RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS

COMMENT LES ANTICIPER ET RÉAGIR EN CAS D'INCIDENT ?

SOMMAIRE

AVANT-PROPOS

Les organisations de notre pays, qu'elles soient publiques ou privées, petites ou grandes, entrevoient désormais leur avenir à la lumière des transformations numériques. Parce que les bénéfices de ces évolutions sont considérables, nous souhaitons que les entreprises et les administrations françaises puissent s'y appuyer dans un climat de confiance.

Or ces progrès n'arrivent pas seuls. Ils sont un terrain de jeu formidable pour quantité d'attaquants dont les motivations sont aussi variées que les profils. Parmi les menaces ainsi véhiculées, un effort particulier doit être mené à l'égard de l'une d'elles : la cybercriminalité. Pourquoi ? D'une part parce que les attaques appartenant à cette catégorie constituent un véritable fléau pour les organisations victimes. Et d'autre part parce qu'il est possible – la plupart du temps – de ramener ce risque à un niveau résiduel par l'application de bonnes pratiques de sécurité numérique.

Parmi les actes de cybercriminalité recensés, les rançongiciels représentent aujourd'hui la menace la plus sérieuse. Ils augmentent en nombre, en fréquence, en sophistication et peuvent être lourds de conséquences sur la continuité d'activité voire la survie de l'entité victime. Pour lutter contre ces nouvelles formes de cybercriminalité, notre nation s'organise. Pour preuve, il existe désormais une compétence spécifique au sein du parquet de Paris dont la mission est de poursuivre les auteurs de ces infractions.

Ajoutons que la réponse mobilise au-delà de ces affaires puisque le gouvernement mène une réflexion sur les mesures à même de réduire le risque que représentent les rançongiciels en vue de casser le modèle économique des attaquants et diminuer de manière drastique leur sentiment d'impunité. L'élaboration de ce guide de sensibilisation à destination des entreprises, mais aussi des collectivités, apporte une première pierre à cet édifice.

Cet effort n'aura de portée que si l'ensemble de l'organisation – de la direction aux collaborateurs – se saisit de ces questions et renouvelle sa vigilance, ses priorités d'investissement et sa gestion des risques avant qu'il ne soit trop tard.

Loin de vouloir effrayer, la juste voie en la matière est bel et bien d'informer, de démystifier et de responsabiliser afin d'influencer positivement la prise de décision.

Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Catherine Pignon, directrice des Affaires criminelles et des grâces (DACG)

QU'EST-CE QU'UN RANÇONGICIEL ?

Un rançongiciel – *ransomware* en anglais – est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Les rançongiciels figurent au catalogue des outils auxquels ont recours les cybercriminels motivés par l'appât du gain.

Lors d'une attaque par rançongiciel, l'attaquant met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible. En pratique, la plupart des rançongiciels chiffrent par des mécanismes cryptographiques les données de l'ordinateur ou du système, rendant leur consultation ou leur utilisation impossibles. L'attaquant adresse alors un message non chiffré à la victime où il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.

TENDANCES

La grande majorité des attaques par rançongiciels sont opportunistes et profitent du faible niveau de maturité en sécurité numérique de leurs victimes. Cependant, depuis 2018, on observe une croissance de ces attaques menées par des groupes cybercriminels qui, après avoir ciblé des particuliers, s'en prennent désormais à des organisations aux moyens financiers importants ou aux activités particulièrement critiques.

Cette tendance fait entrer les rançongiciels dans la catégorie des attaques dites « *Big Game Hunting* » en raison de l'importance de leurs cibles. Pour une portée démultipliée, il arrive parfois qu'un attaquant associe au rançongiciel un ou plusieurs autres programmes malveillants (crypto mineurs, cheval de Troie, etc.). Il devient dès lors possible d'utiliser de manière illégale les ressources matérielles des équipements compromis ou de s'emparer des données présentes sur le système d'information. Phénomène relativement récent, certains groupes criminels associent désormais la menace de publication de données sensibles à l'utilisation de raçongiciels. Ceci afin d'accroitre la pression exercée sur leurs victimes pour qu'elles paient la rançon.

Les attaquants à l'origine de ces opérations disposent le plus souvent de ressources financières et de compétences techniques importantes. En effet, le niveau de sophistication atteint équivaut parfois aux opérations d'espionnage conduites par les États. Alors que les montants habituels des rançons s'élèvent à plusieurs centaines ou milliers d'euros, celles demandées lors des attaques de type « *Big Game Hunting* » sont à la mesure des moyens financiers de l'entité victime et peuvent atteindre des sommes allant jusqu'à plusieurs millions d'euros. En outre, de récentes attaques par rançongiciels ont mis en évidence le danger d'un impact systémique sur un secteur d'activité qui, en ciblant des entreprises sous-traitantes ou clés du secteur, pourrait amener à le déstabiliser. On parle alors d'attaques indirectes et celles-ci ▶

constituent aujourd'hui une autre tendance notable.

