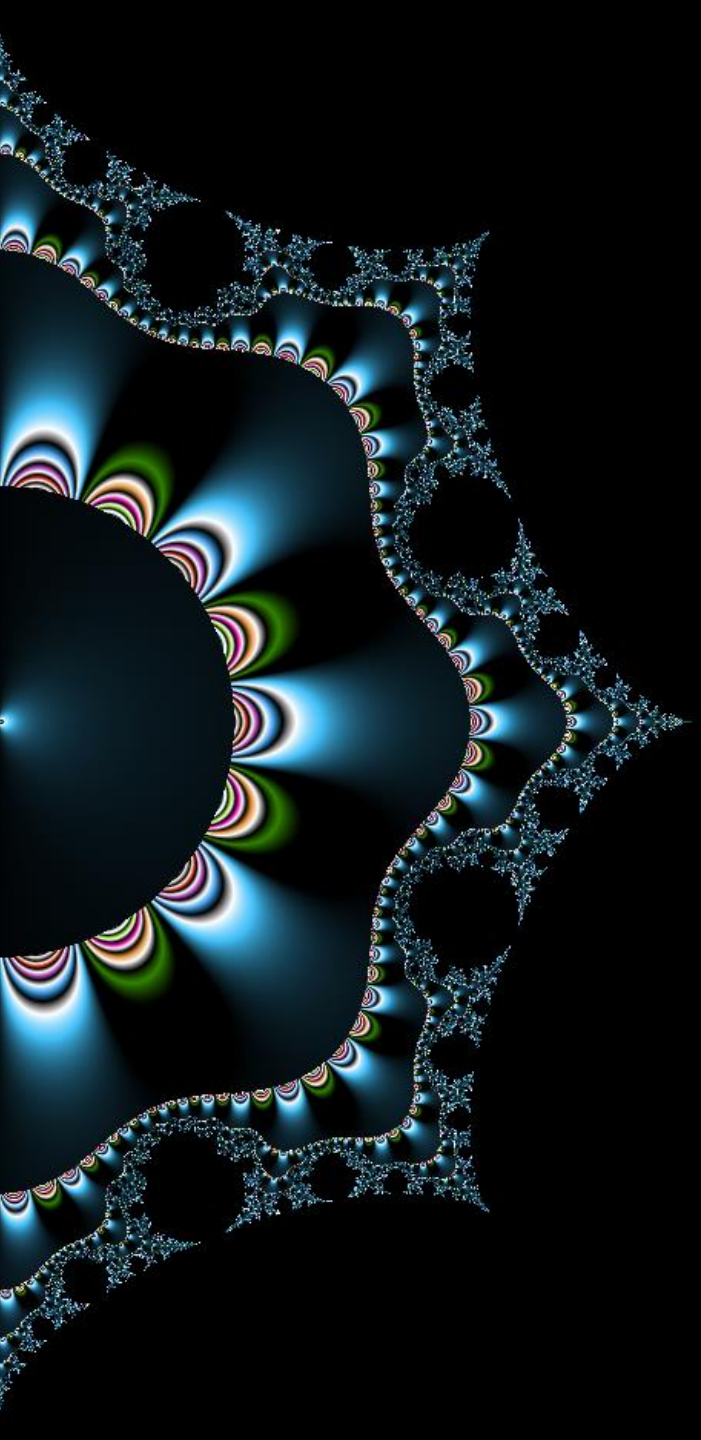

EBIOS RM

Cas Pratique, Partie 1
Ateliers 1, 2, 3

Thibaut HENIN

tbowan@arsouyes.org

Entreprise de communication

Conception, réalisation et hébergement de site web professionnels

Atelier 1

Cadrage et socle de sécurité

1 - Cadrage

Analyse de risque et mise en œuvre d’une PSSI

(Pérennisation de l’entreprise et Conformité RGPD)

2 - Périmètre métier

Valeur	Commerce	Développement	Hébergement
Nature	processus	processus	information
Description	Acquisition et suivi des clients.	Réalisation des sites et des modules spécifiques.	Sites web des clients
Responsable	DG	Dev.	Admin.
Biens associés (et description)	PC Portable Fichiers clients Comptabilité	PC Fixe Dépôts git Maquettes	Serveurs physiques Machines virtuelles Accès internet
Responsable	-	-	-

3 – Événements redoutés

Métier	Évenement	Impact	Gravité
Commerce	Perte du fichier de prospection	Commercial (perte de contrats)	3
	Perte de la comptabilité	Financier & juridique	4
	Vol des fichiers clients	Commercial (concurrence) Juridique (RGPD)	2
Développement	Perte du code source	Fonctionnement	3
	Vol du code source	Concurrence	1
Hébergement	Perte d'exploitation Accès frauduleux	Financier (pénalités) Commercial (image de marque) Juridique (RGPD)	4

4 – Socle

Référentiel	Etat	Justifications
RGPD	Néant	
Guides d'hygiène de l'ANSSI	Partiel	Hébergement uniquement

Atelier 2

Sources de risques

Sources de Risques / Objectifs visés

Source de risque	Objectifs visés	Motivation	Ressources	Activités	Pertinente
Criminels	Extorsion (ransomware)	+++	++	+++	Haute
Criminels	Recel (cambriolage)	++	++	+++	Haute
Kiddies	Defaçage, botnet, …	++	++	++	Moyenne
Vengeur	Sabotage	+	++	++	Moyenne
Concurrent	Vol d’informations	++	+	+	Faible
Concurrent	Sabotage	+	++	+	Faible

Atelier 3

Scénarios stratégiques

Parties prenantes

Catégorie	Partie prenante	Dépendance	Pénétration	Maturité	Confiance	Niveau
Clients	PME / TPE	4	1	1	1	4
Prestataires	Infogérance	1	4	2	3	0,6
	FAI	4	1	3	4	0,3
Partenaire	Graphiste	2	3	1	2	3

Scénarios stratégiques

Source de risque	Objectif Visé	Chemin d'attaque	Gravité
Criminel	Extorsion	1. Ransomware, après phishing, un malware contamine les ordinateurs de l'entreprise. 2. Chantage, après intrusion sur une application web, menace de publication des données	4
Criminel	Recel	1. Cambriolage, après s'être introduit dans les locaux, vol du matériel informatique.	4
Kiddie	Defaçage	1. Defaçage, après intrusion sur une application (credential stuffing), modification des sites.	3
Vengeur	Sabotage	1. Sites web, après utilsation d'un accès, vol/suppression des données. 2. SI, après utilisation du réseau de l'entreprise, suppression des fichiers (commerce, comptabilité, codes sources, …).	3

Mesures de sécurité

Partie prenante	Chemin D'attaque	Mesure De sécurité
PME / TPE	Accès frauduleux	Sensibilisation des clients aux bonnes pratiques via la newsletter.
Graphiste	Accès frauduleux	Suppression de l'accès privilégié

Catégorie	Partie prenante	Dépendance	Pénétration	Maturité	Confiance	Niveau
Clients	PME / TPE	4	1	1 ↗ 2	1	2
Prestataires	Infogérance	1	4	2	3	0,6
	FAI	4	1	3	4	0,3
Partenaire	Graphiste	2	3 ↘ 1	1	2	3 ↘ 1