PLOUZENNEC Eliaz

Compte rendu : La méthode EBIOS

08/11/24

Sommaire :

Introduction :

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une approche conçue pour évaluer et gérer les risques liés aux systèmes d'information. Créée en 1995 par la DCSSI (Direction centrale de la sécurité des systèmes d'information) et maintenue aujourd'hui par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), elle est devenue un standard pour l'analyse des risques en matière de sécurité informatique. La version EBIOS Risk Manager représente une évolution récente, mieux adaptée aux défis actuels du numérique et axée sur l'intégration des risques au niveau stratégique des organisations.

A quoi sert-elle ?

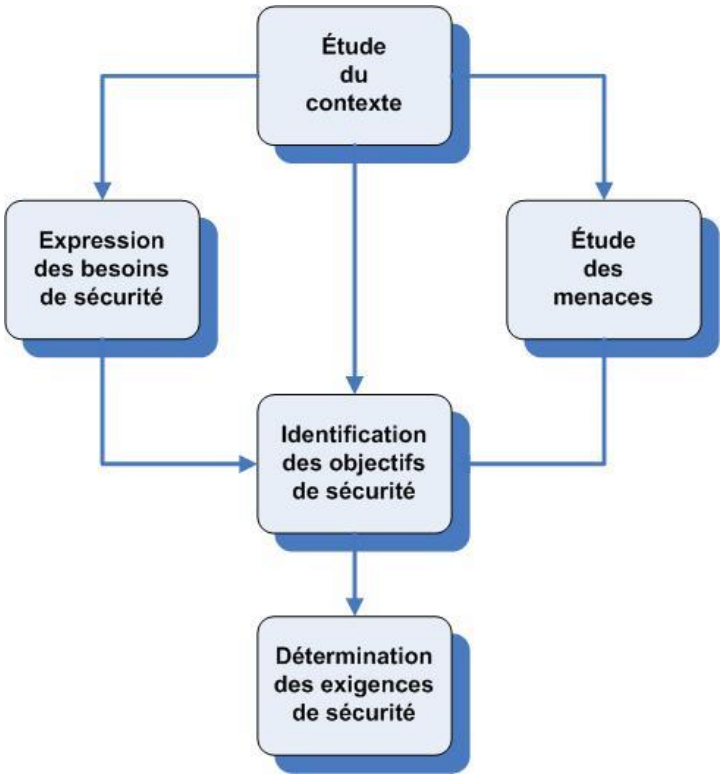
La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) sert à gérer les risques numériques de manière systématique et méthodique. Elle permet aux organisations d'identifier, d'analyser, d'évaluer et de traiter les risques liés à la sécurité des systèmes d'information. En offrant une vision complète et stratégique des menaces potentielles, EBIOS aide les entreprises à renforcer leur posture de sécurité et à adopter les mesures de protection nécessaires.

Elle est utile à plusieurs niveaux, notamment pour :

- **Élaborer un processus de gestion des risques** : En structurant les étapes nécessaires pour évaluer et traiter les risques, EBIOS facilite la mise en place d'un processus de management des risques numériques, adapté à l'évolution constante des menaces.
- **Homologuer un projet numérique** : Lorsqu'un projet nécessite une validation ou une autorisation officielle pour garantir un certain niveau de sécurité, EBIOS permet d'évaluer les risques spécifiques liés à ce projet et de définir les mesures de protection à mettre en place.

- **Définir des exigences de sécurité** : Dans le cadre de la conception de produits ou de services, la méthode permet de spécifier les exigences en matière de sécurité selon les cas d'usage envisagés et les risques identifiés. Cela peut être utile dans le contexte d'une certification ou d'un agrément.
- **Améliorer la communication** : En proposant une vue d'ensemble des risques et des mesures mises en œuvre pour y faire face, EBIOS facilite la communication interne et externe autour de la sécurité, notamment avec les parties prenantes, les clients, ou les partenaires.

Les étape clés de la méthode



Schema methode EBIOS

1. Étude du contexte

Cette étape définit le cadre et le périmètre du système à sécuriser. Elle comprend trois sous-activités :

- **Étude de l'organisme** : Collecte d'informations sur l'organisation et son environnement pour comprendre son contexte global.

- **Étude du système-cible** : Détail des composants du système d'information à analyser (projet, système existant, etc.).
- **Détermination de la cible de sécurité** : Identification des biens essentiels à protéger, qu'ils soient matériels ou immatériels (données, infrastructures).

2. Étude des événements redoutés

Cette étape identifie les besoins en sécurité et les impacts des menaces :

- **Réalisation des fiches de besoins** : Recueil des attentes en matière de sécurité (confidentialité, intégrité, disponibilité).
- **Synthèse des besoins de sécurité** : Priorisation des besoins et attribution des exigences aux éléments essentiels.

3. Étude des scénarios de menaces

Cette étape analyse les menaces et vulnérabilités du système-cible :

- **Identification des menaces** : Recensement des menaces potentielles (humaines, environnementales, techniques).
- **Analyse des éléments menaçants** : Identification des sources des menaces.
- **Étude des méthodes d'attaque** : Examen des façons dont les menaces pourraient exploiter les vulnérabilités.
- **Identification des vulnérabilités** : Analyse des failles exploitables dans le système-cible.
- **Modélisation des scénarios** : Création de scénarios de risques en combinant menaces, méthodes d'attaque et vulnérabilités.

4. Étude des risques

Cette étape évalue et hiérarchise les risques identifiés :

- **Confrontation des menaces aux besoins de sécurité** : Correspondance entre les menaces et les besoins pour évaluer les risques.
- **Hiérarchisation des risques** : Priorisation des risques en fonction de leur impact et probabilité.
- **Détermination des objectifs de sécurité** : Définition des objectifs de protection pour chaque risque.
- **Détermination des niveaux de sécurité** : Évaluation des niveaux de résistance nécessaires pour chaque objectif de sécurité.

5. Étude des mesures de sécurité

Cette phase consiste à mettre en œuvre les mesures pour atteindre les objectifs de sécurité :

- **Spécification des mesures fonctionnelles et techniques** : Choix des solutions pour mitiger les risques.
- **Vérification de la couverture des objectifs de sécurité** : Vérification finale que chaque objectif de sécurité a été correctement adressé.

Bénéfices pour les organisations

Il y a plusieurs bénéfices :

1. **Vision complète des risques** : EBIOS fournit une analyse détaillée des risques, couvrant les aspects techniques, organisationnels et contextuels, ce qui permet de mieux anticiper les menaces et vulnérabilités spécifiques au SI.
2. **Adaptabilité et flexibilité** : La méthode est flexible et peut être personnalisée pour s'adapter aux besoins d'organisations de toutes tailles et secteurs, facilitant l'adhésion de toutes les parties prenantes.
3. **Conformité aux normes internationales** : EBIOS est compatible avec des normes internationales comme ISO 27005, facilitant la conformité aux exigences de sécurité réglementaires.
4. **Amélioration de la résilience** : En hiérarchisant les risques et en définissant des objectifs de sécurité, EBIOS aide à renforcer la protection des actifs critiques et la résilience face aux menaces.
5. **Collaboration et implication accrue** : La méthode favorise une approche collaborative, impliquant à la fois les experts techniques et les décideurs, ce qui renforce la culture de la sécurité au sein de l'organisation.

Conclusion

EBIOS est une méthode efficace pour la gestion des risques numériques, offrant une analyse détaillée des menaces et des vulnérabilités tout en facilitant la mise en place de mesures de sécurité adaptées. Elle est flexible, conforme aux normes internationales et améliore la communication sur les enjeux de sécurité. En aidant les organisations à anticiper et à protéger leurs systèmes d'information, EBIOS renforce leur résilience face aux risques émergents.

Source

https://cyber.gouv.fr/la-methode-ebios-risk-manager

https://www.ssi.gouv.fr/