Messaging, Malware and Mobile Anti-Abuse Working Group

Recommandations du groupe de travail M³AAWG en cas d'attaque par ransomware

Mai 2023

L'URL de référence de ce document est la suivante :
https://www.m3aawg.org/ransomware_bcp_2023_fr

Table des matières

Table des illustrations

T**ermes, définitions, abréviations et acronymes**

Ce document utilise les abréviations suivantes.

ARRA	Plan de relance économique des États-Unis de 2009 (American Recovery and Reinvestment Act)
BC/DR	Continuité des opérations (Business Continuity - BC) et reprise après incident (Disaster Recovery - DC)
C&C	Commande et contrôle
CCPA	Loi californienne sur la protection de la vie privée (California Consumer Privacy Act)
CISA	Agence de cybersécurité et de sécurité des infrastructures (Cybersecurity & Infrastructure Security Agency) - division du DHS, États-Unis
RSSI, Chief Officers, etc.	Voir la section 2.6 « Collaborateurs »
COPPA	Children's Online Privacy Protection Act (États-Unis)
CPRA	California Privacy Rights Act
DFIR	Investigation numérique et réponse aux incidents (Digital Forensics and Incident Response)
DHS	Département de la Sécurité intérieure des États-Unis (Department of Homeland Security)
FBI	Federal Bureau of Investigation (États-Unis)
RGPD	Règlement général sur la protection des données (UE)
HIPAA	Health Insurance Portability and Accountability Act (États-Unis)
GIA	Gestion des identités et des accès
IDS	Système de détection d'intrusion
IPS	Système de prévention d'intrusion
Adresse MAC	Adresse de contrôle d'accès au support (identifiant normalement unique)

LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques (Canada)
SOC	Centre des opérations de sécurité (SOC)
TCPA	Telephone Consumer Protection Act (États-Unis)

1 Portée du document

1.1 Présentation et vue d'ensemble

Le ransomware est un type de malware, ou logiciel malveillant, introduit par des hackers sur une plateforme, par exemple votre ordinateur, un serveur d'entreprise, des baies de stockage des données, des fichiers système ou encore d'autres supports vulnérables. Le ransomware prend en otage des ressources telles que des fichiers, services, sauvegardes, journaux, bases de données et autres outils, en vue d'extorquer une rançon à ceux qui exploitent ces ressources.[1] Si la restriction de l'accès passe le plus souvent par le chiffrement des fichiers, les techniques varient selon les intentions des malfaiteurs : exfiltration (vol) des fichiers, suppression ou encore défacement (altération de données originales). Dans la plupart des cas, les attaquants communiquent leurs instructions de paiement sur le site de l'attaque : rédigées sous forme de notes de bureau, envoyées à l'imprimante ou carrément affichées sur le fond d'écran modifié. Notez que vous pourriez être contacté par d'autres moyens. Chaque fois, la promesse est simple : en échange d'une rançon, ces derniers fourniront la clé et restaureront le système. Hélas, les choses se déroulent rarement ainsi.

Le ransomware est devenu une pratique répandue, d'autant plus courante qu'elle est relativement simple à employer pour les hackers, même novices.[2] Chez les victimes, c'est l'incompréhension : comment en sont-elles arrivées là, et pourquoi ? Bien loin de mener une croisade personnelle, les malfaiteurs agissent avant tout par appât du gain[3] [4], et les malheureuses victimes ont simplement commis l'erreur de laisser dans leur système une vulnérabilité exploitable. Mais tous les attaquants ne partagent pas les mêmes motivations : il se peut qu'ils s'intéressent aux fichiers en eux-mêmes, qu'ils pratiquent l'espionnage industriel ou qu'ils tentent d'interrompre un service.[5] Il arrive qu'ils tiennent leur promesse et restituent les données une fois la rançon versée[6,7]. De leur côté, les victimes peuvent être plus ou moins contraintes (signalement, interdiction de payer la rançon, intervention de la police) selon leur juridiction ou la nature des données compromises. C'est notamment le cas des données de santé aux États-Unis, dont la compromission entraîne une obligation de notification lorsque la victime compromise fait partie des catégories « Covered Entity » ou « Business Associate ».

1.2 Objectif du document

Ce document passe en revue vos options lorsque vous êtes victime d'une attaque. Il vous explique comment évaluer les risques et les solutions de reprise et de continuité des opérations, et comment gérer la situation.

Ce document s'adresse en priorité à l'équipe informatique en interne, tout particulièrement les RSSI (responsables de la sécurité des systèmes d'information) et CPO (Chief Privacy Officers) en poste au sein

[1] https://www.cisecurity.org/insights/spotlight/election-security-spotlight-ransomware-attacks
[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
[3] Dans l'Union européenne, on estime à 10,1 Mds€ les sommes rançonnées au cours de l'année 2019, soit 3,3 Mds€ de plus que l'année précédente. La même année, les détections ont bondi de 365 %, et 66 % des organismes de santé ont été la cible d'une attaque par ransomware. Source : https://www.enisa.europa.eu/publications/ransomware.
[4] Sophos, Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year. Sophos, 27 avril 2021, https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.
[5] https://www.cisa.gov/stopransomware/ransomware-reference-materials-students
[6] https://www.nomoreransom.org/
[7] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

des petites et moyennes entreprises. La plupart des recommandations s'appliquent également à des entreprises plus grandes, bien qu'elles puissent présenter une structure organisationnelle différente. Les premiers acteurs de la reprise des activités après une attaque par ransomware sont listés dans la section 2.6 « Collaborateurs ».

Ce document a pour objet de vous offrir un parcours de reprise simplifié suite à une attaque par ransomware. Il vous aidera à prendre en compte les différentes options et vous éclairera sur les acteurs à solliciter à chaque étape, comme les services de police, la direction de l'entreprise, l'assurance, les équipes juridiques, etc. Nous aborderons également les outils recommandés, les options de récupération, les probabilités de déchiffrement, la conformité réglementaire et bien plus. L'objectif n'est PAS de proposer une approche universelle face aux attaques par ransomware, ni de vous apporter une méthode de résolution à chaque moment décisif. De fait, ces paramètres varient en fonction des organisations et dépendent d'un contexte qui vous est propre.

Les ransomwares, cela n'arrive pas qu'aux autres, et les victimes le comprennent souvent trop tard. Si vous pensez avoir été victime d'une attaque et que votre priorité est de réagir au plus vite, rendez-vous directement à la section « Attaque par ransomware : réponse de première intention ». Cette section vous offre de l'aide si vous êtes, ou avez été récemment, victime d'une attaque. Elle vous fournit un guide des décisions à prendre au cours d'une attaque et en détaille les aspects les plus urgents.

Si vous avez besoin d'aide pour **vous préparer face à la menace des ransomwares** ou pour **finaliser votre reprise d'activité**, vous trouverez des ressources externes dans la section 2.8 « Après l'incident ».

2. Attaque par ransomware : réponse de première intention

Notre conseil

Lisez d'abord ce document dans son intégralité.

Vous pensez peut-être ne pas avoir le temps, mais il est important d'anticiper et de comprendre toutes les étapes qui vous attendent. N'oubliez pas que votre situation est unique. Les évènements ne se présenteront pas forcément dans l'ordre indiqué ici : certains collaborateurs seront indisponibles, certaines décisions s'avéreront inutiles, d'autres devront être prises plus tôt que prévu, d'autres encore ne figurent pas dans ce document. **Consignez tout à partir de maintenant.**

2.1 Runbook

Face à une attaque par ransomware, orchestrez votre réponse par étapes. Considérez ce processus comme une checklist, et cochez les cases au fur et à mesure. Chaque étape impliquera des postes différents. Vous trouverez des informations ainsi que la disponibilité éventuelle de ces postes dans les sections 2.6.1 « Ressources en interne » et 2.6.2 « Ressources et services externes ».

Notre conseil Prenez un nouveau carnet, ouvrez une application de prise de notes ou bien créez un espace dédié à vos recherches et à votre documentation au fil de cette activité. Si vous ne disposez pas encore d'une copie physique hors ligne de ce document, c'est le bon moment de la créer.

