RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

GUIDE EBIOS RISK MANAGER

FICHE METHODE 8 - Atelier 4

ÉVALUER LA VRAISEMBLANCE DES SCENARIOS OPERATIONNELS

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.

La **vraisemblance** d'un scénario opérationnel reflète le degré de faisabilité ou de possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. La vraisemblance est un indicateur d'aide à la décision. Combinée à la gravité, elle permet d'estimer le niveau de risque et de déduire la stratégie de traitement du risque.

QUELLE ECHELLE DE VRAISEMBLANCE UTILISER ?

Une échelle de niveaux de vraisemblance doit être comprise et utilisable par les personnes chargées d'évaluer la possibilité qu'un risque se concrétise. Son élaboration peut utilement être réalisée en collaboration avec les personnes qui vont estimer ces niveaux : ainsi les valeurs auront une signification concrète et seront cohérentes.
Le recours à une échelle de 4 ou 5 niveaux est guidé par les considérations suivantes :

- la cohérence du nombre de niveaux entre les échelles de gravité et de vraisemblance (si vous utilisez une échelle de gravité à 4 niveaux, utilisez une échelle de vraisemblance à 4 niveaux) ;
- la nécessité d'estimer plus ou moins finement ces vraisemblances.

NOTE : l'estimation de la vraisemblance d'un scénario opérationnel n'a pas vocation à être prédictive (elle ne traduit pas la probabilité que la source de risque réalisera son attaque selon ce scénario [1]). Par contre, si l'attaquant décide de mener son attaque via le mode opératoire concerné, alors sa vraisemblance de réussite sera celle estimée.

Si vous ne disposez pas d'échelle de vraisemblance, établissez-en une au début de **l'atelier 4**. Pour cela, vous pouvez utiliser et adapter l'échelle générique ci-après.

ÉCHELLE DE VRAISEMBLANCE D'UN SCÉNARIO OPÉRATIONNEL	
NIVEAU DE L'ÉCHELLE	DESCRIPTION
V4 – QUASI-CERTAIN	La source de risque va très certainement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est très élevée.
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est élevée.
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est significative.
V1 – PEU VRAISEMBLABLE	La source de risque a relativement peu de chances d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est faible.
V0 – INVRAISEMBLABLE	La source de risque a très peu de chances d'atteindre son objectif visé en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est très faible.

QUELLE APPROCHE CHOISIR POUR COTER LA VRAISEMBLANCE DU SCENARIO OPERATIONNEL ?

Voici trois approches proposées pour estimer la vraisemblance du scénario opérationnel :

- méthode expresse : cotation directe de la vraisemblance du scénario ;
- méthode standard : cotation de la « probabilité de succès » de chaque action élémentaire du scénario, du point de vue de l'attaquant.
- méthode avancée : en plus de la « probabilité de succès », cotation de la « difficulté technique » de chaque action élémentaire du scénario, du point de vue de l'attaquant.

NOTE: ici la « probabilité » ne doit pas être entendue au sens mathématique du terme.

a MÉTHODE EXPRESSE : COTATION DIRECTE DE LA VRAISEMBLANCE GLOBALE DU SCÉNARIO

Dans les méthodes présentées ci-après (standard et avancée), on évalue la vraisemblance globale du scénario à partir de la cotation des actions élémentaires. La méthode expresse consiste à évaluer directement la vraisemblance globale du scénario, sur la base de considérations générales relatives à la source de risque (motivations, ressources) et à la sécurité des biens supports ciblés dans le scénario (exposition, vulnérabilités). La section « Comment coter les actions élémentaires ? » sera d'une aide précieuse pour l'appréciation. Il est possible de considérer séparément les modes opératoires envisagés dans le scénario opérationnel et d'identifier celui qui semble être le plus vraisemblable.
Dans cette approche, vous pouvez :

- estimer directement le niveau de vraisemblance du scénario ;
- ou coter sa probabilité de succès et sa difficulté technique en vue de déduire par croisement la vraisemblance du scénario selon la matrice type présentée ci-après.

