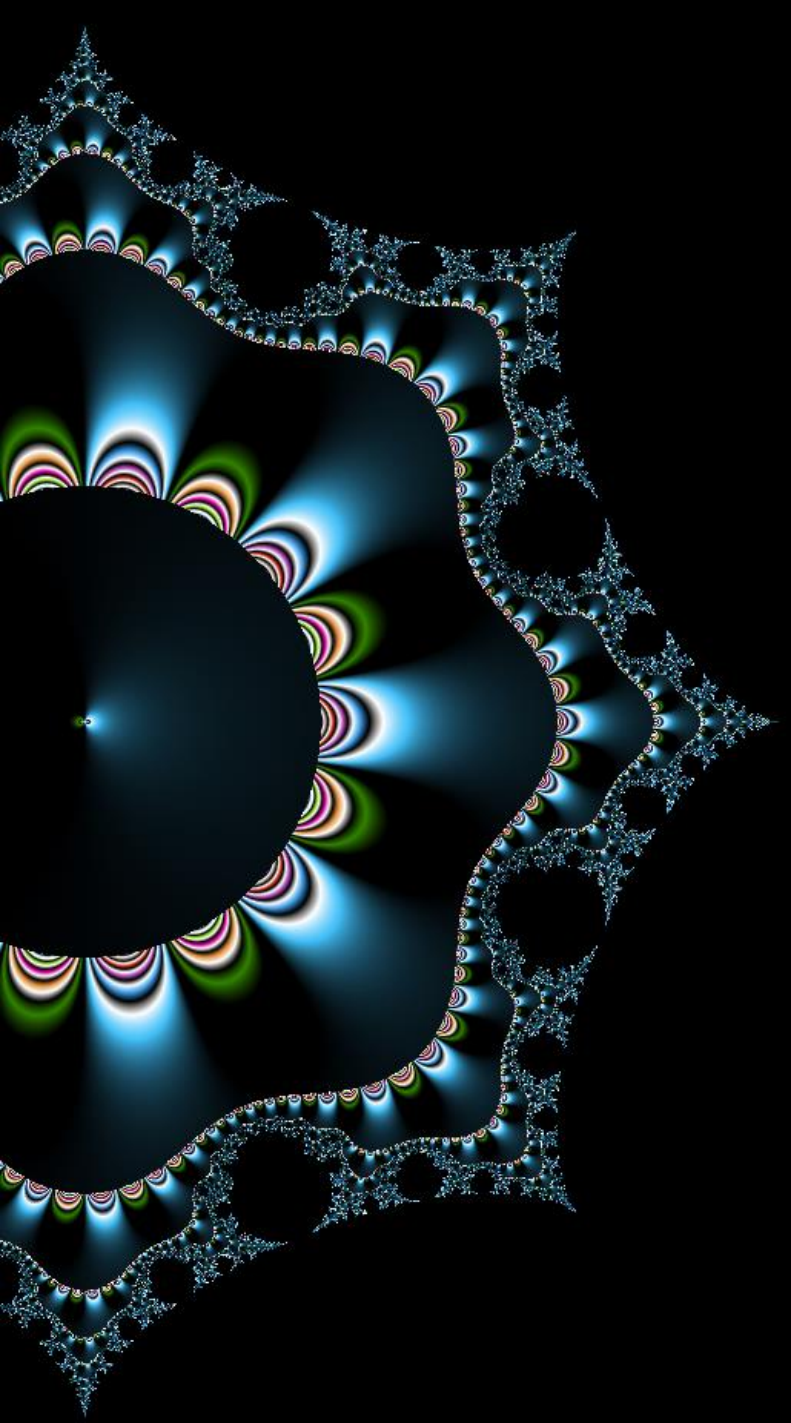


03 Introduction

Vulnérabilités, 0day, PSSI…

Corinne HENIN

www.arsouyes.org

C’est quoi une vulnérabilité ?