Notre conseil **N'ÉTEIGNEZ PAS LES MACHINES QUE VOUS PENSEZ COMPROMISES.**

Il est tentant d'éteindre une machine en cas de suspicion de compromission, mais vous auriez tort de le faire. Nous vous expliquons pourquoi dans la suite.

Conseil ***DÉCONNECTEZ*** **LES MACHINES COMPROMISES DU RÉSEAU. Si elles sont reliées à un câble Ethernet, débranchez simplement ce câble**. Toute connexion directe au réseau d'une machine compromise doit être coupée.

Notre conseil Il est possible que les machines infectées soient connectées au Wi-Fi, voire à plusieurs points d'accès ou amplificateurs. À ce stade, il est bon de rappeler que vous n'avez peut-être pas identifié toutes les machines infectées. Votre premier réflexe pourrait alors être de débrancher les routeurs Wi-Fi ou de créer un nouveau mot de passe pour votre réseau (SSID). **Ne faites pas ça.** Cette action pourrait mettre hors service des dispositifs connectés à votre système et indispensables à vos activités, votre sécurité ou votre sûreté (par exemple : un DNS, des pompes à insulines, des alarmes système). **Optez plutôt pour la segmentation du réseau, la mise en quarantaine des appareils et l'activation du filtrage par adresse MAC afin de mettre en place des listes d'autorisation et de blocage en vue de gérer les connexions au réseau**. Identifiez chaque accès depuis l'extérieur à votre réseau, les systèmes dotés d'une connectivité cellulaire, les routeurs connectés au même réseau, etc.

Notre conseil Isolez et/ou inspectez le système d'authentification et d'autorisation de l'entreprise (par exemple, Active Directory). Ces systèmes sont bien souvent la première cible d'infiltration et peuvent servir à atteindre le réseau après ou pendant la phase de reprise.

Notre conseil Priorisez la protection de vos systèmes de sauvegarde ou l'accès à ces systèmes. Cette action est déterminante pour la suite des opérations : vous devez isoler puis confirmer l'intégrité des sauvegardes.

Moment décisif [8]À ce stade, vous faites face à un dilemme très concret : souhaitez-vous faire appel à votre compagnie d'assurance, et quand ? Consultez la section 2.5.1 « Faire intervenir votre assurance cybersécurité et l'équipe de réponse aux incidents ».

Notre conseil Vous n'en êtes qu'au tout début du processus. Ne précipitez pas les choses.

8

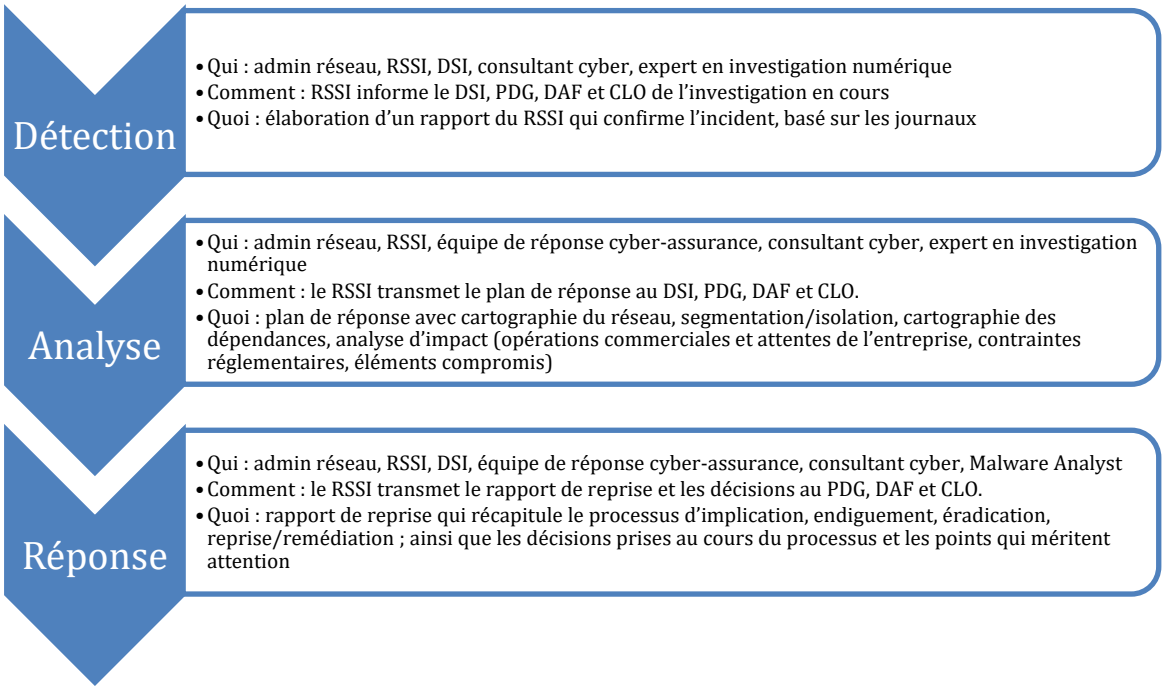

Schéma 1 : Vue d'ensemble du processus

2.2 Détection

Par qui ?

- Administrateur réseau
- Responsable de la sécurité des systèmes d'information (RSSI)
- Directeur des systèmes d'information (DSI)
- Consultant en cybersécurité (voir la section 2.6.2 « Ressources et services externes »)
- Expertise en investigation numérique (voir la section 2.6.2, « Ressources et services externes »)

Comment : le RSSI informe les postes suivants qu'une investigation est en cours :

- DSI
- PDG
- Directeur administratif et financier (DAF)
- Directeur juridique (CLO)

Les signes d'une attaque par ransomware

Il s'agit de la première étape de la réponse aux incidents. Avant tout, vérifiez qu'un incident s'est bien produit et déterminez le type d'attaque. Les attaques par ransomware présentent généralement des signes distincts.

- Les fichiers sont renommés avec de nouvelles extensions.
- Les fichiers .doc ou .docx présentent des noms inhabituels.
- Les fichiers sont inaccessibles ou illisibles.
- Le système peut se montrer instable ou bien crasher à cause du chiffrement de fichiers critiques.
- Les sites web peuvent être défacés ou altérés. Cette action peut constituer aussi bien un signe de l'attaque que l'attaque en elle-même. Analysez les zones compromises et la conduite à adopter.
- La note de rançon a peut-être été envoyée sur une imprimante du système.
- Les attaquants ont peut-être fait parler d'eux sur d'autres canaux (par exemple dans la presse ou sur les réseaux sociaux).

Il faut aussi envisager le coup de bluff : les victimes sont notifiées, souvent par voie électronique (SMS, e-mail, etc.), mais ne sont pas réellement victimes d'une intrusion dans leur système. Le but ici est de vous pousser à agir dans l'urgence.

Assurez-vous que les systèmes fonctionnent, qu'ils sont accessibles et que vos défenses sont intactes.

- Utilisez des outils capables de scanner les fichiers malveillants ou activités suspectes.
- Consultez les enregistrements des journaux.
- Confirmez toute modification des autorisations.
- Examinez toutes les tentatives d'authentification.

Vous confirmez avoir été victime d'une attaque : pouvez-vous identifier les systèmes touchés et ceux qui sont intacts ?

Après l'identification, il est temps de passer à l'étape suivante.

Si vous ne pensez pas avoir été victime ou que vous n'avez pas de certitude, reportez-vous à la section 2.4 « Réponse », pour connaître le reste des activités à examiner. Ne relâchez pas votre vigilance : il est possible qu'un acteur malveillant ait toujours accès à une partie de vos systèmes ou réseaux, et que vous deviez réactualiser ou renforcer vos défenses.

Vous devez vous préparer à répondre à l'objectif (voir ci-dessous) de cette étape : comment votre organisation compte-t-elle répondre ? Qui prend les décisions ? Quelle est la marche à suivre ? Qui interagira avec les systèmes ? Et comment allez-vous procéder ?

Objectif Le RSSI partage ensuite les résultats de l'activité de détection, notamment :

- sa portée initiale ;
- les systèmes touchés ; et
- une communication claire à propos des prochaines étapes (voir la section « Analyse » ci-dessous).

Le RSSI doit informer les acteurs concernés de ce qui suit :

- les opérations commerciales sont susceptibles d'être interrompues ;
- cette activité malveillante appelle à des décisions ; et
- d'autres ressources d'assistance pourraient s'avérer nécessaires.