PROBABILITÉ DE SUCCÈS DU SCÉNARIO OPÉRATIONNEL	DIFFICULTÉ TECHNIQUE DU SCÉNARIO OPÉRATIONNEL				
	0 – NÉGLIGEABLE	1 – FAIBLE	2 – MODÉRÉE	3 – ÉLEVÉE	4 – TRÈS ÉLEVÉE
4 – QUASI CERTAINE	4	4	3	2	1
3 – TRÈS ÉLEVÉE	4	3	3	2	1
2 – SIGNIFICATIVE	3	3	2	2	1
1 – FAIBLE	2	2	2	1	0
0 – TRÈS FAIBLE	1	1	1	0	0

b MÉTHODE STANDARD : PROBABILITÉ DE SUCCÈS DES ACTIONS ÉLÉMENTAIRES

Dans la méthode standard, vous allez coter chaque action élémentaire selon un indice de probabilité de succès vu de l'attaquant. L'échelle suivante peut être adoptée, les pourcentages de chance sont mentionnés à titre indicatif pour faciliter la cotation :

ÉCHELLE DE PROBABILITÉ DE SUCCÈS D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	DESCRIPTION
4 – QUASI-CERTAINE	Probabilité de succès quasi-certaine > 90%
3 – TRÈS ÉLEVÉE	Probabilité de succès très élevée > 60%
2 – SIGNIFICATIVE	Probabilité de succès significative > 20%
1 – FAIBLE	Probabilité de succès faible < 20%
0 – TRÈS FAIBLE	Probabilité de succès très faible < 3%

Par exemple, un indice de « 3 – très élevée » pour une action élémentaire d'intrusion par mail piégé (spearfishing) signifiera que vous estimez que l'attaquant a de très fortes chances de réussir son action, c'est-à-dire que l'un des utilisateurs ciblés par la campagne de spearfishing clique sur la pièce jointe piégée.

NOTE : les échelles de cotation des actions élémentaires doivent avoir autant de niveaux que l'échelle de vraisemblance.

c MÉTHODE AVANCÉE : PROBABILITÉ DE SUCCÈS ET DIFFICULTÉ TECHNIQUE DES ACTIONS ÉLÉMENTAIRES

Dans la méthode avancée, vous allez également coter la difficulté technique de réalisation de l'action élémentaire, du point de vue de l'attaquant. Elle permet d'estimer les ressources que l'attaquant devra engager pour mener son action et accroître ses chances de réussite. L'échelle suivante peut être adoptée :

ÉCHELLE DE DIFFICULTÉ TECHNIQUE D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	DESCRIPTION
4 – TRÈS ÉLEVÉE	Difficulté très élevée : l'attaquant engagera des ressources très importantes pour mener à bien son action.
3 – ÉLEVÉE	Difficulté élevée : l'attaquant engagera des ressources importantes pour mener à bien son action.
2 – MODÉRÉE	Difficulté modérée : l'attaquant engagera des ressources significatives pour mener à bien son action.
1 – FAIBLE	Difficulté faible : les ressources engagées par l'attaquant seront faibles.
0 – NÉGLIGEABLE	Difficulté négligeable, voire nulle : les ressources engagées par l'attaquant seront négligeables ou déjà disponibles.

NOTES :

- La méthode avancée permet une appréciation plus fine de la vraisemblance: elle prend en compte le niveau d'expertise et de ressources dont l'attaquant aura besoin pour mener son attaque, compte tenu de la sécurité du système ciblé. De fait, cette méthode permet de considérer le retour sur investissement pour l'attaquant et donc de bâtir une stratégie de traitement du risque pilotée par une logique de découragement.
- Les critères de cotation « difficulté technique » et « probabilité de succès » ne sont pas rigoureusement indépendants. Néanmoins, la « difficulté technique » est plus particulièrement liée au niveau de protection de la cible (son exposition et ses vulnérabilités), alors que la « probabilité de succès » est davantage influencée par son niveau de défense et de résilience (capacités de supervision, de réaction en cas d'incident et de continuité d'activité).

METHODES STANDARD ET AVANCEE : COMMENT COTER LES ACTIONS ELEMENTAIRES ?

La cotation des actions élémentaires n'est pas forcément aisée. En effet, elle doit prendre en compte et confronter :

- d'une part la motivation/détermination et les ressources/capacités de la source de risque ;
- d'autre part la sécurité du système ciblé au sein de son écosystème.