Le préjudice va alors bien au-delà de la perte des données ou du paiement d'une rançon puisque les organisations victimes doivent faire face à de nombreuses autres conséquences : arrêt de la production, chute du chiffre d'affaires, risques juridiques (par exemple liés au RGPD [1] dans le cas où des données personnelles ne sont plus accessibles), altération de la réputation, perte de confiance des clients, etc. Ces attaques génèrent souvent une rupture ou une dégradation d'activité chez la victime. Dans le cas d'une entreprise, il peut en aller de sa survie. Le rançongiciel est une menace sérieuse aux conséquences potentiellement durables pour les organisations comme pour les particuliers qui offre aux cybercriminels un modèle économique très rentable. Il est essentiel de rappeler et de retenir que le paiement des rançons entretient cette activité criminelle et ne garantit pas à la victime la récupération de ses données.

1 Le règlement général sur la protection des données.

ILS L'ONT VÉCU. ILS TÉMOIGNENT.

Le 15 novembre 2019, à la veille du week-end, un interne des services d'urgence signale un problème de droits d'accès à une application métier. Peu après, la DSI constate le chiffrement d'une grande partie des postes de travail et serveurs du CHU. Très vite, le diagnostic tombe : c'est un rançongiciel.

Cédric Hamelin
Responsable adjoint à la sécurité du système d'information, CHU de Rouen

Durant la nuit du 11 au 12 octobre 2019, le groupe a fait l'objet d'une violente cyber attaque de type *ransomware*. Je passe sur le réveil très matinal pour un samedi, une actualité très chargée et la rédaction radio sous pression maximale, n'ayant plus d'accès Internet. La question « Que puis-je faire sans ordinateur ? » était dans tous les esprits. En à peine deux heures, tout le monde était sur le pont !

Jérôme Lefébure
CFO, membre du directoire en charge des métiers de support, Groupe M6

Dans la nuit du 10 au 11 avril 2019, une attaque par rançongiciel a obligé l'entreprise à couper toute liaison Internet et avec les ensembles applicatifs. Conséquence directe de l'attaque : arrêt total de l'activité pendant trois jours et fonctionnement en mode dégradé pendant deux semaines.

Laurent Babin
Responsable de la sécurité systèmes d'information, Fleury Michon

RÉDUIRE LE RISQUE D'ATTAQUE

Les mesures qui suivent, issues du Guide d'hygiène informatique *de l'ANSSI, permettront d'éviter qu'une attaque par rançongiciel atteigne l'organisation ou réduiront les pertes liées à une telle attaque.*

L'objectif principal d'un rançongiciel est d'empêcher la victime d'accéder à ses données, le plus souvent par le chiffrement de ces dernières. Devant cette menace, la réalisation de sauvegardes régulières des données apparait comme la mesure prioritaire pour réduire les pertes liées à une attaque par rançongiciel.

Parmi les mesures permettant de réduire significativement les risques d'infection et de propagation d'un rançongiciel sur l'ensemble du système d'information, citons : le maintien en condition de sécurité des socles système par l'application des correctifs de sécurité ; la mise à jour des signatures antivirus ; la mise en œuvre d'une politique de filtrage sur les postes de travail ; et la désactivation des droits d'administrateur pour les utilisateurs de ces postes.

Par ailleurs, l'application du principe de défense en profondeur sur les différents éléments du système d'information permettra de limiter le risque d'indisponibilité totale. Ce principe passe notamment par une segmentation réseau par zones de sensibilité et d'exposition des différents éléments du système d'information, par la limitation des privilèges accordés aux utilisateurs ou encore par la maîtrise des accès à Internet.

Enfin, sensibiliser les utilisateurs aux risques, évaluer l'opportunité de souscrire à une assurance cyber, préparer un plan de réponse aux cyberattaques et la stratégie de communication associée restent des actions importantes à mener.

SAUVEGARDER LES DONNÉES

Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques doivent être réalisées. Il s'agit de garder à l'esprit que ces sauvegardes peuvent aussi être affectées par un rançongiciel. En effet, de plus en plus de cybercriminels cherchent à s'en prendre aux sauvegardes pour limiter les possibilités pour la victime de retrouver ses données et ainsi maximiser les chances qu'elle paie la rançon.

Ces sauvegardes, au moins pour les plus critiques, doivent être déconnectées du système d'information pour prévenir leur chiffrement, à l'instar des autres fichiers. L'usage de solutions de stockage à froid, comme des disques durs externes ou des bandes magnétiques, permettent de protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité. À cet égard, il est important de noter que les architectures « *backup-less* [2] » protègent efficacement contre la destruction de données isolées, lorsqu'elle est due à une panne matérielle. En revanche, elles ne protègent pas contre les attaques ciblées par rançongiciel car les attaquants s'emploient à chiffrer les données de l'ensemble des serveurs.

2 Méthode d'utilisation de photographie du système (*snapshots*) pour protéger les données sans utiliser de logiciel de sauvegarde traditionnel.

MAINTENIR À JOUR LES LOGICIELS ET LES SYSTÈMES

Les vulnérabilités non corrigées des systèmes d'exploitation ou des logiciels présents sur le système d'information peuvent être utilisées pour infecter le système ou favoriser la propagation de l'infection. Des mises à jour incluant des correctifs de sécurité sont régulièrement publiées par les éditeurs de ces solutions. Il est crucial de les installer dans un délai court et selon un processus maîtrisé. En cas d'impossibilité avérée, pour des raisons métier par exemple, il s'agira de mettre en œuvre des mesures d'isolement pour les systèmes concernés.

