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

MÉMENTO

Version du 4 février 2004

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

Pourquoi EBIOS a-t-elle tant de succès ?

Une méthode de référence en matière d'analyse des risques SSI

La démarche méthodologique proposée par EBIOS apporte **une vision globale et cohérente** de la sécurité des systèmes d'information (SSI). Ainsi, elle fournit un vocabulaire et des concepts communs, permet d'être exhaustif et de déterminer des objectifs et des exigences de sécurité adaptés. La méthode prend en compte toutes les entités techniques (logiciels, matériels, réseaux) et non techniques (organisation, aspects humains, sécurité physique). Elle permet d'impliquer l'ensemble des acteurs du SI dans la problématique de sécurité et propose par ailleurs une démarche dynamique qui favorise les interactions entre les différents métiers et fonctions de l'organisation en étudiant l'ensemble du cycle de vie du système (conception, réalisation, mise en œuvre, maintenance…).

Promue par la DCSSI et **reconnue par les administrations françaises, EBIOS est aussi une référence dans le secteur privé et à l'étranger**. Dans ce contexte, sa traduction en anglais et la convergence vers les normes internationales lui ouvrent des perspectives nouvelles. En 2002, des comparaisons internationales placent EBIOS dans les trois meilleures méthodes d'analyse des risques SSI.

De nombreux organismes du secteur public et privé utilisent la méthode **pour faire ou pour réaliser eux-mêmes des analyses de risques SSI** : les administrations (employée de manière systématique dans certaines, encouragée dans les autres), le Centre national d'études spatiales (CNES), le Commissariat à l'énergie atomique (CEA), la Caisse nationale d'assurance maladie (CNAM), le Groupement des Cartes Bancaires "CB", ALCATEL CIT, des agences sanitaires, les Aéroports de Paris (ADP), le Conseil de l'Union européenne…

Par ailleurs, **plusieurs sociétés de conseil ont adopté la démarche EBIOS** dans leur rôle d'assistance aux maîtrises d'ouvrage.

Rappelons enfin qu'un ministère ou un industriel doit rédiger une Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS) dès lors qu'un système traite des informations classifiées de défense. EBIOS est l'outil idéal pour ce travail puisque ses résultats s'intègrent directement dans une FEROS.

Une démarche simple et des résultats adaptés

EBIOS est une méthode **facile à comprendre et à appliquer**. En effet, sa philosophie générale est simple et intuitive, et son déroulement naturel. Elle consiste à formaliser les besoins de sécurité et les menaces, et à déterminer les risques pesant sur l'organisme.

Chacun peut s'approprier la méthode et adapter son approche selon les sujets étudiés. EBIOS a été appliquée aussi bien sur des systèmes simples (serveur web) que sur des systèmes complexes (système de gestion des concours et du personnel impliquant différentes interconnexions), sur des systèmes à concevoir que sur des systèmes existants, ou encore sur des systèmes d'information entiers que sur des sous-systèmes.

Un seul et même outil permet de réaliser différentes démarches sécuritaires liées à la gestion des risques SSI. EBIOS est en effet utilisée pour contribuer à l'élaboration d'un schéma directeur SSI, pour réaliser les premières étapes d'une politique SSI et d'un tableau de bord SSI, pour contribuer à la rédaction d'un Profil de Protection (PP), pour rédiger une FEROS ou encore pour tout autre cahier des charges SSI.

EBIOS contribue à l'élaboration des tâches que la maîtrise d'ouvrage doit réaliser. Elle permet en effet de déterminer le périmètre de l'étude tout en gardant une vision globale du système étudié dans son contexte, d'exprimer des besoins (liés aux biens à protéger), d'identifier des menaces et de définir un plan de projets et des responsabilités.

La méthode EBIOS est un outil de choix et d'appréciation de la maîtrise d'œuvre pour adhérer aux objectifs exprimés par la maîtrise d'ouvrage, pour répondre aux questions relatives à la faisabilité, aux coûts et aux délais induits, et enfin pour choisir des solutions.

C'est aussi un outil de mesure d'impact et de négociation entre la maîtrise d'ouvrage et la direction (du projet, de l'organisme…) offrant à celle-ci la possibilité de contrôler l'adéquation des SI et de centraliser les études et la SSI.

La **compatibilité avec d'autres outils méthodologiques SSI** permet de garder une parfaite cohérence dans le processus de gestion des risques SSI. Par exemple, l'ISO/IEC 15408 et l'ISO/IEC 17799 peuvent être utilisés pour déterminer les objectifs et exigences de sécurité.

Un logiciel d'assistance sous licence libre

Le logiciel est gratuit et disponible sur simple demande auprès de la DCSSI (conseil.dcssi@sgdn.pm.gouv.fr). D'une prise en main facile, il **facilite de manière significative la réalisation des analyses de risques** et donne la possibilité de préparer différents documents de synthèse (ensemble des données, FEROS, synthèse de FEROS, PP, recueil d'éléments stratégiques, politique de sécurité…). En outre, il permet de réutiliser des bases de connaissances et des études. Livré avec ses sources et sa documentation de conception, il peut être amélioré par tous les utilisateurs. Le logiciel est édité sous une licence libre, conçu en UML et réalisé en Java et XML.

