ANSSI Agence nationale de la sécurité des systèmes d'information

EBIOS : la méthode de gestion des risques SSI
Un outil simple et puissant

La gestion des risques est largement décrite et préconisée dans la presse, les normes, la réglementation… EBIOS® (Expression des Besoins et Identification des Objectifs de Sécurité) est la méthode de gestion des risques de l'ANSSI. Opérationnelle, modulaire et alignée avec les normes, c'est la boîte à outils indispensable pour toute réflexion de sécurité des systèmes d'information (SSI). Voici comment EBIOS peut vous être utile.

Le risque SSI dans EBIOS : un exemple éclairant

Définition du risque : c'est un scénario qui combine un événement redouté (sources de menaces, bien essentiel, critère de sécurité, besoin de sécurité, impacts) et un ou plusieurs scénarios de menaces (sources de menaces, bien support, critère de sécurité, menaces, vulnérabilités).

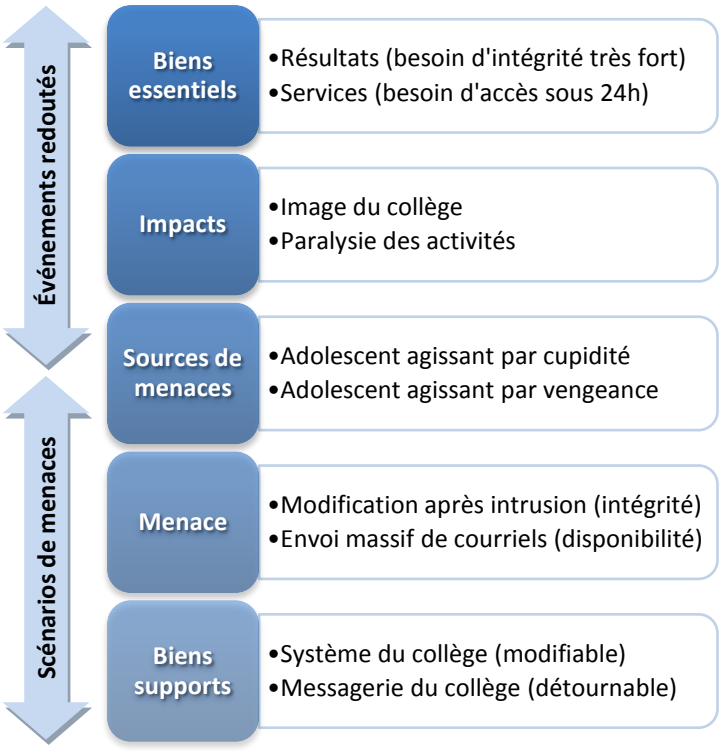
On estime son niveau par sa gravité (hauteur des impacts) et sa vraisemblance (possibilité qu'il se réalise).

Un adolescent de 15 ans « pirate » le système informatique de son collège pour améliorer ses notes.

Un adolescent de quinze ans a en effet été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.

[Sources Internet : Le Point.fr et ZDNet]

À partir de ce fait divers et de la définition du risque d'EBIOS, nous pouvons mettre deux risques en évidence :



Risque 1

Altération des résultats

Un adolescent agissant par cupidité s'introduit dans le système du collège et modifie ses résultats, qui doivent rester parfaitement intègres, ce qui ternit l'image du collège.

Risque 2

Indisponibilité des services

Par vengeance, un adolescent sature la messagerie par un envoi massif de courriels, ce qui bloque les services du collège et paralyse ses activités.

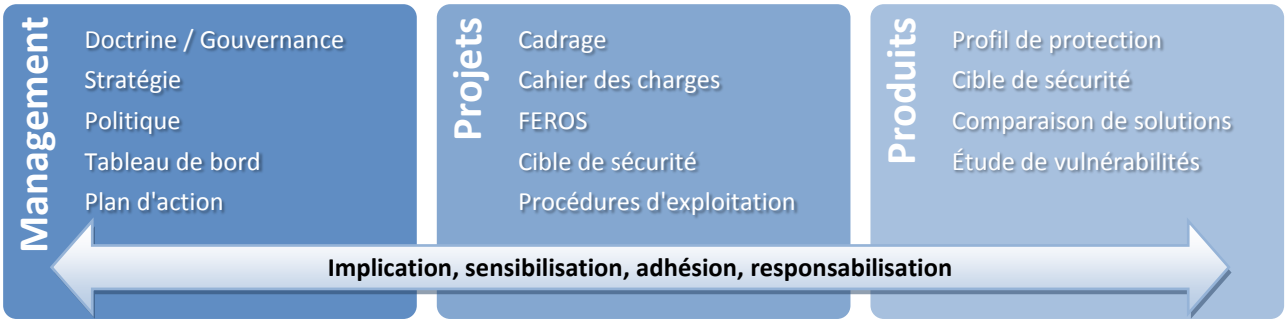
Une étude EBIOS appliquée au système du collège aurait permis, simplement et rapidement :

- d'identifier ces deux risques, ainsi que tous les autres qui pèsent sur le système d'information du collège ;
- d'estimer leur niveau (gravité, vraisemblance), les cartographier et prendre des décisions en conséquence ;
- de choisir les mesures nécessaires et suffisantes en termes de prévention, de protection et de récupération.

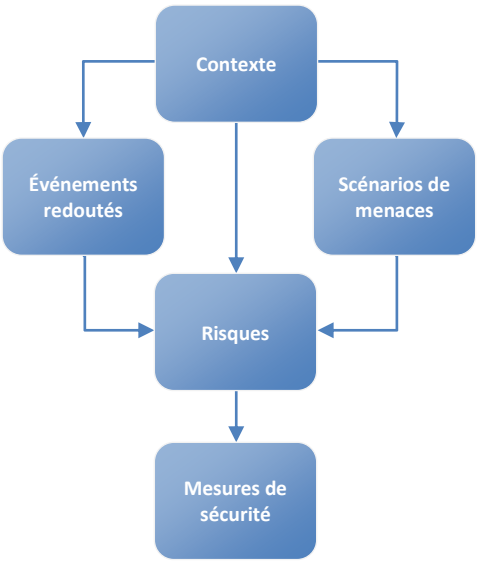
ANSSI

Agence nationale de la sécurité des systèmes d'information

EBIOS est le "tout terrain" pour gérer les risques



Les 10 questions essentielles pour gérer les risques



Contexte	•Pourquoi et comment va-t-on gérer les risques ? •Quel est le sujet de l'étude ?
Evénements redoutés	•Quels sont tous les événements craints ? •Quels seraient les plus graves ?
Scénarios de menaces	•Quels sont tous les scénarios possibles ? •Quels sont les plus vraisemblables ?
Risques	•Quelle est la cartographie des risques ? •Comment choisit-on de les traiter ?
Mesures de sécurité	•Quelles mesures devrait-on appliquer ? •Les risques résiduels sont-ils acceptables ?

Grands principes à appliquer

Pour réussir une étude et son application, il convient de respecter 4 grands principes de mise en œuvre :

- employer EBIOS comme une boîte à outils pour une efficacité maximale ;
- utiliser la méthode avec souplesse pour adhérer au langage et aux pratiques de l'organisme ;
- améliorer progressivement l'étude, en temps réel, pour rester cohérent avec la réalité ;
- rechercher une adhésion des acteurs du système d'information pour élaborer des solutions de protection.

Une mise en œuvre facilitée

La méthode dispose de bases de connaissances riches et enrichissables, d'un logiciel libre et gratuit, de formations et d'une documentation variée.

La communauté des experts et utilisateurs de gestion des risques (industriels, administrations, prestataires, universitaires…) se réunit régulièrement au Club EBIOS pour échanger des expériences et enrichir le référentiel.

EBIOS ne vous protège pas des risques, elle vous permet d'en faire prendre conscience aux décideurs.

Informations : http://www.ssi.gouv.fr/ebios
Contact : ebios@ssi.gouv.fr