Les logiciels installés sur les postes utilisateur (navigateurs web, suites bureautiques, lecteurs PDF, lecteurs multimédias, etc.) doivent faire l'objet d'une attention particulière. Il est donc important d'anticiper les échéances du cycle de vie des matériels et des logiciels présents sur votre système d'information afin de de les maintenir à jour.

De la même manière, les ressources exposées sur Internet non mises à jour (services de messagerie électronique, hébergement web, extranet, etc.) sont régulièrement exploitées par les attaquants. Il est donc essentiel de porter une attention toute particulière à l'application de correctifs de sécurité dans les plus brefs délais.

Par ailleurs, assurer une veille permanente permet de rester informé de la découverte des vulnérabilités logicielles et matérielles des services utilisés dans votre entité et de la disponibilité des correctifs. Le site web du CERT-FR (*www.cert.ssi.gouv.fr*) pourra vous aider dans cette démarche.

UTILISER ET MAINTENIR À JOUR LES LOGICIELS ANTIVIRUS

L'utilisation d'antivirus pour se protéger contre les rançongiciels reste aujourd'hui nécessaire sur les ressources exposées (exemple : postes de travail, serveurs de fichier, etc.). Ces outils ne garantissent pas de protéger votre entité de rançongiciels encore inconnus mais peuvent, dans la majorité des cas, empêcher une compromission et éviter le chiffrement de vos fichiers. Toutefois, pour que ces outils soient efficaces, il est important d'effectuer une mise à jour fréquente des signatures et du moteur du logiciel et de s'assurer régulièrement de l'absence de logiciel malveillant connu sur les espaces de stockage des fichiers de l'entité.

CLOISONNER LE SYSTÈME D'INFORMATION

Sans mesure de protection et à partir d'une seule machine infectée, le rançongiciel peut se propager sur l'ensemble de votre système d'information et infecter la plupart des machines accessibles. Sur un réseau informatique qui n'est pas cloisonné, un attaquant est susceptible de prendre le contrôle d'un grand nombre de ressources et ainsi amplifier les conséquences de l'attaque. Il pourrait par exemple accéder aux fonctions d'administration ou aux équipements réservés aux administrateurs.

Pour limiter le risque de propagation, il convient de mettre en place un ou plusieurs dispositifs de filtrage permettant un cloisonnement entre les différentes zones réseaux plus ou moins critiques du système d'information (exemple : zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, etc.).

Un cloisonnement des niveaux d'administration peut également être mis en place afin de s'assurer que les niveaux d'administration les plus hauts soient difficilement atteignables par les attaquants.

Par ailleurs, les connexions entre les postes des utilisateurs doivent être interdites par défaut. Configurer de façon *ad hoc* le pare-feu logiciel des postes de travail empêchera les flux de données entre ces postes et permettra de réduire le risque de propagation du rançongiciel.

> Quand le diagnostic tombe et confirme l'attaque, la tension est très forte et nos premières décisions sont 100 % opérationnelles. Nos équipes d'astreinte ont d'abord coupé le lien entre l'attaquant et notre réseau par des mesures de fermeture des cloisons et d'isolement.
>
> Jérôme Lefebure

LIMITER LES DROITS DES UTILISATEURS ET LES AUTORISATIONS DES APPLICATIONS

Une première bonne pratique consiste à vérifier que les utilisateurs ne sont pas administrateurs de leur poste de travail. Ainsi, l'installation de logiciels et l'exécution involontaire de codes malveillants seront impossibles par défaut.

Une autre bonne pratique consiste à dédier et à limiter les comptes d'administration sur les ressources du système d'information et à mettre en place des postes de travail dédiés à l'administration, sans accès à Internet. En effet, lors d'une compromission, on constate que les attaquants s'emploient souvent à accéder à ces comptes privilégiés. Les actions de propagation du rançongiciel au sein du système d'information sont généralement réalisées à l'aide de comptes d'administration, notamment lors des attaques de type « *Big Game Hunting* ». Il est donc nécessaire de limiter le nombre de ces comptes au strict nécessaire et de porter une attention particulière à l'utilisation qui en est faite. Ces restrictions empêcheront le rançongiciel de s'exécuter ou limiteront sa capacité à chiffrer les fichiers.

Afin de réduire d'avantage le risque d'une attaque par rançongiciel, il est recommandé de procéder au durcissement [3] de la configuration des équipements suivants : postes de travail, serveurs et applications les plus courantes, en particulier celles exposées sur Internet ou traitant des données en provenance d'Internet. Parmi les règles de sécurité supplémentaires applicables, les stratégies de restriction d'exécution logicielle (Windows Defender ATP et Applocker sous Windows) permettent de limiter l'exécution de logiciels malveillants.

3 Consiste à améliorer la sécurité d'un système, d'un réseau ou d'une application via la fortification de sa configuration ou de sa structure en réduisant le nombre d'objets (utilisateurs, services, bibliothèques, applications, etc.) présents sur le système, en ne gardant que ceux qui sont nécessaires au bon fonctionnement de l'équipement et du service rendu par ce dernier.