Une forte demande de formation

La formation à EBIOS facilite la compréhension de la méthode et de son application. Elle permet aux stagiaires de connaître les bonnes pratiques de mise en œuvre et de dialoguer avec des utilisateurs de la méthode. Cette formation de deux jours est dispensée au CFSSI (http://www.ssi.gouv.fr/formation/index.html). Elle est illustrée par une étude de cas, qui concrétise la démarche et fournit des exemples auxquels il est possible de se référer lors des premières utilisations de la méthode.
Par ailleurs, une session pour formateurs à la méthode EBIOS a également été mise en place dans le but de créer des relais au sein même des administrations.

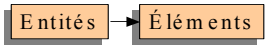
La création du club EBIOS

Afin de partager les expériences et d'améliorer la méthode et son outillage, la DCSSI a créé un club EBIOS en 2003.

Il permet de réunir régulièrement une communauté d'utilisateurs soucieux de contribuer au développement de la méthode et de disposer des dernières informations à son sujet.

Les principes de la méthode EBIOS

L'étude du contexte



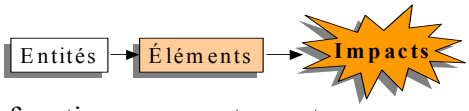
Un système d'information repose sur des **éléments essentiels**, fonctions et informations, qui constituent la valeur ajoutée du système d'information pour l'organisme.

Par exemple, un système de contrôle de trajectoire pour le lancement d'une fusée repose sur diverses informations telles que des paramètres ou des résultats de calculs et sur diverses fonctions permettant de réaliser ces calculs.

Les éléments essentiels sont liés à un ensemble d'**entités** de différents types : matériels, logiciels, réseaux, organisations, personnels et sites.

Prenons l'exemple d'un paramètre de calcul de trajectoire pour le lancement d'une fusée. Il est lié aux ordinateurs de contrôle, aux logiciels de traitement, aux opérateurs, à la fusée, aux réglementations du domaine…

L'expression des besoins de sécurité

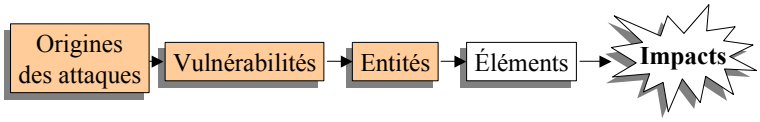


Chaque élément essentiel a un **besoin de sécurité** pour que le métier fonctionne correctement.

Ce besoin de sécurité s'exprime selon différents **critères de sécurité** tels que la disponibilité, l'intégrité et la confidentialité. Si ce besoin n'est pas respecté, l'organisme en sera impacté. Cet **impact** peut revêtir différentes formes : pertes financières, atteinte au bon déroulement des activités, atteinte à l'image de marque, atteinte à la sécurité des personnels, pollution …

Reprenons l'exemple du paramètre de calcul de trajectoire pour le lancement d'une fusée. Il s'agit d'une information qui devrait avoir un fort besoin de disponibilité et d'intégrité pour éviter l'atteinte à la sécurité du personnel.

L'étude des menaces



Par ailleurs, chaque organisme est exposé à divers **éléments menaçants**, de par son environnement naturel, sa culture, son image, son domaine…

Un élément menaçant peut être caractérisé selon son **type** (naturel, humain ou environnemental) et selon sa **cause** (accidentelle ou délibérée).

Il peut employer diverses **méthodes d'attaque** qu'il convient alors d'identifier.

Une méthode d'attaque est caractérisée par les critères de sécurité (disponibilité, intégrité, confidentialité…) qu'elle peut affecter et par les éléments menaçants susceptibles de l'utiliser.

Poursuivons notre exemple. Un organisme qui lance des fusées doit prendre en comptent un grand nombre de méthodes d'attaque et d'éléments menaçants :

- *les accidents physiques (ex : incendie),*
- *les événements naturels (ex : phénomène sismique),*
- *les pertes de services essentiels (ex : perte d'alimentation électrique),*
- *la compromissions des informations (ex : piégeage du logiciel),*
- *les défaillance techniques (ex : dysfonctionnement du matériel),*
- *les agressions physiques (ex : sabotage),*
- *les erreurs (ex : erreur d'interprétation)…*

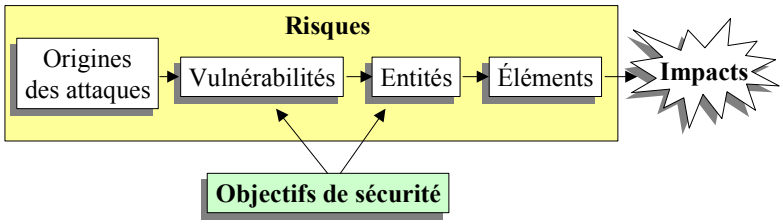
Chaque entité possède des **vulnérabilités** qui pourront être exploitées par les éléments menaçants selon chaque méthode d'attaque.