La cotation peut être effectuée par jugement d'expert, ce qui implique de disposer dans le groupe de travail d'une expertise suffisante en cyberattaques et d'une connaissance fine du niveau de sécurité de l'objet de l'étude au sein de son écosystème. Ces estimations déclaratives peuvent utilement être justifiées par d'autres travaux (audits techniques, contrôle interne, etc.). Il est même recommandé d'utiliser les scénarios opérationnels pour orienter un audit technique. Pour vous aider dans ce travail de cotation et le rendre plus objectif et reproductible, vous trouverez en fin de fiche les principaux critères pour déterminer la probabilité de succès ou la difficulté technique d'une action élémentaire.

METHODES STANDARD ET AVANCEE : COMMENT CALCULER LA VRAISEMBLANCE DU SCENARIO OPERATIONNEL ?

L'objectif est ici de hiérarchiser la vraisemblance des scénarios opérationnels. De nombreuses techniques peuvent être employées. Ainsi, pour des études simples, il peut suffire de classer les scénarios opérationnels par ordre décroissant de vraisemblance, au jugé. Toutefois, pour des études plus riches, deux techniques sont proposées.

NOTE : l'estimation de la vraisemblance n'est pas toujours triviale et facilement automatisable. Elle peut demander une véritable expertise afin de tenir compte des réalités techniques et d'assurer la cohérence méthodologique.

a MÉTHODE STANDARD

Vous avez coté dans l'étape précédente chaque action élémentaire selon un indice de probabilité de succès. Vous pouvez évaluer l'indice global de probabilité de succès du scénario en appliquant la règle suivante. Le principe est de progresser dans un mode opératoire en évaluant de proche en proche à chaque action élémentaire « AEn » d'un nœud « n », un indice de probabilité cumulé intermédiaire à partir de l'indice élémentaire de « AEn » et des indices cumulés intermédiaires du nœud précédent « n-1 » :

$$\underset{n}{\text{Indice\_Pr}}\,(AE) = \text{Min}\,\{\underset{n}{\text{Indice\_Pr}}\,(AE),\ \text{Max}\,(\underset{n}{\text{Indices\_Pr}}\,(AE\_1))\}$$

n cumulé intermédiaire — *n cumulés intermédiaires*

L'indice global de probabilité de succès (étape finale) est obtenu en prenant l'indice de probabilité cumulé intermédiaire le plus élevé parmi les modes opératoires qui aboutissent à l'étape finale. Il correspond au(x) mode(s) opératoire(s) dont la chance de succès parait la plus élevée.

Le graphe d'attaque peut être vu comme un automate : les actions élémentaires et représentent les opérations de l'automate et les étapes d'attaque représentent ses états : la vraisemblance de chaque étape est la vraisemblance maximale des différents parcours possibles au sein du graphe d'attaque pour y parvenir.
La vraisemblance du scénario opérationnel obtenue à l'issue de ces opérations correspond à l'indice global de probabilité de succès.

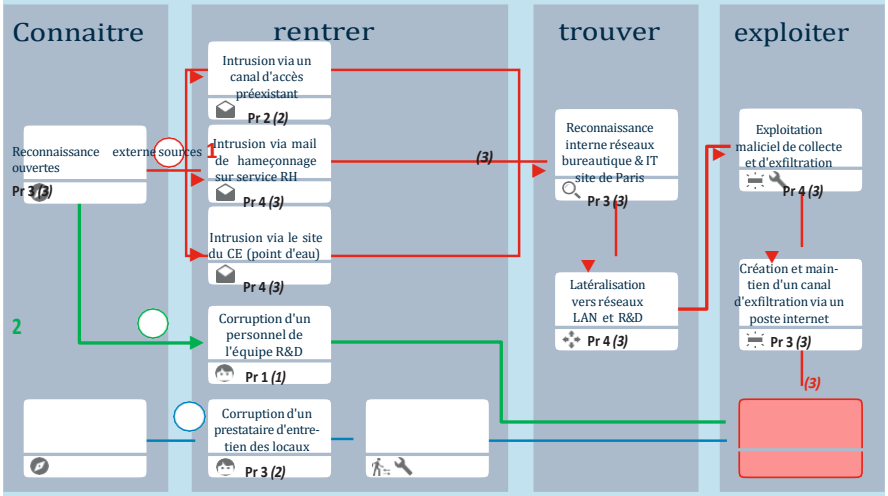
NOTE : la règle de calcul ci-dessus permet une évaluation relativement simple et rapide de l'indice global de probabilité de succès.
Elle trouve toutefois ses limites lorsqu'une séquence d'un mode opératoire comporte une longue chaîne d'étapes en série (environ une dizaine à titre indicatif). L'évaluation aura alors tendance à surestimer la probabilité de succès du mode opératoire correspondant, aboutissant à une vraisemblance surestimée du scénario opérationnel. Pour les séquences de mode opératoire concernées, vous pouvez compenser cette limite en diminuant d'un niveau l'indice de probabilité cumulé intermédiaire obtenu en bout de séquence.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

L'évaluation de la vraisemblance a été réalisée avec des échelles à 4 niveaux :

- Pour la probabilité de succès : « Pr 1 » – probabilité faible à « Pr 4 » – quasi-certaine.
- Pour la vraisemblance : « V1 » – peu vraisemblable à « V4 » – quasi-certain.