MAÎTRISER LES ACCÈS INTERNET

Les rançongiciels utilisent souvent les accès Internet des entités pour communiquer avec une infrastructure hébergée en ligne par les cybercriminels. Par ailleurs, en naviguant sur un site web compromis, un collaborateur pourra sans le savoir télécharger et provoquer l'installation automatique du programme malveillant sur son poste de travail.

Aussi, la mise en œuvre d'une passerelle Internet sécurisée permettant de bloquer les flux illégitimes avec des relais applicatifs incontournables implémentant des fonctions de sécurité (exemple : serveur mandataire pour les accès web, résolveur DNS pour les requêtes de noms de domaine publics) réduira les risques relatifs aux rançongiciels. Ce relai pourra notamment permettre de filtrer les tentatives de connexion en fonction de la catégorisation ou de la réputation des sites que vos collaborateurs tentent de visiter et identifier les activités anormales (exemple : transmission d'un volume de données important depuis le système d'information vers un serveur étranger à la structure et à ses prestataires de service).

> D'un point de vue purement technique, les premières actions entreprises ont été de couper tout accès à Internet et d'interrompre les applicatifs. Aussitôt, nous nous sommes attachés à qualifier avec précision le périmètre concerné par l'attaque et avons organisé la communication pour informer les équipes de l'incident et de son impact sur leur activité.
>
> Laurent Babin

METTRE EN ŒUVRE UNE SUPERVISION DES JOURNAUX

Assurer une supervision des incidents de sécurité informatique nécessite de mettre en place une politique de journalisation sur les différentes ressources du système d'information. Elle comprend les serveurs d'infrastructure système, les postes d'administration et postes utilisateur, les serveurs métier et les équipements réseau et de sécurité situés en périphérie ou au cœur du système d'information (en particulier sur les serveurs Active Directory, les serveurs DNS, la messagerie et les proxys web).

Cette politique doit permettre d'enregistrer les évènements générés par les différents services hébergés. En complément, elle doit permettre d'enregistrer les évènements associés à l'authentification, à la gestion des comptes et des droits (une attention particulière doit être portée aux objets associés à de forts privilèges), à l'accès aux ressources, aux modifications des stratégies de sécurité ainsi qu'à l'activité des processus et du système sous-jacent.

Un système de supervision des évènements journalisés doit être mis en place. Il permettra de détecter une éventuelle compromission et de réagir le plus tôt possible pour éviter le chiffrement des données par l'attaquant. Par ailleurs, en cas d'incident, ces évènements permettront de gagner du temps dans la compréhension de l'incident.

> À son arrivée, l'ANSSI s'est attachée, avec nos équipes DSI et techniques, à comprendre l'attaque en vue de reconstruire différemment. Le redémarrage des systèmes s'est ensuite fait par étapes : la messagerie au bout d'une semaine, les applicatifs métiers par ordre de priorité…
>
> Jérôme Lefébure

SENSIBILISER LES COLLABORATEURS

Le plus souvent, l'attaque par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace même si elle ne constitue pas un rempart absolu. L'objectif est également de faire naître ou de renforcer certains réflexes chez les utilisateurs en les invitant à signaler au service informatique de l'organisation tout élément suspect (exemple : pièce-jointe ou courriel douteux, clé USB offerte, requêtes inhabituelles, etc.).

Selon les caractéristiques de l'organisation (taille et effectifs, sensibilité de l'activité et enjeux, niveau de connaissance des collaborateurs, moyens de communication disponibles, etc.), des opérations de sensibilisation de différentes natures peuvent être envisagées : réunions d'information, quizz, campagnes d'affichage ou encore distribution de guides de bonnes pratiques. Pour accompagner les organisations dans la mise en œuvre de telles initiatives, plusieurs entités publiques, dont l'ANSSI ou cybermalveillance.gouv.fr (cf. ressources utiles), mettent à disposition de nombreuses ressources pédagogiques adaptées à chaque public.

L'expérience a montré que les équipes informatiques doivent aussi être sensibilisées sur leur utilisation spécifique des outils d'administration. En effet, les administrateurs possèdent des droits plus élevés sur le système d'information. À ce titre, ils sont une cible privilégiée pour un attaquant bien informé. Il est donc important de former cette population sur les mesures d'hygiène informatique à mettre en œuvre en matière d'administration en vue d'éviter une compromission rapide de l'ensemble du système.

> Dans ces moments-là (quand survient une attaque), on réalise à quel point un tel événement traumatise et rapproche à la fois les hommes…
>
> Jérôme Lefébure

ÉVALUER L'OPPORTUNITÉ DE SOUSCRIRE À UNE ASSURANCE CYBER

Aujourd'hui, les contrats d'assurance cyber permettent d'accompagner les entités victimes de cyberattaques en leur fournissant, en cas de sinistre, une assistance juridique ainsi qu'une couverture financière du préjudice (matériel, immatériel, etc.). Cependant, le marché est encore naissant et doit poursuivre son développement, en particulier en matière de jurisprudence concernant l'activation ou non des clauses d'exclusion.

