2024

Collectivités & cybermenaces : entre exposition aux risques et moyens, comment placer le curseur au bon niveau ?

Un livre blanc SOFTEAM
UNE MARQUE DE DOCAPOSTE

www.softeam.com

Sommaire

Introduction

Qu'est-ce qu'un risque pour une collectivité territoriale ?

La première idée est sans doute de penser aux nombreux risques qui ont toujours ponctué la vie de nos sociétés : le risque de catastrophes naturelles, renforcé par le réchauffement climatique ; le risque sanitaire, à l'image du Covid-19 ; le risque sécuritaire et bien d'autres.

Ces différents risques se définissent par le danger qu'ils font porter sur la vie de nos concitoyens.

Il en existe un, plus récent, souvent moins mis en avant du fait des conséquences humaines moins graves que les autres mais qu'il serait néanmoins dommageable d'ignorer : le risque cybernétique.

Avec la profonde transformation numérique de notre société, la dépendance aux outils informatiques s'est accentuée. Il en découle également une complexification des écosystèmes numériques, avec une multiplication du nombre d'acteurs – prestataires, partenaires, clients, etc. Bien que cette transformation apporte de nombreux bénéfices, elle a fait naître de nouvelles préoccupations pour la continuité des services publics et la protection des données de nos concitoyens face au risque cybernétique. En effet, cette digitalisation a attiré l'attention des cybercriminels, qui ont trouvé là un terrain de jeu idéal.

Le cabinet Asterès, dans son étude sur « le coût des attaques cyber réussies », donnait l'exemple en 2022 d'un coût total des cyberattaques réussies en France, tout secteur confondu, de 2 milliards d'euros, avec un coût moyen de 59 000 euros par attaque et des pertes de production estimées à 7 millions d'heures de travail[1].

La cybersécurité est, aujourd'hui, devenue un sujet aussi incontournable que la gestion de la voirie ou le bon fonctionnement de l'éclairage public pour maintenir une vie publique sereine et fluide pour les citoyens.

Ce livre blanc a pour ambition de vous donner les clés pour mieux appréhender le risque cyber et les enjeux associés pour une collectivité territoriale. Quelle que soit votre situation ou le stade auquel vous en êtes dans la mise en œuvre de mesures de sécurité, ce guide a été conçu pour relever ce défi crucial. Il vous donnera les outils pour non seulement maîtriser les risques numériques, mais aussi dessiner une stratégie cyber adaptée à vos besoins et vos ressources.

Nous nous adressons ici avant tout aux principaux décideurs des collectivités locales et leurs équipes concernées : les élus, les directions générales des services ou les directions des services informatiques, dont l'engagement est crucial pour instaurer un environnement numérique de confiance au sein de nos collectivités territoriales.

Chapitre 1
Comprendre le contexte cyber des collectivités territoriales : où en sommes-nous ?

Des collectivités territoriales exposées

Les politiques des collectivités territoriales ne prennent pas forcément en compte la portée de ces nouveaux enjeux. D'après une étude réalisée par Opinion Way pour Cybermalveillance.gouv.fr[2,3] auprès des collectivités de moins de 25 000 habitants, on constate une prise en compte limitée des questions de cybersécurité, avec un budget de moins de 2 000€ pour 75% d'entre elles et 12% seulement prévoient une augmentation des budgets cyber dans les prochaines années. Pour beaucoup par exemple, embaucher un responsable de la sécurité des systèmes d'information (RSSI) en interne n'est pas une priorité, mais un luxe qu'elles ne peuvent se permettre. Bien que l'on puisse observer une demande de conseils, d'outils et de solutions techniques pour la moitié de ces collectivités, le premier pas vers la cybersécurité reste, dans les faits, difficile à faire.

À titre de comparaison, 58% des PME françaises indiquent une hausse de leur budget consacré à la cybersécurité en 2024 selon HarfangLab[4].

Face aux nombreuses problématiques, sécuritaires, sanitaires, ... auxquelles sont confrontées les collectivités dans un contexte de manque structurel de ressources financières, ces chiffres peuvent refléter une priorisation plus faible de la cybersécurité.

Ce constat laisse apparaitre une capacité moindre du secteur public face au risque cyber, dans une période où la menace prend de l'ampleur, se professionnalise, affine ses modes opératoires, dans un contexte géopolitique tendu où la France devient une cible de choix pour de nombreux acteurs hostiles.

La stratégie du chalutage

Vincent Strubel, directeur de l'Anssi, a déclaré :

« Aujourd'hui, le crime organisé attaque de manière massive, il s'est outillé pour attraper tout ce qu'il peut, en particulier les plus fragiles[5] »

Ainsi, plus besoin d'être ciblé pour devenir une victime de cyberattaque :

- Les cyberattaquants ciblent large, à l'image d'un chalutier face à un banc de poissons, attrapant ce qui passe
- Les entités les moins préparées sont et seront les plus vulnérables

État de la menace cyber : des collectivités territoriales vulnérables

Aujourd'hui les menaces sont multiples, de plus en plus agressives, le risque numérique s'accroît au fur et à mesure que prolifèrent les attaques non-ciblées, massives et diffusées, à l'image de la « stratégie du chalutage ».

Les modes opératoires d'attaques se complexifient fortement ces dernières années. L'avènement de l'IA joue un rôle, permettant aux attaquants de scanner plus facilement un système pour y déceler des vulnérabilités ou d'envoyer des mails d'arnaques difficilement identifiables même pour un oeil averti.

De même, l'écosystème des acteurs malveillants évolue, alors que ce monde restait plutôt confidentiel, il s'est démocratisé à des acteurs moins initiés au monde numérique. On observe aujourd'hui le développement d'une économie parallèle de groupes criminels, qui louent l'utilisation de leurs programmes malveillants pour mener des attaques sur mesures.

Attaques à but lucratif

De nombreuses campagnes de cyberattaques sont menées par le crime organisé, car le retour sur investissement est très profitable. En raison du contexte géopolitique actuel, ils peuvent recevoir un soutien de la part de puissances étrangères, ayant des intérêts divergents des nôtres, soutien leur permettant d'opérer en toute impunité depuis le territoire de ces Etats.

Les attaques à but lucratif passent, par exemple, par l'injection d'un rançongiciel, qui bloque vos données en vous demandant une rançon.
Les cybercriminels cherchent, de surcroit, à exfiltrer vos données afin de les revendre à des acteurs malveillants.
Une collectivité peut stocker des données d'administrés qui ont une certaine valeur sur le marché noir.

Opérations de déstabilisation

Les attaques visant la France s'inscrivent dans une stratégie globale de déstabilisation des sociétés occidentales. Des puissances hostiles vont cibler des infrastructures, des entreprises, des administrations, que ce soit par leurs propres moyens, à travers le crime organisé, ou avec le concours de groupes d'hacktivistes, des hackeurs indépendants hostiles à la politique française, pour générer un sentiment d'insécurité chez nos concitoyens et entrainer une défiance envers l'état Français, ses institutions et ses politiques. Ces menaces sont renforcées par le contexte géopolitique actuel : guerre en Ukraine et confrontation indirecte avec la Russie, fortes tensions au Moyen Orient, au Sahel.

Contre les collectivités territoriales, l'attaquant va chercher à dégrader les services publics, soit en bloquant les équipements permettant la réalisation de ses missions, soit en défigurant un site internet, comme l'ont subi des centaines de communes après les attentats de Charlie Hebdo, avec des piratages de leurs sites affichant des messages idéologiques.[6]

Autres objectifs

D'autres objectifs peuvent décider un attaquant à cibler une collectivité territoriale.
Par exemple :

- La vengeance : une potentielle menace est celle d'un (ex-) employé qui cherche à se venger de son organisation ; En utilisant sa connaissance des systèmes et ses accès, il peut infliger des dommages importants.
- Le défi : certains hackeurs en herbe peuvent chercher à faire leurs armes sur des sites internet ou des systèmes d'information vulnérables et viser une collectivité territoriale.
- L'espionnage : en fonction de la taille et de l'importance stratégique d'une collectivité territoriale ainsi que des données sont elles disposent, elle peut faire l'objet de campagne d'espionnage de la part d'une puissance étrangère (hostile ou non).

