RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

COLLECTION GESTION DES RISQUES CYBER

GUIDE EBIOS RISK MANAGER
FICHE METHODE 4 – Atelier 2

IDENTIFIER ET CARACTERISER LES SOURCES DE RISQUE

Les fiches méthodes permettent aux responsables de la démarche d'analyse de risque d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

1 / CATEGORIES DE SOURCES DE RISQUE (SR) ET D'OBJECTIFS VISES (OV)

Cet atelier sur les sources de risque numérique, qui détermine le niveau de menace, est utile pour déterminer l'exposition du système d'information et donc le niveau de démarche d'homologation explicité dans le point 3.2 du guide sur l'homologation de sécurité[1]. Il est utile de faire appel aux experts en Cyber Threat Intelligence.

CATÉGORIES DE SOURCES DE RISQUE

Les profils d'attaquants peuvent être regroupés selon trois types de menace :

■ La menace activiste ou isolée qui regroupe des individus ayant peu de moyens, utilisant des outils peu sophistiqués. Ils peuvent néanmoins bénéficier d'accès privilégiés.

■ La menace systémique peut affecter une large proportion d'entités. Les attaques liées à cette menace ont principalement un but lucratif. Les auteurs

[1] https://messervices.cyber.gouv.fr/documents-guides/guide-homologation-securite-web-04-2025.pdf page 62.

de ces attaques utilisent généralement des outils du marché de type rançongiciels.

■ Enfin la menace stratégique s'illustre par la conduite d'attaques informatiques persistantes et ciblées. Elles peuvent être orchestrées par des états ou des grandes organisations, motivées et possédant d'importantes ressources.

Ces catégories peuvent collaborer de façon opportuniste ou organisée.

EXEMPLE : organisation terroriste faisant appel à un officines spécialisées (qui apparaîtra comme une unique source de risques). Les sources de risque peuvent être externes ou internes.

La grille suivante présente des catégories génériques de sources de risque intentionnelles et d'objectifs visés, que vous pouvez utiliser pour identifier les couples SR/OV.

◆

PROFILS D'ATTAQUANTS	EXEMPLES ET MODES OPÉRATOIRES HABITUELS
ORGANISATION ÉTATIQUE	États, agences de renseignement. *Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire prédéfinis. Ce profil d'attaquant se caractérise par sa capacité à réaliser une opération offensive sur un temps long (ressources stables, procédures) et à adapter ses outils et méthodes à la topologie de la cible. Par extension, ces acteurs ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day) et certains sont capables d'infiltrer des réseaux isolés et de réaliser des attaques successives pour atteindre une ou des cibles (par exemple au moyen d'une attaque visant la chaîne d'approvisionnement).*

ORGANISATION CRIMINELLE	Organisations cybercriminelles (mafias, gangs, crime organisé). *Arnaque en ligne ou au président, demande de rançon ou attaque par rançongiciel, exploitation de réseaux de « machines robots » (botnet), etc. En raison notamment de la prolifération de kits d'attaques facilement accessibles en ligne, les cybercriminels mènent des opérations de plus en plus sophistiquées et organisées à des fins lucratives ou de fraude. Certains ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day).*
ORGANISATION TERRORISTE	Cyberterroristes, cybermilices. *Attaques habituellement peu sophistiquées mais menées avec détermination à des fins de déstabilisation et de destruction : déni de service (visant par exemple à rendre indisponibles les services d'urgence d'un centre hospitalier, arrêts intempestifs d'un système industriel de production d'énergie), exploitation de vulnérabilités de sites Internet et défigurations.*
CONCURRENT	Concurrents déloyaux, ils peuvent faire appel à des officines spécialisée en paravent. *Vol d'information ou sabotage pour obtenir un avantage concurrentiel.*
ACTIVISTE	Cyber-activistes, groupements d'intérêt, sectes. *Modes opératoires et sophistication des attaques relativement similaires à ceux des cyberterroristes mais motivés par des intentions moins destructrices. Certains acteurs vont mener ces attaques pour véhiculer une idéologie, un message (exemple : utilisation massive des réseaux sociaux comme caisse de résonnance).*
OFFICINE SPECIALISEE	Ce profil est doté de capacités informatiques généralement élevées sur le plan technique. Il est de ce fait à distinguer des *script-kiddies* avec qui il partage toutefois l'esprit de défi et la quête de reconnaissance mais avec un objectif lucratif. De tels groupes peuvent s'organiser en officines spécialisées proposant de véritables services de piratage. *Ce type de hacker chevronné est souvent à l'origine de la conception et de la création d'outils et kits d'attaques[2] accessibles en ligne (éventuellement monnayés) qui sont ensuite utilisables « clés en main » par d'autres groupes d'attaquants. Il n'a pas de motivations particulières autres que le gain financier.*
AMATEUR	Profil du hacker « *script-kiddies* » ou doté de bonnes connaissances informatiques, et motivé par une quête de reconnaissance sociale, d'amusement, de défi. *Attaques basiques mais capacité à utiliser les kits d'attaques accessibles en ligne.*
COLLABORATEUR	Collaborateur actuel ou passé d'une organisation. Il possède des connaissances sur la structure interne de l'entreprise, le ou les systèmes d'information utilisés (et leur version) ainsi que les différents collaborateurs. *Ce profil d'attaquant se caractérise par sa connaissance interne des systèmes et processus organisationnels, ce qui peut le rendre redoutable et lui conférer un pouvoir de nuisance important.*
TIERS OPPORTUNISTE	Les motivations de ce profil d'attaquant sont d'ordre opportuniste et parfois guidées par l'appât du gain (***exemples : client malhonnête, escroc, fraudeur etc).*** *Ici, l'attaquant va découvrir de manière fortuite une vulnérabilité qu'il va tenter d'exploiter.*

CATÉGORIES D'OBJECTIFS VISÉS

FINALITÉS	DESCRIPTION

2 Citons les services de type *Crimeware as a Service* (CaaS)

POURSUIVIES	
ESPIONNAGE	Opération de renseignement (étatique, économique). Dans de nombreux cas, l'attaquant s'installe durablement dans le système d'information et en toute discrétion. L'armement, le spatial, l'aéronautique, le secteur pharmaceutique, l'énergie ou encore certaines activités de l'État (économie, finances, affaires étrangères) constituent des cibles privilégiées.
PRÉPOSITIONNEMENT STRATÉGIQUE	Prépositionnement visant généralement une attaque sur le long terme, sans que la finalité poursuivie soit clairement établie (exemples: compromission de réseaux d'opérateurs de télécommunication, infiltration de sites Internet d'information de masse pour lancer une opération d'influence politique ou économique à fort écho). La compromission soudaine et massive d'ordinateurs afin de constituer un réseau de robots peut être affiliée à cette catégorie.
INFLUENCE	Opération visant à diffuser de fausses informations ou à les altérer, mobiliser les leaders d'opinion sur les réseaux sociaux, détruire des réputations, divulguer des informations confidentielles, dégrader l'image d'une organisation ou d'un État. La finalité est généralement la déstabilisation ou la modification des perceptions.
ENTRAVE AU FONCTIONNEMENT	Opération de sabotage visant par exemple à rendre indisponible un site Internet, à provoquer une saturation informationnelle, à empêcher l'usage d'une ressource numérique, à rendre indisponible une installation physique. Les systèmes industriels peuvent être particulièrement exposés et vulnérables au travers des réseaux informatiques auxquels ils sont interconnectés (exemple : envoi de commandes afin de générer un dommage matériel ou une panne nécessitant une maintenance lourde). Les attaques en déni de service distribué (DDoS) sont des techniques largement utilisées pour neutraliser des ressources numériques.
LUCRATIF	Opération visant un gain financier, de façon directe ou indirecte. Généralement liée au crime organisé, on peut citer : escroquerie sur Internet, blanchiment d'argent, extorsion ou détournement d'argent, manipulation de marchés financiers, falsification de documents administratifs, usurpation d'identité, etc. Il est à noter que certaines opérations à but lucratif peuvent recourir à un mode opératoire relevant des catégories ci-dessus (exemple: espionnage et vol de données, rançongiciel pour neutraliser une activité) mais l'objectif final reste financier.
DÉFI, AMUSEMENT	Opération visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de simple amusement. Même si l'objectif est essentiellement ludique et sans volonté particulière de nuire, ce type d'opération peut avoir de lourdes conséquences pour la victime.

2 / Formalisation des couples SR/OV

L'analyse des couples SR/OV peut être documentée dans un tableau, tel que celui proposé ci-après (P1 : couple SR/OV prioritaire, P2 : couple secondaire) :

IDENTIFICATION		COTATION			CARACTÉRISATION				ÉVALUATION	
Source de risque (SR)	Objectif visé (OV)	Motivation	Ressources	*Activité*	*Modes opératoires*	*Secteurs d'activités*	*Arsenal d'attaque*	*Faits d'armes*	Pertinence du couple SR/OV	Choix P1/P2

Les ressources incluent à la fois les capacités financières et matérielles de la source de risque, et son niveau de compétence en matière de cyberattaques. Cette compétence peut être également recherchée auprès d'officies spécialisées **(sophistication des modes opératoires, arsenal d'outils d'attaque, etc.).**

Les informations en *italique* sont optionnelles. Elles permettent de caractériser plus finement les sources de risque et nécessitent généralement le support d'une expertise avancée ou de bases de connaissances solides en analyse de la menace. Le niveau de pertinence d'un couple SR/OV peut être évalué à partir du niveau de motivation, des ressources et de l'activité. En l'absence d'informations suffisantes sur l'activité de la source de risque dans votre secteur, vous pouvez évaluer chaque couple SR/OV sur la seule base de sa motivation et de ses ressources, en utilisant par exemple la métrique ci-après :

		MOTIVATION			
		Faible	Significative	Importante	Maximale
RESSOURCES	Maximales	Moyen	Moyen	Elevé	Elevé
	Importantes	Faible	Moyen	Elevé	Elevé
	Significatives	Faible	Faible	Moyen	Elevé
	Faibles	Faible	Faible	Moyen	Moyen

Une représentation sur des cartographies visuelles de type radar est également recommandée pour faciliter la sélection des couples SR/OV prioritaires et valoriser les résultats de l'atelier. Dans l'illustration ci-après, deux angles de vue sont représentés (par sources de risque et par objectifs visés), ce qui permet d'affiner l'exploitation des résultats de l'atelier.

La distance radiale correspond au niveau de pertinence évalué pour l'élément (plus les cercles sont proches du centre, plus ils sont estimés dangereux pour l'objet de l'étude). La sélection des couples SR/OV est réalisée en privilégiant des couples situés près du centre et suffisamment éloignés les uns des autres, afin de disposer d'un panel de sources de risque et d'objectifs visés varié.