> Passés ces « gestes de premiers secours », nous avons contacté notre assurance qui nous a mis en rapport avec des juristes et des experts en SSI pour nous accompagner vers la sortie de crise. Ainsi, nous avons pu identifier l'origine de l'attaque et sécuriser l'environnement.
>
> Laurent Babin

METTRE EN ŒUVRE UN PLAN DE RÉPONSE AUX CYBERATTAQUES

La spécificité des attaques par rançongiciel est leur potentiel effet déstabilisateur sur les organisations. Les fonctions support comme la téléphonie, la messagerie mais aussi les applications métier peuvent être mises hors d'usage. Il s'agit alors de passer en fonctionnement dégradé et dans certains cas, cela signifie revenir au papier et au crayon. L'attaque cause en général une interruption d'activité partielle et, dans les cas les plus graves, une interruption totale.

> De nouveaux canaux de communication interne ont été mis en place pour prévenir les collaborateurs et maintenir le contact au cours des prochains jours. Cela allait de la messagerie instantanée au papier-crayon et aux déplacements de bureaux en bureaux.
>
> Jérôme Lefébure

Il est donc crucial pour les organisations de définir un plan de réponse aux cyberattaques associé au dispositif de gestion de crise – quand il existe – visant à assurer la continuité d'activité puis son retour à un état nominal. La mise en œuvre d'un plan de continuité informatique doit permettre à votre organisation de continuer à fonctionner quand survient une altération plus ou moins sévère du système d'information. Des moyens de communication de secours propres au plan de continuité informatique doivent être sérieusement envisagés. Le plan de reprise informatique vise, quant à lui, à remettre en service les systèmes d'information qui ont dysfonctionné. Il doit notamment prévoir la restauration des systèmes et des données. ▶

> Au moment de l'attaque, nous disposions déjà d'une procédure de gestion des incidents de sécurité mise à jour quelques mois auparavant. Nous avons donc pu la mettre en œuvre très rapidement à travers le déclenchement successif de trois niveaux d'astreinte et la constitution de la cellule de crise.
>
> Cédric Hamelin

Le plan de réponse dans sa globalité doit régulièrement être actualisé et éprouvé à l'aide d'exercices. L'élaboration du plan et les exercices doivent impliquer toutes les parties prenantes de l'organisation, les domaines fonctionnels, les domaines techniques et la direction.

> Tout au long de la crise, il faut saluer la réactivité et la mobilisation de nombreux collaborateurs. Lorsque c'est arrivé, le groupe disposait déjà d'une cellule de crise mais celle-ci n'avait jamais anticipé la survenance d'une cyberattaque parmi ses scénarios de crise.
>
> Laurent Babin

PENSER SA STRATÉGIE DE COMMUNICATION DE CRISE CYBER

Pour faire face à une attaque par rançongiciel, il est essentiel de définir la stratégie de communication globale de l'organisation qu'il serait nécessaire d'adopter dès les premières heures pour limiter les impacts de la crise sur l'image et la réputation de l'entité, tant en interne qu'en externe.

> La communication externe assurée au niveau du groupe et la communication interne ont été maitrisées, bien qu'un effort reste à faire en matière d'éléments de langage. Le temps de la pédagogie est essentiel afin d'expliquer comment on fait les choses et pourquoi.
>
> Laurent Babin

L'élaboration d'une stratégie de communication de crise adaptée repose sur la mise en relation préalable des équipes « métiers » (chaine de production, finances, juridique, communication, logistique, etc.) et des personnes en charge de la sécurité numérique. Ensemble, elles définiront un plan d'action et des messages adaptés à présenter à la direction de l'entité. Par exemple, un communicant disposera d'une connaissance fine de l'audience (interne et externe) de l'entité ainsi que des moyens de communication disponibles. Le responsable informatique sera, quant à lui, capable de rendre compte en temps réel de la situation et de ses possibles évolutions. Informer et rassurer, en adoptant une posture de transparence, doit être au cœur de la stratégie de communication de crise.

Ensemble, ils peuvent élaborer une stratégie qui prend en compte :

- la cartographie des publics et les objectifs de communication associés : public interne, clients, partenaires, autorités, grand public/médias ;

- la cartographie des parties prenantes de la communication avec qui il sera nécessaire de se coordonner : prestataires, filiales, autorités, etc. ;
- les actions à mener à court, moyen et long terme vis-à-vis de l'externe (relations presse, communication web, etc.) comme des collaborateurs.

Dans le cas d'un rançongiciel, les moyens classiques de communication peuvent être indisponibles, ce qui contribue à la déstabilisation des équipes. À noter que la communication de crise peut être testée lors des exercices de gestion d'une crise d'origine cyber afin de vérifier la cohérence et la pertinence de la stratégie de communication définie en anticipation.