Informez calmement vos collaborateurs de la mise en place d'un plan et d'une stratégie à suivre pour assurer la priorisation des ressources au fil du processus. Il n'est pas rare qu'un tel incident suscite des réactions diverses, il est donc recommandé de se rapprocher du DRH pour étudier les possibilités de suivi des collaborateurs.

2.3 Analyse

Par qui ?

- Administrateur réseau
- RSSI
- DSI
- CLO
- Équipe de réponse aux incidents de votre assurance cybersécurité (voir la section 2.6.2 « Ressources et services externes »)
- Consultant en cybersécurité (voir la section 2.6.2 « Ressources et services externes »)
- Expertise en investigation numérique (voir la section 2.6.2 « Ressources et services externes »)
- Éventuellement, juriste externe (voir la section 2.6.2 « Ressources et services externes »)

Comment : le RSSI partage le plan de réponse avec les postes suivants :

- DSI

- PDG
- DAF

Une fois l'attaque confirmée, votre organisation doit impérativement préciser les contours de la menace pour comprendre ce à quoi elle fait face. Cette activité s'étend aux :

- systèmes touchés ;
- limites des données ;
- utilisateurs concernés ;
- projets/produits/services touchés ;
- éléments destinés au client ; et
- éléments destinés au public.

Vous devez évaluer l'étendue de vos capacités face au type de compromission. Les attaquants ont-ils pu accéder à des données non chiffrées ? Les attaquants ont-ils réussi à modifier des données ? Votre organisation est-elle en mesure de déterminer si des données ont été modifiées ?

Tâchez d'identifier le type de malware utilisé, la façon dont le réseau a été compromis et les systèmes qui y sont reliés. Veillez à consigner toutes les vulnérabilités découvertes au cours de ce processus. L'aide d'un Malware Analyst (voir la section 2.6.2 « Ressources et services externes ») peut s'avérer utile à ce stade.

Notre conseil Au cours de ce processus, CONSIGNEZ TOUTES VOS NOTES dans le carnet (ou support) mentionné au début de cette section.

Notre conseil Réservez une section de votre carnet aux informations descriptives à propos du malware. Posez-vous les questions suivantes :

- Les fichiers sont-ils toujours utilisables ?
- Devez-vous répondre dans un délai imparti ?
- Quelles sont les exigences des malfaiteurs ?
- Avez-vous affaire à une menace unique ou à plusieurs acteurs/exigences ?
- Avec quelle facilité l'entreprise peut-elle changer sa méthode de génération des revenus et de gestion des activités ?

Notre conseil Pour évaluer la portée de l'attaque, réunissez les informations suivantes et procédez à une évaluation systématique :

- cartographiez le réseau ;
- identifiez les points de connexion/points de routage ;
- cartographiez les segmentations en interne.

- Identifiez les protections que vous offre la segmentation et préparez-vous à les activer.

Donnez la priorité à ce qui suit :

- opérations critiques ;
- sécurité du réseau ;
- stockage des données sensibles ;
- fichiers personnels ;
- systèmes liés à la fonction financière.

Notre conseil

- Mettez à jour votre logiciel anti-malware/antivirus et scannez toutes les machines à la recherche du malware, y compris les machines qui ne présentent pas d'activité suspecte.
- Déterminez le type de malware ou ransomware trouvé.
- Consultez les descriptions en ligne de ce malware en particulier afin de connaître ses effets et ses cibles.
- Dressez une liste des machines connues infectées.

Notre conseil Procédez avec l'aide d'un consultant en cybersécurité, de l'équipe de réponse aux incidents de votre assurance cybersécurité et d'un expert de l'investigation numérique.

- Exécutez l'analyse et la capture des journaux et commencez l'investigation numérique des machines infectées.
- Planifiez de façon optimale la segmentation et l'isolation des systèmes.

Pensez à examiner les journaux pour trouver des systèmes de détection d'intrusion (IDS) ou des systèmes de prévention d'intrusion (IPS), des pare-feu, périmètres ou autres systèmes de défense en interne. Même s'ils ne paraissent pas touchés par l'attaque, ils peuvent vous aider à identifier d'autres systèmes compromis.

Notre conseil Avec l'aide du directeur juridique, et au besoin d'un juriste externe :

- déterminez les obligations de notification prévues par la législation locale, régionale ou nationale ;
- déterminez les contraintes de temps, les attentes en matière de contenu et les parties prenantes de ces informations.

Le directeur juridique doit communiquer ces informations avec les autres cadres et gérer les échanges avec le CMO.

Les actions de notification interviennent généralement dans la partie « Réponse », ci-dessous, mais la chronologie des évènements peuvent vous obliger à anticiper.

Ce qu'il faut retenir de cette étape est la nécessité de mettre en place un plan de réponse comprenant les éléments suivants. (REMARQUE : certains de ces documents existent peut-être déjà, et peuvent vous servir de point de départ.)

1. Une cartographie du réseau mettant en évidence les systèmes infectés, les limites déjà en place et celles nouvellement définies en amont des activités de réponse.

2. Un plan de segmentation et d'isolation pour les systèmes infectés.

3. Une cartographie des dépendances entre les systèmes. Les bases de données, par exemple, peuvent être utilisées par différents systèmes. Un manque d'intégrité et de cohérence entre les bases de données, par exemple avec la restauration de l'une d'entre elles, mais pas des autres, peut entraîner des erreurs d'application ou d'accès.

4. Une évaluation de l'impact sur les opérations commerciales et un récapitulatif des attentes pour l'entreprise. Cette évaluation indique également le type de données compromises (ou menacées de compromission) : transactions commerciales, données financières, informations confidentielles, données médicales, registres du personnel et autres données protégées. Des exigences réglementaires s'appliquent-elles en cas de compromission de ce type de données ? Auquel cas, êtes-vous dans l'obligation de notifier l'incident ? Ces exigences incluent, sans pour autant s'y limiter, les lois suivantes : HIPAA, COPPA, TCPA, RGPD, CCPA, CPRA et LPRPDE.

5. Le service juridique pourrait avoir d'autres attentes et questions concernant la responsabilité légale, les rapports de solvabilité et les autres exigences réglementaires. Tout ceci dépend principalement de la nature de vos activités.

6. Un plan de sauvegarde/restauration pour chaque système mis en évidence ou système dépendant.

Le plan de réponse doit être passé en revue par l'équipe d'analyse pour confirmer son exhaustivité et son exactitude avant d'être partagé par le RSSI.

Moment décisif Le RSSI partagera le plan de réponse avec le reste de l'équipe. L'entreprise s'appuiera sur le plan de réponse pour déterminer la nécessité ou non de faire appel aux services de police, ainsi que la portée de cette implication (si toutefois il est possible de la contrôler). Veuillez consulter la section 2.5.2 « Quand faire appel aux services de police ».

La prochaine étape consiste à se prémunir de dégâts ou d'intrusions supplémentaires.

2.4 Réponse

La phase de réponse se divise elle-même en quatre phases successives : implication, endiguement, éradication et reprise/remédiation.

Notre conseil Au cours de la phase d'analyse qui précède, vous avez identifié les protections que vous offre la segmentation de votre réseau. Activez-les conformément au plan. C'est au cours de la phase de réponse que l'équipe entreprendra la première action concrète sur le réseau et les appareils.

Notre conseil La phase d'analyse inclut également un conseil sur les obligations de notification qui s'imposent à votre entreprise. Au cours de la phase de réponse, le CMO, souvent de concert avec un juriste externe et avec le directeur juridique, adressera aux autorités la déclaration conforme aux obligations de notification relatives à la détection d'un ransomware. Les obligations légales varient en fonction du cadre réglementaire. À ce stade, notez toutefois que ces informations seront transmises au nom de votre entreprise.

Par qui ?

- Administrateur réseau
- RSSI
- DSI
- CMO
- Équipe de réponse aux incidents de votre assurance cybersécurité
- Consultant en cybersécurité
- Malware Analyst

Comment : le RSSI partage le rapport de reprise et les décisions prises avec les postes suivants :

- PDG
- DAF
- Directeur juridique

2.4.1 Implication

Vos chances de parvenir à gérer cet incident par vous-même sont plutôt minces. Le processus qui vous attend sera long et douloureux. D'emblée, constituez votre équipe de réponse afin de gagner du temps et vous épargner des efforts. Examinez l'équipe, le budget et les ressources dont vous disposez. Votre premier objectif est d'assigner des tâches et d'attribuer des rôles.

