

TIW4 : SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANALYSE DES RISQUES DE SÉCURITÉ : EBIOS

romuald.thion@univ-lyon1.fr

<http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4>



Master « Technologies de l'Information »

Plan

- 1 Introduction
- 2 La méthode EBIOS
- 3 Les modules EBIOS
- 4 Conclusion

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Objectifs

- dégager une vision globale des aspects sécurité
- acquérir & utiliser un vocabulaire
- savoir mener une évaluation des risques de sécurité
- du *global* (politique) à *local* (mesures techniques)

Pourquoi la méthode EBIOS ?

- référence nationale
- largement applicable
- compatible avec ISO
- base documentaire

ANSSI

Agence nationale de la
sécurité des systèmes
d'information

<http://www.ssi.gouv.fr/>

- 1 Introduction
 - Objectifs
 - **Autres méthodes**
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Autres méthodes

Méthode	Création	Auteur	Secteur	Pays
EBIOS	1995	DGSSI	Gouvernement	France
Melisa		DGA	Armement	France
Marion	1980	CLUSIF	Association	France
Mehari	1995	CLUSIF	Association	France
Octave	1999	Carnegie Mellon	Universitaire	Etats-Unis
Cramm	1986	Siemens	Gouvernement	Angleterre
SPRINT	1995	ISF	Association	Angleterre
SCORE	2004	Ageris Consulting	Secteur privé	France
CALLIO	2001	CALLIO Tech.	Secteur privé	Canada
COBRA	2001	C&A Sys. Security	Secteur privé	Angleterre
ISAMM	2002	Evosec	Secteur privé	Belgique
RA2	2000	Aaxis	Secteur privé	Allemagne

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Gérer les risques

Notion générale de risque :

- gestion de projet
- sécurité des personnes
- financier (chiffré !)
- sûreté de fonctionnement
- **sécurité des systèmes**

Sécurité = protéger le patrimoine informationnel

La *valeur* au sein du SI

- opportunités offertes en utilisation correcte
- versus conséquences négatives

sélection de *biens essentiels* (protéger *information* ≠ *données*)

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Une méthode

Intérêt d'*une* méthodologie

- langage commun
- démarche claire & structurée
- référentiel, expérience
- exhaustivité des actions (e.g. la base de connaissance)
- réutilisable, extensions/généralisations

En sécurité de l'information

{ *apprécier les, traiter les, valider les traitements des, communiquer sur, suivre les* } risques

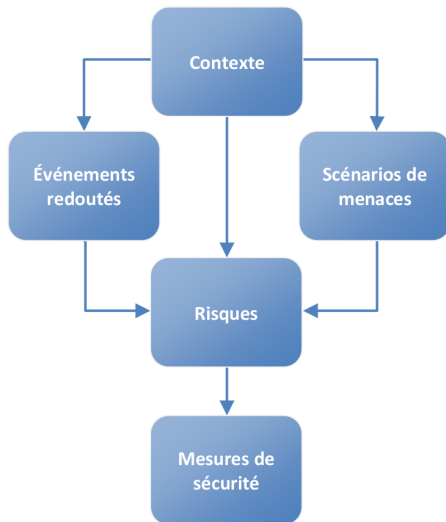
On *peut* confondre sys. d'**information** et **informatique**

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Conduite de la méthode

- 1 cadre, métrique, biens
- 2 besoins & impacts
- 3 menaces & vulnérabilités exploitables
- 4 événements *versus* scénarii : les risques
- 5 évaluer les risques résiduels

Tout est dans le schéma



- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Exemple

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. Dépit 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.

Quels sont les deux risques mis en évidence dans cet exemple ?

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Étude du contexte

- pourquoi & comment gérer les risques ?
- quel est le sujet de l'étude ?