La gestion de risques

Biens
définition

Une ressource de l’entreprise

(information, matériel, fonction, …)

Qui doit être protégée

(accès frauduleux)

Propriété de sécurité

Triptyque sacré

Confidentialité

(la ressource n'est accessible qu'aux personnes autorisées)

Disponibilité

(la ressource est accessible quand on en a besoin)

Intégrité

(la ressource n'est modifiée que par des actions légitimes)

Mais aussi
(attention au schisme)

Authenticité

(la ressource est celle qu'auteur m'a envoyé)

Traçabilité

(Les accès et tentatives d'accès à la ressources sont tracés et les traces sont conservées)

Non répudiation

(Personne ne peut contester les actions qu'il effectuer sur une ressource
Personne ne peut s'attribuer les actions d'une autre personne)

Matrice de couverture

Des biens par les propriétés

Bien	Confidentialité	Disponibilité	Intégrité
Articles du blog			✓
Navigateur web	✓		✓
Mots de passe	✓		✓
Fichiers de configuration	✓		✓
Code source			✓

Exemple fictif d'un blog

Menaces

Evènement redouté

(panne d'internet, ransomware, cambriolage, insider …)

Matrice de couverture

Des biens par les menaces

Bien	Besoin	Modification d'un article	Exécution de code sur navigateur	Modification de fichiers source
Articles de blog	Intégrité	✓	✓	✓
Navigateurs	Intégrité		✓	✓
	Confidentialité		✓	✓
Mots de passe	Intégrité			✓
	Confidentialité			✓
Fichiers de conf	Intégrité			✓
	Confidentialité			✓
Code source	Intégrité			✓

Exemple fictif d'un blog

Criticité

Produit de deux paramètres

Gravité

conséquences d'un incident sur un bien

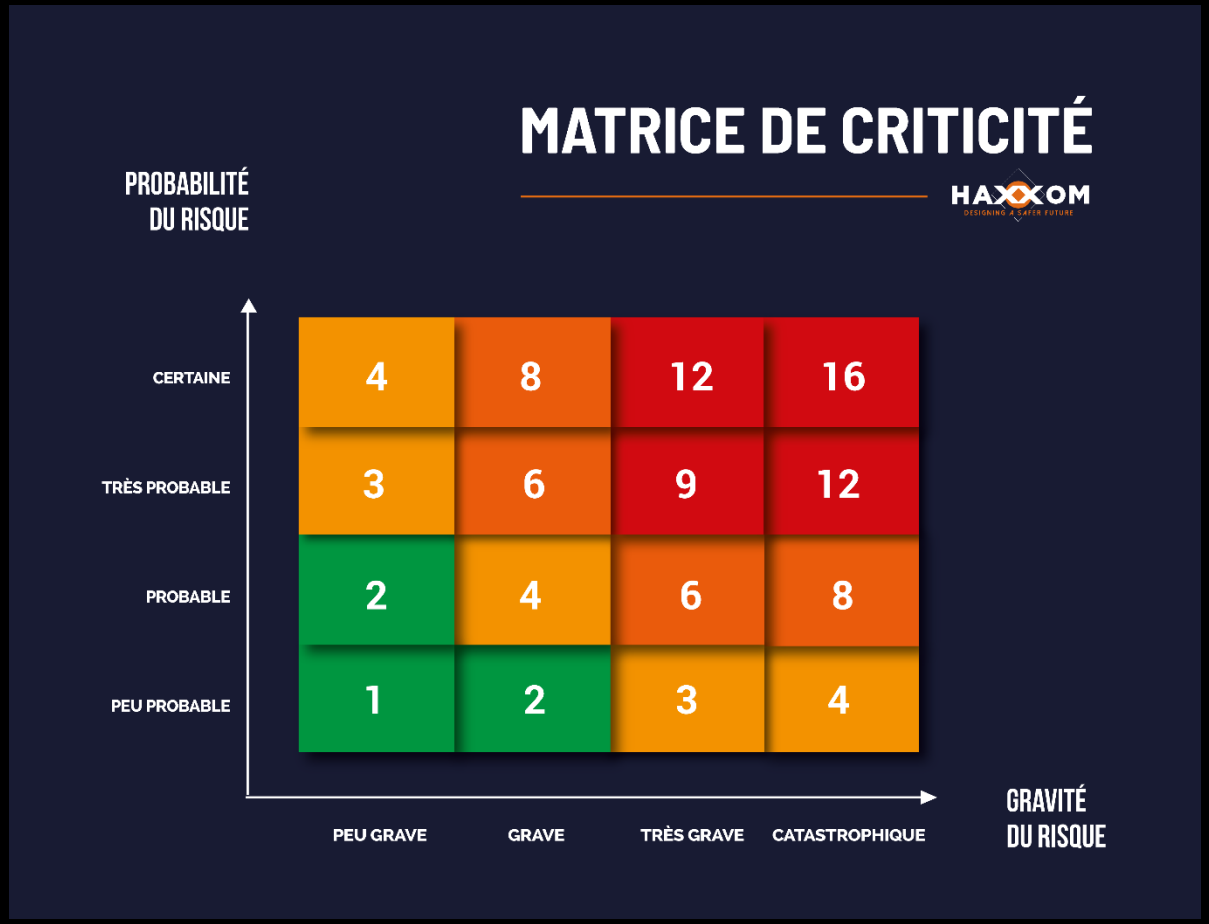
e.g. Sans connexion internet, pas de visio-conférence