Un risque cyber à prendre en compte et à prévenir

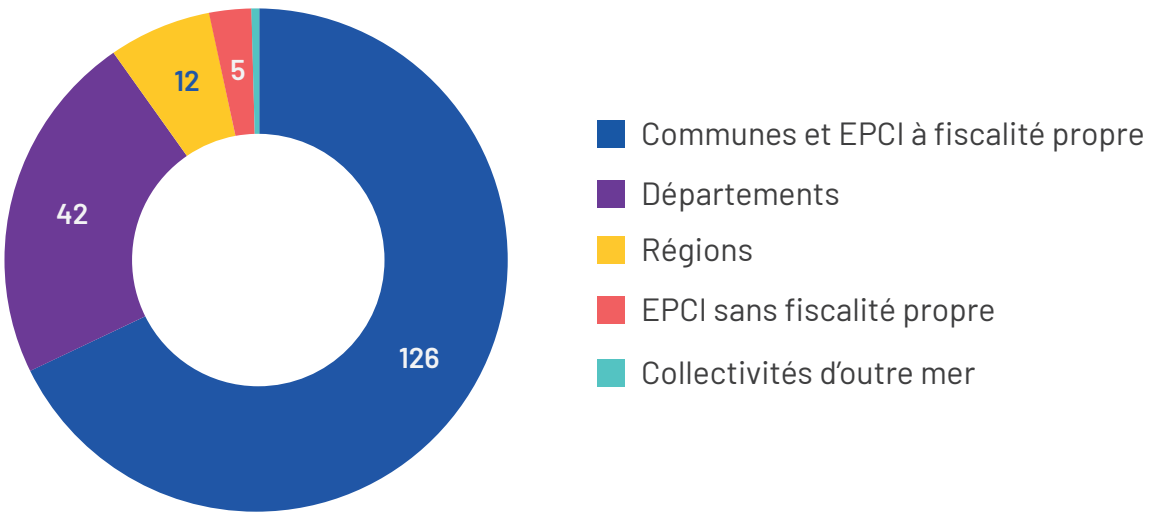
Lorsqu'une collectivité est concernée par un risque, elle cherche à le prévenir. Prenons un exemple concret : une commune se situant en zone inondable se prépare au risque d'inondation, en mettant en place des procédures à suivre en cas d'intempéries, des mesures d'évacuation, etc. De même, les collectivités qui, par nature, sont exposées au risque cyber devraient chercher à s'en prévenir, en mettant en œuvre les mesures usuelles nécessaires, de maitrise des risques, de détection de la menace, de réponse à incident, etc.

En France, entre janvier 2022 et juin 2023, l'Anssi, l'Agence nationale de la sécurité des systèmes d'information, a traité 187 cyberattaques contre des collectivités territoriales, affectant des communes comme des régions. Ce chiffre ne représente que les cyberattaques notifiées, donc les plus sévères[7].

Selon l'étude de cybermalveillance.gouv.fr citée plus haut, on observe une augmentation significative (multiplication par deux) de la volonté d'augmenter leur budget cyber pour les collectivités qui ont subi une cyberattaque. Pourquoi ? Parce qu'elles ont été confrontées aux conséquences de ces attaques et ont arbitré en faveur de l'allocation de ressources supplémentaires à la prévention de ce risque : « désormais, mieux vaut prévenir que guérir ».

La cybersécurité représente, pour une collectivité, un poste de dépense non négligeable face aux ressources limitées dont elle dispose et de ses nombreuses autres priorités. On ne se rend (malheureusement) compte de sa pertinence que lorsqu'elle nous fait défaut et que l'on en subit les conséquences.

Nombre d'incidents par type de collectivités territoriales



Les différents impacts d'une cyberattaque sur une collectivité territoriale

Financier

Peut entrainer de lourdes pertes financières en reprise d'activité et reconstruction du système d'information.

Exemple :

- Cyberattaque de la mairie de Lille en mars 2024.
- Le coût de l'attaque est évalué à un million d'euros, notamment en démarches administratives papiers a réaliser à posteriori.[8]

Opérationnel

Peut entrainer la dégradation, voire l'arrêt, de nombreuses activités d'une collectivité territoriale, avec l'impossibilité d'utiliser certaines applications et d'accéder à de nombreuses données.

Exemple :

- La cyberattaque de la mairie de Fleury-les-Aubrais en juin 2024 a entrainé la paralysie de nombreux services : état civil, cantine, inscription scolaire,
- Organisation des législatives après la dissolution de l'Assemblée Nationale fortement complexifiée,
- Les conséquences toujours perceptibles plusieurs mois après.[9]

Image

Peut entrainer la dégradation de l'image de la collectivité et de ses élus, avec une forte médiatisation de la crise.

Exemple :

- Cyberattaque de la mairie de Saint-Nazaire en avril 2024.
- Plusieurs dizaines d'articles de presse sur la cyberattaque et ses conséquences ont été publiés, de la presse locale à la presse nationale, spécialisée ou non.
- L'attaque a également été évoquée à la télévision et la radio nationale.
- Les conséquences sont toujours visibles 6 mois après, avec des articles encore publiés.

Par ailleurs, il ne faut pas oublier les potentiels autres impacts, juridiques (en cas de négligence, ou de non-conformité vis-à-vis la réglementation en vigueur : le RGS sur la sécurisation des communications et des systèmes d'information, le RGPD sur la protection des données, etc.), ainsi que psychosociaux (anxiété, stress, culpabilité, etc.).

Bien dimensionner sa réponse

Commençons par rappeler une réalité : le risque zéro n'existe pas en cybersécurité, quels que soient les investissements et les efforts mis en œuvre.

Cependant, mener une stratégie cyber générique sans connaître vos risques actuels peut vous amener à des investissements (financiers, humains) conséquents sans réel impact mesurable sur ceux-ci et plus globalement sur votre maturité cyber.

Comprendre vos enjeux et évaluer, en fonction de votre appétence aux risques, de vos contraintes financières et de vos spécificités, vos besoins en cybersécurité permet non seulement de contrôler vos coûts, mais également de faire un pas nécessaire vers votre résilience numérique, à destination de vos administrés. Et plus tôt vous vous y prenez, plus vous aurez de retombées positives.

Chapitre 2

Comment mettre en place un cadre numérique de confiance au sein de votre organisation ?

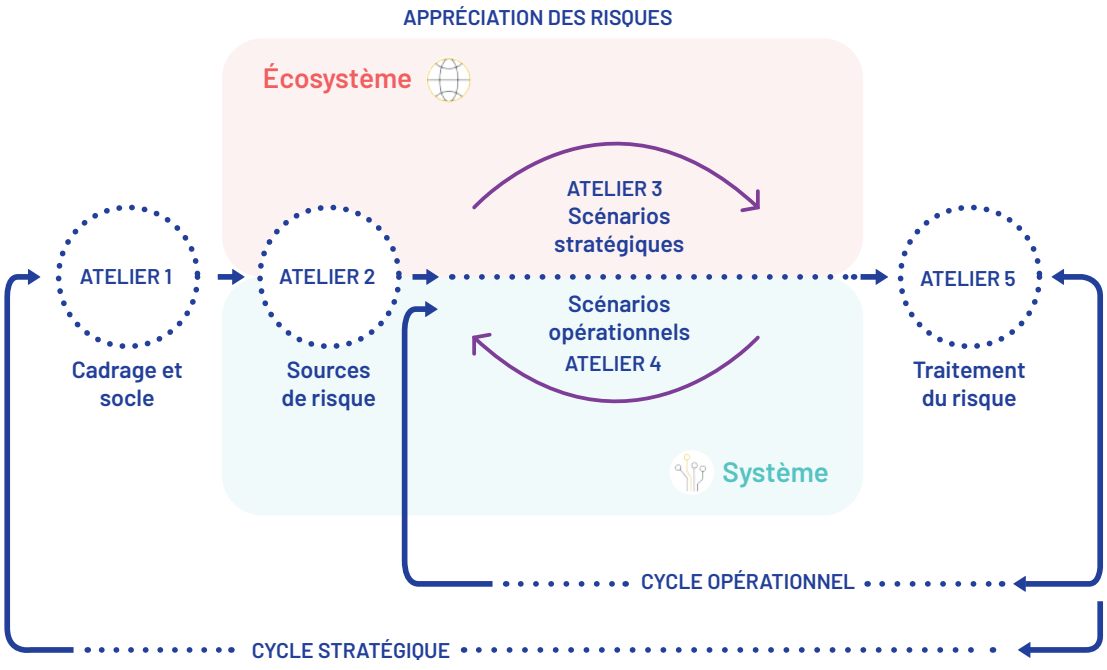
Rappelons que la cybersécurité n'est pas simplement la mise en place d'un antivirus ou d'un mot de passe, c'est surtout une discipline de gestion du risque : savoir évaluer sa maturité cyber, où allouer ses ressources humaines, techniques et financières, en fonction de ses lacunes et ses forces, pour maitriser ses risques. Pour mettre en place cette gestion du risque, la première étape consiste à mener une analyse de risque sur le périmètre concerné.

