

1

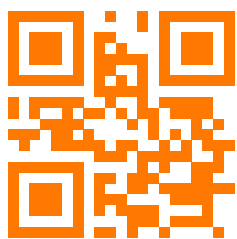
CYBERDEF 101

Cyber Risques

ERIC DUPUIS

2023





Téléchargez une version à jour



2023 EDUF@CTION PUBLICATION (CC-BY-NC-ND)

Ce document est issu des supports de notes du cours SEC 101
du Conservatoire National des Arts et MétiersBretagne sous licence (CC-BY-NC-ND)

Tous droits de reproduction, d'adaptation et de traduction, intégrale ou partielle
de ce document réservés pour tous pays.

L'auteur est seul propriétaire des droits et responsable du contenu de cet ouvrage.

Edition étudiants Orange Campus Cyber

*Edition du 22 janvier 2023 pour la deuxième EDITION, Publication limitée pour le
Conservatoire National des Arts et Métiers et Orange Campus Cyber, réalisé sous
L^AT_EX(MacTex) avec Texifier 🍏*

Merci à Véronique Legrand, titulaire de la chaire de Cybersécurité du CNAM et Eric Bornette de la Délégation Général pour l'Armement sans qui cette aventure d'un cours introductif à la cyberdéfense d'entreprise n'aurait pu démarrer.

Un grand merci aussi à nos auditeurs du Conservatoire de National des Arts et Métiers (CNAM) pour leur participation active à ce cours SEC101 grâce à qui cette compilation des notes d'enseignement a pu voir le jour, avec une mention spéciale aux contributeurs.

Contributions

(2019-2020) **David BATANY** - Cnam SEC101 : *Architecture et fonctionnement des Botnets*

(2020) **Céline JUBY** - Orange Cyberdefense : *Contributions d'amélioration et re-lectures*

Table des matières

I	CYBERRISK SEC101	
1	La gestion des risques	9
1.1	La gestion du risque numérique	9
1.2	L'analyse des risques	10
1.3	L'analyse de risque au coeur de l'architecture de gouvernance	13
II	Références et Index	
	Bibliographie	17
	Articles	17
	Ouvrages	18
	Index	18
	Index	18





CYBERRISK SEC101

1	La gestion des risques	9
1.1	La gestion du risque numérique	
1.2	L'analyse des risques	
1.3	L'analyse de risque au coeur de l'architecture de gouvernance	

La gestion des risques

1.1 La gestion du risque numérique

Avant de parler de gestion des risques, il convient de rappeler la simple définition du risque.

Le risque est la probabilité qu'un évènement ayant un impact négatif se produise. Il peut être lié à différents domaines, tels que l'investissement, la santé, la sécurité, etc. Dans le contexte de l'investissement, le risque peut être défini comme la possibilité de perdre de l'argent en raison de fluctuations imprévues des marchés financiers. Dans le domaine de la santé, le risque peut être lié à la probabilité de contracter une maladie ou d'avoir un accident. Dans le domaine de la sécurité, le risque peut être lié à la probabilité d'un incident ou d'une catastrophe. En général, le risque peut être considéré comme la possibilité d'une perte ou d'un dommage.

Le petit Robert nous donne 3 définitions :

- ▶ (1) Danger éventuel plus ou moins prévisible

- ▶ Éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage.
- ▶ Fait de s'exposer à un danger.

La gestion du risque numérique est un enjeu à large spectre dans l'entreprise. Il inclut les processus de planification et de mise en œuvre de mesures pour gérer et minimiser les risques de sécurité liés à l'utilisation de systèmes et technologies numériques. Il faut y inclure les systèmes internes (Systèmes d'information d'entreprise, produits et services vendus, et les services externes utilisées qu'ils soient des services dans le cloud, ou des services de communication ou de réseaux sociaux). Elle implique de prendre en compte les risques potentiels sur toutes les dimensions de d'usage auxquels une organisation peut être exposée en raison de l'utilisation de ces technologies et de déterminer les mesures de sécurité appropriées pour les gérer.

La gestion du risque numérique implique généralement trois grandes étapes :

- ▶ Identification des risques : Identifier les menaces et les vulnérabilités potentielles auxquelles une organisation peut être exposée en raison de l'utilisation du numérique ;
- ▶ Évaluation des risques : Déterminer l'impact potentiel et la probabilité de chaque risque identifié ;
- ▶ Gestion des risques : Décider des mesures de sécurité appropriées pour gérer les risques identifiés, en fonction de leur impact et de leur probabilité.