> Une fois les choses rentrées dans l'ordre, nous avons cherché à savoir de quelle manière cela avait été vécu en interne. Sur le site industriel, les collaborateurs ont la vision d'une crise surmontée avec professionnalisme. Pour les fonctions supports et filiales en revanche, les impressions sont plus nuancées. Certains déplorent un manque de communication et de coordination ainsi qu'une récupération trop tardive des applicatifs.
>
> Laurent Babin

RÉAGIR EN CAS D'ATTAQUE

L'objectif des mesures qui suivent est d'aider les organisations victimes à réagir à une attaque par rançongiciel. Les premières actions techniques proposées, quand elles sont mises en œuvre rapidement, permettent de réduire les pertes liées à une telle attaque.

ADOPTER LES BONS RÉFLEXES

Le premier réflexe est d'ouvrir une main courante permettant de tracer les actions et les évènements liés à l'incident. Chaque entrée de ce document doit contenir, à minima :

- l'heure et la date de l'action ou de l'évènement ;
- le nom de la personne à l'origine de cette action ou ayant informé sur l'évènement ;
- la description de l'action ou de l'évènement.

Ce document doit permettre à tout moment de renseigner les décideurs sur l'état d'avancement des actions entreprises.

> La tenue d'une main courante régulièrement alimentée tout au long de l'incident a considérablement facilité le suivi des actions à chaque étape. Par la suite, cette main courante nous a été d'une aide précieuse pour mener des RETEX et relever les axes d'améliorations.
>
> Cédric Hamelin

Afin d'éviter une propagation du rançongiciel sur les autres équipements informatiques de l'entité, il est important de déconnecter au plus tôt vos supports de sauvegardes après vous être assurés qu'ils ne sont pas infectés et d'isoler les équipements infectés du SI en les déconnectant du réseau. Il peut être utile de vérifier la présence ou non d'une éventuelle connexion sans fil sur ces équipements et, le cas échéant, de la désactiver.

Afin de couper l'accès de votre système d'information à un attaquant agissant depuis Internet, il est important d'isoler votre système d'information en bloquant toutes les communications vers et depuis Internet. Ainsi, l'attaquant ne sera plus en mesure de piloter son rançongiciel ni de déclencher une nouvelle vague de chiffrement. Cela évitera également l'exfiltration éventuelle de données. Cette mesure peut avoir des conséquences importantes sur l'activité de l'entité (perte d'accès à certaines applications externalisées, gel de l'envoi de courriels avec l'extérieur, etc.) qu'il convient de gérer en parallèle.

> L'une des premières actions mises en œuvre a été de couper les accès au réseau Internet et au réseau interne puis d'isoler tous les composants non impactés, à commencer par les sauvegardes, les bases de données ainsi que les baies de stockages.
>
> Cédric Hamelin

Une fois les programmes malveillants à l'origine de l'infection identifiés, il sera possible de rechercher dans les journaux du système d'information les éventuelles caractéristiques de ceux-ci (exemple : URL utilisées pour communiquer avec l'infrastructure de l'attaquant, nom de fichier, condensat, objet du courrier électronique, etc.). Ces éléments pourront être utilisés sur les passerelles applicatives ou sur les équipements de filtrage réseau pour éviter de nouvelles infections. En particulier, si une adresse IP est identifiée comme étant malveillante, il sera possible de mettre en place une règle au niveau des pare-feux.

Si l'ensemble des fichiers d'une machine ont été chiffrés, son extinction électrique peut réduire les chances de retrouver dans la mémoire de l'équipement des éléments permettant de recouvrer les fichiers chiffrés. Si la machine infectée le permet, il est donc recommandé d'activer la mise en veille prolongée afin de faire cesser l'activité du programme malveillant tout en préservant la mémoire en vue d'une analyse ultérieure.

Afin de limiter la diffusion du rançongiciel et le chiffrement de données sur de nouvelles machines, il est préférable de laisser éteints les équipements non démarrés (par exemple : retour de congés d'un employé ou démarrage d'une machine en début de journée) et d'interdire l'utilisation de supports de stockage amovibles (clé USB, disque dur externe, etc.).

Malgré le chiffrement des données par le rançongiciel, il est possible qu'une solution de chiffrement soit découverte et rendue publique ultérieurement. Aussi, il est important de conserver les données chiffrées. Le projet ***No More Ransom***, d'Europol, du National High Tech Crime Unit de la police néerlandaise et de l'éditeur McAfee recense les moyens de déchiffrement applicables à un grand nombre de rançongiciels.

PILOTER LA GESTION DE LA CRISE CYBER

Les enjeux induits par une telle attaque vont bien au-delà de la perte de données ou du paiement d'une rançon. En effet, les organisations victimes doivent faire face à de nombreuses autres conséquences, c'est pourquoi il est recommandé de mettre en place une cellule de crise au plus haut niveau de l'organisation, indépendante des groupes de travail opérationnels qui auront des responsabilités de pilotage et d'exécution.

Cette cellule aura pour objectif de répondre aux enjeux de niveau stratégique de la crise en établissant, par exemple, les stratégies de communication interne comme externe et les éléments à fournir en vue de la judiciarisation ou de la notification règlementaire, notamment pour la Commission nationale de l'informatique et des libertés (CNIL) en cas de violation de données personnelles. Dans ce dernier cas, avec l'appui du délégué à la protection des données (DPO), cette cellule devra identifier le niveau de risque engendré pour les personnes dont les données sont concernées par la violation et les avertir en conséquence (employés, clients, membres, etc.). Plus globalement, cette cellule aura également pour mission d'identifier les impacts de ces dysfonctionnements sur les activités de l'organisation et d'organiser la réponse dans ces champs.