Activités

- (1.1) Le cadre de la gestion des risques
- (1.2) Préparer les métriques
- (1.3) Identifier les biens

Le cadre de la gestion des risques (1.1)

Définir le cadre

Objectifs	circonscrire le périmètre, définir comment la gestion sera menée
Avantages	légitimité & faisabilité de l'étude, orientation des travaux en fonction des objectifs réels (†)

Actions

- (1.1.1) Cadrer l'étude
- (1.1.2) Contexte général
- (1.1.3) Périmètre de l'étude
- (1.1.4) Paramètres
- (1.1.5) Sources de menaces

Sources de menaces

Quels critères pour analyser/catégoriser les sources de menaces ?
(Hint : identifier des critères orthogonaux)

Sources de menaces

Typologie des menaces génériques

Base de connaissances

- Menaces : *humaines* ou *non-humaines*
- Menaces *non-humaines* : *code, phénomènes naturels, catastrophes naturelles, animaux, événements internes*
- Menaces *humaines* : les critères **orthogonaux**
 - interne ou externe
 - malveillant ou bienveillant
 - capacités faibles, fortes ou illimitées

On ne retient que les combinaisons pertinentes, on donne des exemples sur le cas d'étude

Préparer les métriques (1.2)

Activité

Objectifs	Fixer des échelles, harmoniser différentes études
Avantages	Homogénéité, répétabilité

Actions

- (1.2.1) Définir les **critères** & l'**échelle** des besoins
- (1.2.2) Échelle de niveaux de **gravité**
- (1.2.3) Échelle de niveaux de **vraisemblance**
- (1.2.4) Critères de gestion des risques

Critères de sécurité

Quels sont les (sous-)critères de la sécurité ?

Métriques

Critères = $\{C, I, A\}$ (†)

- **Confidentiality** : *Public* $\preceq$ *Limité* $\preceq$ *Réservé* $\preceq$ *Secret*
- **Integrity** : *DéTECTABLE* $\preceq$ *Maîtrisé* $\preceq$ *Intègre*
- **Availability** : $[72h..∞[\preceq [24h..72h[\preceq [4h..24h[\preceq [0..4h[$

L'essence du risque

- *Gravité* : *Négligeable* $\preceq$ *Limitée* $\preceq$ *Importante* $\preceq$ *Critique*
- *Vraisemblance* : *Minime* $\preceq$ *Significative* $\preceq$ *Forte* $\preceq$ *Maximale*

Action (1.2.4) : déterminer *un produit*

$Gravité \times Vraisemblance \rightarrow$
Négligeable $\preceq$ *Significatif* $\preceq$ *Intolérable* (†)

Identifier les biens (1.3)

Activité

Objectifs	Mise en évidence des éléments nécessaires aux autres activités
Avantages	Comprendre le fonctionnement du cas, prendre en compte l'existant

Actions

- (1.3.1) Identifier les biens **essentiels**
- (1.3.2) Identifier les biens **supports**
- (1.3.3) Déterminer leurs relations
- (1.3.4) Identifier les mesures de sécurité existantes
Prévention, Récupération, Protection

Identification des biens

Essentiels : dont le non respect des critères mettrait en cause la responsabilité du dépositaire ou causerait un préjudice $\cong$ fonctionnalités attendues

Biens essentiels

Processus	Biens	Dépositaire
Émission	Carte vierge, OS , clefs ...	Émetteur
Attribution	Carte préparée, PII ...	Émetteur
Inscription	Application, inscription ...	Porteur, fournisseur
Désinscription	...	Porteur, fournisseur
Utilisation	...	Porteur
Déploiement	...	Fournisseur

Supports : sur lesquels reposent les bien essentiels, possèdent des vulnérabilités (†)

Biens supports génériques

Base de connaissance

- Systèmes informatiques & téléphoniques
 - Matériels
 - Logiciels
 - Canaux
- Organisations
 - Personnes
 - Support papier
 - Canaux interpersonnels
- Locaux

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Étude des événements redoutés

- quels sont *tous* les événements craints ?
- quels seraient les plus graves ?