1. Réponse technique : équipe et leader
2. Réponse aux communications internes : équipe et leader
3. Réponse aux communications externes : équipe et leader.

La section 2.6 « Collaborateurs », vous fournira des informations précises quant à l'affectation des responsabilités.

2.4.2 Endiguement

Cette section englobe plusieurs activités.

- Isolez les sauvegardes des autres systèmes.
- Coupez les systèmes infectés du réseau, mais **N'ÉTEIGNEZ PAS CES SYSTÈMES**.
- Scannez sans tarder les ports des systèmes restants pour vérifier qu'aucun port n'a été ouvert à votre insu.
- Exécutez en local une détection des malwares sur chaque système afin de découvrir d'éventuelles vulnérabilités.
- Assurez-vous d'avoir configuré des mesures d'authentification robustes pour chaque système. Mettez à jour les mots de passe/identifiants d'accès/CERT de l'ensemble des systèmes et du personnel, même s'ils n'ont pas été touchés. Partez du principe que l'intégralité de vos données d'authentification ont été compromises et qu'elles ne sont pas fiables.
- Cette étape comprend notamment une investigation numérique des machines infectées, dont l'importance va au-delà de la conformité, puisqu'elle permet d'identifier le mode opératoire des attaquants. En retour, vous découvrirez peut-être d'autres systèmes à examiner.

Notre conseil Les machines retirées du réseau devront probablement être conservées (et éventuellement remises aux enquêteurs). Considérez-les comme perdues : renoncez à les « réinitialiser » pour les réaffecter par la suite. S'il s'agit de machines virtuelles, créez-en de nouvelles lorsque vous arriverez à l'étape « Reprise et remédiation » ci-dessous (section 2.4.4). S'il s'agit de machines physiques, c'est le bon moment de mettre à niveau ces systèmes et d'installer ces nouvelles versions. Vous devrez peut-être répondre à d'autres exigences légales ou réglementaires, ou aux demandes des services de police, notamment si votre activité touche à la santé. Par ailleurs, des investigations plus poussées pourraient révéler la perte ou l'exfiltration de certaines données.

Partez du principe qu'aucune machine n'est « trop importante pour être isolée ». Si une machine est infectée, mieux vaut la supprimer de votre réseau. Si sa fonction est indispensable à votre organisation, trouvez-vous rapidement une option de secours.

2.4.3 Éradication

Chaque attaque, réseau, cartographie de système, mécanisme et menace résiduelle est unique, même si les outils de contre-attaque se ressemblent parfois. Votre équipe chargée de la réponse technique peut désormais s'atteler à débarrasser le réseau de toute trace restante de l'intrusion.

Notre conseil La restauration pose le risque de la réinfection, il faut donc connaître la date et les mécanismes de l'intrusion. La restauration des systèmes peut vous paraître urgente pour assurer la continuité de vos opérations, mais vous ne devez pas pour autant renoncer à identifier la méthode d'accès afin de neutraliser toute interruption future et de ne pas perdre de temps.

2.4.4 Reprise et remédiation

Au cours de cette phase, votre objectif consiste à délimiter et contenir les dégâts, ainsi qu'à organiser au plus vite le retour à la normale de vos opérations. En cas d'urgence, l'utilisation des sauvegardes reste la mesure la plus sûre et la plus fiable. Cette option ne fonctionne néanmoins que si les données sauvegardées sont « propres », c'est-à-dire qu'elles n'ont pas été compromises par l'attaque. Comme indiqué dans la section précédente, l'anticipation reste la clé : mettez au point un plan de reprise par étapes en cas d'urgence. La rapidité et la précision avec lesquelles vous identifiez les données touchées renforcent elles-mêmes la précision de vos contre-mesures. Vos objectifs sont ainsi multiples : reprendre vos activités, gagner du temps et agir efficacement.

Il vous reste peut-être une chance de déchiffrer les fichiers touchés par l'attaque. Certaines clés de chiffrement sont en effet réutilisées au cours de plusieurs attaques lorsque le malfaiteur n'a pas mis à jour ses propres outils. Ces outils sont parfois disponibles sur Internet. Sachez toutefois qu'il ne faut pas systématiquement faire confiance à ces sites. Vous trouverez des exemples dans ces notes de bas de page, mais *faites preuve de vigilance*[9] [10]. La police ainsi que les experts en cybersécurité peuvent vous aider à identifier des ressources fiables pour le déchiffrement.

En plus de vous prémunir de dégâts supplémentaires en limitant la portée de l'attaque et en veillant au bon fonctionnement des opérations au sein de votre environnement informatique, vous devrez également identifier la source de l'attaque. La première infiltration, avant le chiffrement effectif des données, est peut-être bien antérieure à la détection.

Vous ne pourrez pas vous passer de conseillers juridiques et techniques externes. Forts d'une expérience pratique, ils vous éclaireront sur les actions à entreprendre et vous fourniront une analyse indépendante du scénario à l'origine de cette situation.

Si vous avez réussi à identifier et à isoler chaque système infecté, ainsi qu'à déterminer le moment de l'infection, vous pouvez commencer à rechercher les sauvegardes dont vous avez besoin et à les copier sur un support fonctionnel. Si possible, déployez ces sauvegardes sur un système hors ligne indépendant afin de les réanalyser. Confirmez auprès du Malware Analyst que le système n'est pas infecté et qu'il ne contient pas de malware latent. Dans l'idéal, utilisez cette machine pour remplacer le système infecté. S'il ressort des conclusions du Malware Analyst que ce nouveau système est toujours infecté, cela signifie alors que la date de l'infection initiale a été incorrectement évaluée : réitérez et appliquez de nouveau la technique ci-dessus pour trouver une sauvegarde récente et propre. Répétez ce processus pour chaque système infecté.

En fonction de votre situation et des lois en vigueur, vous devrez peut-être classer les données et preuves collectées faisant l'objet d'une obligation de conservation. De ce fait, vous ne devez pas nettoyer ni

[9] https://nomoreransom.org/
[10] https://www.bleib-virenfrei.de/it-sicherheit/ransomware/liste/

réinitialiser les machines infectées, puisqu'elles contiennent probablement des preuves décisives. S'il s'agit de machines virtuelles, un cliché instantané du système devrait suffire. S'il s'agit de machines physiques, saisissez l'occasion de les remplacer. Si toutefois le coût financier est trop élevé, envisagez d'utiliser une sauvegarde propre de la machine infectée avant de la remettre en service.

Moment décisif Dans le cadre de votre réponse, et outre les éventuelles obligations de notification, vous devrez également décider si vous souhaitez rendre l'incident public. (Cette décision vous échappera peut-être si l'entreprise ne contrôle pas sa communication publique, voire interne.) Pour plus de détails, veuillez consulter la section 2.5.5 « Confirmation de l'attaque et obligations de notification ».

2.5 Décisions

Chaque décision a une conséquence (et verrouille un peu plus le champ des possibles pour la suite), il est donc important de comprendre ce à quoi vous vous engagez. L'objectif de ce document est de vous fournir un cadre d'action. À ce titre, la liste des points à prendre en compte et des conséquences éventuelles n'est pas exhaustive.

2.5.1 Faire intervenir votre assurance cybersécurité et l'équipe de réponse aux incidents

Si vous prenez la décision de faire intervenir votre compagnie d'assurance en déclarant le sinistre, vous devez accepter l'éventualité de voir vos primes révisées à l'avenir. Bien que l'inquiétude soit légitime, vous protéger est aussi la raison d'être d'une assurance. Néanmoins, le fait de faire appel à votre assurance plutôt que d'impliquer immédiatement votre équipe n'est pas forcément judicieux du point de vue de la résolution. Si vous êtes en mesure de résoudre la situation sans déclarer de sinistre, il est possible d'éviter cette étape.

Chronologie indicative C'est là une de vos toutes premières décisions, qui intervient généralement lorsque vous confirmez l'attaque par ransomware et évaluez vos chances de reprise. Si la réponse s'impose assez rapidement dans certains cas, d'autres scénarios exigent de plus amples recherches, et monopolisent donc un temps précieux.