Probabilité

facilité d'observation d'un incident

e.g. Des chutes de neiges, cassent des câbles téléphoniques

Criticité
Visuellement



https://www.haxxom.com/processus-management-des-risques/

Criticité

Exemple

Menace	Modification article	Exécution de code	Modification source
Gravité	1 – Peu grave	3 – Très grave	4 - Catastrophique
Vraisemblance	2 – Probable	4 – Très probable	2 –Probable
Criticité	2	9	8

Mesures

Choses à mettre en place pour contrer les menaces

Eg. Contrôle d'accès, sauvegardes, mises à jour, sensibilisation, surveillance du réseau…

Et rendre les risques acceptables

Matrice de couverture

Des menaces par les protections

Mesure	Modification d'article	Exécution de code	Modification des source
Authentification	✓		
Filtrage des données		✓	✓

Menace	Modification d'article	Exécution de code	Modification des source
Gravité	1 → 1 – Peu grave	3 ↘ 2 – Grave	4 ↘ 2 – Grave
Vraisemblance	2 ↘ 1 – Peu probable	4 ↘ 1 – Peu probable	4 ↘ 2 – Probable
Criticité	2 ↘ 1	9 ↘ 3	8 ↘ 4

Exemple fictif d'un blog

PSSI

Ou comment gérer ces risques

Définition…

Plan d'actions définies
pour maintenir
un certain niveau de sécurité

(wikipedia)

Du coup,
c’est quoi une vulnérabilité ?

Vulnérabilité

Contournement de la PSSI

Exploit

Programme qui automatise la vulnérabilité

Naissance

Pourquoi il y a des vulnérabilités ?

Par Négligence

« Tant que ça marche, on ne touche à rien »

Par conservatisme

« On a toujours fait comme ça ! »

Par dette technique

« C’est trop long de faire propre »

« On corrigera plus tard »

Par Incompétence

« Je ne savais pas »

Par Paresse

« C’est trop chiant »

L’erreur est humaine

« Mince, je ne l’avais pas vu »

Découverte

Par qui ? Pourquoi ?

C’est un métier
plutôt deux fois qu’une

Audit de sécurité

Dans le cadre d’une mission planifiée par l’entreprise ou l’éditeur.

Bug Bounty

Programme de rémunération

Opportuniste (vs organisé)

Publier ou pas ?

Troll des années 90

Full disclosure

(publier)

No Disclosure

(garder pour soi)

Forcer la correction

(et devenir célèbre)

Éviter l’exploitation

(et devenir riche)

Responsible Disclosure

Le meilleur des deux mondes

Avertir l’éditeur

(négocier un délais)

Ne publier qu’ensuite

(et devenir célèbre)

Et toucher une récompense

(et devenir riche)

Registre des vulnérabilités

CVE

(Common Vulnerability and Exposure)

Identifiant unique

(CVE-AAAA-NNNN)

Edité par le MITRE :

https://www.cve.org/

Mesure du Risque (score cvss)

Score de base

Options

Vraisemblance

Exploitation

Vecteur, Complexité, Authentification

Temporelle

Exploit, correctif, confiance

Gravité

Impact

Confidentialité, Intégrité, Disponibilité

Environnement

Contexte d’utilisation

Que faire ?

En tant qu'éditeur du logiciel vulnérable

Contexte

Dissymétrie de l'affrontement

	Blue team (défenseurs)	Red team (attaquants)
Défaite	Conséquences Globalement graves	-
Victoire	-	Conséquences Globalement positives

Autruche optimiste

Ça marche, tout va bien

On verra plus tard

Qui voudrait nous attaquer ?

Perfectionniste paranoïaque

Tout doit être parfait

Une vulnérabilité est preuve d’incompétence

Il reste toujours un risque

Humilité constructive

Où sont les faiblesses

Comment les corriger

Amélioration continue

« Ce n’est pas parfait, mais on y travaille »