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

BEST PRACTICES FÜR DAS IT-SICHERHEITS-RISIKOMANAGEMENT

Ergebnisauswertung der EBIOS® Methode im Rahmen einer BS 7799 Vorgehensweise

Version vom 21. März 2003

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

Was ist der BS 7799?

Der *British Standard* 7799 (BS 7799) besteht aus zwei Leitfäden, der ISO/IEC 17799:2000 und der BS 7799-2:2002.
Der ISO/IEC 17799:2000 ist ein Katalog mit 36 Kontrollzielen, die in 127 Kontrollmaßnahmen unterteilt sind und die sich auf 10 Bereiche beziehen (Sicherheitspolitik, Personalsicherheit, Zugangskontrolle, usw.). Diese Kontrollziele legen ein zu erreichendes Ziel dar und das, was unternommen werden muss, um es zu erreichen. Sie werden anschließend in Kontrollmaßnahmen unterteilt, die mehr oder weniger im Detail die Punkte erläutern, die umgesetzt werden müssen, um diese Maßnahmen zu implementieren.
Der BS 7799-2:2002 präsentiert ein Informationssicherheitsmanagementsystem (*Information Security Management System - ISMS*) in vier rekurrenten Schritten (planen, umsetzen, überprüfen, verbessern), die sich den Qualitätsnormen ISO 9001 und ISO 14001 annähren. Der Planungsschritt empfiehlt, den ISO/IEC 17799:2000 einzusetzen.

Welche Vorteile bietet die EBIOS Methode im Rahmen einer BS 7799 Vorgehensweise?

Die vorherige Realisierung einer EBIOS Studie bietet mehrere Vorteile:

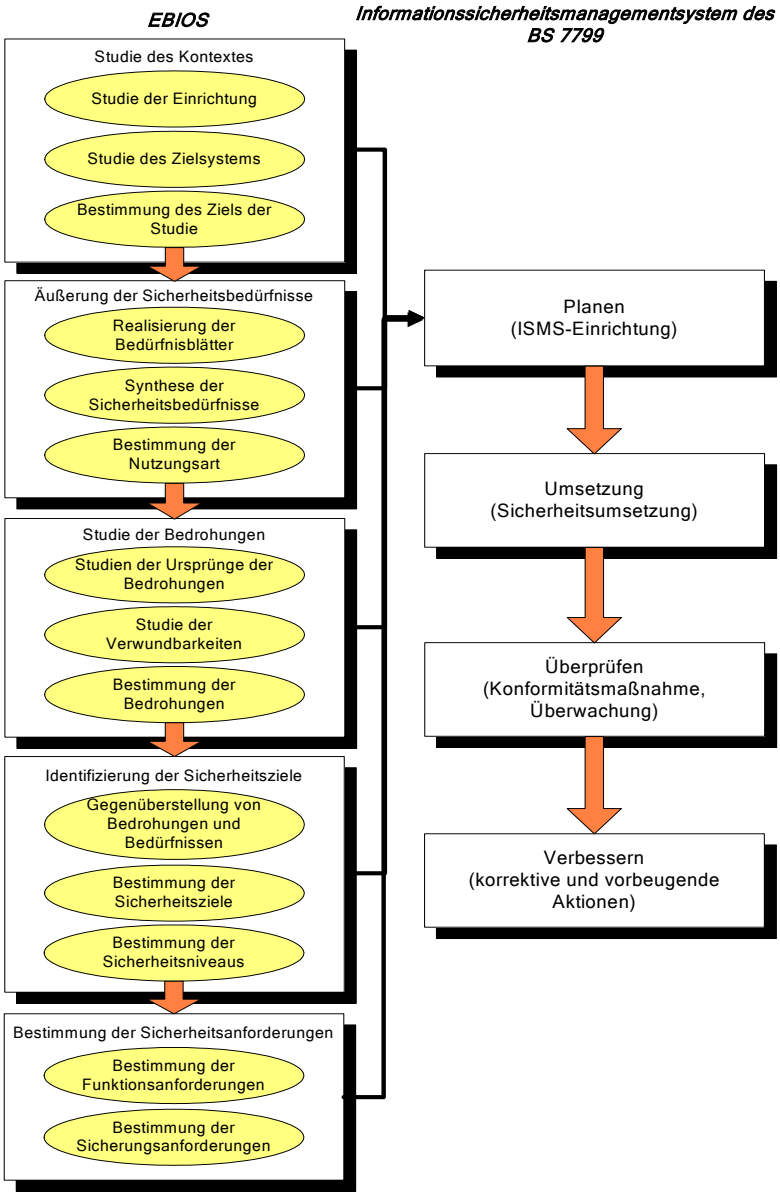
- die Rechtfertigung der Wahl der Kontrollziele und -maßnahmen in Abhängigkeit von den tatsächlichen Bedürfnissen der Einrichtung,
- die Einhaltung des Rahmens der im BS 7799 vorgeschlagenen Vorgehensweise, die eine Bewertung der Risiken vor der Wahl der der Kontrollziele und -maßnahmen empfiehlt,
- die Lieferung wiederverwendbarer Ergebnisse (Kontext, Sicherheitsbedarfe, Bedrohungen, Risiken, Sicherheitsziele, Sicherheitsanforderungen) in Hinsicht auf die späteren Iterationen des Informationssicherheitsmanagementsystems,

Wie wird eine BS 7799 Vorgehensweise mit EBIOS umgesetzt?

Eine effiziente Lösung, um eine BS 7799 Vorgehensweise umzusetzen, besteht darin:

- den Anwendungsbereich des Informationssicherheitsmanagementsystems zu definieren (den Perimeter formalisieren),
- eine IT-Sicherheits-Policy auszuarbeiten,
- eine globale EBIOS Studie zu realisieren, um die Analyse, die Bewertung und die Risikobehandlung auszuführen, indem die Kontrollziele und -maßnahmen gewählt werden, mit denen die zu reduzierenden Risiken gedeckt werden können,
- eine Erklärung der Anwendbarkeit vorzubereiten,
- die Folge des Prozesses mit anderen Werkzeugen zu realisieren.

Hierzu handelt es sich bei den auswertbaren Daten um folgende:



(Zusatzinformationen unter: ebios.dcssi@sgdn.pm.gouv.fr)