Ainsi, on pourra mettre en évidence plusieurs vulnérabilités liées aux entités de l'organisme qui lance des fusées :

- *la possibilité d'existence de fonctions cachées introduites en phase de conception ou de développement (logiciels),*
- *l'utilisation de matériels non évalués (matériels),*
- *la possibilité de créer ou modifier des commandes systèmes (réseaux),*
- *le réseau permet d'agir sur les logiciels des ressources du système (réseaux),*
- *la facilité de pénétrer sur le site par des accès indirects (locaux),*
- *le non respect des consignes de la part de certains opérateurs (personnels),*
- *l'absence de mesures de sécurité dans les phases de conception, installation et exploitation (organisation)…*

L'expression des objectifs de sécurité

Il ne reste plus qu'à déterminer comment les éléments essentiels peuvent être affectés par les éléments menaçants et par leurs méthodes d'attaque : il s'agit du **risque**.



Le risque représente un sinistre possible. C'est le fait qu'un élément menaçant puisse affecter des éléments essentiels en exploitant les vulnérabilités des entités sur lesquelles ils reposent avec une méthode d'attaque particulière.

Dans notre exemple, un risque consiste en la compromission d'informations sensibles par piégeage du logiciel du fait de la possibilité de créer ou modifier des commandes systèmes liées au réseau, ce qui pourrait avoir un impact sur la sécurité des personnels et sur l'image de marque.

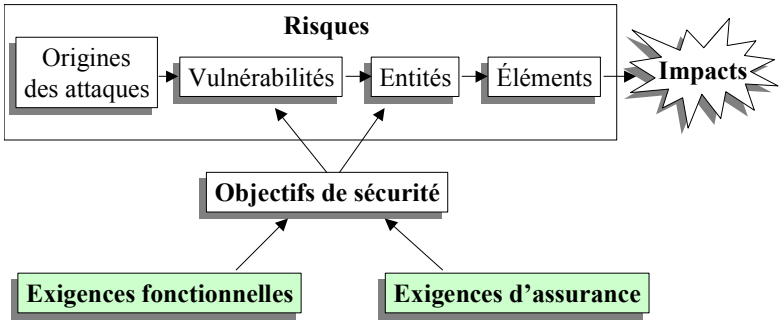
Les **objectifs de sécurité** consistent principalement à couvrir les vulnérabilités des entités qui composent l'ensemble des risques retenus.

En effet, il est inutile de protéger ce qui n'est pas exposé. On note aussi que plus le potentiel d'attaque est important et plus le niveau des objectifs de sécurité sera important. Ces objectifs constituent ainsi un cahier des charges parfaitement adapté.

L'un des objectifs de sécurité pour l'organisme qui lance des fusées est de sécuriser la création et la modification des commandes systèmes liées au réseau.

La détermination des exigences de sécurité

L'équipe en charge de la mise en œuvre de la démarche doit ensuite spécifier de manière précise les fonctionnalités attendues en matière de sécurité. Elle doit alors démontrer la parfaite couverture des objectifs de sécurité par ces **exigences fonctionnelles**.



Dans notre exemple, l'une des exigences fonctionnelles couvrant la sécurisation de la création et de la modification des commandes systèmes liées au réseau est la suivante : le système doit exécuter une suite d'autotests de façon périodique pendant le fonctionnement normal pour démontrer son fonctionnement correct.

L'équipe en charge doit enfin spécifier les **exigences d'assurance** qui permettent d'obtenir le niveau de confiance requis, pour ensuite le démontrer.

L'une des exigences d'assurance est la suivante : le développeur doit effectuer une analyse de la résistance des fonctions de sécurité du système selon le niveau de résistance requis.

En résumé

EBIOS formalise une démarche d'appréciation et de traitement des risques dans le domaine de la sécurité des systèmes d'information.

Son approche simple et modulaire permet de s'adapter à tous les contextes et à différentes actions de sécurité. En outre, EBIOS s'avère être un excellent outil de négociation, d'arbitrage et de sensibilisation.

La convergence vers les normes internationales, son logiciel libre, la formation et le club des utilisateurs font d'EBIOS une méthode riche et maintenue au plus haut niveau par les experts du domaine de la sécurité des systèmes d'information.

Pour de plus amples informations :

- le site web de la DCSSI http://www.ssi.gouv.fr
- la boîte aux lettres EBIOS ebios.dcssi@sgdn.pm.gouv.fr
- la boîte aux lettres du Bureau Conseil conseil.dcssi@sgdn.pm.gouv.fr