Les indices de probabilité cumulés intermédiaires sont indiqués entre parenthèses et en *italique*.



L'indice global de probabilité de succès du scénario est estimé à « 3 – Très élevé » : l'atteinte de l'objectif visé par la source de risque selon l'un ou l'autre des modes opératoires du scénario opérationnel est considérée comme très vraisemblable (V3). Le mode opératoire le plus facile ou faisable étant le rouge numéroté.

b MÉTHODE AVANCÉE

Commencez par calculer l'indice global de probabilité de succès de chaque mode opératoire du scénario opérationnel selon la démarche exposée précédemment.

Calculez ensuite l'indice de difficulté technique de chaque mode opératoire selon les modalités ci-après. Le principe est de progresser sur une séquence d'un mode opératoire en évaluant de proche en proche à chaque action élémentaire « AEn » d'un nœud « n », un indice de difficulté cumulé intermédiaire à partir de la difficulté élémentaire de « AEn » et des difficultés cumulées intermédiaires du nœud précédent « n-1 » :

$$(AE_n) = \text{Max}\ \{\text{Indice\_Diff}(AE_n), \underbrace{\text{Min}\ (\text{Indices\_Diff}(AE_n\_1))}_{\textit{cumulés intermédiaires}}\}$$

NOTE : la règle de calcul ci-dessus permet une évaluation relativement simple et rapide de l'indice global de difficulté technique. Elle trouve toutefois sa limite lorsqu'une séquence d'un mode opératoire comporte une longue chaîne d'étapes en série (environ une dizaine [3]). L'évaluation aura alors tendance à sous-estimer la difficulté du mode opératoire correspondant, aboutissant à une vraisemblance sous-estimée du scénario opérationnel. Pour les séquences de mode opératoire concernées, vous pouvez compenser cette limite en augmentant d'un niveau l'indice de difficulté cumulé intermédiaire obtenu en bout de séquence.

Vous pourriez également retenir comme vraisemblance celle obtenue en croisant l'indice global de probabilité de succès et l'indice global de difficulté technique obtenus. Mais votre résultat pourrait être faussé en cas de croisement des indices de probabilité et de difficulté relatifs à des modes opératoires différents. Dans ce cas, la vraisemblance du scénario opérationnel serait surestimée.

Enfin, si les actions élémentaires correspondantes ont des indices de difficulté identiques, vous pouvez déduire la vraisemblance globale du scénario opérationnel en procédant comme suit :

- évaluez le niveau de vraisemblance de chaque mode opératoire aboutissant à l'étape finale, en utilisant la grille croisée ci-après (qui peut être adaptée);
- le niveau de vraisemblance pour le scénario opérationnel est celui du mode opératoire le plus vraisemblable ;
- ce niveau de vraisemblance peut ensuite être pondéré selon la nature de la source de risque (motivation et ressources). Si vous estimez celle-ci comme particulièrement déterminée à atteindre son objectif – et donc, prête à solliciter des moyens conséquents et à persévérer en cas d'échecs successifs, alors vous pouvez décider d'augmenter d'un niveau la vraisemblance obtenue.