1.2 L'analyse des risques

👁 avec une rappel de la définition du risque :


$$Risque = \frac{Evènement\ redouté \otimes Fragilités \otimes Gain\ pour\ attaquant}{Moyens \otimes Risques\ pour\ attaquant} \quad (1.1)$$

On ne peut démarrer sur la cybersécurité d'entreprise sans se poser la question des enjeux de cette défense. Les premiers pas d'une démarche de cybersécurité est de passer par l'identification de ces risques que l'on appelle généralement



Éléments de Sécurité Opérationnelle

« management par les risques ». L'identification des actifs les plus sensibles de l'organisation ou de l'entreprise nécessite de bien identifier les fondamentaux de l'organisation. Il ne faut surtout pas se focaliser sur les problématiques techniques ou technologiques lorsque l'on souhaite sécuriser ces systèmes d'information. En effet les activités techniques ne représentent qu'un aspect de la démarche qui, pour réussir, doit couvrir l'ensemble du spectre des activités de l'entreprise. Avant donc de mettre en proposer des processus décrits dans des procédures ou des mesures techniques, il est indispensable de conduire une analyse des risques (gestion des risques) qui permettra de rédiger par la suite une politique de sécurité sur la base des éléments les « plus » importants pour la continuité de l'entreprise. Il existe un corpus normatif sur la gestion de risque au sein de l'ISO quoi se concrétise par la norme ISO/CEI 27005 publiée initialement en 2008. Cette norme adresse la gestion des risques dans le domaine de la Sécurité des Systèmes d'information. Cette norme a été structurée pour aider à déployer une approche méthodique de gestion du risque. Son usage s'inscrit dans un cadre plus large du déploiement du « Système de Management de la Sécurité de l'information », où cette norme vient directement en appui des concepts généraux énoncés dans la norme ISO 27001, dont elle complète le chapitre 4.2. La norme ISO 27005 ne décrit qu'une démarche et un vocabulaire de référence, c'est pour cela qu'ont émergé des méthodes plus opérationnelle pour conduire les analyses de risques de manière guidées et plus détaillées. En France, la méthode Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) soutenue par l'ANSSI est celle la plus largement utilisée, mais certains utilisent des méthodes comme CRAMM, MEHARI etc...

Cette partie est un condensé très rapide des éléments sur l'analyse de risque. Pour disposer des méthodes précises et des outils techniques pour pratiquer des analyses de risques lisibles et compréhensibles par tous les acteurs de la sécurité, le lecteur pourra se référer au site de l'ANSSI ou l'ensemble de la méthode EBIOS ¹ est décrite.

La méthode EBIOS, est une méthode qui permet à la fois d'identifier les risques et

1. <https://www.ssi.gouv.fr/guide/EBIOS-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/>

de les hiérarchiser dans le but de proposer des contre-mesures à ceux ci. EBIOS se compose de cinq modules. Les axes importants de cette méthodologie sont :

- ▶ Etude du contexte fonctionnel et technique ;
- ▶ Expression des besoins de sécurité ;
- ▶ Étude des menaces (fonctionnelles et techniques) pesant sur le périmètre audité ;
- ▶ Expression des objectifs de sécurité ;
- ▶ Détermination des exigences de sécurité.

Le premier module, étude du contexte, consiste à définir le contexte de travail avec le client. Ce dernier délimite un périmètre pour l'analyse de risques, qui pourra être redéfini avec la société d'étude grâce à son expérience afin de vérifier et d'ajuster le périmètre pour qu'il soit en adéquation avec l'étude. Le premier module est la principale force de la méthode EBIOS car il permet à la démarche de s'adapter au contexte de l'entreprise et d'être ajustée à ses outils.

Le second module, événements redoutés, se concentre uniquement sur les biens essentiels (information, service,....) que l'on cherche à protéger. Ce besoin de sécurité s'exprime selon des critères de sécurité suivants : la confidentialité, l'intégrité et la disponibilité (CID). Il faut ainsi identifier ces biens essentiels, estimer leurs valeurs, mettre en évidence les sources de menaces (gravité et vraisemblance) et montrer les impacts (économique, juridique....) sur l'organisme si les besoins ne sont pas respectés.

Le troisième module, les scénarios de menace, de la méthodologie EBIOS se concentre sur les biens supports. Ce sont les composants "réels/physiques" qui portent les biens essentiels. Les biens supports sont analysés concrètement à travers leur architecture, leur flux,... et les menaces et leurs sources sont identifiées.

Le quatrième module, les risques, a pour but de lister les risques qui sont des événements redoutés lié à des scénarios.