Les coordonnées du centre de réponse aux incidents pour la couverture des cyber-risques se trouvent généralement dans votre police d'assurance. **Il va de soi que la police d'assurance doit être conservée hors ligne, là où elle n'est pas accessible via le réseau.**[11]

Votre assurance vous demandera généralement de soumettre un formulaire avant d'intervenir. Cependant, les compagnies d'assurance proposent parfois un accompagnement avant une demande formelle. Dans tous les cas, votre objectif est d'obtenir de l'aide de l'équipe de réponse aux incidents de votre assurance cybersécurité.

Il faut à tout prix déterminer la couverture et le plafond d'assurance (le cas échéant), ainsi que les coûts non pris en charge, comme l'intervention d'un tiers ou les coûts de sauvegarde et de restauration.

[11]Et pour cause, les acteurs malveillants recherchent en ligne les contrats pour connaître les sommes qu'ils sont en mesure de réclamer et les limites couvertes par chaque police. Ces informations doivent demeurer hors ligne et être mises à disposition du service juridique (et autres services concernés) en temps voulu.

2.5.2 Quand faire appel aux services de police

Faire appel aux services de police n'est pas toujours une décision facile ni évidente. Les équipes de la direction et de la sécurité informatique, les services juridique et marketing, ainsi que le conseil d'administration voudront probablement prendre part à cette décision, de même qu'aux décisions concernant la chronologie.

Chronologie indicative Vous pouvez prendre cette décision dès que la réalité de l'attaque est confirmée. Il est possible que vous n'ayez jamais à le faire, comme il est possible que la situation soit déjà entièrement résolue à ce moment-là. Dans le cadre du plan de réponse fixé comme objectif de la section Analyse, préparez-vous à devoir confirmer cette décision et le moment où vous la prendrez.

Avant d'alerter les services de police, assurez-vous qu'un crime a bien été commis au moyen d'une investigation numérique de l'incident.

Pensez également aux répercussions d'une telle information : vos politiques d'entreprise seront passées au peigne fin, vous devrez répondre à des questions et informer des tiers de votre avancement, ce qui pourrait retarder votre réponse à l'incident et vous obliger à partager vos conclusions et résultats (et engager votre responsabilité civile).12 Vous devrez par ailleurs fournir des preuves issues de l'investigation numérique, sans compter que vos systèmes seront considérés comme une scène de crime, avec des conséquences sur votre capacité à opérer. Aux États-Unis, les agences faisant autorité dans ces domaines sont le FBI, DHS et les services secrets. Il existe des institutions similaires dans de nombreux pays. Dans l'idéal, la relation avec les services de police préexiste à l'incident, mais ce n'est pas toujours envisageable, et encore moins réaliste. Selon les circonstances, les services de police encouragent certains comportements avec plus ou moins d'insistance. Par exemple, s'ils s'opposent au paiement de la rançon, de façon plus ou moins contraignante, vous aurez alors les mains liées.

Le concours des services de police présente plusieurs avantages, dont l'expérience, la possibilité d'identifier le vecteur d'attaque, la capacité de négociation et, dans certains cas, le déchiffrement (par exemple avec une clé utilisée au cours d'une autre cyberattaque). Cependant, n'attendez pas de la police qu'elle vous aide à restaurer ou à sécuriser vos systèmes. Son travail concerne uniquement le crime commis. Les institutions chargées de l'application de la loi s'efforcent d'ailleurs de rappeler qu'elles sont là pour accompagner les victimes, et qu'elles feront de leur mieux pour interrompre le moins possible vos opérations.

Selon votre juridiction, vous êtes peut-être dans l'obligation d'alerter les services de police ou autres institutions en charge de l'application de la loi. Le manquement à ce devoir dans les délais impartis pourrait d'ailleurs placer votre organisation et ses collaborateurs dans une situation de non-conformité. Le directeur juridique doit être tenu informé pour vous permettre de prendre une décision éclairée.

Pour signaler un cyber-incident aux États-Unis, rendez-vous sur l'Internet Crime Complaint Center du FBI à cette adresse : https://www.ic3.gov/.

[12]David Burns et Brian Williamson, *Should companies cooperate with law enforcement during ransomware attacks?*, dans Global Investigations Review, octobre 2022, https://www.gibsondunn.com/wp-content/uploads/2021/10/Burns-Williamson-Should-companies-cooperate-with-law-enforcement-during-ransomware-attacks-GIR-10-08-2021.pdf

2.5.3 Paiement de la rançon

Le paiement de la rançon ne fait pas partie des solutions préconisées par le M3AAWG. Pourquoi ? Parce que le paiement ne vous garantit pas de pouvoir restaurer vos systèmes ni de récupérer l'accès à vos données. En outre, le fait de céder aux exigences de l'acteur malveillant pourrait faire de vous la cible d'autres tentatives d'extorsion par ce même acteur.

La décision de payer la rançon n'est jamais évidente, et de nombreux paramètres entrent en ligne de compte. Assurez-vous de prendre le temps d'aborder la question à différents niveaux de l'organisation. Pour chacun de ces entretiens, sollicitez la présence du service juridique.

Sur la question des ransomwares, la stratégie de cybersécurité nationale établie en 2023 par la Maison Blanche énonce ce qui suit :

« À terme, la meilleure façon de saper les motivations des cybercriminels consiste à réduire leurs gains potentiels. Par conséquent, l'administration déconseille fortement de payer les rançons exigées. De leur côté, les victimes d'une attaque par ransomware, qu'elles choisissent ou non de payer la rançon, doivent signaler l'incident auprès de la police et autres agences concernées. »13

Chronologie indicative Cette décision intervient souvent après la phase d'analyse. Parfois, l'investigation ou la reprise s'avèrent plus coûteuses que le paiement de la rançon. Il n'empêche que le paiement est généralement accepté en dernier recours. La perte de certaines données ultérieures à la dernière sauvegarde peut avoir des effets dévastateurs sur l'entreprise, à vous d'établir la balance du bénéfice-risque.

Une des toutes premières questions que vous devrez vous poser est de savoir si le paiement des rançons est légal dans votre juridiction. Impliquez votre service juridique au plus tôt, et chaque fois que cet aspect sera évoqué. Il est à noter que certaines juridictions interdisent ou limitent le paiement des rançons de quelque nature que ce soit. D'autres, comme l'Office of Foreign Assets Control (OFAC, États-Unis),[14] mettent en place des mesures restrictives. Dans certains cas, ces restrictions s'inscrivent dans le cadre de la lutte contre le financement du terrorisme. Si le malfaiteur est inscrit sur une liste noire, le payer pourrait alors constituer un délit et exposer votre entreprise à des poursuites. Outre les options limitées qui s'offrent à vous dans le cas où de telles restrictions existent, certaines juridictions infligent par ailleurs des sanctions pénales ou civiles aux décisionnaires.

S'il est important de saisir toutes les nuances dans ce contexte précis, la motivation des malfaiteurs est un élément essentiel. De fait, les rançons sont négociables. Même si vous décidez de payer, vous seriez bien avisé de vous informer sur les « tarifs » pratiqués (tout juste 10 % de la somme réclamée dans certains cas). Tâchez également de cerner les personnes auxquelles vous avez affaire et la propension de ces acteurs à véritablement fournir une clé de déchiffrement qui vous restituera vos données. Une fois ces informations en main, renseignez-vous aussi sur les outils employés, les dispositifs de déchiffrement existants et là où vous pourrez les trouver.

[13] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[14] https://www.globalcompliancenews.com/2021/10/28/ofac-issues-updated-ransomware-advisory-and-designates-suex-as-an-sdn181021/

Le paiement des rançons a cela de problématique qu'il perpétue un modèle commercial : c'est le caractère lucratif de l'extorsion qui pousse les acteurs malveillants à recourir aux ransomwares. Bien que factuel, toutes les entreprises visées n'ont pas le luxe d'adhérer à ce constat, puisqu'elles doivent souvent composer avec des ressources limitées. De fait, elles n'ont pas toujours la capacité ni le temps d'examiner les autres options. Ainsi le paiement est-il inévitable dans certains cas, même si le refus de payer sera toujours préconisé.