L'Anssi a développé la méthode EBIOS RM, une méthode d'appréciation et de traitement du risque numérique, pour répondre à cette problématique, et mettre en place un cadre numérique de confiance au sein de votre organisation.

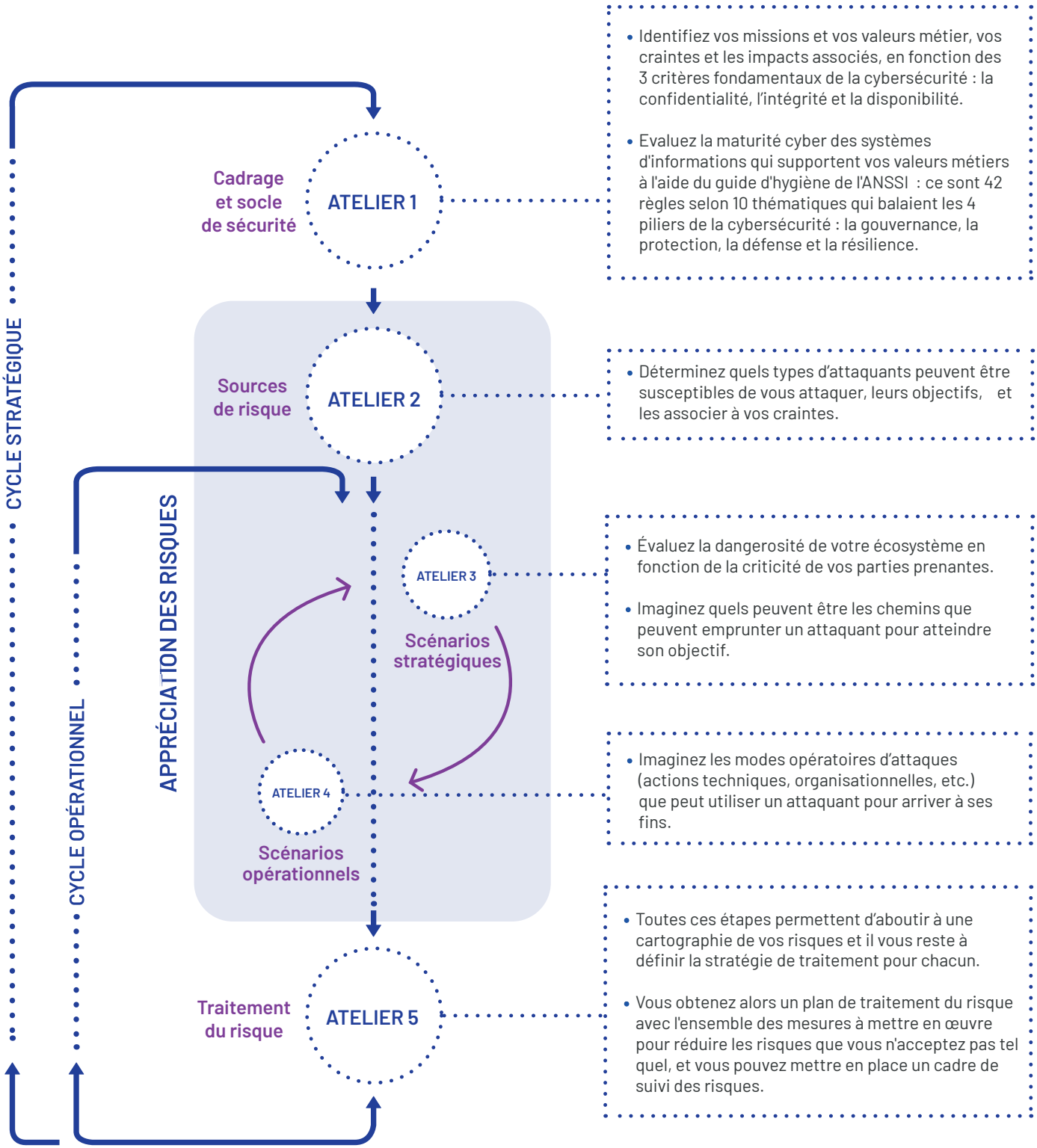
Construite autour de 5 ateliers interactifs, la méthode parcourt votre organisation de l'échelle stratégique à l'échelle technique, pour identifier les risques les plus critiques auxquels est confrontée une organisation, selon deux approches, par la conformité et par les risques. EBIOS RM ne cherche pas à être exhaustive, elle propose plutôt, pour chacun des ateliers, des pistes de priorisation en fonction du temps alloué à l'analyse de risque.

Son objectif est de donner aux décideurs des clés de compréhension des enjeux et des risques auxquels sont confrontés leur organisation, pour permettre un traitement des risques éclairé, une montée en maturité cyber avec une sécurisation renforcée de vos systèmes et une allocation optimale de vos ressources.

La méthode EBIOS RM en un schéma



La méthode EBIOS RM en une page



Dans la suite de ce livre blanc, nous allons expliquer plus en détail les grands principes de la méthode EBIOS RM, en vous donnant des clés de réussite et en les appliquant à un exemple à destination des collectivités territoriales.

Atelier 1 : cadrage et socle de sécurité

Périmètre de l'étude

On aborde toujours une analyse de risque du point de vue du défenseur, c'est-à-dire vous, afin de cadrer votre périmètre métier, technique et réglementaire.

La première étape est la détermination de ce qui a de la valeur pour vous, ce qui doit être protégé.

Il peut s'agir d'informations ou de processus clés liés à vos missions, on appelle cela les valeurs métier. Dans le cadre d'une collectivité locale, on peut par exemple penser aux activités de gestion de l'État Civil, des écoles, d'urbanisme.

Listez également ce qui supporte ces valeurs métiers, que ce soit un système d'information, un sous-ensemble d'un système d'information, un réseau spécifique et/ou des logiciels particuliers.

Ensuite, déterminez les besoins de sécurité de vos valeurs métier à l'aide des 3 critères fondamentaux (la confidentialité, l'intégrité et la disponibilité) selon une échelle que vous définirez.

Par exemple :

- Telle information peut-elle être diffusée à des partenaires ou doit-elle rester au sein de l'entité ? Doit-elle être restreinte à certains agents uniquement ?
- Quelle indisponibilité de telle activité est acceptable ? 4 heures ? 2 jours ? Pas plus de 5 minutes ?

Enfin, évaluez les impacts en cas de dépassement des besoins de sécurité que vous avez défini, autrement dit en cas de réalisation de l'événement redouté. Pensez aux impacts financiers, opérationnels, juridiques, liés à l'image, etc.

Il ne vous reste plus qu'à décider quels événements redoutés conserver pour la suite, en considérant en priorité ceux ayant des impacts forts pour vous.

Astuce

- En tant que collectivité, vous êtes en charge de missions extrêmement variées et pourriez donc être tentée de les matérialiser sous forme de nombreuses valeurs métier. Cependant, la méthode EBIOS RM est construite de telle manière que, sans entrer dans les subtilités, si l'on prend l'image d'un arbre, chaque atelier permet créer des branches que l'atelier suivant devra emprunter pour créer lui-même de nouvelles branches.

  Ainsi, l'activité d'analyse de risques peut devenir rapidement très chronophage si vous ne vous concentrez pas, pour chaque atelier, sur le plus important. S'il y a bien quelque chose à retenir, c'est que vous ne devez pas hésiter à mettre de côté des points moins critiques tant que vous tracez et justifiez toutes vos exclusions. Ainsi, ces points ne sont pas « perdus » et pourront être potentiellement traités lors d'une future itération de l'analyse de risque. Ce conseil est valable pour l'ensemble des ateliers que nous allons vous détailler dans ce livre blanc.