> Pour garantir la sécurité des patients, les urgences non vitales ont été déportées vers d'autres établissements le temps de reconstruire les applications critiques. Et pour préserver l'activité des personnels, la cellule de crise de la DSI était gouvernée par quatre personnes pour absorber la pression résultant de l'incident et assurer l'interface avec les différentes parties prenantes impliquées.
>
> Cédric Hamelin

TROUVER DE L'ASSISTANCE TECHNIQUE

Certaines entités ne disposent ni des ressources ni de l'expertise nécessaires pour traiter un incident de sécurité. En ces circonstances, elles pourront faire appel à des prestataires spécialisés dans la réponse aux incidents de sécurité.

Pour les particuliers et les petites entreprises, le Gouvernement a mis en place la plateforme cybermalveillance.gouv.fr qui permet d'entrer en contact avec des prestataires de proximité [4].

> Sur place, plusieurs prestataires sont intervenus. Si certains fournisseurs et éditeurs de solutions nous ont accompagnés dans le cadre du contrat de maintenance que nous avons avec eux, d'autres sociétés, notamment locales, nous ont proposé leur aide de manière spontanée.
>
> Cédric Hamelin

> Des prestataires nous ont très vite rejoints pour procéder à la phase de reconstruction. Ils ont fait preuve d'un fort niveau d'engagement à nos côtés.
>
> Laurent Babin

> Il est évident que nous ne pouvions pas faire face seuls à la situation. Le matin du 12 octobre, nous avons donc fait appel à l'ANSSI, à un cabinet forensic pour amorcer l'analyse et au C3N pour déposer une plainte, sans oublier de déclarer le sinistre à la CNIL et à notre assureur.
>
> Jérôme Lefébure

4 https://ssi.gouv.fr/en-cas-dincident/

COMMUNIQUER AU JUSTE NIVEAU

En cas d'attaque avérée, la stratégie de communication définie par anticipation, voire testée, en amont par les équipes « métiers » et les équipes techniques peut être déployée en lien avec la direction.

Pour définir les postures et les actions à mener, il est important de s'appuyer sur le contexte dans lequel s'inscrit l'attaque : état des lieux technique, médiatique (presse spécialisée cyber) et social (perception interne) au moment de l'attaque, scénarios d'évolution, etc.

Également, il est nécessaire de penser très rapidement à l'accompagnement des collaborateurs et des collaboratrices par une communication interne adaptée. La présence du rançongiciel se manifeste souvent par l'affichage sur les écrans d'une demande de rançon, voire d'un décompte. Ce mode opératoire génère très souvent émoi et anxiété chez l'entité victime.

Une position de prudence consiste à demander aux collaborateurs d'appliquer la clause de confidentialité de leur contrat de travail concernant les différentes sollicitations et les publications médiatiques (média, réseaux sociaux, etc.). Dans tous les cas, il est nécessaire de s'assurer que les collaborateurs transmettent toutes les sollicitations extérieures au service communication de l'entité ou, à défaut, au dirigeant responsable.

> Tout au long de la crise, un réel effort de transparence et de communication de la DSI vers les personnels et services les plus critiques (urgences, SAMU…) a été fourni et apprécié. Nous avons également informés de la situation le FSSI du ministère de la Santé ainsi que le CERT-FR avec qui nous sommes entrés en relation sur les conseils du délégué territorial ANSSI de notre région.
>
> Cédric Hamelin

NE PAS PAYER LA RANÇON

Il est recommandé de ne jamais payer la rançon. Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux. De plus, le paiement de la rançon n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels.

Par ailleurs, l'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (exemple : un fichier de base de données).

DÉPOSER PLAINTE

Lors d'une attaque par rançongiciel, il est fortement recommandé de déposer plainte auprès des services de police ou de gendarmerie. D'une part, un dépôt de plainte permet de réaliser une enquête suivie d'une « chasse aux clés » à l'issue de laquelle il sera éventuellement possible de déchiffrer les données altérées. D'autre part, le dépôt de plainte conditionne généralement la réparation du sinistre et peut permettre d'identifier, d'interpeller et de présenter les auteurs de l'attaque à la Justice.

Les éléments suivants peuvent être demandés ou pourront être recherchés dans le cadre de l'enquête. En fonction du profil de votre entité, ils peuvent diverger :

- le détail et la chronologie des événements relatant l'incident (la main courante), notamment la date de la demande de rançon et les faits constatés ;
- les emplacements des appareils potentiellement infectés ;
- les journaux de sécurité associés à l'incident ;
- l'analyse technique de l'attaque ;
- la collecte d'échantillons de fichiers chiffrés ;
- la préservation des supports ou des machines (quand c'est possible) sur lesquels le rançongiciel s'est exécuté (disque système) ;
- les adresses de messagerie électronique et adresses de cryptomonnaie fournies par les cybercriminels ;
- le texte de demande de rançon ;
- les coordonnées des témoins de l'incident.