		DIFFICULTÉ TECHNIQUE DU MODE OPÉRATIONNEL				
		0 – NÉGLIGEABLE	1 – FAIBLE	2 – MODÉRÉE	3 – ÉLEVÉE	4 – TRÈS ÉLEVÉE
PROBABILITÉ DE SUCCÈS DU MODE OPÉRATIONNEL	4 – QUASI-CERTAINE	4	4	3	2	1
	3 – TRÈS ÉLEVÉE	4	3	3	2	1
	2 – SIGNIFICATIVE	3	3	2	2	1
	1 – FAIBLE	2	2	2	1	0
	0 – TRÈS FAIBLE	1	1	1	0	0

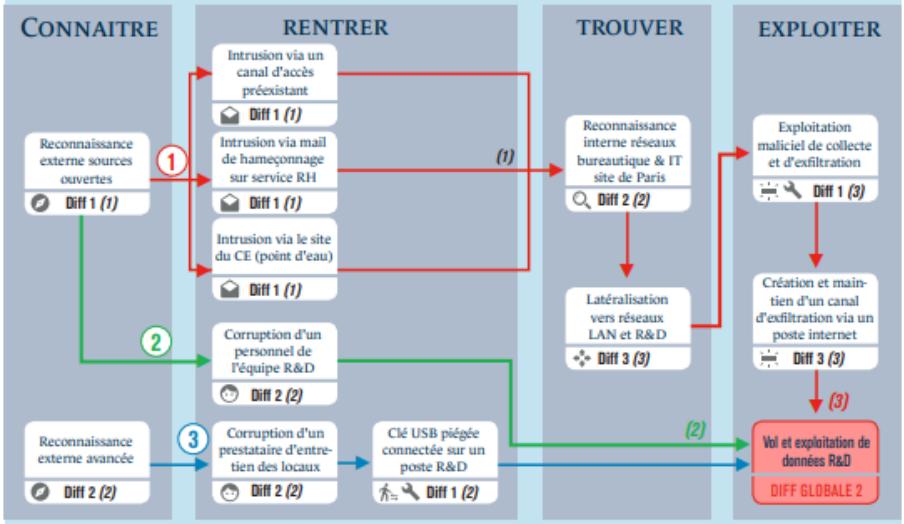
NOTES :

■ Le modèle suppose les probabilités de succès indépendantes entre elles, ce qui n'est pas nécessairement vrai. La même remarque s'applique pour les difficultés techniques. D'autre part, pour certaines catégories d'actions (telle que la corruption d'un membre du personnel), la probabilité de succès peut être dépendante de la difficulté, ce qui n'est pas capturé par défaut dans le modèle.

■ L'utilisation d'un logiciel de construction et de cotation de graphes d'attaque est fortement recommandée.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

Les indices de difficulté cumulés intermédiaires sont indiqués entre parenthèses et en italique.



La difficulté technique du scénario est estimée globalement à « 2 – Modéré », les modes opératoires les moins difficiles techniquement étant ceux numérotés ② et ③. Compte-tenu des probabilités de succès évaluées précédemment, il est possible d'établir la synthèse suivante :

	Probabilité succès	Difficulté technique	Vraisemblance
Chemin ①	3 – Très élevée	3 – Élevée	V2 – Vraisemblable
Chemin ②	1 – Faible	2 – Modérée	V2 – Vraisemblable
Chemin ③	2 – Significative	2 – Modérée	V2 – Vraisemblable
		Scénario global	V2 – Vraisemblable

Les trois modes opératoires envisagés dans le graphe d'attaque ont le même niveau de vraisemblance. On aboutit à une vraisemblance **« V2 – Vraisemblable »** pour le scénario. Par rapport à l'évaluation réalisée avec la méthode standard (V3), la vraisemblance estimée est moindre. La prise en compte du critère de difficulté technique apporte une pondération sur l'estimation du niveau de vraisemblance. En effet, si le mode opératoire ① apparaît comme ayant la probabilité de succès la plus élevée, il présente également une difficulté technique relativement élevée.

5/ Éléments d'aide pour la cotation des actions elementaires

Cette section présente pour chaque catégorie d'action élémentaire (voir fiche méthode 7) les éléments majeurs qui déterminent sa probabilité de succès ou sa difficulté technique.

Recrutement d'une source, corruption de personnel

a. Nombre de cibles potentielles ayant accès aux informations visées, aux biens supports critiques ou à leur environnement physique. Plus les cibles potentielles sont nombreuses, plus il sera facile pour l'attaquant de trouver une cible corruptible. .

b. Personnels, prestataires, fournisseurs susceptibles d'être animés par un esprit de vengeance. EXEMPLE: salarié mécontent licencié récemment.

c. Personnels ayant fait l'objet d'un processus d'habilitation de sécurité et/ou d'une enquête, qui apporte un certain niveau d'assurance sur leur intégrité.

d. Satisfaction des cibles à l'égard de leur salaire ou de leur considération au sein de l'organisation.

e. Adhésion des cibles potentielles aux valeurs de l'entreprise. Des personnes mal considérées et mal payées seront naturellement plus faciles à corrompre. Il ne faut pas sous-estimer ces leviers.