À ce propos, il est à noter que l'utilisation de la clé de déchiffrement fournie après le paiement n'est pas sans risque. Si votre reprise après incident n'est pas définitive, il se peut que l'acteur, encore présent dans vos systèmes, arrive à identifier les données déchiffrées ou non supprimées. Vous pourriez malgré vous fournir des informations supplémentaires aux hackers, qu'ils utiliseront pour lancer de nouvelles attaques. Si vous prenez la décision de payer, reportez-vous à la section suivante, « Négocier le paiement de la rançon ».

2.5.4 Négocier le paiement de la rançon

Avez-vous déjà entendu parler des négociateurs professionnels ? Sachez qu'ils existent. Ce sont même parfois eux qui viennent à vous après avoir eu vent de l'incident. À vous de juger de leur fiabilité. Vous pourrez également solliciter leurs conseils sur des questions diverses. Dans certains cas, ils pourront même vous inciter à revenir sur votre décision de payer la rançon.

Chronologie indicative La négociation de la somme à payer intervient après avoir pris la décision de s'acquitter de la rançon. Pour autant, cela ne signifie pas que vous ne devriez pas vous rapprocher d'un négociateur avant cela. Vous aurez sûrement besoin des conseils d'un professionnel pour envisager toutes vos options et comprendre ce qu'impliquent vos décisions.

2.5.5 Confirmation de l'attaque et obligations de notification

La médiatisation de votre attaque, ou de toute attaque passée, n'est pas une décision à prendre à la légère : elle aura des répercussions sur les équipes chargées des aspects juridiques, de la conformité et du marketing, ainsi que sur d'autres services.

Chronologie indicative Généralement, les acteurs malveillants préfèrent rester dans l'ombre. L'attention du public peut en effet contrecarrer leurs objectifs, sans compter que les chances de déclencher une enquête de police sont plus élevées. La décision de confirmer l'attaque découle bien souvent du contexte réglementaire. C'est le rôle des services juridiques et de conformité d'en apprécier la nécessité. Dans certains cas, les victimes ne reconnaissent jamais l'attaque. Dans d'autres, la confirmation est immédiate.

Dans tous les cas, cette décision peut avoir des effets dévastateurs pour l'entreprise, notamment le cours des actions, les évaluations, la solvabilité, la confiance des clients, le fonds commercial, la réputation de la marque, etc.

Il se peut aussi que le contexte légal ne laisse pas le choix aux victimes, qui sont alors dans l'obligation de notifier l'attaque. Parfois, cette obligation est créée dès lors que la victime a connaissance de l'attaque. Quoi qu'il en soit, vous devez impérativement comprendre le cadre législatif dans lequel se trouve votre entreprise. (Bien souvent, ces lois ne s'appliquent qu'à des entreprises d'une certaine taille ou d'un statut

défini, [15] dans des secteurs bien précis). Vous trouverez des informations à propos du signalement aux États-Unis ici : stopransomware.gov.[16]

Outre les exigences réglementaires, il faut également tenir compte des obligations de signalement imposées contractuellement aux acteurs de la chaîne d'approvisionnement (et accrues au fil des ans). De fait, votre organisation est peut-être tenue de déclarer l'incident à ses fournisseurs ou clients. C'est pourquoi vous devez impérativement veiller à impliquer le directeur juridique dans l'examen des obligations contractuelles relatives à l'incident.

Quelles sont vos responsabilités en tant que victime d'une attaque ? Qui doit être mis au courant, et quand ? Quel est l'impact sur votre entreprise ? Vos clients ont-ils été touchés ? Vos clients ont-ils été informés ? Êtes-vous dans l'obligation de leur faire part de l'incident ? Les malfaiteurs ont-ils déjà contacté les sujets des données ? Quelles sont les dimensions morales et éthiques à prendre en compte ? Voici les personnes et entités que vous pourriez être dans l'obligation de notifier :

- services de police ;
- organismes réglementaires ;
- organismes publics ;
- organismes professionnels ;
- clients ;
- partenaires ;
- fournisseurs ;
- personnel de maintenance.

Les exigences de notification varient en fonction du secteur ou de la taille de l'entreprise dans certaines juridictions. C'est notamment le cas des États-Unis, où la loi HIPAA s'étend aux informations de santé des individus. Ce qui constitue ou non une violation des données est ainsi clairement défini. Le cas échéant, vous serez tenu de signaler l'incident aux sujets des données, mais également au Department of Health and Human Services (États-Unis). Outre la réponse spécifique aux ransomwares et malwares, voici d'autres lois encadrant la protection des données : le RGPD en Union européenne, la LPRDE au Canada et les lois COPPA/HIPPAA/ARRA/GLBA aux États-Unis. Dans plusieurs juridictions des États-Unis, de nouvelles lois contraignent d'autant plus les victimes dans certaines situations (CPRA, CCPA, etc.). En plus du Canada, de l'Union européenne et des États-Unis, 16 autres pays ont adopté des lois de protection de la confidentialité, dont la plupart disposent d'obligations de signalement. Ces questions sont à adresser au service juridique et au directeur juridique dès lors qu'ils ont pris connaissance de l'incident.

Un autre risque à anticiper est la confirmation par inadvertance, à savoir la soumission de documents ou de journaux comportant des signes ou logos permettant d'identifier votre entreprise. De même, prenez garde à

[15] https://www.google.com/url?q=https://www.sec.gov/rules/proposed/2022/33-11038.pdf&sa=D&source=docs&ust=1676059185887151&usg=AOvVaw26lE3B9FzA1LHlK7uiZqyy
[16] https://www.cisa.gov/news-events/news/getting-ahead-ransomware-epidemic-cisas-pre-ransomware-notifications-help-organizations-stop-attacks

la façon dont sont rédigées vos communications qui admettent une faute, car cela pourrait avoir des répercussions sur l'assurance ou sur la réponse des autorités.

2.6 Collaborateurs

Veillez à avertir les parties prenantes dans le bon ordre. Cette étape implique de solliciter un certain nombre de vos collaborateurs, de comités, de conseils ou de groupes. À vous de déterminer s'il ne serait pas plus opportun de les affecter à des tâches plus utiles. Demandez-vous également si vous ne devriez pas informer à l'avance certaines personnes. Chaque organisation possède sa propre structure. Par exemple, le processus de signalement entre les cadres n'est pas toujours identique. Les postes suivants doivent être impliqués au cours de la réponse :