- Notre second conseil concerne la cotation des besoins de sécurité et des impacts. Bien qu'il soit possible de les classer selon des critères non quantifiables (« négligeables », « très importants » par exemple), nous vous recommandons de privilégier des échelles qui ne laissent que peu de place à l'interprétation et donc à des remises en question de la pertinence de tel scénario d'attaque ou de telle mesure de sécurité à ajouter.

Exemple d'échelles de besoin de sécurité en disponibilité :

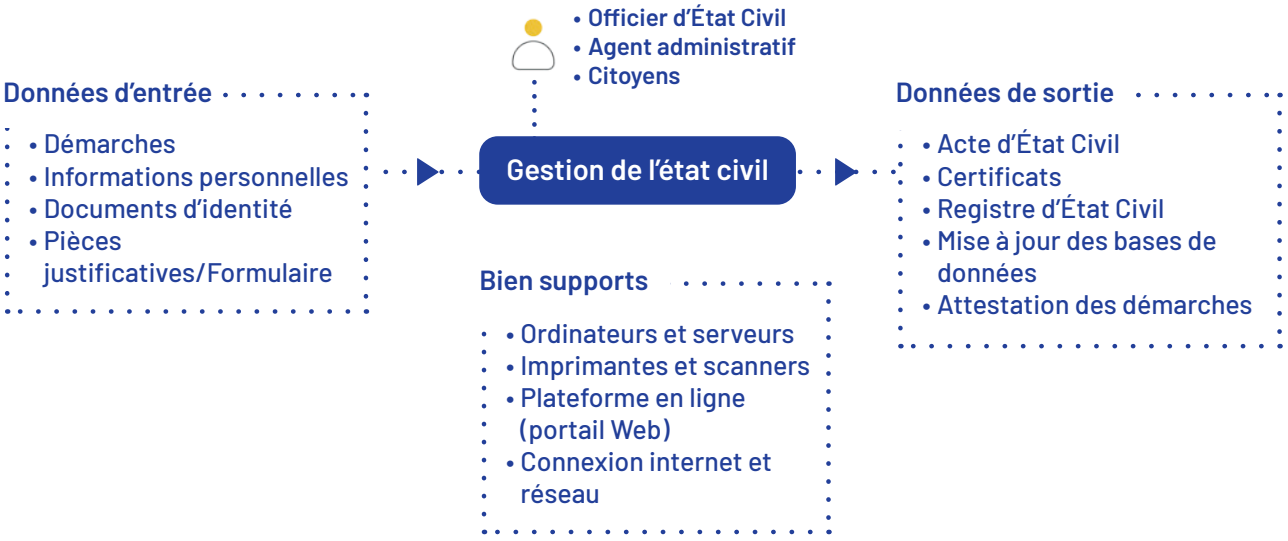
	Besoins de sécurité en disponibilité
1-Faible	Une indisponibilité de plus de 5 jours est acceptable. DIMA (délai d'indisponibilité maximal admissible) supérieur à 72 heures cumulées sur une période de 1 mois.
2-Moyen	Une indisponibilité entre 48 heures et 5 jours est acceptable et inacceptable au-delà de 5 jours. DIMA comprise entre 8 heures et 72 heures cumulées sur une période de 1 mois.
3-Important	Une indisponibilité entre 4 heures et 48 heures est acceptable et inacceptable au-delà de 48 heures. DIMA comprise entre 4 heures et 8 heures cumulées sur une période de 1 mois.
4-Critique	Une indisponibilité au-delà de 4 heures est inacceptable DIMA inférieure à 4 heures cumulées sur une période de 1 mois.

Pour appuyer notre démonstration, nous allons décliner un exemple unique de l'étude d'une des activités d'une collectivité territoriale, la gestion de l'État Civil.

Exemple

Activité : gestion du service de l'État Civil

L'activité de gestion de l'État Civil dans une commune englobe l'ensemble des tâches administratives liées à l'enregistrement et à la documentation des événements importants dans la vie des citoyens, tels que les mariages, décès, reconnaissances et autres changements d'État Civil. Cette activité est généralement assurée par le service d'État Civil de la mairie.



Besoins de sécurité		
Disponibilité	3-Important	Délai d'indisponibilité maximale admise : 6h
Intégrité	3-Important	Il peut y avoir une altération temporaire de l'intégrité si cela est identifiable et corrigible
Confidentalité	2-Moyen	Sensible, devant être diffusé de façon limitée à une liste publiée de destinatataires internes et externes

Activité	Événement redouté	Impacts	
		Opérations	Image
Gestion de l'État Civil	Accès non autorisé et modification des données personnelles	2-Moyen Justification : besoin de potentiellement provoquer une interruption de service pour enquêter ou restaurer des données.	3-Important Justification : médiatisation possible de l'évènement redouté, au minimum dans la presse régionale, induisant une dégradation de l'image de la collectivité.
	Indisponibilité du service causée par un rançongiciel	3-Important Justification : le service n'est plus rendu, nécessitant la mobilisation importante des acteurs IT et de potentiels prestataires, reconstruction potentielle des systèmes à organiser.	3-Important Justification : la dégradation du service public et la médiation possible de l'évènement, au minimum dans la presse régionale, porte atteinte à l'image de la collectivité.

Déterminer et évaluer le socle de sécurité

Après avoir cadré votre étude et formalisé vos besoins de sécurité relatifs à vos activités, l'approche par la conformité permet d'identifier les différents référentiels de sécurité qui s'appliquent au périmètre étudié. On observe plusieurs niveaux de référentiels de sécurité : des textes réglementaires (RGS, NIS 2, etc.), des politiques de sécurité internes à votre organisation, des normes, des règles d'hygiènes informatiques, etc.

Évaluez l'état d'application de ces référentiels, puis documentez et justifiez les écarts identifiés.

Vous venez alors de formaliser votre socle de sécurité, qui comprend l'ensemble des référentiels de sécurité applicables et l'état d'application de ces derniers.

Astuce

Lorsque votre périmètre d'étude n'est pas soumis à une réglementation, comme le RGS - Référentiel Général de Sécurité - ou NIS 2, nous vous préconisons tout d'abord d'utiliser le guide d'hygiène informatique de l'Anssi comme référentiel de base de votre socle de sécurité. Ce dernier décrit 42 règles de sécurité informatique réparties en 10 thématiques traitant les 4 piliers de la cybersécurité (Gouvernance, Protection, Défense, Résilience). Il constitue une base solide en matière de sécurité numérique, permettant de se tourner a posteriori vers d'autres référentiels de sécurité plus exhaustifs, comme par exemple, les normes de la famille ISO 27000.
L'étude de votre socle de sécurité peut être chronophage en fonction de la complexité technique du périmètre de votre étude, mais elle reste essentielle car elle permet d'obtenir une photographie de votre périmètre (tout d'abord déclarative, pouvant être complétée par des audits). À noter que la transparence et la sincérité sont nécessaires lors de l'évaluation de la mise en œuvre des différents référentiels, afin d'obtenir une photographie fidèle faisant ressortir les forces et les faiblesses au niveau du périmètre étudié.

Exemple

Type de référentiel	Nom du référentiel	État d'application	Écarts	Justification des écarts
Hygiène informatique	Guide d'Hygiène Informatique de l'Anssi	Partiel	Non-conformité avec la mesure 5 du guide de l'Anssi, qui recommande de maintenir les systèmes à jour pour prévenir les failles de sécurité.	L'antivirus n'est pas mis à jour assez fréquemment sur l'ensemble du parc.
			Non-conformité avec la mesure 19 de l'Anssi, qui préconise de segmenter les réseaux pour limiter les mouvements latéraux et protéger les systèmes sensibles.	Les systèmes de la mairie, y compris ceux contenant des données sensibles et ceux utilisés pour des services courants, ne sont pas segmentés de manière adéquate.

Atelier 2 : source de risque

Maintenant que vous avez défini votre socle de sécurité, que vous connaissez votre périmètre, son état de sécurisation et vos craintes, la prochaine question à vous poser est : qui est susceptible de vous attaquer et pour quelles raisons ?

En premier lieu, cherchez à identifier les sources de risques pertinentes pour votre organisation.

De nombreux attaquants peuvent en effet chercher à vous atteindre, comme vu précédemment :

- le crime organisé (groupes cybercriminels, à l'origine des rançongiciels),
- des vengeurs, qui sont des employés (ou ex employés) cherchant à vous nuire,
- des états hostiles etc.

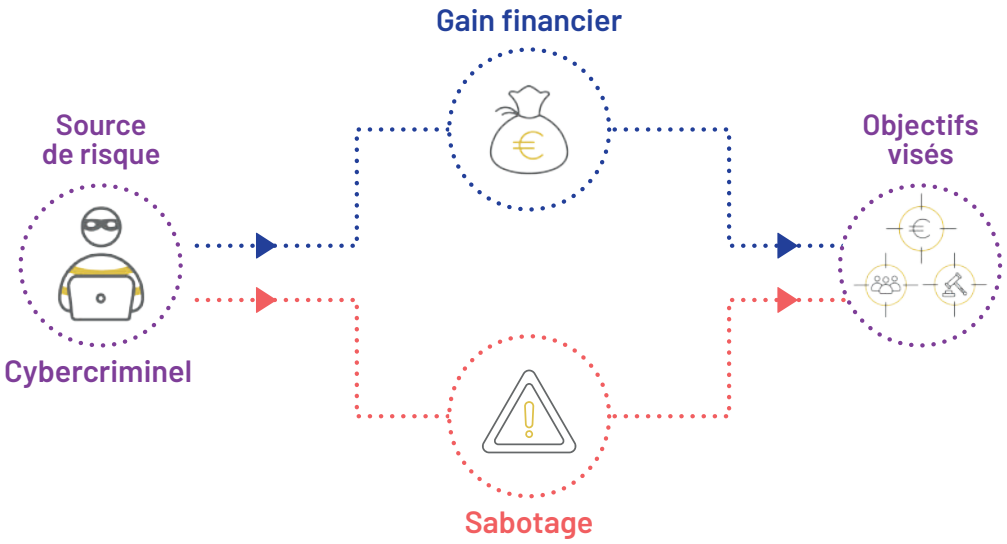
Pour chaque source de risque, regardez quels peuvent être leurs objectifs : par exemple appât du gain, influence, etc.
Évaluez alors la pertinence de chaque couple source de risque / objectif visé en fonction des ressources dont ils peuvent disposer et de la motivation dont ils peuvent faire preuve pour atteindre leurs objectifs. Cela afin de ne retenir que les plus pertinents pour la suite de l'analyse de risque.

Astuce

Assurez-vous que les couples source de risque / objectif visé que vous conservez couvrent les évènements redoutés retenus dans l'atelier 1. En effet, il faut s'assurer de l'adéquation entre le point de vue défenseur et le point de vue attaquant.

Ne sous-estimez pas la source de risque interne, ie les vengeurs, qui peut être pertinente dans de nombreux cas. Ils ne disposent que de peu de ressources financières, mais par leur nature possèdent une grande connaissance de vos processus et de votre système d'information, ainsi que des accès potentiels. De plus leur motivation à vous nuire est souvent importante. Un exemple de vengeur : un ex-employé d'une entreprise informatique singapourienne, après avoir conservé des accès dans les systèmes de son ancien employeur, se venge en supprimant 180 serveurs virtuels, entrainant des pertes s'élevant à $678,000[10].

Exemple



Source de risque	Objectif visé	Ressources et motivation	Pertinence
Cybercriminel	Gain financier (par rançongiciel)	**Ressources importantes** Justification : niveau de compétences élevées / accès facile à des outils sophistiqués **Motivation modérée** Justification : la collectivité concernée fait partie des cibles intéressantes pour un cybercriminel, mais celui-ci utilisant plutôt une technique de chalutage, cette collectivité n'est pas spécifiquement ciblée	**Retenu** Compte tenu de l'état de la menace cyber et des nombreuses attaques par rançongiciel recensées contre les collectivités territoriales.
Étatique	Influence (défiguration de sites)	**Ressources illimitées** Justification : ressources financières très importantes, à la pointe de la technique (ressources humaines très qualifiées, etc... **Motivation faible** Justification : cherche à cibler principalement des collectivités territoriales majeures	**Non retenu** Cible peu pertinente pour un acteur étatique (peu de retentissement en cas de réussite de l'attaque). Pourra être retenu lors d'une prochaine itération.

Atelier 3 : scénarios stratégiques

Votre organisation, comme vu dans l'atelier précédent, peut représenter une cible pour diverses sources de risque, aux objectifs variés.

Mais par quels chemins peuvent passer les sources de risques ? C'est une des questions à laquelle vous devez répondre dans cet atelier.

En effet, une source de risque peut, pour atteindre son objectif, vous attaquer directement. Mais ne pourrait-elle pas aussi passer par une partie prenante de votre écosystème, c'est-à-dire un client, un prestataire, un partenaire, etc., pour vous atteindre et obtenir l'effet désiré ?

Il est ici nécessaire de réaliser une cartographie de votre écosystème, puis d'évaluer la criticité de chacune des parties prenantes qui la compose, d'un point de vue cybersécurité. La criticité dépend de critères tels que la maturité en cybersécurité, la confiance de la partie prenante, la pénétration dans les systèmes d'information et la dépendance de la collectivité à leurs services.

Finalement, pour chaque couple source de risque / objectif visé, vous pouvez élaborer un scénario stratégique, qui décrit les différents chemins (en privilégiant les parties prenantes les plus critiques) que peut emprunter la source de risque pour atteindre l'objectif visé.

Astuce

À ce stade, en fonction du placement de vos parties prenantes sur votre cartographie, c'est-à-dire de leur criticité, vous pouvez réfléchir à des mesures de sécurité à mettre en œuvre ou à faire porter à vos parties prenantes les plus critiques, afin de réduire la menace qu'ils représentent pour votre organisation. On peut penser à des mesures réduisant leur pénétration dans votre système, votre dépendance à ces dernières permettant de les faire monter en maturité ou de renforcer votre confiance.

Comme pour les autres ateliers, vous pouvez ici rationaliser votre analyse de risque. La cotation des parties prenantes permet de hiérarchiser la dangerosité vis-à-vis du périmètre d'étude. S'il faut faire des choix pour limiter l'analyse, privilégiez les plus dangereuses dans vos scénarios stratégiques. De la même manière, une partie prenante qui a une dangerosité extrêmement faible (par exemple aucune pénétration ou très faible dépendance) ne sera que rarement pertinente dans un chemin d'attaque stratégique.

Exemple

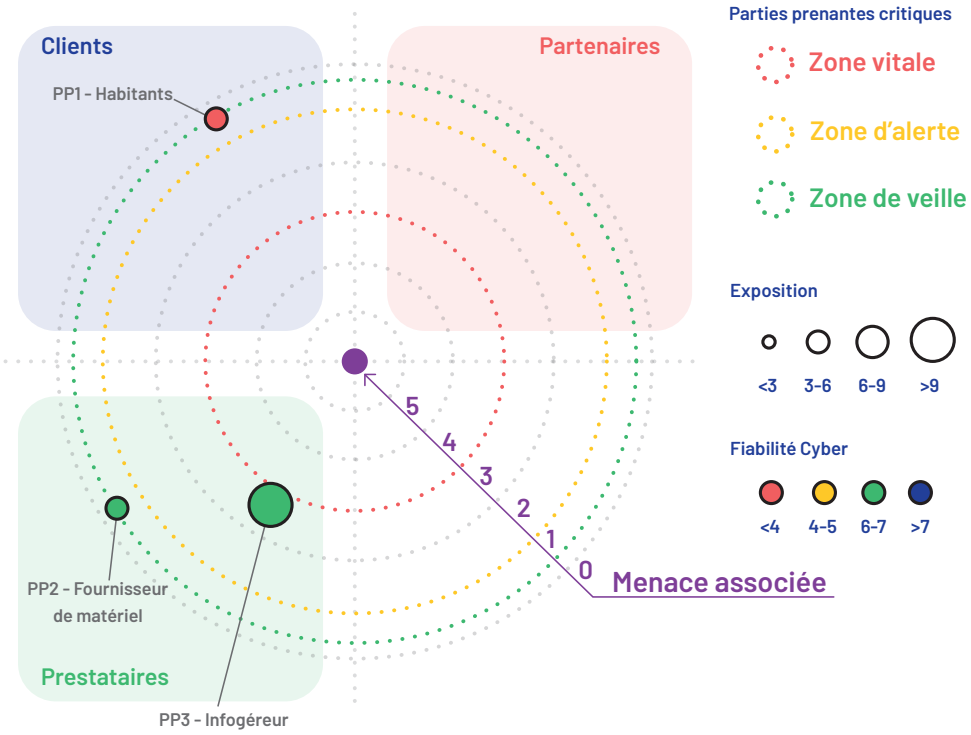
Pour continuer notre exemple, considérons les parties prenantes suivantes :