Reconnaissance externe de la cible

- Informations sur **l'entité et son écosystème** facilement accessibles sur Internet (sites web, forums de discussions en ligne, réseaux socio- professionnels, etc.).
- Participation régulière de l'entité, de ses partenaires (fournisseurs, sous-traitants, clients) ou d'anciens salariés à des **salons professionnels ou forums en ligne**. Beaucoup d'informations sont aisément obtenues au travers d'approches informelles dans les milieux professionnels. Lors de démarches commerciales notamment, de nombreuses informations sensibles sont souvent échangées. **EXEMPLE**: faux client, réponse à un appel d'offres.
- Usage du **chiffrement** dans les relations de l'entité avec l'extérieur, dans les services offerts par l'entité à l'extérieur. Les protocoles de chiffrement permettent de limiter l'impact des fuites de données, en particulier vis-à-vis des interceptions ou détournements de trafic.
- Compétences particulières nécessaires pour la recherche des informations, compte tenu du **domaine d'activité de l'entité.** Des attaques nécessitant de fortes compétences dans un ou plusieurs domaines d'expertise en lien avec l'activité de la cible. **EXEMPLE**: contrôle aérien, risque NRBC – nucléaire, radiologique, bactériologique, chimique, signalisation ferroviaire) sont naturellement plus coûteuses et difficiles à identifier et traiter que des attaques mettant en œuvre des procédés essentiellement techniques.

Intrusion depuis internet ou des réseaux informatiques tiers

Les critères diffèrent selon la technique d'intrusion utilisée par l'attaquant.

Attaque frontale de services

- Nombre de services et/ou d'applicatifs exposés sur Internet.
- Services exposés ayant fait l'objet d'une homologation ou d'un processus de développement intégrant la sécurité.
- Technologie de filtrage mise en place. Ces outils fonctionnent sur la base de signatures et sont assez

efficaces pour détecter les attaques les plus grossières. EXEMPLE : reverse proxy, waf, etc.

■ Utilisation de biens supports « de frontière » certifiés ou qualifiés. Une technologie qualifiée ou certifiée est plus robuste vis-à-vis des exploits, car elle a fait l'objet d'une qualité de développement accrue, avec une attention importante donnée à la sécurité, et a fait l'objet de tests d'intrusion. **EXEMPLE** : certification de sécurité de premier niveau, critères communs, agrément, référentiel général de sécurité.

HAMEÇONNAGE / POINT D'EAU

■ Nombre d'utilisateurs susceptibles d'être visés. Plus il y a d'utilisateurs, plus il est facile de tester plusieurs cibles jusqu'à ce que l'une d'elles réalise l'opération attendue.

■ Utilisateurs régulièrement **sensibilisés** et formés à réagir aux attaques par hameçonnage et point d'eau.

■ **Filtre anti-spam performant mis en place.** Ce type d'outil est assez efficace pour détecter les attaques les plus grossières (hameçonnage de masse, par exemple envoi d'un courriel piégé contenant un rançongiciel non ciblé).

■ **Capacité de filtrage de la navigation Internet des utilisateurs mise en place.** Les solutions de filtrage de la navigation permettent à la fois de filtrer ce qui est connu comme hébergeant une activité malveillante et d'enregistrer le trafic à des fins d'investigation poussée dans le cadre d'une supervision de sécurité. EXEMPLE : proxy, IPS.

■ **Filtrage des sites Internet reposant sur une liste blanche** (liste de sites autorisés). Les navigations autorisées par listes blanches sont relativement complexes à contourner par un attaquant qui souhaite mener une attaque par point d'eau.

INTRUSION VIA UN RÉSEAU SANS FIL

■ Existence de réseaux sans fil (Wi-Fi) dans l'environnement bureautique ou industriel de l'entité.

■ Accès Wi-Fi sécurisés, par exemple selon le guide technique de l'ANSSI[1].

INTRUSION VIA UN LOGICIEL OU UN CORRECTIF LÉGITIME

■ Existence d'une politique de sécurité relative aux mises à jour des logiciels, applications métier et firmware. La mise en place de mesures de sécurisation des mises à jour logicielles et firmware peut rendre beaucoup plus difficile une attaque de type cheval de Troie. EXEMPLE: sas antivirus (certifié) avant application des mises à jour, procédures de contrôle d'intégrité des patchs et correctifs.