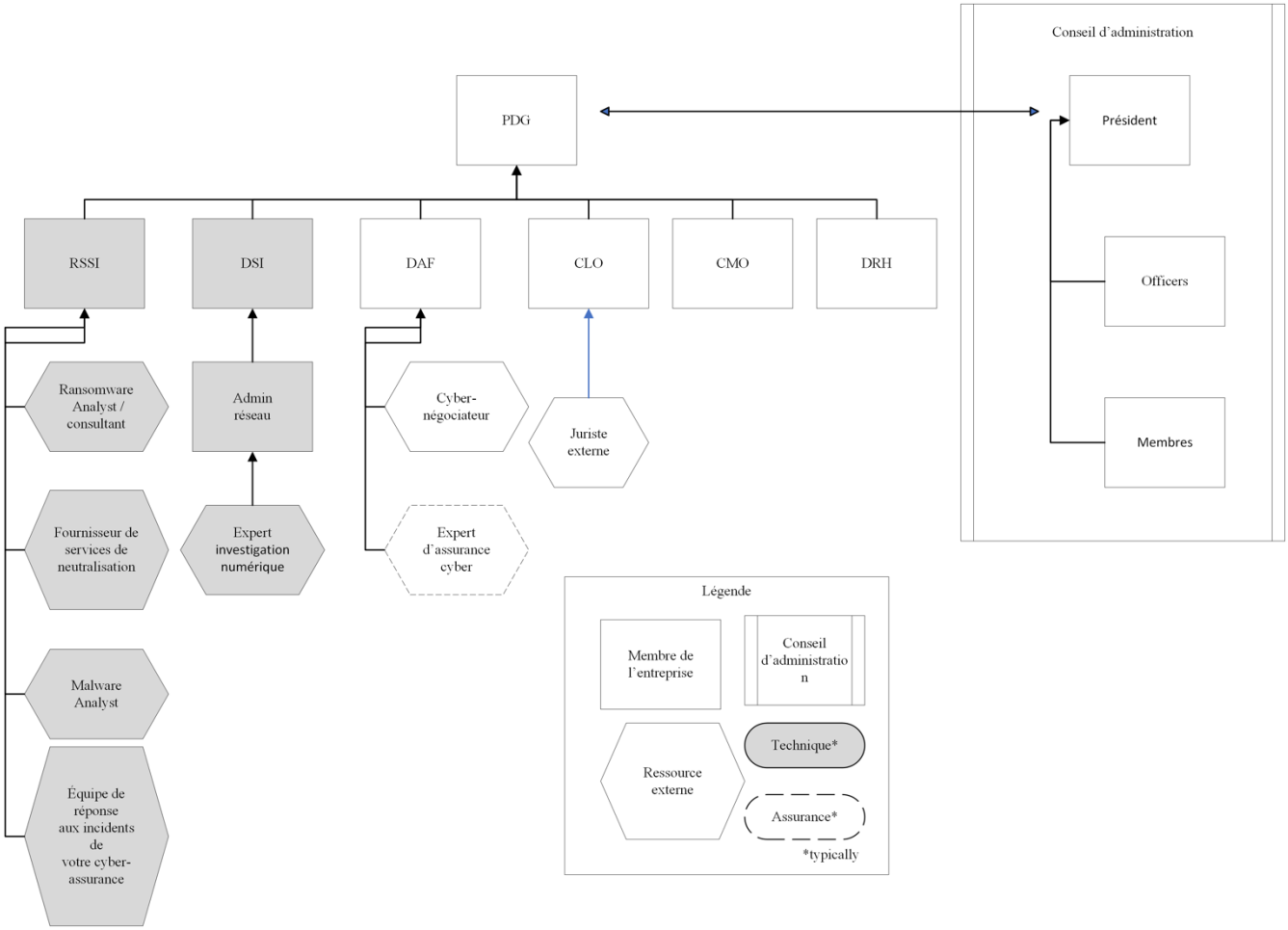

Schéma 2 : Postes généralement impliqués dans la neutralisation d'un ransomware

2.6.1 Ressources en interne

RSSI : le responsable de la sécurité des systèmes d'information (RSSI), ou la personne responsable en premier lieu de la sécurité des données, ressources, opérations informatiques et techniques de l'entreprise. Le RSSI est généralement le premier informé. Dans un monde idéal, il existerait un manuel pour vous indiquer les prochaines étapes, mais cette situation n'a rien d'idéal. Le RSSI doit disposer des coordonnées des autres parties, et c'est à lui d'assumer la délicate (et urgente) tâche de reprise des activités et de neutralisation de l'incident. Certaines organisations ont créé un poste de Chief Security Officer (CSO), en charge ou non de la sécurité technique, la nécessité de l'impliquer reste donc à déterminer si aucun accès physique n'est constaté.

DSI : le directeur des systèmes d'information (DSI) est responsable de l'ensemble des systèmes d'information et données. En fonction de sa relation avec le RSSI, la direction ou le conseil d'administration, son implication sera plus ou moins importante au cours du processus. Il n'est pas rare que le DSI assure également le rôle du RSSI. Les autres postes à impliquer dans ce processus sont notamment le Data Protection Officer (DPO) ou le CDO (Chief Data Officer).

PDG : le PDG, ou le numéro un de l'organisation (président, directeur, etc.), doit être informé de l'activité malveillante, des actions entreprises jusque là, du plan mis en place (notamment les mesures de notification) ainsi que du statut de la réponse. Ne faites pas l'impasse sur ces échanges, l'objectif étant ici d'informer, de solliciter une assistance ou des ressources, de contrôler les canaux de communication et d'anticiper les décisions importantes à venir.

DAF : le directeur des affaires financières (DAF), ainsi que l'ensemble de son service, doit être averti de la menace et du statut des investigations en lien avec le ransomware. La posture de sécurité et de vérification actuelle de l'entreprise devra sans doute être renforcée si l'acteur malveillant est connu. Le DAF aura également voix au chapitre des décisions financières en lien avec les ressources externes impliquées, des négociations avec les assureurs et de la décision de payer la rançon.

Directeur juridique : le directeur juridique (CLO), votre juriste ou un juriste externe communiquera avec les services de police sur l'attaque ; il s'assurera de la conformité auprès des organismes régulateurs (interaction avec les malfaiteurs figurant sur liste noire dans certaines juridictions, violation de contenu et protection des données) et prendra éventuellement part aux négociations avec les malfaiteurs. Certaines organisations emploient également un Chief Privacy Officer (CPO), généralement très axé sur les questions légales, mais qui peut aussi répondre aux questions techniques et s'occuper de plusieurs aspects liés aux services juridique et informatique.

CMO : le Chief Marketing Officer est souvent responsable de la réputation de l'entreprise, des relations avec la presse et de la communication externe. À la tête de son équipe, le CMO doit prendre des décisions concernant les réponses à donner et les informations à publier, mais aussi prendre le pouls des réseaux sociaux, du web et des médias traditionnels pour savoir ce qui se dit de l'évènement.

DRH : le directeur des ressources humaines (DRH), ou toute personne en charge des ressources humaines au sein de l'entreprise, sera impliqué si des données des employés ont été compromises au cours de l'attaque. La chronologie et l'étendue des communications sont peut-être soumises à des exigences légales et réglementaires, et donc sujettes à des conséquences.

Conseil d'administration : le conseil peut se composer de leaders expérimentés extérieurs à l'entreprise. En règle général, c'est le PDG ou un cadre supérieur qui s'occupe de communiquer avec le conseil à propos du ransomware et des conséquences. Le dernier mot revient souvent au conseil lorsqu'il faut prendre des décisions difficiles, et il devra être informé de l'avancement de l'enquête et des efforts de neutralisation déployés.

Administrateur réseau : la ou les personnes responsables de l'architecture réseau, et des points et méthodes de connexion des systèmes. Dans certaines entreprises, ce poste est le même que celui du DSI ou du RSSI, mais ces responsabilités peuvent être réparties entre plusieurs postes dans d'autres structures. Ces ressources techniques seront indispensables aux phases d'analyse et de neutralisation.

2.6.2 Ressources et services externes

Juriste externe : le rôle d'un juriste externe est d'offrir à l'équipe juridique une expertise supplémentaire en matière de paiement des rançons, de listes de surveillance des activités terroristes, d'interprétation des politiques de cybersécurité et de règles sur la protection des données, le tout conformément aux exigences légales et réglementaires qui régissent les activités de l'entreprise.

Équipe de réponse aux incidents de votre assurance cybersécurité : la politique d'assurance de l'entreprise, le cas échéant, inclut peut-être l'accès à une expertise ou à des ressources sur les techniques et les ransomwares. L'accès à ces ressources est souvent conditionné à la déclaration d'un sinistre. Il peut s'agir d'un centre d'appel, de consultants présents sur site, d'une expertise à distance, de documents, d'outils ou d'une combinaison de ces ressources. Ce groupe sera dénommé Équipe de réponse aux incidents de votre assurance cybersécurité.

Expert d'assurance cybersécurité : l'assureur fournit souvent les services d'un expert et d'une équipe spécialisée en ransomwares dans le cadre du contrat. Les décisions concernant l'assistance fournie et les limites de l'engagement sont abordées au niveau exécutif de l'entreprise.

Malware Analyst : ce spécialiste peut collaborer avec l'Équipe de réponse aux incidents de votre assurance cybersécurité, voire en être un membre. La mission du Malware Analyst est d'aider à scanner, identifier et supprimer le malware des systèmes et du réseau. En outre, son aide peut s'avérer précieuse pour déterminer l'heure et la date de la première intrusion, ainsi que le vecteur de l'attaque. Ces informations vous aideront ensuite à identifier des vulnérabilités qui doivent être corrigées.

Expertise en investigation numérique : que s'est-il passé exactement, quand et comment ? Vous devez absolument répondre à ces questions pour faire avancer le processus, et le plus tôt possible. Un expert en investigation numérique se spécialise dans la préservation, l'analyse et la découverte des méthodes, outils et techniques employés par les acteurs malveillants. Si une grande partie des organisations ne disposent pas d'un tel poste en interne, les consultants ne manquent pas sur le marché.