Activités

- (2.1) Apprécier les événements redoutés

Apprécier les événements redoutés (2.1)

Activité

Objectifs	identifier les événements, indépendamment de comment ils peuvent survenir
Avantages	comparer l'importance des biens, hiérarchiser les événements redoutés

Actions

- (2.1.1) Analyser *tous* les événements
- (2.1.2) Évaluer chaque événement

Analyse des événements redoutés

∀ *processus essentiel*, ∀ *critère* :

- *besoin* de sécurité (cf. échelle (1.2.1))
- $\subseteq$ *sources* de menaces (cf. liste (1.1.5))
- $\subseteq$ *biens essentiels* (cf. liste (1.3.1))
- exemples *d'impacts* & *gravité* (cf. échelle (1.2.2))

Ex : *processus utilisation service*

Evt.	Besoin	Source	Impacts	Gravité
Fraude	3. Intègre	Voleur, fraudeur, hacker	pertes F&I	1. limitée

Impacts génériques

Base de connaissance

- sur le fonctionnement
sur les mission, sur la décision
- humains
sécurité, lien social
- sur les biens
patrimoine, financier, image
- autres
non-conformité, juridiques, environnement

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scenarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Étude des scenarii de menaces

- quels sont *tous* les scenarii possibles ?
- quels sont les plus vraisemblables ?

Activités

- (3.1) Apprécier les scenarii de menaces

Apprécier les scenarii de menaces (3.1)

Activité

Objectifs	Actions possibles sur les biens supports
Avantages	Réaliser la diversité des menaces, exhaustivité

Actions

- (3.1.1) Analyser *tous* les scenarii
- (3.1.2) Évaluer chaque scenario

Analyser les menaces

∀ *bien support* (∀ *critère*) :

- $\subseteq$ *sources* de menaces (cf. liste (1.1.5))
- *vraisemblance* (cf. échelle (1.2.3))

Ex : support *Internet*

Menace	Source	Vraisemblance
Ecoute passive	Script-kiddies, hacker, collaborateur	1. significative
Ecoute "MitM"	<i>idem</i>	1. significative
Saturation	<i>idem</i>	1. significative

Menaces & vulnérabilités génériques

Base de connaissance

- Sur les matériels : *détournement d'usage, espionnage, dépassement des limites de fonctionnement, détérioration, modification, perte*
- Sur les **logiciels** : *détournement d'usage, analyse, dépassement des limites de fonctionnement, suppression, modification, disparition*
- Sur les **canaux** : *Attaque du milieu, écoute passive, saturation, dégradation, modification, disparition*
- Sur les personnes : *Dissipation, espionnage, surcharge, atteinte physique, influence, départ*
- Sur les supports papiers : *Détournement, espionnage, détérioration, perte*
- Sur les canaux interpersonnels : *Manipulation, espionnage, saturation, dégradation, modification, disparition*

Étude des scenarii de menaces

Centre d'Expertise Gouvernemental de Réponse et de Traitement des
Attaques informatiques (CERTA)

<http://www.certa.ssi.gouv.fr/>

Documents accessibles

- **Alertes** : prévenir d'un danger immédiat
- **Avis** : état de vulnérabilités et des moyens de s'en prémunir
- **Bulletin** : illustration par l'actualité récente de certaines mesures pragmatiques à appliquer
- **Notes** d'information : état de phénomènes à portée générale

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Études des risques

- quelle est la cartographie des risques (niveau = gravité $\times$ vraisemblance) ?
- comment les traiter ?

Activités

- (4.1) Apprécier les risques
- (4.2) Identifier les objectifs

Apprécier les risques (4.1)

Activité

Objectifs	Mettre en évidence les risques réels
Avantages	Justifier l'utilité des mesures, écarter les scénarii qui ne constituent pas un risque, forcer à s'interroger sur le niveau des risques

Actions

- (4.1.1) Analyser les risques
- (4.1.2) Évaluer les risques

Apprécier les risques (4.1)

Un risque = produit de

- un événement redouté (**gravité**)
- des scénarii de menaces concernés (**vraisemblance**)
 - on garde evt.sources $\cap$ menace.sources
 - on garde les menaces pour le même critère

En pratique : vulnérabilités des biens supports

On attribue un niveau de risque **gravité** $\times$ **vraisemblance**

On identifie les mesures existantes

Risques liés au vol de carte

- 1 *Utilisation frauduleuse de services* : gravité **importante**
- 2 *Menace de vol* : vraisemblance **forte**
- 3 *Mesures procédure d'opposition*

Apprécier les risques (4.1)

Gravité × Vraisemblance

Critique				
Importante				
Limitée				
Négligeable				
	Minime	Significative	Forte	Maximale

Risques

Négligeable	Significatif	Intolérable
--------------------	---------------------	--------------------

Identifier les objectifs (4.2)