■ Sources et canaux de confiance (voire certifiés ou qualifiés), vérification de l'identité des signataires pour les mises à jour.

INTRUSION OU PIÈGE PHYSIQUE

■ **Maîtrise des interventions des prestataires: gestion des accès aux locaux, supervision, journalisation, etc.** Des interventions réalisées en dehors des heures ouvrées ou en l'absence de toute vigilance/présence humaine facilitent une activité frauduleuse ou illégitime. Il en est de même si un prestataire dispose d'un badge d'accès lui permettant de circuler librement dans toutes les zones.

■ Processus **d'habilitation** de sécurité ou enquête préliminaire réalisés pour les prestataires qui interviennent sur site.

■ Utilisation de **matériels informatiques gérés par l'organisation** pour que les prestataires effectuent les interventions sur les biens supports de l'entité. **EXEMPLE** : valise de maintenance, clé USB de *firmware* (le fait qu'un prestataire utilise ses propres moyens d'intervention pour, par exemple, effectuer la maintenance d'un

---

[1] Note technique – Recommandations de sécurité relatives aux réseaux Wi-Fi, ANSSI, 2013.

automate ou la mise à jour d'un réseau informatique, accroît le risque d'introduction d'un éventuel code malveillant ciblé ou non, éventuellement à l'insu du prestataire.

- Nombre et facilité **d'accès des points de connexion physique et logique** aux réseaux informatiques de l'entité.
- Existence de liens de télémaintenance ou de connexions avec des réseaux tiers sécurisés.
- Existence d'une politique de sécurité pour la **chaîne d'approvisionnement industrielle**. **EXEMPLE**: exigences contractuelles, audits de sécurité des fournisseurs, etc.
- Existence de mesures de sécurité pour la **maintenance des biens supports**. **EXEMPLE** : retrait des supports de stockage à mémoire non volatile, scellement physique, application du référentiel d'exigences de l'ANSSI relatif à l'intégration et à la maintenance des systèmes industriels.
- Existence de mesures de **sécurité physique** et type de technologie utilisée : contrôle d'accès. **EXEMPLE**: portique, badge, digicode, biométrie, vidéo protection, etc.
- **Supervision** de la sécurité physique et réactivité des équipes d'intervention en cas de détection d'intrusion (sur place, à distance, 24/7, seulement heures ouvrées).
- Nombre de **barrières** à franchir pour accéder physiquement aux biens supports critiques. Il est recommandé de disposer d'au moins trois barrières physiques pour accéder aux biens supports critiques.
- Personnels de sécurité formés au risque d'introduction physique de matériels d'écoute.
- Utilisateurs sensibilisés, voire entraînés, à la vigilance vis-à-vis des intrusions physiques.
- Connaissance mutuelle des personnes pouvant avoir un accès légitime.
- Existence d'une politique de sécurité pour les déplacements professionnels, sensibilisation des salariés aux risques lors de leurs missions.

LATÉRALISATION ET ÉLÉVATION DE PRIVILÈGES

Les éléments majeurs qui influent sur la probabilité de succès ou la difficulté technique d'une reconnaissance interne, d'une latéralisation ou d'une élévation de privilèges sont relativement similaires et regroupés.

- Utilisateurs ayant des droits d'administrateur sur leur poste car cela facilite grandement les opérations de reconnaissance interne, latéralisation et élévation de privilèges
- Existence d'une politique de gestion des profils d'utilisateurs et de leurs droits d'accès, application du principe du moindre privilège.
- Connexions à distance sur les systèmes limitées à des machines dédiées à l'administration, sans accès à Internet.
- Existence d'un centre de supervision de la sécurité (SOC).
- Existence d'une politique d'authentification sur les réseaux EXEMPLE de moyens d'authentification du plus sécurisé au moins sécurisé : authentification forte, mot de passe avec politique contraignante, mot de passe sans politique, pas d'authentification, carte à puce.
- Cloisonnement des réseaux informatiques de l'entité par domaines de confiance ou de sensibilité des données (par exemple selon les guides de recommandations de l'ANSSI).
- Administration sécurisée des réseaux et services (par exemple selon les guides de recommandations de l'ANSSI).
- Niveau d'hétérogénéité du parc informatique. Plus le niveau d'hétérogénéité est élevé, plus la surface

d'attaque est importante et plus il est facile de trouver une vulnérabilité exploitable. À titre indicatif: hétérogénéité élevée (évolutions externes, BYOD, services disparates, etc.), hétérogénéité moyenne (rationalisation progressive, convergence des applicatifs, etc.), hétérogénéité faible et maîtrisée (applicatifs standards, etc.).