Consultants en cybersécurité et fournisseurs de services de neutralisation : il peut s'agir d'organisations, d'individus et de services à l'expérience et aux capacités variables. Les experts d'assurance et les services de police peuvent vous aider à trouver et à évaluer de tels services, mais leurs recommandations seront inévitablement subjectives.

Cyber-négociateur : un spécialiste dont la mission se rapproche de celle du consultant en cybersécurité et que vous trouverez en suivant les instructions précédentes. Les négociateurs connaissent les tarifs

d'extorsion pratiqués par les acteurs malveillants et savent dans quelle mesure ces derniers accepteront de négocier la somme. Leur intervention peut donc vous faire réaliser de belles économies.

2.7 Technologie

La détection d'un ransomware et la réponse à cet incident s'effectuent avec diverses technologies, au premier rang desquelles se trouvent les outils de protection des terminaux, comme les logiciels anti-malwares et les solutions de gestion des vulnérabilités. Ces outils peuvent et doivent être installés après une infection par ransomware, afin de vous assurer que vous utilisez la version la plus récente. Une précaution d'autant plus importante que les malwares sont connus pour désactiver ou endommager les solutions de sécurité déjà installées. Vous trouverez également de nombreux outils de scan des virus, mais sachez que leurs fonctionnalités sont parfois limitées par rapport aux solutions payantes. Aussi, l'utilisation d'un outil de scan en ligne vous oblige à importer vos fichiers (potentiellement infectés) sur le site web. **Ces sites sont susceptibles de conserver les fichiers importés et de rendre ces informatiques publiques**, votre confidentialité n'est donc pas garantie.

Les outils de détection des attaques et de réponse au niveau des terminaux présentent des fonctionnalités avancées et exploitables en temps quasi réel. Ce type de logiciel est conçu pour protéger les appareils individuels, comme les ordinateurs et les smartphones, des malwares et autres menaces. Selon la taille de votre entreprise, vous pouvez également souscrire à des services gérés qui vous fourniront ces outils. L'avantage d'une telle solution est qu'elle vous permet, une fois déployée au sein de votre environnement, de mieux cerner l'ampleur de l'attaque. Évaluer l'impact de l'attaque et récupérer les données perdues sont des opérations plus délicates, qui entreront également en ligne de compte dans votre décision de payer ou non. Vous trouverez sans doute opportun d'installer des logiciels de détection au niveau des terminaux après la première détection d'un ransomware, car ils pourraient empêcher le virus d'effectuer d'autres modifications malveillantes sur la machine et vous aider à identifier des processus ou programmes suspects. Notez toutefois que cette action ne permet pas d'annuler les dégâts causés par le ransomware. En outre, l'installation d'un outil de détection et de réponse au niveau des terminaux ne vous met pas définitivement à l'abri. De fait, la sécurité de votre organisation repose sur des pratiques bien ancrées qui réduiront vos risques de subir une autre attaque par ransomware.

Vos sauvegardes vous permettront non seulement de restaurer vos données, mais vous serviront également à mesurer la portée de l'infection. Pour cela, comparez les fichiers avec les dernières sauvegardes afin de découvrir toute modification récente. Veillez naturellement à accéder à votre sauvegarde à partir d'une machine non infectée. (L'intention des attaquants est peut-être de subtiliser vos données, et l'accès non sécurisé aux sauvegardes peut leur ouvrir une brèche vers une véritable mine d'informations). De même, vérifiez que vos sauvegardes n'ont pas été elles aussi compromises. Pour cela, assurez-vous que vos sauvegardes sont en mode lecture seule, ou bien créez une somme de contrôle des sauvegardes dans un autre emplacement (inaltérable) afin de détecter toutes les modifications.

Les solutions de stockage dans le cloud offrent parfois des sauvegardes intégrées, ou bien des « versions précédentes » des fichiers stockés. Vous pouvez donc restaurer ces versions pour repérer les modifications éventuelles.

Lors d'une attaque par ransomware, vous pouvez tenter de récupérer vos données à l'aide d'un outil de déchiffrement. Ces outils parviennent dans certains cas à annuler l'opération de chiffrement du ransomware.

Vous récupérez alors l'accès à vos fichiers sans avoir à payer la rançon. Cependant, l'efficacité de ces outils varie en fonction du ransomware, le succès de l'opération n'est donc pas garanti. Vous pourrez trouver de tels outils de déchiffrement en ligne[17,18] attention toutefois à choisir des ressources fiables. Tournez-vous plutôt vers les sites officiels du gouvernement.

2.8 Après l'incident

Dernière ligne droite de la réponse aux incidents, la phase post-incident a son importance : c'est l'occasion d'analyser minutieusement l'incident, de tirer des enseignements de la situation et de mettre en place des mesures visant à prévenir la survenue d'incidents similaires à l'avenir. Cette phase est déterminante pour le succès global du processus de réponse aux incidents : c'est à ce moment que l'entreprise pourra identifier les améliorations à apporter et les actions à entreprendre pour se protéger à l'avenir.

Objectif Au cours de la phase post-incident, un rapport d'incident détaillé devra être élaboré. Ce rapport doit récapituler l'incident, les actions entreprises pour le contenir et le résoudre, ainsi que l'impact sur l'organisation. Ce rapport devra être examiné par tous les membres de l'équipe de réponse aux incidents et par la direction en vue de suggérer des améliorations du processus de réponse aux incidents.

Notre conseil Les enseignements tirés de l'incident doivent être consignés et partagés avec qui de droit. Ces enseignements vous serviront à mettre à jour vos plans et procédures de réponse aux incidents, et à mieux former votre personnel concernant l'identification des vulnérabilités et la réponse à apporter aux incidents futurs.[19]

Notre conseil La phase post-incident doit inclure une analyse exhaustive des contrôles et systèmes de sécurité de l'organisation afin d'identifier les vulnérabilités exploitées dans le cadre de l'incident. Sur la base des conclusions de cette analyse, des mesures devront être prises pour atténuer ou éliminer ces vulnérabilités afin d'éviter qu'un autre incident se reproduise. À présent que vous vous êtes ménagé un moment de répit avant la prochaine attaque, voici quelques ressources disponibles[20] pour vous aider à vous organiser.

3.Conclusion

Ce document a pour objectif principal de fournir un plan d'action au moment où l'attaque par ransomware vient d'être découverte. La gestion de votre temps, la structuration des sauvegardes et les différentes

[17] https://nomoreransom.org/
[18] https://www.bleib-virenfrei.de/it-sicherheit/ransomware/liste/ (Allemagne)
[19] https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot
[20] Ensemble, le NIST et le National Cybersecurity Center of Excellence (NCCoE) ont publié Ransomware Risk Management: A Cybersecurity Framework Profile, Barker, Fisher, Scarfone & Souppaya, 2022, https://csrc.nist.gov/publications/detail/nistir/8374/final

méthodes de récupération dépassent la portée de ce document, de même que la protection renforcée des terminaux en amont de l'infection. Ce document se contente de fournir une réponse de première intention à l'attaque en cours. La défense et la prévention face aux ransomwares forment un vaste sujet, qui va de la préparation avant l'attaque à la reprise totale des activités. D'excellentes ressources sont disponibles pour mieux comprendre la définition, la préparation, la portée légale et réglementaire ainsi que le suivi post-incident[21] [22].

Avertissement légal : ce document n'a pas valeur de conseil juridique. Le M3AAWG recommande vivement à ses lecteurs de collaborer avec le service juridique de leur organisation ou de se faire assister par un juriste externe pour connaître leurs droits, responsabilités et obligations légales.

Ce document est tenu à jour par le Messaging Malware Mobile Anti-Abuse Working Group (M³AAWG). Comme tous les documents que nous publions, il est sujet à des modifications. Pour vous tenir au courant ou pour proposer une correction, rendez-vous sur le site web du M3AAWG (www.m3aawg.org) ici.

M3AAWG-145

[21] Ibid.

[22] Département de la Sécurité intérieure des États-Unis (DHS), Cybersecurity Infrastructure Security Agency (CISA) ; Tips & Tactics: Preparing Your Organization for Ransomware Attacks, mai 2021, https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf