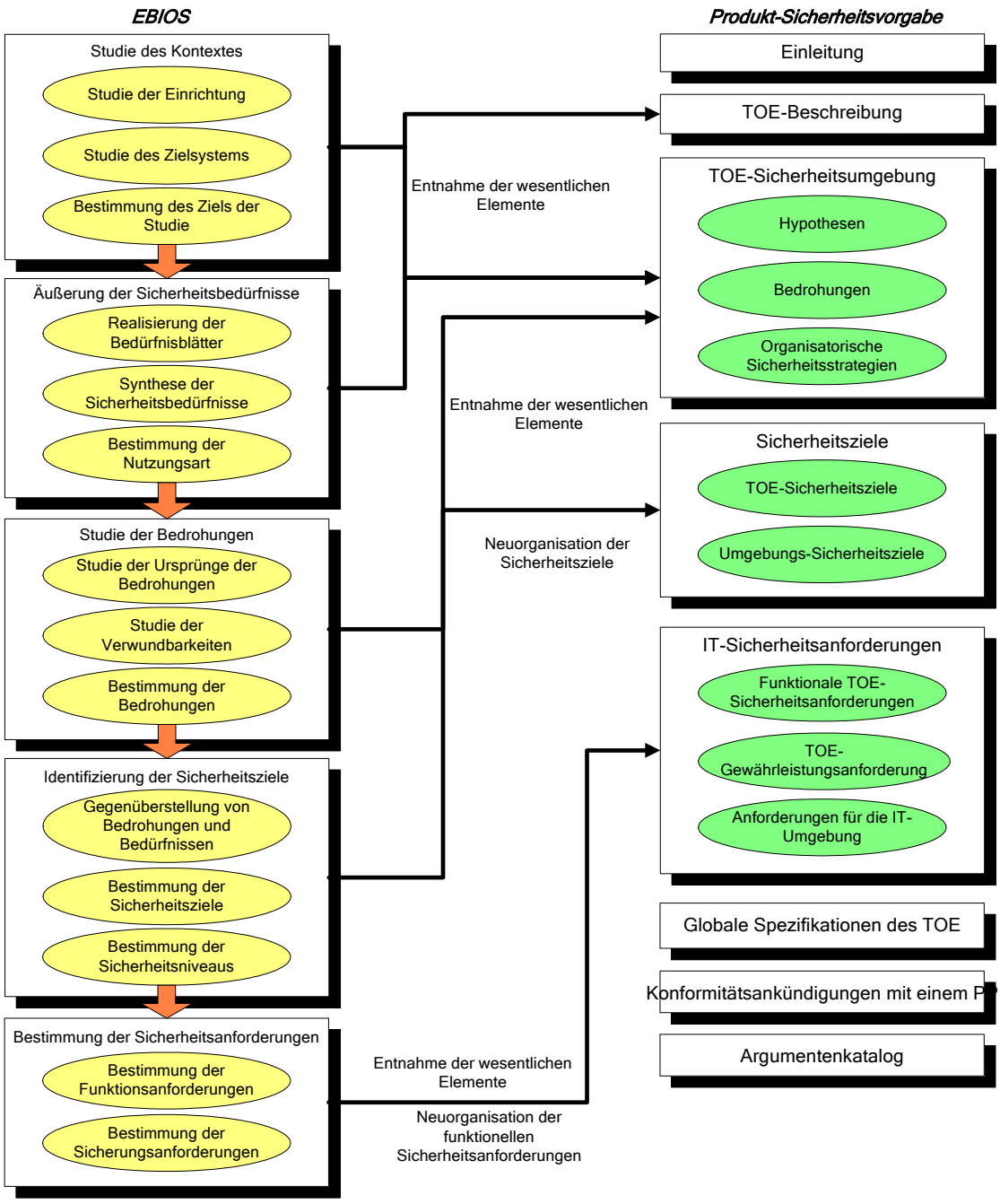
Die Aktivitäten der EBIOS-Methode werden dazu folgendermaßen eingesetzt:

EBIOS Aktivitäten	**Umsetzung zwecks Ausarbeitung eines Produkt-ST**
SCHRITT 1 Kontextstudie	Kurz gesagt: Die Kontextstudie ist nur auf die Informationen gerichtet, die zur Ausarbeitung einer Sicherheitsvorgabe notwendig sind
1.1 - Studie der Institution	Es kann nützlich sein, die Institutionen oder Institutionstypen zu beschreiben, in denen das Sicherheitsprodukt eingesetzt werden soll, um Umgebungshypothesen definieren zu können. Dennoch kommt diese Aktivität in der Regel nicht zum Einsatz.
1.2 - Studie des Zielsystems	Der Schwerpunkt liegt auf der Zusammenstellung der zur Abfassung eines ST notwendigen Elemente: - Vorstellung des TOE und funktionelle Beschreibung, - Liste der wesentlichen Elemente, - Liste der Hypothesen, - Liste der Sicherheitsvorschriften. Die sonstigen Elemente dieser Aktivität sind nur dann zu untersuchen, wenn sie in Bezug auf die obige Liste eine Bereicherung darstellen.
1.3 - Bestimmung des Ziels der Sicherheitsstudie	Diese Aktivität muss detailliert und vollständig sein, obwohl das Interesse hauptsächlich den technischen Einheiten wie z. B. der Software, Hardware oder den Netzwerken gilt.
SCHRITT 2 Bedarfsanalyse	Kurz gesagt: Die Sicherheitsbedarfe werden nach einer einfachen Bedürfnisskala bestimmt
2.1 – Realisierung der Bedürfnisblätter	Die gewählten Sicherheitsgrundwerte, Bedürfnisskalen und Auswirkungen müssen einfach sein und beispielsweise folgende Definitionen enthalten: - Die drei gewöhnlichen Sicherheitsgrundwerte (Verfügbarkeit, Integrität und Vertraulichkeit), - eventuell ein oder zwei Auswirkungen (hauptsächlich im Zusammenhang mit dem Verlust an Zuverlässigkeit der Mechanismen) - eine binäre Skala.
2.2 - Zusammenfassung der Sicherheitsbedarfe	Die Zusammenfassung der Sicherheitsbedarfe kann direkt und ohne Berücksichtigung der einzelnen Sicherheitsbedarfsblätter erfolgen.

EBIOS Aktivitäten	Umsetzung zwecks Ausarbeitung eines Produkt-ST
SCHRITT 3 Bedrohungsanalyse	Kurz gesagt: Die Untersuchung der Bedrohungen wird detailliert
3.1 - Untersuchung der Ursprünge der Bedrohungen	Die Aktivität muss detailliert und vollständig sein. Die Charakterisierung der Angriffsmethoden und der bedrohenden Elemente muss besonders klar und präzise sein. Das Angriffspotential jeden bedrohenden Elements ist anzugeben, zu erläutern und zu rechtfertigen. Die nicht berücksichtigten Angriffsmethoden sind mit Begründung aufzulisten.
3.2 – Studie der Schwachstellen	Die Schwachstellen können aus den Wissensdatenbanken der EBIOS-Methode abgeleitet werden, im Allgemeinen werden jedoch technischere und ausführlichere Referenzdokumente heranzgezogen. Die Bestimmung von Schwachstellenniveaus ist nur zur Hierarchisierung der Bedrohungen für den weiteren Verlauf der Studie von Interesse.
3.3 - Formalisierung der Bedrohungen	Diese Aktivität muss klar (zu Kommunikationszwecken) und präzise sein. Die Bedrohungen sollten einheitlich, homogen, spezifisch (eine Schwachstelle pro Bedrohung) und in Einklang mit den bestehenden Schutzprofilen und ST formuliert werden.
SCHRITT 4 Identifizierung der Sicherheitsziele	Kurz gesagt: Die Risiken drücken die Konsequenzen von Bedrohungen aus, Restrisiken müssen zugunsten von Änderungen des Kontextes "verschwinden"
4.1 – Gegenüberstellung von Bedrohungen und Bedürfnissen	Die Risiken müssen auf Basis der formulierten Bedrohungen einheitlich identifiziert und formuliert werden. Anstelle der Bedrohungen (weniger präzise in Bezug auf die Konsequenzen) können die Risiken in das ST integriert werden.
4.2 - Formalisierung der Sicherheitsziele	Die Abfassung der Sicherheitsziele muss klar; präzise und einheitlich sein, um sie inhaltlich rechtfertigen zu können. Die Sicherheitsziele sind in zwei Kategorien einzuteilen: - Diejenigen, die den TOE betreffen, - diejenigen, die die Umgebung des TOE betreffen. Eventuell identifizierte Restrisiken müssen Anlass zu einer Änderung des Kontextes geben (insbesondere was die Aktivität 1.2 anbelangt), so dass zu diesem Stand der Studie keine Restrisiken mehr bestehen. Der Nachweis der Abdeckung der Studienelemente durch die Sicherheitsziele muss detailliert werden.
4.3 - Bestimmung der Sicherheitsniveaus	Die Sicherheitsniveaus müssen explizit sein und ausreichend begründet werden.

EBIOS Aktivitäten	Umsetzung zwecks Ausarbeitung eines Produkt-ST
SCHRITT 5 Bestimmung der Sicherheits-anforderungen	
5.1 - Bestimmung der funktionellen Sicherheits-anforderungen	Die funktionellen Sicherheitsanforderungen müssen aus ISO 15408 abgeleitet oder unter Berücksichtigung der in der Norm angegebenen Empfehlungen neu erstellt und verfeinert werden, damit die Spezifikationen direkt anwendbar sind. Eventuell identifizierte Restrisiken müssen Anlass zu einer Änderung des Kontextes geben (insbesondere was die Aktivität 1.2 anbelangt), so dass zu diesem Stand der Studie kein einziges Restrisiko mehr besteht. Die Sicherheitsanforderungen sind in zwei Kategorien einzuteilen: - Diejenigen, die den TOE betreffen, - diejenigen, die die Umgebung des TOE betreffen. Der Nachweis der Abdeckung der Sicherheitsziele durch die funktionellen Sicherheitsanforderungen muss detailliert werden.
5.2 - Bestimmung der Sicherheits-gewährleistungs-anforderungen	Die Anforderungen zur Gewährleistung der Sicherheit müssen aus ISO 15408 abgeleitet oder unter Berücksichtigung der in der Norm enthaltenen Empfehlungen neu erstellt werden. Die Argumentation bezüglich der Sicherheitsgewährleistungs-anforderungen muss detailliert werden.

Zusammenfassend sind die verwertbaren Daten die folgenden:



(Zusätzliche Informationen sind erhältlich über: conseil.dcssi@sgdn.pm.gouv.fr