Activité

Objectifs	Déterminer comment traiter le risque
Avantages	Choix entre différentes options, constituer un cahier des charges

Actions

- (4.2.1) Choisir les options de gestion des risques
- (4.2.2) Analyser les risques résiduels

Identifier les objectifs (4.2)

Choisir les options de traitement du risque afin que le risque résiduel devienne acceptable

Options possibles

- l'**éviter** (le refuser), *id est* changer de contexte
- le **réduire**, *id est* diminuer l'impact ou la vraisemblance à l'aide de mesures
- le **prendre** (le maintenir, l'augmenter), *id est* assumer les conséquences sans nouvelles mesures
- le **transférer** (le partager), *id est* partager les pertes, faire assumer la responsabilité

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

Études des mesures de sécurité

- quelles mesures appliquer ? (techniques, organisationnelle, externes)
- quelles sont les mesures existantes ?
- quels sont les risques résiduels une fois les mesures changées ?

Activités

- (5.1) Formaliser les mesures à mettre en œuvre
- (5.2) Mettre en œuvre les mesures

Formaliser les mesures (5.1)

Activité

Objectifs	Déterminer les mesures adéquate, valident formellement les choix
Avantages	Mesurer l'efficacité (ratio coût/effet)

Actions

- (5.1.1) Déterminer les mesures
- (5.1.2) Analyser les risques résiduels
- (5.1.3) Établir une déclaration d'applicabilité

Critères de sécurité

Quelles mesures de sécurité (informatique ou non) connaissez-vous ?

Les mesures de sécurité

Base de connaissance : un bestiaire issu du RGS ou de ISO 27001 et 27002

- à décliner selon les bien support
- transversales à plusieurs risques
- *Prévention, Protection ou Récupération*

Mettre en œuvre

Mesure	Resp.	Diff.	Coût	Terme	État
Ondulation	...				
Destruction docs	...				

Mettre en œuvre (5.2)

Activité

Objectifs	Élaborer et suivre la réalisation du plan de traitement des risques
Avantages	Légitimité des actions, favorise la réalisation et l'application des mesures

Actions

- (5.2.1) Élaborer le plan d'action et suivre sa réalisation
- (5.2.2) Analyser les risques résiduels
- (5.2.3) Prononcer l'homologation de sécurité (**Graal !**)

Mettre en œuvre (5.2)

Gravité × *Vraisemblance*

Critique				
Importante				
Limitée	R''_0	R_0		
Négligeable	R'_0			
	Minime	Significative	Forte	Maximale

- R_0 le risque initialement estimé
 - *exemple : l'intégrité de certains documents*
- R'_0 le risque après traitement, avec *gravité* diminuée
 - *exemple : mise en place des procédure de sauvegarde et de reprise*
- R''_0 le risque après traitement, avec *vraisemblance* diminuée
 - *exemple : mise en place d'une authentification plus forte*

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

- 1 Introduction
 - Objectifs
 - Autres méthodes
- 2 La méthode EBIOS
 - Gérer les risques
 - Une méthode
 - Conduite de la méthode
 - Exemple
- 3 Les modules EBIOS
 - Étude du contexte
 - Étude des événements redoutés
 - Étude des scénarii de menaces
 - Études des risques
 - Études des mesures de sécurité
- 4 Conclusion
 - En conclusion

En conclusion

EBIOS

- méthodologie + boîte à outils
- se poser les bonnes questions sur la sécurité ...
- ... et y répondre !

De l'importance des aspects non-informatiques

- système d'information $\cong$ système informatique
- prévention & récupération *versus* protection
- importance des aspects non-techniques & humains

En conclusion

Le contenu de l'UE à la lumière d'EBIOS

- *mesures de sécurité* : cryptographie
 - chiffrement symétrique
 - chiffrement asymétrique, signature
 - hachage
- *mesures de sécurité* : filtrage et contrôle
 - pare-feux
 - contrôle d'accès et gestion des droits
 - étude et comparaison de modèles
- *menaces et vulnérabilités*
 - menaces « web » : SQLi, CSRF, XSS
 - étude d'exploits : Adobe Reader, XOrg, Scheduler windows
 - attaques des mots de passe



SECURITY

doin it wrong.....

VERY DEMOTIVATIONAL .com