ROYAUME DU MAROC
ADMINISTRATION DE LA DÉFENSE NATIONALE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉFÉRENTIEL
DE GESTION DES INCIDENTS DE CYBERSÉCURITÉ

Edition 2022

INFORMATIONS

PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :

REDIGE PAR	VERSION	DATE
DGSSI	1.1	2022

ÉVOLUTION DU DOCUMENT :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	2017	VERSION INITIALE
1.1	2022	

PUBLIC CONCERNÉ PAR CE DOCUMENT :

POUR TOUTE REMARQUE :

CONTACT	EMAIL
DGSSI	CONTACT@DGSSI.GOV.MA

SOMMAIRE

I. Introduction

1. Contexte

Dans un monde de plus en plus connecté et une dématérialisation des process et des activités qui ne cesse de croitre, le Maroc n'est pas en reste. Au cours des vingt (20) dernières années, le secteur des télécommunications et du digital a connu une progression substantielle, faisant du Royaume l'un des pays les mieux connectés à Internet en Afrique. Cette progression profite également aux cybercriminels, dont le mode opératoire est toujours plus sophistiqué.

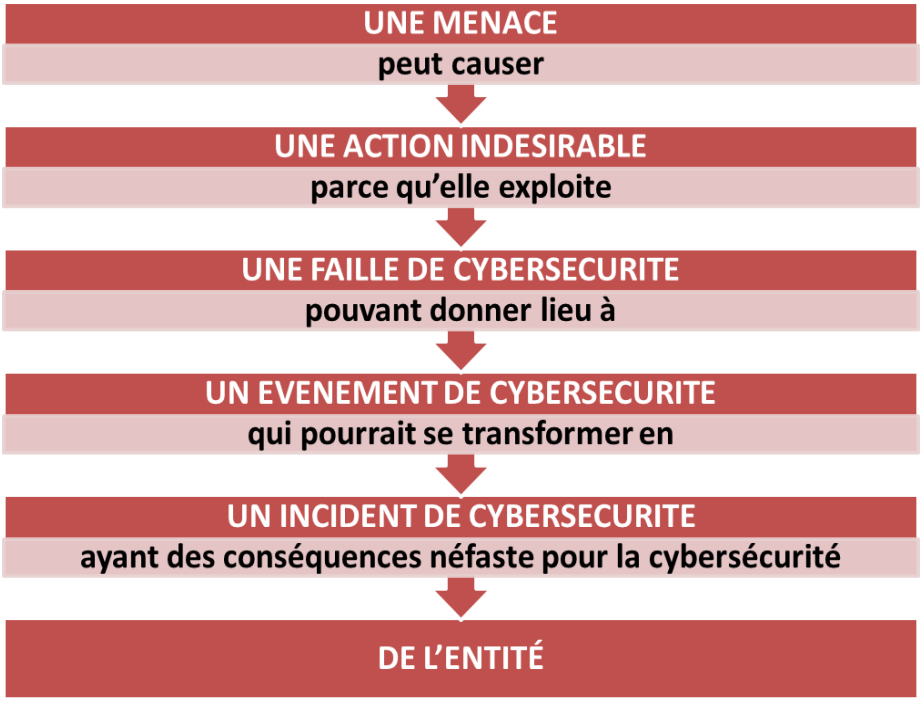
En effet, force est de constater que cette forte digitalisation s'est accompagnée par a une explosion du nombre de cyberattaques. De nos jours, personne n'est à l'abri d'une cyberattaque, le monde s'est habitué à ce type d'incident faisant de la cybersécurité un sujet important avec lequel il va falloir composer de plus en plus.

Ainsi, en matière de gestion de risque et d'élaboration du plan de reprise des activités, la réaction aux cyberattaques est devenue une des capacités primordiales à détenir par les gouvernements et les entreprises. A ce titre, il est fondamental d'identifier et de comprendre les risques susceptibles d'affecter un système d'information et de développer l'agilité nécessaire pour faire face aux nouvelles menaces. Pour ce faire, la gestion des incidents de cybersécurité est devenue l'un des piliers de la sécurité des systèmes d'information. Cette activité requiert de nouvelles expertises et nécessite l'implication forte des responsables métiers et des cadres de direction (Top Management).

Pour permettre aux entités, au sens de la loi 05-20, de gérer dans des délais raisonnables tout incident informatique, l'article 42 du décret d'application de la loi 05-20 relative à la cybersécurité prévoit l'élaboration d'un référentiel de gestion des incidents de cybersécurité. Ce référentiel vise à mettre en place les moyens et les processus adéquats pour détecter rapidement les cyber incidents, minimiser leurs impacts, éliminer les failles exploitées et restaurer au plutôt les services assurés par un système d'information.

2. Rappel de la chaine d'incident de cybersécurité

Selon la norme de gestion des incidents de sécurité de l'information ISO 27035, la chaine d'incident de cybersécurité se présente comme suit :



Les termes et définitions utilisés sont conformes à la norme ISO / CEI 27000 :

- **Investigation sur la sécurité de l'information :** Application d'examens, d'analyses et d'interprétations pour aider à comprendre un incident de sécurité de l'information.
- **Équipe d'intervention en cas d'incident :** Équipe de membres de l'organisation qualifiés et de confiance qui répondent et résolvent les incidents sous la coordination du gestionnaire des incidents.
- **Événement de sécurité de l'information :** Événement indiquant une possible violation de la sécurité de l'information ou une défaillance des contrôles.
- **Incident de sécurité de l'information :** Un ou plusieurs événements de sécurité de l'information liés et identifiés qui peuvent nuire aux actifs d'une organisation ou compromettre ses opérations.
- **Gestion des incidents de sécurité de l'information :** Exercice d'une approche cohérente et efficace du traitement des incidents de sécurité de l'information.
- **Gestion des incidents :** Actions de détection, de signalement, d'évaluation, de réponse, de traitement et d'apprentissage des incidents de sécurité de l'information.

- ☞ **Réponse aux incidents :** Les mesures prises pour atténuer ou résoudre un incident de sécurité de l'information, y compris celles prises pour protéger et restaurer les conditions opérationnelles normales d'un système d'information et les informations qui y sont stockées.

- ☞ **Point de contact :** Fonction ou rôle organisationnel défini servant de coordonnateur ou de point focal d'information concernant les activités de gestion des incidents.

- ☞ **Gestionnaire d'incidents (incident manager) :** Personne chargée de diriger toutes les activités d'intervention en cas d'incident et de coordonner l'équipe d'intervention en cas d'incident (IRT).

3. Objet du document

Un système de gestion des incidents de cybersécurité comprend six (06) phases à savoir : planification et préparation, détection et triage, analyse et endiguement, éradication, récupération et enfin retour d'expérience et actions post-incident.

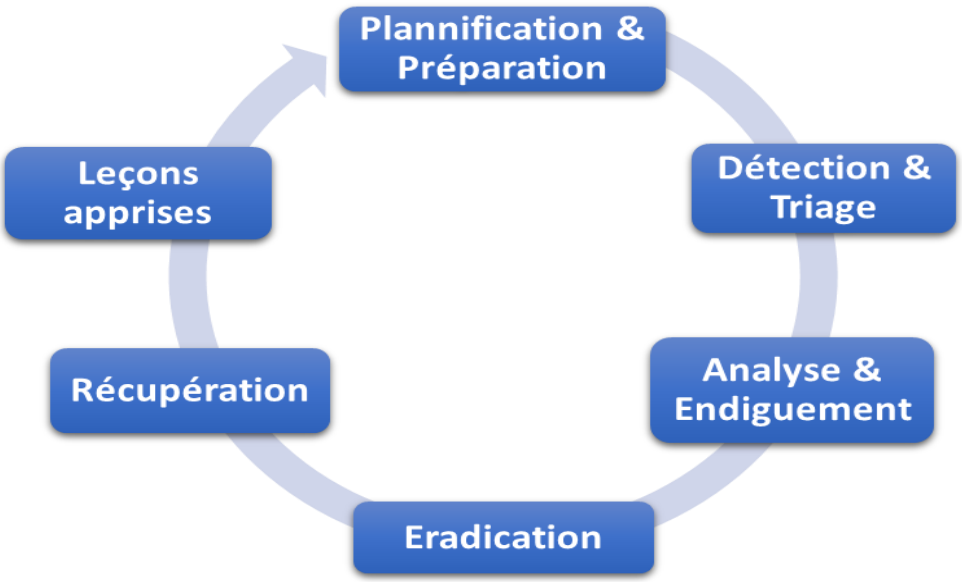
Généralement, les objectifs escomptés de la mise en place d'un tel système sont :

- la neutralisation de certains incidents de cybersécurité avant qu'ils ne surviennent ;
- la limitation du périmètre d'impact des incidents de cybersécurité ;
- le traitement des menaces et des vulnérabilités dès l'occurrence d'un incident de cybersécurité ;
- l'amélioration de la coordination entre les entités et la DGSSI en matière de gestion des incidents de cybersécurité ;
- la réduction des coûts et des impacts que peuvent engendrés les incidents de cybersécurité sur la confidentialité, la disponibilité ou l'intégrité des services, des actifs informationnels et des activités de l'entité.

Il est important de noter que la « réponse aux incidents » se différencie de « gestion des incidents ». En effet, la réponse aux incidents comporte l'ensemble des composants techniques nécessaires pour analyser et contenir un incident alors que la gestion des incidents comprend les fonctions de logistique, de communication, de coordination et de planification nécessaires pour résoudre définitivement un incident.

II. Processus de gestion des incidents

Afin de concilier efficacité et rapidité, la gestion d'un incident de sécurité ne doit pas s'improviser mais préparée minutieusement et conduite d'une manière structurée.
A ce titre, le schéma ci-après illustre les six phases de gestion d'incident :



1. Planification et préparation

Comme les atteintes à la sécurité sont de plus en plus sophistiquées, un nombre important d'incidents demeure non décelé pendant plusieurs mois. Ceci est dû, d'une part, à l'absence de déploiement de méthodes de prévention avérées et de moyens de détection et de contrôle en matière de cybersécurité, et d'autres part, au manque de compétences techniques.

A cet effet, les articles 4,5 et 7 de la loi 05-20 exigent des entités d'élaborer des politiques de sécurité et une classification de leurs actifs informationnels en se basant sur une analyse de risque et partant déployer les moyens nécessaires afin d'assurer la sécurité de ces actifs et disposer de systèmes de supervision et de détection.

La politique de gestion des incidents de cybersécurité doit fournir les principales démarches pour assurer une mise en œuvre cohérente et appropriée des processus et procédures de détection et de gestion des incidents de cybersécurité. Cette politique doit être déclinée à partir de la stratégie de sécurité de chaque entité et des différentes règlementations en vigueur.

Ainsi, toute politique de gestion des incidents de cybersécurité doit respecter les principes suivants :

- ✓ faire partie de la politique de sécurité des systèmes d'information ;
- ✓ approbation et validation de la hiérarchie ;
- ✓ disposer d'une équipe de réponse aux incidents ;
- ✓ déployer des méthodes et des équipements de détection des incidents et de contrôle (équipements de sécurité, gestion des correctifs, évaluation des vulnérabilités,) ;
- ✓ définir le but et les objectifs de la politique de gestion des incidents ;

- ✓ identifier les catégories et les types d'incidents de cybersécurité pouvant affectés votre entité, en adéquation avec les catégories définies en annexe a ;
- ✓ définir et décrire la criticité des incidents pré-identifiés ;
- ✓ élaborer des plans d'actions et de réponse par catégorie d'incident pré-identifiés ;
- ✓ définir les rôles et les responsabilités des différents intervenants pour chaque phase du processus de gestion des incidents de cybersécurité ;
- ✓ définir les canaux de communication avec les entités externes et formaliser, si nécessaire, des contrats de supports et de maintenances.

Sur le plan technique, l'entité doit en outre :

- ✓ disposer d'une cartographie détaillée de son système d'information : architecture réseau, technologies utilisées et versions, systèmes d'opération et droits d'accès, etc.
- ✓ Identifier les évènements de sécurité ainsi que les moyens à déployer ou à activer afin d'être en mesure de détecter les incidents critiques identifiés dans la politique de gestion des incidents de cybersécurité ;
- ✓ journaliser les activités système et réseau du système d'information de l'entité ;
- ✓ collecter les informations permettant de constituer le contexte de situation d'incident, notamment :
  - système local : trafic réseau et journaux d'activités ;
  - capture du trafic des segments critiques (voir Annexe B) ;
  - actualités politique, social ou économique ayant une relation avec l'incident traité ;
  - flux d'informations externes sur :
    - o les tendances, indicateurs et nouveaux vecteurs d'attaques ;
    - o les nouvelles stratégies et technologies d'atténuation.
- ✓ configurer les outils de détection en adéquation avec les risques et menaces qui pèsent sur l'entité ;
- ✓ assurer un suivi et un monitoring permanent des différents actifs informationnels de l'entité ;
- ✓ planifier des tests réguliers destinés à vérifier les processus et procédures de gestion des incidents de cybersécurité mis en place ;
- ✓ mettre en place des mécanismes qui permettent aux parties externes de signaler à l'entité des incidents (adresse mail et numéro de téléphone sur le site web ainsi que sur la base Whois).

Durant la phase de préparation, il faut également limiter le nombre d'incidents en mettant en œuvre des contrôles et mesures de sécurité préventives en se basant sur les résultats de l'évaluation des risques. Ceci a pour objectif de garder le nombre d'incidents raisonnablement bas pour ne pas perturber les processus métiers et surtout permettre aux équipes de se concentrer sur les incidents les plus dangereux et d'y répondre dans des délais raisonnables.

2. Détection et triage

Cette phase débute par la détection des événements susceptibles de constituer des incidents de cybersécurité. Après leur classement selon des catégories prédéfinies, il faut informer les responsables des systèmes d'information touchés et déclencher le processus de réponse à l'incident.

Une anomalie détectée au niveau d'un système d'information ne peut pas automatiquement être qualifié comme un incident. Les signes d'incidents ainsi que les sources de collecte possibles figurent à l'Annexe C.

En cas d'incident et après classification, il faut recueillir les preuves et événements de sécurité essentiels à la conduite nécessaires des étapes suivantes. Ces événements proviennent de diverses sources, particulièrement les fichiers journaux et les messages d'erreur ainsi que les systèmes de détection d'intrusion et des pares-feux (firewall).

Ensuite vient la phase de triage des incidents. Ce dernier est nécessaire afin de permettre à l'équipe de réponse de savoir les process à adopter et la célérité à y réserver pour assurer une réponse adéquate. Ce triage se base sur le type d'incident, la valeur de l'asset et son impact potentiel.

Ainsi, lors de la phase de détection l'entité doit entreprendre les actions clés suivantes :

- détecter et signaler l'occurrence d'un événement de sécurité informatique ou de la parution d'une vulnérabilité ;
- surveiller les alertes générés par les systèmes de sécurité ;
- analyser les activités anormales remontés par les utilisateurs et traiter sans exception toutes les alertes remontées ;
- prendre en compte au sérieux les informations et les alertes communiquées ou diffusées par les organismes de cybersécurité spécialisés (maCERT, prestataires…) ;
- communiquer toute activité anormale à l'équipe de réponse aux incidents ;
- collecter et stocker d'une manière sécurisée les preuves numériques. Si ces dernières sont requises pour des poursuites judiciaires ou pour des mesures disciplinaires internes, le respect des procédures y afférentes est obligatoire ;
- mettre en place une procédure de gestion des changements pour assurer la surveillance et la mise à jour des systèmes de détection ;
- demander l'aide du niveau supérieur si un besoin pressant d'évaluation avancée ou de prise de décision est nécessaire.
- catégoriser tous les incidents afin de faciliter la tâche aux analystes et accélérer le processus de réponse aux incidents ;
- adopter le processus d'escalade approprié à la catégorie d'incident en cours de traitement ;
- étudier la pertinence de communiquer sur cet incident auprès du public.

Après la détection et la catégorisation d'un incident, chaque entité doit le déclarer à la DGSSI, dès qu'elle en prend connaissance, et ce conformément à l'article 8 de la loi 05-20. Cette notification doit se faire selon la procédure détaillée sur le site Web de la DGSSI : *https://www.dgssi.gov.ma/fr/declaration-dincidents*

Cette déclaration commence par communiquer au maCERT/DGSSI les informations préliminaires à disposition et les compléter au fur et à mesure de l'avancement du processus de réponse à l'incident. L'entité doit également fournir toute information complémentaire demandée par le maCERT et suivre scrupuleusement les directives et recommandations émises par la DGSSI (Articles 3 et 8 de la loi 05-20).

3. Analyse et endiguement

Cette phase a pour objectif de collecter les informations supplémentaires et utiles à la phase analyse afin de pouvoir contenir au plutôt l'attaque.

D'abord, il faut collecter les évidences de tous les actifs informationnels compromis ou susceptible de l'être. Il est recommandé de ne pas mettre ces actifs hors tension afin de préserver des évidences importantes qui se trouvent généralement dans les mémoires volatiles.

Cette collecte des données peut se faire à chaud ou à froid. A froid, elle se fait sur un système en marche (live forensics). L'investigation se base sur des indices « artefacts » collectés à partir des systèmes en marche. Puisque à ce stade les détails de la menace sont encore inconnus, il faut commencer par identifier et quantifier la menace à travers la collecte des informations ci-après :

- la mémoire volatile ;
- les « prefetch files » ;
- les clés de registre ;
- les connexions réseau ouvertes ;
- les comptes système ;
- etc.

En cas d'infection ou intrusion qui touche un parc informatique étendu, cette action s'avère très efficace. Les informations ci-dessus peuvent être collecter, à titre d'exemple, en utilisant l'outil « FastIR ».

Quant à la collecte d'information à froid, elle se fait sur un système hors tension. En termes de temps, la procédure d'acquisition des évidences peut être très longue. Elle repose sur la création des images des disques durs fort probablement compromis au sein du système d'information.

Une fois la collecte des évidences effectuée, différentes actions d'investigation sont menées relativement au type de l'incident. En fonction des résultats des différentes phases atteintes du diagnostic, l'équipe partage avec les responsables du système d'information ciblé les mesures préliminaires jugées nécessaires à limiter l'impact de l'incident. Cet endiguement se fait en deux étapes : mesures d'endiguement immédiat et à court termes.

Les mesures d'endiguement immédiat visent à limiter les dommages dès que possible. Ces mesures peuvent comprendre, à titre d'exemple, l'isolement d'un segment de réseau de postes de travail infectés, ou la mise en arrêt des serveurs de production compromis après basculement vers d'autres serveurs. Les mesures d'endiguement immédiat ne constituent pas la solution définitive, elles servent uniquement à limiter l'impact de l'incident.

Après l'achèvement de l'analyse approfondie des évidences, la phase d'endiguement à court terme intervient afin d'assurer l'intégrité du système dans sa globalité. La reconstruction de nouveaux systèmes propres est à privilégier, sauf si la réparation temporaire des systèmes affectés est nécessaire pour assurer la continuité du service. Durant cette étape, il faut s'assurer que tous les correctifs de sécurité ont été installés et que toutes les failles ont été comblées ; à titre d'exemple, les comptes et fichiers créés par les attaquants sont supprimés.

Cette phase s'achève par la rédaction d'un rapport faisant ressortir principalement les points suivants :

- les évidences collectées ;
- le scénario d'attaque ;
- les indices de compromission réseau et système ;
- les mesures prises pour endiguer l'incident ;
- les mesures à entreprendre pour traiter l'incident ;
- les difficultés rencontrées.

4. Eradication

La phase d'éradication et de restauration consiste en :

- la suppression de tous les éléments corrompus liés à l'incident ;
- la restauration du système d'information à partir d'une sauvegarde saine ou en réinstallant le système en entier ;
- la correction des vulnérabilités exploitées par l'attaquant ;
- s'assurer que les systèmes non affectés, et qui présentent les mêmes vulnérabilités exploitées par l'attaquant, ont été corrigés ;
- forcer éventuellement les utilisateurs à changer leurs mots de passe ;
- bloquer ou surveiller éventuellement toute adresse IP ou noms de domaine, malicieux.

5. Récupération

Le but de cette phase est de rétablir à l'état normal de fonctionnement du système d'information et de s'assurer autant que possible que ce type d'incident ne se reproduise plus. Il est essentiel d'une part, de contrôler si toutes les mesures de réponse recommandées ont été bien implémentées et d'autre part, de sensibiliser les utilisateurs et surveiller le système lors de sa remise en production.

Durant cette phase, les points ci-après doivent être arrêtés conjointement entre l'équipe de réponse à l'incident, les responsables du SI et les responsables métiers :

- ✓ l'heure et la date de reprise des opérations ;
- ✓ la méthodologie à adopter pour tester et vérifier que les systèmes compromis sont propres et entièrement fonctionnels ;
- ✓ la durée de surveillance nécessaire pour observer les éventuels comportements anormaux du système d'information ;
- ✓ les outils nécessaires pour tester, surveiller et valider le comportement du système.

6. Retour d’expérience et actions post-incident

La phase Retour d’expérience et actions post-incident est primordiale pour tirer de nouveaux enseignements et optimiser les pratiques dans le futur, notamment en matière d’amélioration des capacités de gestion des incidents.

Après la finalisation du rapport global de l’incident et des propositions pour améliorer la politique de gestion d’incident, ce rapport devrait répondre aux questions : qui, quoi, où, pourquoi et comment de l’incident.

A ce titre, il est recommandé de tenir une réunion de débriefing impliquant les différentes parties concernées pour présenter les éléments suivants :

- quand le problème a-t-il été détecté pour la première fois et par qui ;
- l'étendue de l'incident ;
- comment il a été endigué et éradiqué ;
- les problèmes rencontrés ;
- travail effectué pendant la récupération ;
- domaines où l’équipe de réponse aux incidents a été efficace ;
- domaines qui doivent être améliorés ;
- mise à jour des procédures ;
- mesures à entreprendre et les moyens à réaliser pour renforcer la sécurité du SI ;
- éventuellement, le contenu du communiqué à publier.

Enfin, il est d’une grande utilité d’utiliser la documentation élaborée lors de l’incident dans la formation et la sensibilisation des nouveaux membres de l'équipe de réponse à l’incident et de s’y référer en cas d’incidents similaires futurs.

III. Annexes :

1. Annexe A : Vecteurs d’attaques

Les vecteurs ci-dessous ne sont pas destinés à fournir le classement définitif des incidents, mais plutôt pour être utilisés lors de la définition de procédures spécifiques de traitement d’incident. Ces procédures sont à définir selon le type vecteur d’attaque utilisé :

- Support externe / amovible : Une attaque exécutée à partir de supports amovibles ou d’un périphérique.
- Attrition : Une attaque qui emploie des méthodes de brute force pour compromettre, dégrader ou détruire les systèmes, réseaux ou services.
- Email : Une attaque exécutée par l'intermédiaire d'un message électronique ou une pièce jointe.
- Utilisation inappropriée : Tout incident résultant de la violation par un utilisateur autorisé de la politique de sécurité des systèmes d’information de l’entité, excepté les catégories ci-dessus.
- Attaque composée : Une attaque qui est composée de plusieurs attaques ci-dessus.
- Perte ou vol d'équipement ou sabotage : La perte ou le vol d'un dispositif informatique ou des médias utilisés par l'entité.

2. Annexe B : Catégories des incidents de cybersécurité les plus répandus

Catégorie d'incident	Type d'incident	Description
Atteinte à la disponibilité	DOS	Attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. La disponibilité peut également être affectée par des actions locales (destruction, perturbation de l'alimentation électrique, etc.).
	DDOS	
	Sabotage	
Infection	Virus, Ver, Trojan, Ransomware, Backdoor…	Un code malicieux qui est intentionnellement inclus ou inséré dans un système à des fins nocives. L'interaction de l'utilisateur est normalement nécessaire pour activer le code.
Tentatives d'intrusion	Exploitation des vulnérabilités	Une tentative de compromettre un système ou de perturber un service en exploitant des vulnérabilités (ex. Buffer overflow, XSS, Sql injection, file upload etc.).
	Tentatives de connexion	Plusieurs tentatives de connexion (deviner / craquer des mots de passe, force brute).
	Phishing	Le but est de dérober des informations personnelles des utilisateurs ou de les piéger à installer un malware
	Nouvelle signature d'attaque	Une tentative d'exploit inconnu.
Intrusion	Compromission d'un compte	Contrôle réussi d'un compte
		Ajout d'un compte
		Changement des droits d'accès ou de mot de passe
	Défiguration d'un site web	Insertion, modification ou suppression d'un contenu web
Collecte d'informations	**Scan**	**Attaques qui envoient des requêtes à un système pour découvrir des points faibles. Ce type d'attaque inclut certains types de processus de test pour collecter des informations sur les hôtes, les services et les comptes.** **Exemples : fingerd, requête DNS, ICMP, SMTP (EXPN, RCPT, ...).**
	Sniffing	Capture et enregistrement du trafic réseau.

	Ingénierie sociale	Collecte des informations d'un être humain dans un environnement non technique (P. Ex. Mensonges, astuces, pots de vin ou menaces)
Atteinte à la sécurité des données	Accès ou modification non autorisée des informations	
	Exfiltration des données	Récupération des données et leur transfert vers une destination externe non légitime.
Autres	Tous les incidents qui ne correspondent pas à l'une des catégories données ci-dessus doivent être classés dans cette classe.	

3. Annexe C : Catégorie des incidents à remonter au maCERT

Catégorie	Type
Tentative d'intrusion	Tentative d'exploitation d'une vulnérabilité nouvelle
	Tentative d'authentification (Bruteforce)
	Phishing (Compagne de phishing ciblée)
Intrusion	Compromission d'un compte privilégié
	Compromission d'un compte non privilégié
	Bot
	Installation Backdoor
Code Malicieux	Virus/Worm
	Ransomware
	Cryptominer
	Autre
Disponibilité	DoS/DDoS
	Sabotage
	Panne (pas de malice)
	Autre
Sécurité des données	Accès non autorisé
	Modification non autorisé
	Autre

4. Annexe D : Fiche de déclaration d'un incident

Fiche de déclaration d'incident de cybersécurité

Contact

- Nom de l'organisation : ----------
- Nom du responsable (s) à contacter : ----------
- Fonction : ----------
- Email : ----------
- Téléphone : ----------

Détails sur l'incident

- Type de l'incident : ----------
- Impact de l'incident : ----------
- Date et heure d'occurrence : ----------
- Date et heure de détection de l'incident : ----------
- Vecteur d'attaque susceptible : ----------

Complément d'Informations

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

Actions prises par l'équipe IT :

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

---------- ---------- ----------

5. Annexe E : Les signes d'un incident et les sources de collecte

Les signes d'un incident

La partie la plus difficile du processus de réponse aux incidents est la précision lors de la détection et la validation des incidents probables en déterminant si un incident a eu lieu et, le cas échéant, le type, l'étendue et l'ampleur du problème. Cette difficulté est due à la combinaison de trois facteurs :

- ✓ Les incidents peuvent être détectés par de nombreux moyens, avec des niveaux différents de détail et de précision. Les incidents peuvent être détectés par des moyens automatisés (IDPS, les logiciels antivirus, SIEM, …) comme ils peuvent être signalés par les utilisateurs. Certains incidents ont des signes manifestes qui peuvent être facilement détectés, alors que d'autres sont difficilement détectables.
- ✓ Le nombre de signes potentiels d'incident est généralement élevé. Il est fréquent pour une entité de recevoir quotidiennement des centaines d'alertes, générées par les systèmes de détection. Un nombre important d'entre eux sont des faux positifs.
- ✓ Une analyse efficiente des données liées à l'incident nécessite des compétences techniques spécifiques avancées ainsi qu'une large expérience dans ce domaine.

Les signes d'un incident peuvent soit :

- ✓ Annoncer la probabilité ou les prémices d'occurrence d'un incident. L'entité peut éviter l'incident en modifiant sa posture de sécurité afin de protéger la cible objet de l'attaque. Sinon l'entité peut au moins surveiller l'activité liée étroitement à la cible. Ces signes sont relativement rares on citera comme exemples :
  - Les logs de serveur Web qui indique l'utilisation d'un scanneur de vulnérabilités ;
  - L'annonce d'un nouvel exploit qui cible une vulnérabilité au niveau d'un composant utilisé par l'entité ;
  - Une menace émanant d'un groupe indiquant une attaque ciblant l'entité.
- ✓ Indiquer qu'un incident a eu lieu ou il est en train de se produire en ce moment. Ce type de signes est le plus courant. La liste ci-après n'est pas exhaustive :
  - Alerte générée par un IPS réseau lorsqu'une tentative de débordement de tampon se produit sur un serveur ;
  - Alerte générée par la solution antivirale ;
  - Découverte d'un nom de fichier avec des caractères inhabituels ;
  - Changement illégitime de configuration au niveau d'un composant du SI ;
  - Des événements d'une application indiquant de multiple échec de tentative de connexion à partir d'un système distant inconnu ;
  - Un administrateur de messagerie voit un grand nombre d'e-mails avec un contenu suspect ;
  - Un administrateur réseau constate un écart inhabituel par rapport au trafic réseau normal ;
  - Les comptes ou les mots de passe ne fonctionnent plus ;
  - Le site Internet de l'entité renferme des modifications non autorisées ;
  - Il n'y a plus d'espace disque ou de mémoire disponible ;
  - Le système gèle à répétition ou se réinitialise de façon imprévue ;
  - Les contrôles de sécurité des terminaux, comme les antivirus, ne fonctionnent plus.

Les sources de collecte pour la détection des incidents

Les signes d'incidents sont identifiés à l'aide de nombreuses sources différentes. Les plus connues sont les solutions de sécurité, les événements de sécurité (log), les informations publiques, et les personnes. Le tableau ci-dessous répertorie les sources les plus utilisées pour la détection des incidents.

Source	Description
Alertes	
IDS/IPS	Les IDS/IPS identifient les événements suspects et enregistrent les données pertinentes à leur égard, entre autres la date et l'heure de la détection de l'attaque, le type d'attaque et les adresses IP source et destination. La plupart des produits IDS/IPS se basent sur des signatures pour identifier les activités malveillantes ; la base de données des signatures doit être tenue à jour pour pouvoir détecter les plus récentes attaques. Les IDS/IPS produisent de fausses alertes (des faux positifs). Pour minimiser les faux positifs, un effort important doit être fourni lors de la configuration de l'IDS/IPS. Les analystes doivent, à cet effet, valider manuellement ces alertes soit en examinant de près les données justificatives enregistrées ou en obtenant d'autres données à partir d'autres sources. Pour tirer profit de ces outils, il est recommandé d'ajouter des signatures spécifiques aux menaces et risques que l'entité a déjà identifié dans les phases préparation ou post-incident.
SIEM	Le SIEM (Security Information and Event Management) est un point de concentration des événements de sécurité doté de fonctions d'analyse intelligente. Il génère des alertes basées sur l'analyse et la corrélation de plusieurs sources d'événements de sécurité. La collecte de ces événements doit être très large tout en privilégiant l'équilibre entre les bruits réseau et les signaux faibles (la qualité d'un SIEM dépend de la qualité de ses sources). De plus, l'équipe sécurité doit définir les cas d'usages possibles à savoir les scénarios, les règles de corrélation et de dépassement de seuils. Par conséquent, la configuration et la personnalisation de ces systèmes est une tâche complexe et primordiale qui nécessite des compétences techniques et une bonne connaissance du système d'information à superviser et qui doit être inscrite dans le temps.
Les Antivirus et Antispam	Le logiciel antivirus détecte diverses formes de logiciels malveillants, génère des alertes, et empêche les logiciels malveillants d'infecter les machines. Les produits antivirus actuels sont efficaces pour arrêter de nombreux exemples de logiciels malveillants si leurs signatures sont tenues à jour. Le logiciel Antispam est utilisé pour détecter les spams ciblant les boîtes de messagerie des utilisateurs. Le Spam peut contenir des logiciels malveillants, des attaques de phishing, et autres contenus malveillants. Une alerte générée par un anti-spam indique des tentatives d'attaque via E-mail.

Logiciel de vérification d'intégrité des fichiers	Le Logiciel de vérification de l'intégrité des fichiers peut détecter les modifications apportées aux fichiers importants pendant les incidents. Il utilise un algorithme de hachage pour obtenir une somme de contrôle cryptographique pour chaque fichier désigné. En recalculant régulièrement ces sommes de contrôle et en les comparant avec les valeurs précédentes, les modifications de fichiers peuvent être détectées.
Les services externes de veille et d'alerte	Ils offrent une variété de services d'abonnement et de services de veille et d'alerte. Un exemple, le service de détection externe peut notifier une entité en cas où ses adresses IP, des noms de domaine, etc., sont associés à une activité malveillante (source de malware ou de spam, appartient à un réseau de botnet,). Certains sites publient en temps réel des listes noires avec des informations similaires.
Événements (Logs)	
Événements générés par les systèmes d'exploitation, les services et les applications	Les événements (Logs) des systèmes d'exploitation, des services et des applications (en particulier les événements liés à la sécurité) sont souvent d'une grande valeur pour la détection et le traitement d'un incident, telles que l'enregistrement des événements relatifs à l'accès aux comptes et les actions qui ont été réalisées. Les entités doivent mettre en place des références exigeant l'activation des logs sur tous les systèmes et surtout sur les systèmes critiques sans oublier les postes utilisateurs. Ces logs peuvent être analysés en utilisant des règles de corrélation. Une alerte peut être générée suite à cette analyse pour indiquer un incident.
Événements des équipements réseaux et FW	Les événements (Logs) générés par ces équipements identifient les connexions bloquées et aussi autorisées, même s'ils fournissent peu d'informations sur la nature de l'activité. Ils peuvent être utiles pour identifier les tendances du réseau et faire des analyses comportementales comme ils peuvent être corrélés avec d'autres événements détectés par d'autres sources.
NetFlow	Les routeurs, les switchs et autres périphériques réseau peuvent fournir ces métadonnées relatives au protocole TCP/IP. Ces informations sur le flux réseau, peuvent être utilisées pour identifier des activités anormales provoquées par des logiciels malveillants, exfiltration de données, et d'autres actes de malveillance.
Information publique	
Informations sur les nouvelles vulnérabilités et les nouveaux exploits	La veille concernant les nouvelles vulnérabilités et nouveaux exploits peut empêcher certains incidents de se produire et aider à détecter et analyser de nouvelles attaques. Ces informations sont disponibles publiquement au niveau de différents sites. Elles peuvent être reçues des éditeurs de logiciel et équipements que l'entité utilise dans le cadre du contrat de maintenance et de support. Elles peuvent être aussi reçu du maCERT ou à travers un prestataire de service spécialisé dans ce domaine.
Personnes	
Personnel de l'entité	Les utilisateurs, les administrateurs système, les administrateurs réseau, l'équipe sé d'autres membres de l'entité peuvent signaler des signes d'incidents. Il est imp valider toutes les notifications et de recueillir des informations supplément l'incident pour aider l'équipe qui se charge de l'analyse de l'incident.

Personnel externe à l'entité	Les rapports d'incidents qui proviennent de l'extérieur doivent être pris au sérieux. Par exemple, l'entité peut être contacté par une entité qui notifie qu'un de ces systèmes est en train de l'attaquer. Les utilisateurs externes peuvent également signaler d'autres indicateurs, comme une page Web illisible ou un service indisponible. D'autres équipes de réponse aux incidents peuvent également signaler les incidents. Il est important de mettre en place des mécanismes pour permettre aux parties externes de signaler des incidents et surveiller attentivement ces mécanismes. Cela peut être aussi simple que la mise en place d'un numéro de téléphone et une adresse e-mail pour transmettre des messages de ce genre.

6. Annexe F : Importance de la capture du trafic dans le traitement de certains incidents

La capture du trafic permet l'enregistrement complet et permanent du trafic, elle peut être assimilée à une caméra de sécurité qui surveille l'entrée et la sortie d'un immeuble.
La plupart des outils de sécurité réseau reposent sur un modèle de sécurité passif qui se base sur des signatures spécifiques pour détecter le trafic malveillant. Le problème majeur de ce modèle est son inefficacité face aux exploits Zero-Day, qui sont tout simplement de nouveaux programmes malveillants ou attaques informatiques qui ne sont pas encore connu publiquement et partant les signatures permettant leurs détections ne sont pas encore disponibles.
D'où l'importance de la capture du trafic qui permet à un analyste de sécurité d'examiner toutes les communications du système pour détecter d'éventuelles actions malveillantes non détectées par les autres moyens de sécurité mis en place. Cette capture permet aussi la rétrospection du trafic pour déterminer éventuellement si une exploitation a eu lieu avant la publication des signatures ou avant l'application d'un patch. Les données recueillies peuvent également être utilisées afin d'enrichir les signatures de détection et parfois pour extraire les exploits ou les malwares utilisés lors de l'attaque.
Le déploiement d'un système complet de capture de paquets dépend de l'architecture du réseau et l'objectif visé.
La mise en œuvre réussie de ce système repose sur trois facteurs :

- ✓ Les exigences propres à l'entité notamment le temps minimal de conservation de traces et les emplacements des points de capture ;
- ✓ L'envoi du trafic non altéré au système de capture de paquets en respectant les exigences de sécurité ;
- ✓ Le dimensionnement du système de capture pour pouvoir traiter et stocker l'ensemble du trafic souhaité.

Il existe une variété de solutions « open source » et commerciales pour implémenter cette capture. Certaines solutions sont des logiciels à installer sur du hardware préparé par l'entité. D'autres solutions sont entièrement intégrées sous forme d'équipements (hardware et software). Le choix de la solution de capture à mettre en place dépendra de l'architecture de déploiement, des compétences de l'équipe, du budget disponible et des exigences pour la préservation des données

7. Annexe G : Gestion des incidents de phishing

Étant donné que le courrier électronique (email) est largement déployé et utilisé pour communiquer avec des organisations externes non toujours fiables, il est fréquemment la cible d'attaques. Les attaquants peuvent exploiter le courrier électronique pour prendre le contrôle d'une entité, accéder à des informations confidentielles ou perturber l'accès informatique aux ressources. Les menaces courantes contre les systèmes de messagerie sont les suivantes :

- **Spam** : Le spam fait référence aux e-mails indésirables utilisés pour distribuer des liens et des pièces jointes malveillants, provoquer une congestion du réseau en consommant la bande passante des serveurs de messagerie (attaque DoS), effectuer du phishing et fraudes financières.
- **Phishing** : fait référence à l'utilisation de moyens informatiques trompeurs pour amener les individus à répondre à l'e-mail et à divulguer des informations sensibles. Des systèmes de messagerie compromis sont souvent utilisés pour envoyer des messages de spam et mener des attaques de phishing à l'aide d'une adresse e-mail par ailleurs fiable.
- **Spear-phishing** : Le Spear-phishing est une tentative ciblée de voler des informations sensibles telles que les identifiants de compte ou les informations financières d'une victime spécifique, souvent pour des raisons malveillantes. Ceci est réalisé en obtenant des informations personnelles sur la victime, telles que ses amis, sa ville natale, son employeur, les lieux qu'elle fréquente et ce qu'elle a récemment acheté en ligne.
- **Ingénierie sociale** : Les attaquants utilisent le courrier électronique pour recueillir des informations sensibles auprès des utilisateurs d'une entité ou amener les utilisateurs à effectuer des actions qui favorisent une attaque. Une attaque d'ingénierie sociale courante est l'usurpation de courrier électronique, dans laquelle une personne ou un programme se fait passer pour un autre en falsifiant les informations de l'expéditeur affichées dans les courriers électroniques pour masquer la véritable adresse d'origine.
- **Malware** : De plus en plus, les attaquants profitent de la messagerie électronique pour lancer diverses attaques contre des entités via l'utilisation de logiciels malveillants, ou « Malware », qui incluent des virus, des vers, des chevaux de Troie et des logiciels espions. Ces attaques, si elles réussissent, peuvent donner aux personnes malveillantes le contrôle des postes de travail et des serveurs, qui peuvent ensuite être exploités pour modifier les privilèges, accéder à des informations sensibles, surveiller les activités des utilisateurs et effectuer d'autres actions malveillantes.

Processus de gestion des incidents relative aux emails est une application directe du processus général de gestion des incidents de cyber sécurité.

1. <u>Préparation</u>

Cette phase, souvent négligée par les administrateurs systèmes, reste la plus importante de toute. Sans aucune préparation adéquate il serait très difficile de faire face à ce genre d'incident.

Les points essentiels à mettre en place pour réussir la phase de préparation sont :

- mettre en place un système de filtrage ;

- monitorer les communications par email à l'aide d'outil ;
- mettre en place un système d'analyse de logs (SIEM) ;
- faire des backups réguliers ;
- mettre en place une politique de sécurité raisonnable et connue de tous les employés ;
- communication rapide ;
- dérouler des exercices d'entrainement pour sensibiliser les utilisateurs.

La phase de préparation ne se limite pas seulement aux points cités ci-dessus, chaque entité peut adapter son plan de gestion d'incident en fonction des actifs qu'elle possède et les risques y afférents.

2. Détection

La phase de détection a pour but d'analyser les alertes remontées par les systèmes de détection ainsi que celles remontées par les utilisateurs. Puis faire une analyse préliminaire pour voir s'il y a vraiment incident. Quelques indications d'une attaque par email sont :

- impossibilité d'accéder au système ou aux comptes de messagerie après l'ouverture d'un e-mail ;
- système montrant des signes d'attaque de logiciels malveillants après l'ouverture d'un lien ou d'une pièce jointe à partir d'un e-mail, par exemple en trouvant un processus suspect en cours d'exécution sur votre système ;
- augmentation soudaine du trafic de la messagerie et des spams ;
- apparition de nouveaux fichiers sur le serveur de messagerie.

Ces points résument un peu les symptômes ou indices qui doivent soulever les soupçons du responsable pour mener une analyse plus approfondie.

À titre d'exemple la détection des emails de phishing et du spam se base sur les points suivants :

- réception d'une pièce jointe inattendue d'un utilisateur, d'un client, d'un fournisseur ou d'une partie tierce ;
- pièces jointes avec des formats inhabituels ou non reconnus ;
- différence entre l'identifiant de messagerie de l'expéditeur et le nom d'affichage ;
- les identifiants de courrier électronique dont le nom de l'organisation est incomplet ou incorrect ou qui utilisent des chiffres à la place des lettres dans le nom ;
- e-mails avec des liens, qui affichent un site Web ou une URL différent lorsqu'ils sont survolés ou ont une URL avec un nom ou un domaine incorrect ;
- des e-mails présentant des offres trop attrayantes pour être vraies, comme gagner à la loterie, un concours, un abonnement gratuit, des vacances et des offres d'emploi ;
- e-mails qui semblent provenir d'une banque, d'une institution financière, d'une organisation, d'un fournisseur de services et d'un autre associé de l'utilisateur, qui demandent des informations sensibles ou de se connecter à des comptes à l'aide des liens fournis ou d'installer des mises à jour.

Pour faciliter cette tâche on a souvent recours à des solutions automatisées telles que les antispam au niveau des serveurs de messagerie, les HIDS au niveau des postes utilisateurs et ajouter à cela une sensibilisation pour tous les utilisateurs.

3. Analyse et endiguement

Après la détection d'un incident via email et afin de le contenir rapidement il est recommandé de suivre les étapes suivantes :

- isoler immédiatement toutes les machines suspectes du réseau de l'entité après la détection de tout incident ;
- tous les emails malicieux ou suspects doivent être bloqués et mis en quarantaine ;
- reporter l'incident au maCERT via la procédure en place ;
- interrogez les utilisateurs sur l'incident par email pour trouver les détails de l'attaque et des actions des utilisateurs ;
- interroger les utilisateurs pour savoir s'ils ont téléchargé des fichiers joints ou cliqué sur les liens ;
- si le mail contient des liens malicieux, faire une analyse comportementale dans un environnement isolé et sécurisé (sandbox), puis bloquer les IPs et/ou es noms de domaines malicieux ;
- au cas où le mail contient une pièce-jointe malicieuse, l'analyste doit ouvrir l'email dans une environnement isolé et sécurisé (sandbox) pour mener son analyse en déclenchant le process de gestion des incidents relatifs aux programmes malveillants (malware) ;
- en cas de spam ou d'e-mails de phishing, envoyez une notification à tous les utilisateurs pour savoir si d'autres ont été confrontés au même problème.

Après ces actions préliminaires il faut entamer l'analyse du mail malicieux. Cette analyse ne peut être complète que si elle traite l'entête du mail ainsi que son contenu (lien et/ou fichier malicieux).

Les en-têtes des e-mails contiennent des informations de suivi pour un e-mail individuel, détaillant le chemin emprunté par un message lors de son passage sur divers serveurs de messagerie. Les en-têtes contiennent des horodatages, des adresses IP et des informations sur l'expéditeur/le destinataire. Ces informations sont importantes pour mener l'analyse et déterminer la nature et l'origine du mail.

Même si la forme de l'en-tête du mail change d'un constructeur à un autre, elle garde les éléments suivants :

- chemin de retour ;
- adresse e-mail du destinataire ;
- nom du serveur de messagerie ;
- type de serveur d'envoi d'e-mails ;
- adresse IP du serveur d'envoi ;
- numéro de message unique ;
- date et heure d'envoi de l'e-mail ;

- informations sur le fichier joint ;
- Sender Policy Framework (SPF) ;
- courrier identifié par clé de domaine (DKIM).

L'une des mesures de protections importantes à mettre en place pour contrer le spoofing est le **SPF** (**S**ender **P**olicy **F**ramework)**.** C'est une norme de vérification du nom de domaine de l'expéditeur d'un courrier électronique, normalisée dans la ***RFC 7208***.

Ainsi les intervenants en cas d'incident peuvent analyser l'authenticité de l'expéditeur à l'aide des résultats SPF. Cette vérification peut être implémenter dans les serveurs de messagerie et après chaque vérification il y a trois résultats possibles :

1) **None** : aucun enregistrement SPF n'a été trouvé pour ce domaine ;
2) **Pass** : les enregistrements SPF existent et l'adresse IP est autorisée, elle inclut le signe plus (+) devant l'IP ;
3) **Fail** : l'adresse IP n'est pas autorisée à envoyer des e-mails pour ce domaine. Ceci est indiqué par une commande –all dans l'enregistrement.

4. <u>Éradication</u>

Après avoir analyser l'incident vient l'étape d'éradication. Cette étape peut être résumée dans les points essentiels suivants :

- collectez les détails de l'incident, tels que l'URL, l'objet, les liens, l'expéditeur et l'adresse IP, à partir de l'analyse des en-têtes des e-mails et bloquez-les sur les serveurs, les outils de sécurité et les périphériques réseau. On peut demander l'aide des FAI pour nous aider à effectuer ces actions ;
- alerter immédiatement les utilisateurs de l'incident et les former à le diagnostiquer, et informer les administrateurs réseau pour guider les employés qui doivent faire face à la situation actuelle ;
- mettez à jour les outils antiphishing et antispam avec les nouvelles signatures trouvées et les détails de l'attaque pour empêcher des attaques similaires à l'avenir ;
- vérifiez les journaux SMTP pour savoir si le même e-mail est envoyé à d'autres employés et supprimez-les des boîtes de réception ;
- renforcez la sécurité du serveur de messagerie et des clients ;
- mettez en liste noire les sites Web malveillants et désactivez le téléchargement automatique sur tous les systèmes et appareils ;
- assurer la suppression des données relatives aux logiciels malveillants des systèmes affectés tels que les fichiers texte, processus exécutés par le logiciel malveillant ;
- bloquez et supprimez les comptes concernés et réémettez de nouveaux comptes aux employés ;
- demander à tous les utilisateurs de changer de mot de passe, et mettre en place une politique de mot passe fort ainsi qu'une authentification fort.

5. <u>Récupération</u>

La phase de récupération est :

- changer les mots de passe des comptes liés à l'incident ;

- informer les partenaires à propos des comptes compromis dans le but de vérifier s'ils ont reçu des emails de ces compte ;
- restaurer le système à partir des sauvegardes ;
- dans le cas où la décision de mener des poursuites judiciaires est prise contacter les autorités compétentes.

6. Leçons apprises

Après tout incident il est important de faire une synthèse et d'en apprendre pour s'améliorer dans le processus de gestion des incidents.

- rédiger un rapport détaillé de l'incident ;
- mettre à jour les équipements de sécurité avec les nouveaux indices de compromission (IoC) ;
- planifier des formations et workshop de sensibilisation pour les utilisateurs ;
- mettre en place une politique

8. Annexe H : Gestion d'incident de défiguration de site web

Pour renforcer la sécurité des applications web et éviter l'intrusion web il est recommander de respecter les bonnes pratiques détaillées dans le guide ci-après : https://www.dgssi.gov.ma/fr/publications/guide-de-securite-des-applications-web

En cas de défiguration de site web, il faut isoler le serveur en attendant de rétablir le site web à partir de la dernière version intègre du site. Cette version doit être préparée à l'avance. La surpression du fichier intrus n'est pas toujours suffisante pour rétablir le site. Il se peut que des fichiers de configuration soient altérés ou infectés.

Il est recommandé de mettre en place une solution de vérification d'intégrité pour tous les fichiers et dossiers du site web. Cette solution permettrait de détecter toute injection de code malicieux ou altération d'un fichier de configuration.

Pour répondre efficacement à ce type d'incident, Il est nécessaire de disposer des logs ci-après pour une période de 3 mois au moins :

- Logs du serveur web ;
- Logs des proxys et Firewall applicatifs (WAF) ;
- Logs des IPS, IDS et Firewall ;
- Logs des serveurs de bases de données.

Il est aussi recommandé de centraliser les logs dans un serveur à part pour garantir que l'attaquant ayant le contrôle du serveur web ne puisse pas effacer ses traces et fausser l'investigation.

La défiguration peut être parfois le début d'une attaque plus approfondie pour contrôler le serveur web et par la suite rebondir vers d'autres systèmes internes pour y persister ou pour l'intégrer à des plateformes Internet de distribution du malware. Dans ce cas, d'autres évidences seront nécessaires pour approfondir l'investigation telles que :

- La capture du trafic ;
- La capture de la RAM ;
- La capture du Disque ;
- Les Logs systèmes et évènements Windows ;
- Les logs de l'annuaire.

9. Annexe I : Gestion d'incident relatif à un malware

Introduction

Un logiciel malveillant, également connu sous le nom d'un programme malicieux, fait référence à un programme inséré secrètement dans un autre programme dans le but de détruire des données, d'exécuter des programmes destructeurs ou intrusifs ou de compromettre la confidentialité, l'intégrité ou la disponibilité des données, applications ou système opératoire. Les logiciels malveillants sont la menace externe la plus courante pour la plupart des hôtes, causant des dommages et des perturbations généralisés et nécessitant des efforts de récupération importants au sein de la plupart des organisations.

Utiliser une stratégie de défense en profondeur

Puisqu'il n'existe aucun moyen de protéger complètement les organisations contre les infections par des logiciels malveillants, il est fortement recommandé d'adopter une approche de « défense en profondeur ». Cela signifie utiliser des couches de défense avec plusieurs atténuations à chaque couche. Ainsi les chances de détection des logiciels malveillants augmentent de façon significative, dans le but de les inhiber ou de limiter au moins leurs impacts.

Quel que soit les mesures de sécurité misent en place pour détecter et stopper les logiciels malveillants, il faut toujours supposer que certains pourraient passer entre les mailles du filet, afin de prendre les mesures adéquates pour limiter l'impact que cela entraînerait et accélérer la réponse. Le processus de gestion des incidents relative aux logiciels malveillants (Malware) est le suivant :

1. **Préparation**

Les organisations doivent prendre des mesures préparatoires pour s'assurer qu'elles peuvent répondre efficacement aux incidents de logiciels malveillants. Les actions recommandées incluent :

- Sensibiliser l'ensemble des utilisateurs sur ce sujet : prévention, détection et déclaration ;
- Installer une solution antivirale dans l'ensemble du système d'information (serveurs et postes, Windows et Linux) et à différents niveau du flux de l'information (proxy mail, proxy web..) ;
- Mettre à jour régulièrement l'ensemble des produits du parc ;
- Mettre en place une politique de sauvegarde respectant les bonnes pratiques ;
- Mettre en place au niveau réseau une politique de micro-segmentation.
- Installer et activer au niveau des postes de travail Windows des outils permettant de générer les évènements et les journaux de sécurité permettant par la suite la détection (exemples : Sysmon & AppLocker).
- Développer et maintenir des compétences capables d'identifier, de traiter et d'analyser les codes malveillants au sein de l'équipe de réponse aux incidents. Etant donné que l'analyse des codes malveillant est une tâche assez ardue et pointue, l'entité peut externaliser cette tâche à un prestataire externe ou un partenaire (éditeur de logiciel antiviral, MMSP, CERT sectoriel ou maCERT).

2. **Détection et analyse**

Les organisations doivent s'efforcer de détecter et de valider rapidement les incidents de logiciels malveillants afin de minimiser le nombre d'hôtes infectés et limiter le dommage subis par l'organisation. Les actions recommandées incluent :

- Analyser les signes suspects détectés et valider qu'ils sont bien le résultat d'un code malveillant (nouveaux process, tentatives d'élévation de privilège, connexions réseaux Intranet…);
- Identifier les hôtes infectés par le logiciel malveillant, afin que les hôtes puissent subir les actions de confinement, d'éradication et de récupération appropriées. L'identification des hôtes infectés est souvent compliquée par la nature dynamique des logiciels malveillants.
- Les organisations doivent examiner attentivement les problèmes d'identification des hôtes avant qu'un incident malveillant à grande échelle ne se produise afin qu'elles soient prêtes à utiliser plusieurs stratégies pour identifier les hôtes infectés dans le cadre de leurs efforts de confinement.
- Les organisations doivent sélectionner une gamme suffisamment large d'approches d'identification et doivent développer des procédures et des capacités techniques pour appliquer efficacement chaque approche sélectionnée lorsqu'un incident majeur de logiciel malveillant se produit.
- Étudier le comportement des logiciels malveillants en les analysant de façon dynamique (exécution du logiciel malveillant dans le cas de dissimilation de la charge virale, Débogage) ou de manière statique (désassemblage, décompilation, Analyse statique du code).
- Identifier les indicateurs de compromission issues de l'analyse statique et dynamique pour le scaling de la détection et préparation de la prochaine phase d'endiguement.

3. Endiguement

L'endiguement des incidents de logiciels malveillants comporte deux éléments principaux : arrêter la propagation des logiciels malveillants et empêcher d'autres dommages aux hôtes. Presque tous les incidents de logiciels malveillants nécessitent des actions de confinement. Lors de la gestion d'un incident, il est important pour une organisation de décider quelles méthodes d'endiguement à utiliser initialement, au début de l'intervention. Les organisations doivent avoir des stratégies et des procédures en place pour prendre des décisions liées à l'endiguement qui reflètent le niveau de risque acceptable pour l'organisation. Les stratégies d'endiguement doivent aider les gestionnaires d'incidents à sélectionner la combinaison appropriée de méthodes d'endiguement en fonction des caractéristiques d'une situation particulière. Les recommandations spécifiques liées à cette étape incluent ce qui suit :

- Il peut être utile de fournir aux utilisateurs des instructions sur la manière d'identifier les infections et sur les mesures à prendre si un hôte est infecté ; cependant, les organisations ne doivent pas compter principalement sur les utilisateurs pour contenir les incidents de logiciels malveillants.
- Si un logiciel malveillant ne peut pas être identifié et contenu par un logiciel antivirus mis à jour, les organisations doivent être prêtes à utiliser d'autres outils de sécurité pour le contenir. Les organisations doivent également être prêtes à soumettre des copies de logiciels malveillants inconnus à leurs fournisseurs de logiciels de sécurité pour analyse, ainsi qu'à contacter des parties de confiance telles que des organisations de réponse aux incidents et des fournisseurs d'antivirus lorsque des conseils sont nécessaires sur la gestion de nouvelles menaces.

- Les organisations doivent être prêtes à fermer ou à bloquer les services utilisés par les logiciels malveillants pour contenir un incident et doivent comprendre les conséquences d'une telle décision. Les organisations doivent également être prêtes à répondre aux problèmes causés par d'autres organisations désactivant leurs propres services en réponse à un incident de logiciel malveillant.
- Les organisations doivent être prêtes à imposer des restrictions temporaires supplémentaires sur la connectivité réseau pour contenir un incident de logiciel malveillant, comme la suspension de l'accès à Internet ou la déconnexion physique des hôtes des réseaux, en reconnaissant l'impact que les restrictions pourraient avoir sur les fonctions organisationnelles.

4. Eradication

L'objectif principal de l'éradication est de supprimer les logiciels malveillants des hôtes infectés. En raison du besoin potentiel d'efforts d'éradication importants, les organisations doivent être prêtes à utiliser simultanément diverses combinaisons de techniques d'éradication pour différentes situations. Les organisations devraient également envisager de mener des activités de sensibilisation qui définissent les attentes en matière d'efforts d'éradication et de rétablissement ; ces activités peuvent être utiles pour réduire le stress que les incidents majeurs de logiciels malveillants peuvent causer.

5. Récupération

Les deux principaux aspects de cette étape sont la restauration des fonctionnalités et des données des hôtes infectés et la suppression des mesures d'endiguement temporaires. Les organisations doivent examiner attentivement les pires scénarios possibles et déterminer comment la récupération doit être effectuée, y compris la reconstruction des hôtes compromis à partir de zéro ou de bonnes sauvegardes connues. Déterminer quand supprimer les mesures d'endiguement temporaires, telles que la suspension des services ou de la connectivité, est souvent une décision difficile lors d'incidents de logiciels malveillants majeurs. Les équipes d'intervention en cas d'incident doivent s'efforcer de maintenir les mesures d'endiguement en place jusqu'à ce que le nombre estimé d'hôtes infectés et d'hôtes vulnérables à l'infection soit suffisamment faible pour que les incidents ultérieurs aient peu de conséquences. Cependant, même si l'équipe d'intervention en cas d'incident doit évaluer les risques de restauration des services ou de la connectivité, la direction devrait en fin de compte être responsable de déterminer ce qui doit être fait en fonction des recommandations de l'équipe d'intervention en cas d'incident et de la compréhension de la direction de l'impact du maintien des mesures de l'endiguement.

6. Leçons apprises

Étant donné que la gestion des incidents de logiciels malveillants peut être extrêmement coûteuse, il est particulièrement important pour les organisations de procéder à une évaluation solide des leçons apprises après des incidents de logiciels malveillants majeurs afin d'éviter que des incidents similaires ne se produisent. La capture des leçons tirées de la gestion de tels incidents devrait aider une organisation à améliorer sa capacité de gestion des incidents et ses défenses contre les logiciels malveillants, y compris l'identification des changements nécessaires à la politique de sécurité, aux configurations logicielles et aux déploiements de logiciels de détection et de prévention des logiciels malveillants.

10. Annexe J : Gestion d'incident de déni de service

Les attaques de déni de service (Denial of Service -DOS) ont pour but de perturber ou dégrader les services en ligne d'une entité. Pour atteindre cet objectif les attaquants peuvent :

- exploiter des failles de sécurité au niveau des composants du SI (réseau, système, applications, …) en exécutant des requêtes à distance de leurs propres machines.
- contrôler plusieurs hôtes sur un ou plusieurs réseaux (botnets), sans que les victimes en soient informées, pour lancer des requêtes automatisées ciblant les services en ligne tels que les DNS (Domain Name Services), les sites Web et les courriels. Il s'agit dans ce cas d'un déni de service distribué (DDOS).

Bien que ces attaques soient très difficiles à empêcher, il existe des stratégies qui peuvent aider à minimiser leur impact sur l'infrastructure ciblée. Ces stratégies doivent être prises en compte par les entités dans leurs processus d'évaluation des risques.

Planification et préparation

La planification et la réponse efficaces sont les meilleures mesures préventives contre les attaques de déni de service. Le temps consacré à la planification et à la préparation va permettre de réagir en temps opportun et d'annuler les effets voulus de l'attaque pour maintenir à un niveau opérationnel acceptable les services critiques.

Lors de la planification et la préparation, il est recommandé de prendre en considération les mesures suivantes :

- ✓ Il faut augmenter la résilience du réseau de l'entité contre les activités DDoS en mettant en œuvre au moins deux liens Internet appartenant à deux FAI (Fournisseur d'Accès Internet) différents. Cela assure au réseau la redondance des connexions pour atténuer l'impact de l'attaque.
- ✓ Envisager le déploiement des serveurs DNS et des serveurs Web supplémentaires sur le réseau pour équilibrer la charge résultante des requêtes entrantes, ou préparer des serveurs de secours en ligne de réserve pour les services critiques. Cela peut inclure plusieurs serveurs DNS et Web ou des serveurs virtuels qui peuvent être mis en ligne rapidement lors d'une attaque.
- ✓ Dimensionner les ressources système de la plateforme de l'application web pour qu'elle puisse fonctionner, en temps normal, à 60% de ses capacités.
- ✓ S'assurer que le fournisseur d'accès à internet (FAI) dispose d'une connexion réseau à Internet avec une bande passante suffisante au-dessus des exigences de l'entité.
- ✓ Assurer que le contrat avec l'opérateur :
  - Inclut la flexibilité d'augmenter temporairement la bande passante de la connexion de l'entité à Internet ;

- Contient un accord de niveau de service acceptable qui répond aux besoins du bon fonctionnement des services en ligne ;
- Indique clairement quels sont les processus et les changements réseaux que l'opérateur doit mettre en place pour surmonter une attaque DDoS.

✓ Concevoir un processus pour hiérarchiser les services fournis aux clients de l'entité et identifier les clients primaires légitimes (par exemple, prioriser les requêtes des adresses nationales par rapport aux demandes internationales).

✓ Segmenter le réseau afin que les services en ligne sortent par des connexions réseaux différentes. Par exemple, les transactions commerciales emprunteront une connexion réseau distincte du réseau de serveurs Web publique. L'utilisation d'une seule connexion réseau pour transporter tout le trafic des services critiques (accès à distance, le courrier électronique, l'hébergement Web…) augmentera la probabilité d'un arrêt total des communications au cours d'une attaque DoS.

✓ Etablir des contrats avec des fournisseurs spécialisés de proxy en ligne qui disposent de grandes bande-passantes et qui offrent une protection contre ces attaques en filtrant le trafic avant de le rediriger vers l'entité. Cela fournit un niveau de résilience et une flexibilité pour bloquer le trafic avec un contenu spécifique que les fournisseurs d'accès à Internet peuvent ne pas détecter tout en gardant les applications et les données de l'entité en interne.

✓ Planifier des tests réguliers de la capacité de l'infrastructure réseau à gérer les requêtes avant qu'elle soit au-dessous des niveaux acceptables (teste de monter en charge).

✓ Elaborer un plan d'intervention contenant des actions précises à suivre en cas d'une attaque DOS en respectant les recommandations ci-dessus.

Réaction aux attaques DOS

✓ Déterminer si l'attaque DOS vise à surcharger la bande-passante du réseau ou les ressources des serveurs. Les exemples présentés ci-dessous ne sont pas exhaustifs mais décrivent le principe d'une attaque DoS et l'importance de déterminer la ressource réseau ciblée :

❖ La bande-passante :

- L'envoie d'une grande quantité de requêtes est une méthode simple mais efficace qui consomme la bande passante disponible et ralentit le traitement des demandes légitimes.
- L'envoi de grands volumes de trafic réseau nécessitant une réponse vers un serveur consomme également la bande passante disponible.

❖ Les ressources serveur :

- L'initiation de multiples tentatives d'ouverture de sessions cryptées SSL ciblent les processeurs du serveur (CPUs) pour ralentir de nombreuses tâches critiques, dans le but de bloquer ou de crasher le serveur

- Les requêtes qui établissent et conservent des sessions Web ouvertes sur un serveur sont conçues pour consommer le nombre maximal de connexions simultanées que le serveur peut maintenir ce qui empêche les autres utilisateurs d'accéder au site.
- L'envoi de plusieurs emails ciblant le serveur de messagerie avec des pièces jointes malicieuses entraîne l'utilisation intensive du processeur et la saturation de l'espace disque du serveur de messagerie.
- La saturation du serveur de noms de domaine par les requêtes DNS empêchera les utilisateurs légitimes de résoudre les adresses IP requises pour accéder aux services en ligne de l'entité.

✓ Comprendre indispensablement, lorsque la ressource ciblée est identifiée, la technique de l'attaque afin d'envisager les plans de remédiation appropriés pour cet incident :

- ❖ Dans le cas des attaques ciblant les serveurs DNS, l'augmentation de la valeur TTL (Time To Live) des enregistrements DNS et le contrôle de la quantité de bande passante réseau allouée au trafic DNS pourrait permettre aux visiteurs légitimes de continuer à accéder au site Web.
- ❖ Si une attaque cible une adresse IP de l'entité, la diminution de la valeur TTL des enregistrements DNS permettra de déplacer le serveur web vers une autre adresse IP afin de permettre aux visiteurs légitimes d'accéder pendant que l'attaquant continue de cibler l'adresse IP qui n'est plus utilisée.

✓ Analyser le trafic réseau afin de définir les signatures qui permettent d'identifier le trafic indésirable. L'utilisation de cette technique en combinaison avec une liste préétablie de clients légitimes, rend l'indentification du trafic indésirable plus efficace. Par exemple, si le trafic d'attaque tente de saturer les ressources des serveurs Web, il devient nécessaire de bloquer les requêtes répétitives sur le même contenu à partir d'une seule adresse IP.

✓ Demander aux opérateurs de bloquer toute adresse IP responsable d'un trafic suspect. Le fournisseur d'accès à Internet peut empêcher le trafic source de l'attaque DOS d'atteindre le réseau de l'entité et ainsi de réduire le risque de consommation des ressources disponibles.

11. Annexe K : Recommandations aux entités lors de l'externalisation du service de réponse à incident

Dans le cas d'externalisation du service de réponse à incident, l'entité doit veiller à respecter les recommandations ci-après :

- Choisir le prestataire dans le catalogue des prestataires qualifiés publié sur le site de la DGSSI.
- Demander au prestataire de lui transmettre son attestation de qualification. Cette attestation identifie notamment les activités pour lesquelles le prestataire est qualifié et la date de validité de la qualification.
- Identifier le type de prestation RIS adaptée à son besoin.
- Demander au prestataire de lui transmettre les attestations individuelles de compétence de chaque analyste intervenant dans le cadre de la prestation.
- Du fait de l'importance d'une intervention rapide du prestataire en cas d'incident de sécurité, il est recommandé que le commanditaire établisse une convention avec le prestataire en amont de toute prestation afin que le prestataire ne soit pas ralenti dans la réponse à incident par l'étape d'établissement de la convention.
- Le prestataire doit signer un accord de non-divulgation avec l'entité afin d'assurer la confidentialité des informations que ce dernier lui transmet. Cet accord doit être signé par un représentant légal du commanditaire et du prestataire.
- Le prestataire peut, dans certains cas d'urgence et avec l'accord de l'entité, réaliser les phases de compréhension de l'incident de sécurité et de son environnement en l'absence de convention, sur la base d'un accord de non-divulgation signé par le prestataire et le commanditaire et à la condition que le prestataire n'intervienne pas sur le système d'information cible.
- La prestation ne doit débuter qu'après une réunion formelle d'ouverture au cours de laquelle les représentants habilités du prestataire et ceux de l'entité confirment leur accord sur l'ensemble des modalités de la prestation.
- Le commanditaire peut déposer auprès de la DGSSI une réclamation contre un prestataire qualifié pour lequel il estime que ce dernier n'a pas respecté une ou plusieurs exigences du présent référentiel ou de la convention. S'il s'avère après instruction de la réclamation que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, et selon la gravité, la qualification du prestataire peut être suspendue retirée ou sa portée de qualification réduite.
- Une prestation d'investigation numérique sur large périmètre, par sa nature imprévisible et non-planifiable, est une démarche itérative nécessitant une révision régulière de la posture à adopter et par conséquent des moyens associés (ressources humaines, budget, disponibilités, etc.). La durée de la prestation peut être révisée dans le temps en fonction

de la compréhension de l'incident de sécurité et de son environnement et peut durer ainsi plusieurs semaines, voire plusieurs mois.

- Il est recommandé de désigner en sein de l'entité un référent de confiance chargé de la gestion des relations avec le prestataire et des modalités de réalisation des activités d'analyse (horaires des interventions, autorisations, etc.).
- Il est recommandé que l'entité prenne les mesures de sauvegarde nécessaires à la protection de son système d'information et des données associées préalablement et au cours de la prestation. Cette démarche doit être réalisée en collaboration avec le prestataire afin de ne pas gêner les activités d'analyse, notamment les équipes informatiques de l'entité ne doivent pas porter atteinte à l'intégrité des traces d'activités malveillantes.
- Il est recommandé que l'entité mette en place une structure projet capable de définir les objectifs, le dispositif et le cadre de la prestation. Elle doit en assurer le suivi et réaliser les arbitrages associés. Cette structure doit avoir le bon niveau de décision. Il est recommandé que l'entité mette en place avec le prestataire une chaîne de décision courte et simplifiée des processus nécessaires au bon déroulement de la prestation, en particulier un comité stratégique et un processus d'achat rapide pour répondre aux besoins immédiats. Les contacts techniques utiles pour la bonne réalisation de la prestation doivent être communiqués au prestataire.
- Il est recommandé que l'entité mette en place une cellule pour gérer une éventuelle crise induite par l'incident de sécurité et que le prestataire soit intégré à cette cellule.
- Il est recommandé que l'entité définisse un plan de communication associé au traitement de l'incident de sécurité. Il doit définir les exigences que doit respecter le prestataire dans le cas où l'incident est divulgué au personnel de l'entité concernée ou au grand public. Il est notamment précisé le niveau de confidentialité à adopter par le prestataire vis-à-vis de l'incident de sécurité (communication aux exploitants, aux sous-traitants, etc.).
- Il est recommandé, afin d'éviter toute dénonciation de vol ou d'abus de confiance, que l'entité évite de remettre au prestataire des matériels dont il n'est pas le titulaire mais tout de même utilisés à des fins professionnelles (BYOD17) en l'absence du titulaire du matériel ou sans son accord explicite.
- Il est recommandé que l'entité trace toutes les modifications qu'il effectue sur le système d'information cible durant la prestation afin de pouvoir identifier les actions illégitimes sur le réseau pendant la prestation.
- Il est recommandé que l'entité informe le prestataire, tout au long de la prestation, des actions qu'elle réalise sur le système d'information cible (opérations d'administration, sauvegardes, etc.) et qui pourraient affecter la prestation.

- Il est recommandé que l'entité mette à disposition du prestataire une zone sécurisée et dédiée pour le stockage d'éléments sensibles (coffre-fort, salle surveillée, etc.). Cette zone doit respecter les contraintes réglementaires associées au niveau de sensibilité ou de classification des données stockées.
- Il est recommandé que l'entité mette à disposition du prestataire les moyens techniques (ex : équipements réseau, connexion Internet, etc.) dont il a besoin pour sa prestation, et que ces moyens constituent un environnement d'analyse sécurisé et déconnecté du système d'information cible.
- Il est recommandé que l'entité mette en œuvre des moyens de communication sécurisés et dédiés pour tous les échanges en rapport avec l'incident de sécurité, en interne et avec le prestataire. Il est recommandé que ces moyens soient déconnectés du système d'information compromis afin de ne pas permettre à l'attaquant de suivre les opérations en cours.
- Il est recommandé que le commanditaire ait la capacité à révoquer un analyste.

Références

- ISO/IEC 27035: Information technology – Security techniques – Information Security incident management.
- ISO/IEC 27035- 1: Principales of Incident Management.
- ISO/IEC 27035- 2: Guidelines to plan and prepare for incident response.
- ISO/IEC 27035- 3: Guidelines for incident response operations.
- Publication spéciale de NIST 800-61r2: Incident handling guide.
- Publication spéciale de l'ENISA: Good Practice Guide for Incident Management.