- **Clients (habitants) :** les habitants de la collectivité utilisent le portail web pour effectuer différentes démarches : demandes de documents, modifications de leurs données d'État Civil, etc.
- **Fournisseur de matériel :** il fournit les ordinateurs et équipements nécessaires au système. Il se charge aussi de l'assistance en cas de panne matérielle.
- **Infogéreur :** il est responsable de l'infogérance des serveurs (systèmes d'exploitation, applications) alloués à la gestion de l'État Civil et de leur maintien en conditions de sécurité (patch management).

On évalue en exemple la criticité de l'infogéreur et on applique la même méthode pour les autres parties prenantes, pour les placer sur la cartographie de nos parties prenantes.

Partie prenante	Dépendance	Pénétration	Maturité Cyber	Confiance	Criticité (DxP/MxC)
Infogéreur	4	4	2	3	2,67
Justification	Relation indispensable et unique.	Accès avec privilèges administrateur au système d'information.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité est conduite en mode réactif.	L'infogéreur est un prestataire de la collectivité depuis de nombreuses années, permettant une certaine confiance.	Zone d'alerte

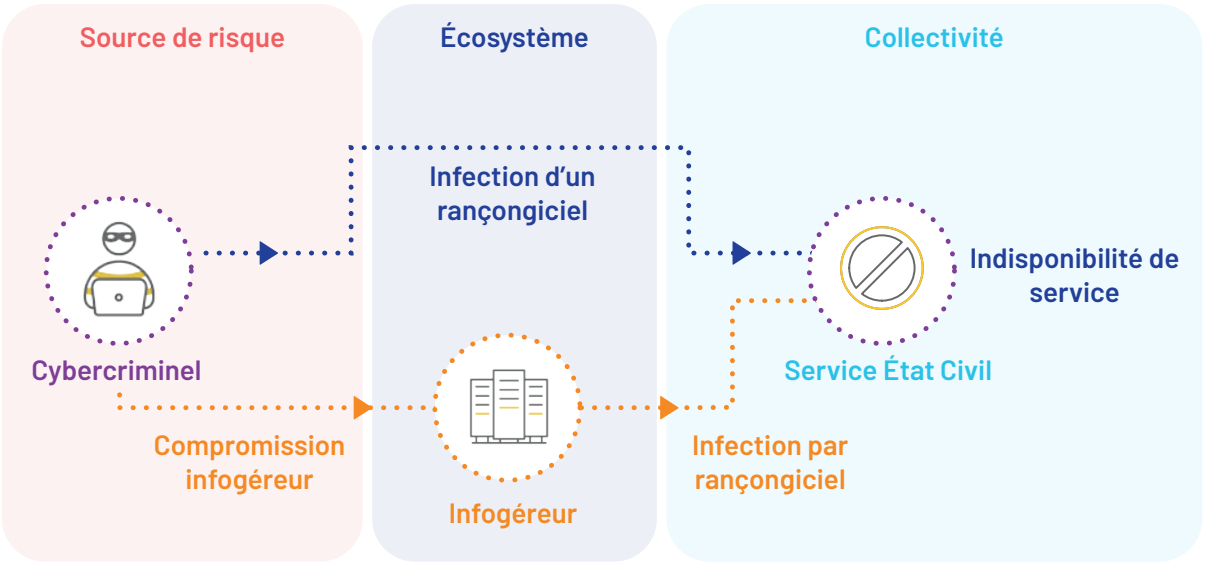
Partie prenante	Dépendance	Pénétration	Maturité	Confiance	Criticité
PP1 - Client (habitant)	1	1	1	2	0,5
PP2 - Fournisseur de matériel	2	2	3	2	0,67



Nous considérons dans notre exemple le scénario stratégique suivant : un cybercriminel paralyse le système de gestion de l'état civil à des fins lucratives. Nous identifions deux chemins d'attaque :

R1 : le cybercriminel injecte un rançongiciel directement sur le système d'information de la collectivité.

R2 : le cybercriminel injecte un rançongiciel chez l'infogéreur, qui se propage au système d'information de la collectivité.



Atelier 4 : scénarios opérationnels

Une fois vos scénarios stratégiques formalisés, il vous reste à décliner les chemins d'attaque stratégiques les plus intéressants sous forme de scénarios opérationnels.

Un scénario opérationnel décrit un ou plusieurs modes opératoires, qui correspondent à des enchaînements d'actions élémentaires (techniques, organisationnelles, etc.) dans votre système d'information, permettant à l'attaquant d'atteindre sa cible. Vous allez donc ici réfléchir à comment la source de risque peut atteindre son objectif visé à travers le chemin qui a été défini.

Pour élaborer vos scénarios opérationnels, utilisez votre socle de sécurité pour :

- Sélectionner les mesures de sécurité déjà mises en œuvre qui permettent de ralentir, détecter ou empêcher l'attaque.
- Déterminer les vulnérabilités issues des écarts qui au contraire peuvent faciliter l'attaque.

Il vous reste à évaluer la vraisemblance de chacun de ces modes opératoires. La vraisemblance du chemin d'attaque stratégique correspond à la vraisemblance la plus élevée parmi tous les modes opératoires du scénario opérationnel.

Astuce

Ne construisez pas de scénarios opérationnels pour chaque chemin d'attaque stratégique, conservez seulement pour cette itération les chemins d'attaque stratégiques qui méritent d'être approfondis.

Pour vous aider à construire et segmenter vos modes opératoires, il existe différentes méthodes, dont les deux suivantes :

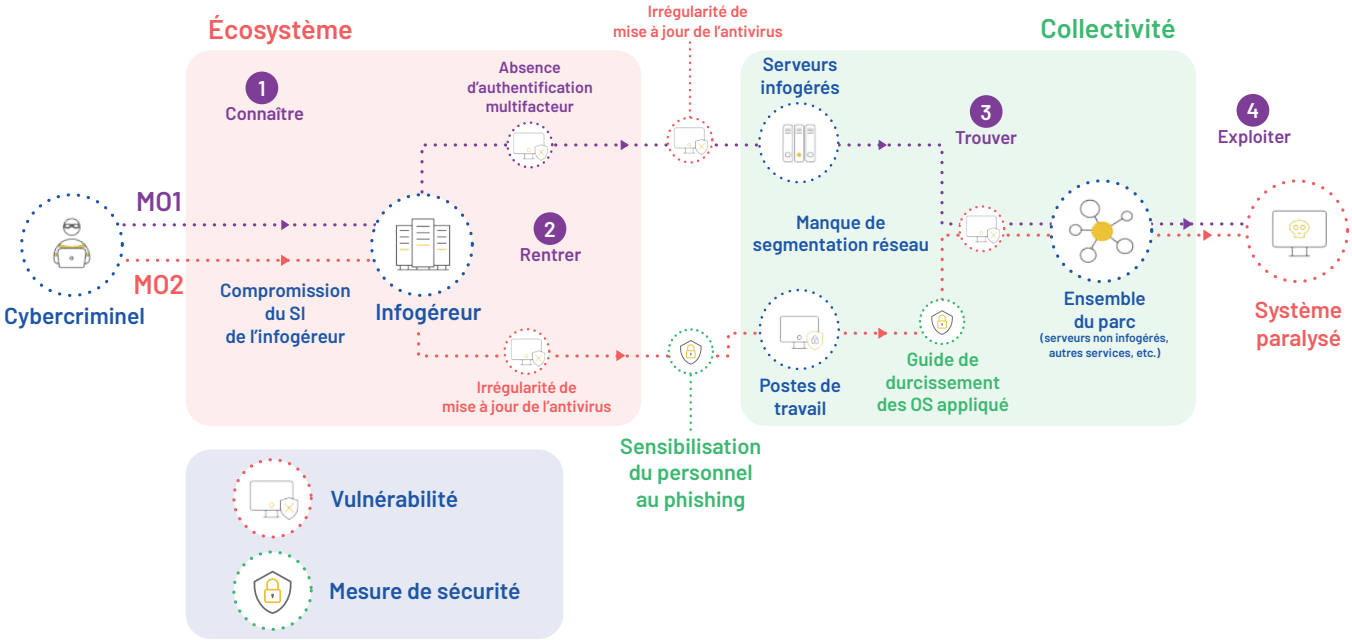
- La Cyber Kill Chain[11].
- MITRE ATT&CK[12].