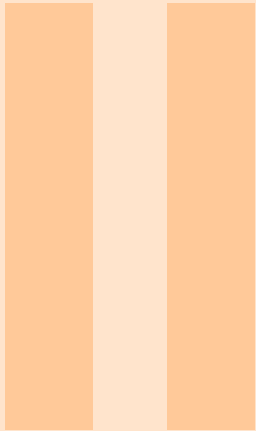
Le but du dernier module, les mesures de sécurité, est de proposer des contre-mesures aux risques identifiés précédemment, afin de réduire la vraisemblance des risques et leurs impacts.



1.3 L'analyse de risque au coeur de l'architecture de gouvernance

⚙️ chapitre en cours de rédaction, DRAFT non publiable ⚙️

Orange Only



Références et Index

Bibliographie 17

Articles

Ouvrages

Index 18

Index 18

Références

Articles

- (1) Sofia BARIM. « Développer la culture sécurité de l'information numérique de son organisation ». In : *I2D-Information, données & documents* 55.3 (2017), pages 49-50.
- (2) Anton CHUVAKIN. « The complete guide to log and event management ». In : *White Paper* (2010).
- (5) Quentin GAUMER. « Cybersécurité dans un contexte d'intelligence économique ». In : *I2D-Information, données & documents* 55.3 (2017), pages 32-33.
- (6) Karen KENT et Murugiah SOUPPAYA. « Guide to computer security log management ». In : *NIST special publication* 92 (2006).
- (9) Fred B SCHNEIDER. « Cybersecurity education in universities ». In : *IEEE Security & Privacy* 11.4 (2013), pages 3-4.
- (10) Bruce SCHNEIER. « Attack trees ». In : *Dr. Dobbs's journal* 24.12 (1999), pages 21-29.
- (11) Lei SHEN. « The NIST cybersecurity framework : Overview and potential impacts ». In : *Scitech Lawyer* 10.4 (2014), page 16.
- (12) Chee-Wooi TEN, Chen-Ching LIU et Govindarasu MANIMARAN. « Vulnerability assessment of cybersecurity for SCADA systems ». In : *IEEE Transactions on Power Systems* 23.4 (2008), pages 1836-1846.



Ouvrages

- (3) Anton CHUVAKIN, Kevin SCHMIDT et Chris PHILLIPS. *Logging and log management : the authoritative guide to understanding the concepts surrounding logging and log management*. Newnes, 2012.
- (13) Daniel VENTRE. *Cyberattaque et cyberdéfense*. Lavoisier, 2011.

index



Index

Risk Management, 9

Orange Only

Aborder la sécurité des systèmes d'information sous l'angle d'une sécurité dynamique est un axe qui depuis quelques années apporte de nouvelle manière d'aborder la protection, la défense, et la résilience des systèmes d'information. La transformation digitale de l'entreprise modifie et rend plus flous les périmètres des systèmes d'informations. Cela nécessite une approche élargie du risque numérique et des nouvelles architectures de cybersécurité. Malgré la mise en place de mesures et de technologies de protection de plus en plus élaborées, l'impact d'une attaque ayant franchi ces barrières a considérablement augmenté. Cette compilation des notes de cours élaborée dans le cadre d'un cours d'introduction à la gouvernance de la cybersécurité aborde une démarche de cyberdéfense d'entreprise construite à partir de quelques éléments fondamentaux. Protéger l'ensemble de l'entreprise alors qu'il est complexe de définir ses frontières est illusoire. Identifier les actifs essentiels ou vitaux et mettre en place les moyens adaptés à leur protection et leur défense est une démarche tactique qui permet de graduellement réduire ses cyber-risques. Issu de ce cours sur le déploiement de politiques de cyberdéfense, cet ouvrage décrit quelques éléments essentiels de sécurité opérationnelle permettant de fixer, à partir d'une analyse des risques, des priorités opérationnelles tant sur l'organisation des processus que des architectures de protection, de défense et de résilience.



Eric DUPUIS (Enseignant SEC101, Cnam Bretagne) est actuellement Directeur d'Orange Campus Cyber, le centre de formation et d'entraînement Cybersécurité et Cyberdéfense du groupe Orange après plusieurs années comme directeur sécurité de la société Orange Cyberdéfense. Ingénieur des corps techniques de l'armement du ministère des armées, il a exercé pendant plusieurs années à la Délégation Générale pour l'Armement / Maîtrise de l'information (DGA/MI) dans les domaines du renseignement, de la lutte informatique et de la cyberdéfense. Ingénieur du Conservatoire National des Art et Métiers, il y enseigne l'ingénierie et la sécurité du numérique. Auditeur de la 50ième session Armement et Economie de Défense de l'IHEDN (Institut des Hautes Etudes de la Défense Nationale), il intervient au profit de la Gendarmerie, en tant qu'Officier de Réserve Cyberdéfense.

CYBERDEF 101