- Nombre et spécificité des services offerts par le système d'information. plus les services métier offerts par le système d'information sont nombreux et spécifiques, plus la surface d'attaque est importante et plus il est facile d'identifier une vulnérabilité exploitable.
- Facilité d'accès des données critiques. la recherche des informations techniques (plans d'adressage, mots de passe, etc.) ou métiers peut être largement complexifiée pour l'attaquant. EXEMPLE par ordre croissant de difficulté: données stockées en clair dans une zone centralisée et facilement identifiable (par leur nommage, etc.), données stockées à de multiples endroits, données chiffrées (pour l'attaquant, il sera alors nécessaire d'obtenir la clé de déchiffrement).

PILOTAGE ET EXPLOITATION DE L'ATTAQUE

Les éléments à considérer peuvent dépendre de l'objectif visé par l'attaquant et du mode d'attaque employé.

- Nature du canal qu'il faudrait mettre en place pour piloter ou exploiter une attaque sur les biens supports visés. Canaux de command & control : canal préexistant déjà en place (backdoor), canal synchrone mis en place pour l'attaque. EXEMPLES : direct, reverse tcp/http, canal asynchrone (exemples : mail, réseaux sociaux), canal physique (exemple : air gap via des supports de stockage amovibles).
- Existence d'un centre de supervision de la sécurité (SOC).
- Existence d'un dispositif anti-DDOS.
- Prise en compte de la menace TEMPEST, liée à l'interception de signaux parasites compromettants, notamment si les locaux de l'entité sont situés dans une zone urbaine de forte densité.
- Contraintes de temps présumées pour l'exploitation de l'attaque : le temps d'exploitation va dépendre de l'objectif visé. Il peut être très court (quelques minutes à quelques heures), par exemple dans le cas d'un sabotage ou d'une attaque en déni de service non persistante, ou relativement long (plusieurs mois, voire années) pour une opération d'espionnage. D'autre part, certaines contraintes de temps peuvent rendre la tâche plus difficile pour l'attaquant. À titre indicatif, par ordre croissant de difficulté : aucune contrainte, l'attaque peut-être portée n'importe quand ; le timing doit être précis, mais le préavis est important; le timing doit être précis et l'attaquant aura peu de préavis ; l'attaque doit être coordonnée sur plusieurs machines, sans connexion à Internet.

OUTILS MALVEILLANTS

La plupart des attaques demande l'installation de logiciels malveillants dans les systèmes ciblés, parfois en plusieurs étapes. Cette section, complémentaire des précédentes, regroupe les éléments majeurs qui déterminent la réussite et le coût d'un projet malveillant (mode opératoire, outil(s), etc.). Elle peut vous aider à affiner l'estimation de la vraisemblance d'une action élémentaire qui nécessiterait l'installation d'un logiciel malveillant.

- Type de technologie des biens supports ciblés par l'outil malveillant. il est rare qu'un logiciel soit développé spécifiquement pour être malveillant et servir un dessein d'attaque.
- Délai d'application des correctifs de sécurité après leur publication. Mise en œuvre des recommandations

de l'ANSSI relatives au MCS. Un bien support à jour en termes de correctifs de sécurité oblige pour l'attaquant le développement d'un exploit dit « *0-day* », donc inconnu du public. Dans le cas contraire, l'attaquant n'a qu'à exploiter une vulnérabilité publique (difficulté nulle et probabilité de succès quasi certaine). Plus le délai d'application d'un correctif de sécurité sur une vulnérabilité connue est long, plus la fenêtre d'opportunité pour obtenir un exploit sans difficulté est important.

- Degré d'ancienneté de la technologie des biens supports ciblés.

Toutefois, selon la technologie des biens supports visés, l'attaquant pourra être amené à adapter ou redévelopper un logiciel malveillant. Dans certains cas, si la technologie ciblée est très spécifique, il devra même acquérir le bien support. EXEMPLE : calculateur aéronautique, automate programmable industriel. Le type de technologie ciblé influe donc énormément sur la difficulté technique.