L'ANSSI propose également plusieurs méthodes d'évaluation de la vraisemblance des modes opératoires d'attaque, de la plus basique à des calculs de probabilité pour chaque action élémentaire.

Exemple

Pour continuer notre exemple, nous avons réalisé un scénario opérationnel pour R2. Il en ressort deux modes opératoires. Le mode opératoire 1 est plus vraisemblable, et est coté à 3 - important.

Pour ne pas surcharger notre exemple, nous n'avons pas représenté le scénario opérationnel qui correspond au chemin d'attaque stratégique R1 : le cybercriminel injecte un rançongiciel directement sur le système d'information de la collectivité, avec une vraisemblance de 3.



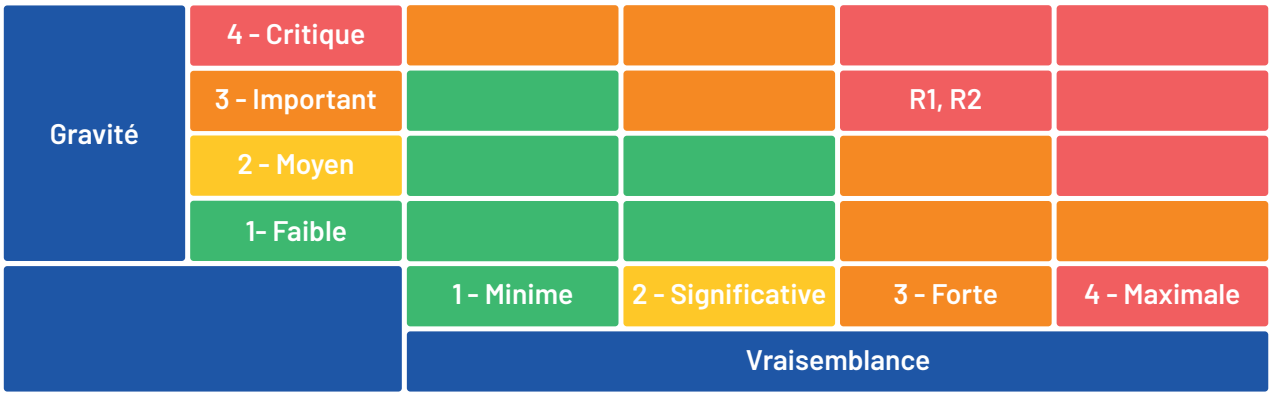
Étapes	1-Connaitre	2-Rentrer	3-Trouver	4-Exploiter	Probabilité de succés
Mode opératoire 1	Identification des comptes administrateurs sur le système d'information de la collectivité	Connexion sur les serveurs infogérés de la collectivité en utilisant les authentifiants de l'infogéreur	Reconnaissance du réseau et latéralisation	Rançongiciel activé sur l'ensemble du périmètre	3
Mode opératoire 2	Récupération d'informations de communication entre l'infogéreur et la collectivité (emails, etc.)	Phishing personnalisé contre la collectivité, en usurpant l'infogéreur, avec des mails contenant une charge virale	Reconnaissance du réseau et latéralisation, remontée du rançongiciel vers les serveurs		2

Atelier 5 : traitement du risque

Étape 1

À partir des précédents ateliers, vous pouvez construire une cartographie vous permettant d'apprécier vos risques et préparer une stratégie de traitement du risque adaptée. Vous faites ici entrer en jeu :

- **Vos scénarios de risque :** chaque scénario de risque correspond à un chemin d'attaque stratégique couplé à son mode opératoire (atelier 3 et 4)
- **Leur gravité :** gravité de l'évènement redouté corrélé à l'objectif visé (atelier 1 et 2)
- **Leur vraisemblance :** vraisemblance du scénario opérationnel d'attaque (atelier 4)



Exemple

Dans notre cas, nous avons traité à titre d'exemple deux scénarios de risque :

R1 : le cybercriminel injecte un rançongiciel directement sur le système d'information de la collectivité

R2 : le cybercriminel injecte un rançongiciel chez l'infogéreur, qui se propage au système d'information de la collectivité

À garder en tête

L'échelle d'acceptabilité du risque, auxquelles correspondent les couleurs de chaque case, permet de déterminer ce que votre organisation considère comme un niveau de risque acceptable, en tenant compte de votre tolérance au risque et de votre capacité à gérer les conséquences potentielles. L'échelle standardise cette perception du risque et établit des seuils clairs pour les actions à entreprendre. On parle de stratégie de traitement des risques.

À noter que l'emplacement des couleurs change en fonction de l'appétence aux risques de chaque organisation et peut donc être différent selon les acteurs réalisant une analyse de risque selon cette méthode.

Niveau de risque	Acceptabilité du risque	Intitulé des décisions et des actions
Faible	Acceptable en l'état	Aucune action n'est à entreprendre.
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme.
Élevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé.

Étape 2

Vos risques positionnés sur la matrice, il reste à définir quelles actions entreprendre pour mener à bien votre stratégie de traitement du risque.

On dispose ici de plusieurs options :

Refus des risques	Réduction des risques	Maintien des risques	Partage des risques
Annulation ou modification d'une ou plusieurs activités liées aux risques.	Introduction, suppression ou modification des mesures pour que le risque résiduel puisse être réapprécié comme étant acceptable.	Décision d'accepter le niveau de risque actuel.	Décision de partager les risques avec les parties externes : assurance ou externalisation.

Étape 3

Une fois une stratégie adoptée pour chacun de vos risques, vous pouvez définir un plan de traitement des risques pour couvrir les différents risques identifiés. Des mesures de sécurité seront définies conformément aux stratégies retenues, qui permettront de faire diminuer la vraisemblance de vos risques.

Exemple

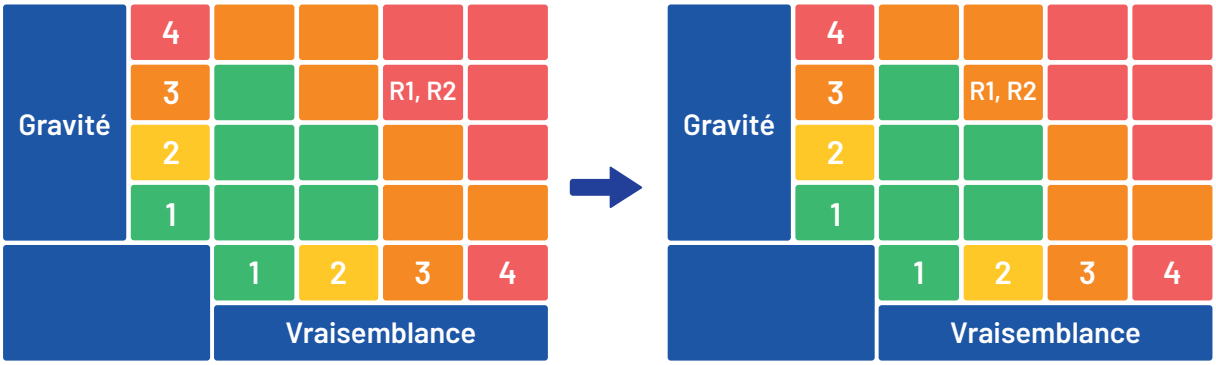
Plan de traitement des risques :

Mesure de sécurité	Scénario de risque associé	Responsable	Complexité
Sensibiliser les administrateurs	R1	Responsable de la sécurité des systèmes d'information	Faible
Mesures techniques de cloisonnement des réseaux (en authorisant uniquement l'activité connue et légitime)	R1, R2	Responsable DSI	Élevée
Élaborer un processus formel de gestion des mises à jour	R1, R2	Responsable DSI	Moyenne
Élaborer un processus formel de gestion des mises à jour	R2	RSSI	Faible

Étape 4

Votre plan de traitement des risques réalisé, évaluez et documentez vos risques résiduels, qui permettront de servir de base d'aide à la décision lors du suivi des risques de votre organisation.

Tableau des risques résiduels :



Le cadre du suivi des risques : se maintenir en condition de sécurité

La gestion des risques cyber demande, après l'analyse de risque que vous avez pu réaliser, de définir un cadre de suivi des risques pour engager un processus d'amélioration continue. Cela exige une gouvernance claire, avec la mise en place d'indicateurs et d'un comité de pilotage, pour évaluer l'efficacité des mesures de sécurité et suivre le plan de traitement des risques que vous avez précédemment conçu.

Astuce

Il est intéressant de définir l'échelle d'acceptabilité du risque et le tableau de la cartographie des risques au début de l'analyse de risque, afin de définir en amont une stratégie d'entreprise. Cela permet au dirigeant de donner un avis non biaisé de son acceptabilité du risque, avant même d'avoir déterminé ses risques. Dans le cas contraire, il pourrait être amené à sous-estimer un risque en fonction du coût des mesures de sécurité à entreprendre.

Un des intérêts de la méthode EBIOS RM réside dans la réitération de votre analyse de risque afin d'approfondir l'appréciation de vos risques à chaque boucle et d'étudier les risques que vous n'avez pas considéré en premier lieu. Cela vous permet d'optimiser l'équilibre entre prise en compte des risques importants et ressources allouées.

Alors,
que retient-on ?

Connaître vos risques, c'est à dire, les formaliser et les évaluer, est un prérequis essentiel pour placer le curseur cybersécurité au bon niveau, en tenant compte de votre appétence aux risques, de vos activités et de vos moyens.

À l'issue des 5 ateliers de la méthodologie EBIOS RM, vous disposez d'une cartographie claire de vos risques actuels vis-à-vis de vos activités essentielles et d'une feuille de route des actions à mener en adéquation avec votre stratégie de traitement.

Cette méthodologie se veut applicable aussi bien aux organisations publiques ou privées, quels que soient leur taille, leur secteur d'activité et que leur systèmes d'information soient en cours d'élaboration ou déjà existants. Vous devrez donc réaliser quelques ajustements et faire des choix de mise en oeuvre afin de l'inscrire pleinement dans l'organisation spécifique d'une collectivité territoriale. Nous avons ajouté à chaque étape de la méthodologie des astuces qui pourront vous éclairer sur ces ajustements et choix, ainsi qu'un exemple déroulé sur les 5 ateliers pour illustrer notre propos.

Vous avez maintenant les outils pour améliorer votre maturité cyber en cohérence avec vos spécificités et vos contraintes.

L'Expertise Cybersécurité SOFTEAM

L'expertise Cyber chez SOFTEAM

Filiale de Docaposte, SOFTEAM et ses équipes Consulting ont développé une forte expertise Cybersécurité au fil des années.

Nous proposons une offre modulaire au service de la maitrise des risques, en adéquation avec les normes actuelles et réglementations applicables (RGS/NIS/LPM...).

Nous vous accompagnons avec une approche pragmatique – adaptée à votre niveau de maturité en cybersécurité afin d'identifier et de **mettre sous contrôle vos risques cyber**.

Nous intervenons lors des différentes phases de gouvernance de vos projets cybersécurité afin d'avoir une cohérence et une vision commune : **diagnostic – conseil – plan d'actions**.

Notre vision EBIOS RM

Nos experts sont les facilitateurs de l'appropriation et la mise en œuvre de la méthodologie EBIOS RM.

Comme chaque collectivité est différente, l'analyse de risque nécessite une phase d'intégration contextuelle (contexte métier, réglementaire, ...) afin de l'adapter à votre contexte, vos enjeux et vos contraintes.

Nos experts s'occupent de cette phase d'accompagnement et de pédagogie pour que l'analyse de risque soit simple et fluide pour vous.

L'analyse de risque s'intègre dans une logique réglementaire ou de montée en maturité cyber visant à concevoir une stratégie de long cours adaptée à vos ressources pour sécuriser votre périmètre d'activité. Nous vous conseillons dans sa conception.

Notre équipe

Sous la conduite du Directeur de la practice, RSSI pendant une quinzaine d'année et ancien de l'Anssi, notre équipe est composée de Senior Managers (ancien RSSI) encadrant de jeunes consultants passionnés par la cyber et souhaitant donner un sens à leur carrière en travaillant au service de l'intérêt collectif.

Des cadres expérimentés :

- Ayant déjà travaillé en environnement complexe et fortement réglementé engageant leur responsabilité
- Ayant déjà travaillé en environnement en tension (projet à plusieurs M€)

Des jeunes possédant majoritairement des doubles compétences :

- Plus de la moitié des juniors ont 2 bac+5

Une politique de certification systématique :

- Tous nos consultants passent leur certification ISO 27001 et une formation à EBIOS RM.

Annelise RIQUIER

Senior Manager du Conseil Cyber

Stéphane DUBREUIL

Directeur de l'expertise Cybersécurité

Jean-Christophe ZAPALOWICZ

Senior Manager du Conseil Cyber

SOFTEAM

SOFTEAM est le cabinet de conseils et de services de Docaposte (Groupe La Poste).

Notre mission ? Mettre le numérique au service des transitions auxquelles nos sociétés font face. Concrètement, cela se traduit dans notre attitude et dans nos engagements.

Nous sommes des partenaires de confiance pour nos clients, en adoptant une posture d'écoute active et en co-construisant des solutions qui répondent à leurs besoins spécifiques.

Nous sommes conscients que les défis auxquels nous faisons face sont complexes et évolutif : la force de notre collectif de consultants experts et engagés pour le bien commun est le socle de notre mission.

Ensemble, nous voulons faire du numérique un levier pour demain. Et cela commence justement par un bon accompagnement Cyber.

Références

(1) https://asteres.fr/site/wp-content/uploads/2023/06/ASTERES-CRIP-Cout-des cyberattaques-reussies-16062023.pdf
(2) https://www.cybermalveillance.gouv.fr/medias/2023/11/231120_Etude_Maturite_Cyber__SCREEN_compressed.pdf
(3) https://www.cybermalveillance.gouv.fr/medias/2023/11/231120_EtudeCollectivites_INFO.pdf
(4) https://discover.harfanglab.io/rapport-pme.html
(5) https://www.francetvinfo.fr/replay-radio/8h30-fauvelle-dely/augmentation-des-cyberattaques-menaces-pendant-les-jeux-olympiques-le-8h30-franceinfo-de-vincent-strubel_6349228.html
(6) https://www.maire-info.com/technologie-de-l'information/des-centaines-de-sites-internet-de-mairies-et-d'institutionsont-ete-pirates-article-17974).
(7) https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-008.pdf
(8) https://www.bfmtv.com/grand-lille/lille-la-cyberattaque-a-coute-1-million-d-euros-a-la-mairie-certains-services-encore-impactes_AN-202305160604.html
(9) https://www.francebleu.fr/infos/faits-divers-justice/la-mairie-de-fleury-les-aubrais-entierement-paralysee-par-une-cyberattaque-majeure-8094912
(10) https://www.digit.in/news/general/fired-employee-hacks-into-companys-system-heres-what-happened-next.html)
(11) https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
(12) https://attack.mitre.org/

Collectivités & cybermenaces : entre exposition aux risques et moyens, comment placer le curseur au bon niveau ?

Vous souhaitez échanger avec nos experts sur vos besoins d'accompagnement Cyber ?
Ils prennent vraiment le temps de vous écouter et comprendre vos enjeux,
votre environnement et vos objectifs.

Contactez directement notre équipe à practice.cyber@softeam.fr

SOFTEAM
UNE MARQUE DE DOCAPOSTE

www.softeam.com