Le dépôt de plainte doit être réalisé au nom de l'entité. Si l'opération est confiée à un collaborateur, il sera nécessaire de préparer une délégation de pouvoir pour cette personne, signée par un représentant légal de la personne morale afin de permettre le dépôt de plainte.

Le ministère de l'Intérieur ouvrira une plateforme de plainte en ligne en matière d'escroqueries sur Internet appelée « THESEE ». Les objectifs de cette plateforme seront :

- d'améliorer le service rendu aux victimes d'escroqueries sur Internet ;
- de soulager les services territoriaux de la réception d'un grand nombre de plaintes ;
- d'améliorer la lutte contre ces escroqueries par la centralisation, l'analyse et le regroupement de ces plaintes ou signalements.

Les infractions commises sur Internet à l'encontre d'un particulier, dont les attaques par rançongiciels, pourront également être déclarées sur cette plateforme.

RESTAURER LES SYSTÈMES DEPUIS DES SOURCES SAINES

Concernant les équipements infectés, il est préférable de réinstaller le système sur un support connu et de restaurer les données depuis les sauvegardes effectuées, de préférence, antérieures à la date de compromission du système. Il s'agit de vérifier que les données restaurées ne sont pas infectées par le rançongiciel. L'efficacité ou l'innocuité de méthodes de nettoyage alternatives sont difficiles à qualifier. Les règles de sécurité suivantes doivent être appliquées sur le support de restauration et sur l'ensemble des machines saines :

- la vulnérabilité intialement utilisée par l'attaquant doit être corrigée afin d'éviter une nouvelle infection (exemple : mise à jour logicielle, modification de la politique de filtrage réseau) ;
- si les recherches ont permis d'identifier le rançongiciel, vérifier l'absence des modifications réalisées par le programme malveillant afin de se maintenir après le redémarrage d'une machine précédemment infectée (exemple : valeurs de registre et fichiers malveillants) ;
- changer les mots de passe ;
- appliquer les mesures de prévention présentées dans ce guide.

ILS VOUS CONSEILLENT

Aujourd'hui, il est important de rappeler aux organisations du secteur de la santé comme aux autres que l'on n'est pas tout seuls pour faire face à ce type de situations. Il ne faut pas hésiter à se faire assister et solliciter un avis extérieur.

Cédric Hamelin
Responsable adjoint à la sécurité du système d'information, CHU de Rouen

Je n'ai pas un mais trois conseils à partager. 1) Gérer une crise cyber, c'est à la fois mettre en œuvre un plan et jouer une partition non écrite. Sur ces deux volets, rien ne se fait seuls ! 2) Rester calme (ne marche que si l'on n'est pas seuls). 3) D'un point de vue plus organisationnel enfin, cette expérience m'a conforté dans l'idée qu'un RSSI doit avoir un accès direct et facilité à tous les acteurs de la gestion de crise – directions et managers compris – pour préparer l'organisation à ces épreuves et y réagir le cas échéant.

Jérôme Lefébure
CFO, membre du directoire en charge des métiers de support, Groupe M6

Préparez-vous sera mon dernier conseil !
On ne peut pas s'en sortir tout seul.

Laurent Babin
Responsable de la sécurité du système d'information, Fleury Michon

RESSOURCES UTILES

ANSSI

- **État de la menace sur les rançongiciels de l'ANSSI :** www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001
- **Guide d'hygiène informatique de l'ANSSI :** www.ssi.gouv.fr/guide/guide-dhygiene-informatique
- **Guide sur la maîtrise des risques numériques de l'ANSSI et de l'AMRAE :** www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf
- **Guide EBIOS Risk manager et son supplément :** www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide
- **Page du site Internet de l'ANSSI à propos des prestataires de réponse aux incidents de sécurité :** www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris

CYBERMALVEILLANCE.GOUV.FR

- **Fiche sur « les mises à jour » de Cybermalveillance :** www.cybermalveillance.gouv.fr/medias/2020/04/fiche_mises_a_jour.pdf
- **Fiche sur « les sauvegardes » de Cybermalveillance :** www.cybermalveillance.gouv.fr/medias/2020/04/fiche_sauvegardes.pdf

- **Fiche sur « les rançongiciels » de Cybermalveillance :** www.cybermalveillance.gouv.fr/medias/2020/04/fiche_ran%C3%A7ongiciels.pdf

COLLECTIF

- **NoMoreRansom :** www.nomoreransom.org

CNIL

- **Guide sur la sécurité des données personnelles :** www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles
- **Notifier une violation de données personnelles :** www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- **Fiche « sauvegarder et prévoir la continuité d'activité » :** www.cnil.fr/fr/securite-sauvegarder-et-prevoir-la-continuite-dactivite

REMERCIEMENTS

Nous remercions chaleureusement la direction des Affaires criminelles et des grâces pour avoir encouragé ce partenariat resserré entre nos deux institutions au service de la protection des organisations et citoyens français face aux rançongiciels.

Parce que cette forme de cybercriminalité en plein essor ne s'appréhende correctement qu'au moyen de plusieurs éclairages, un grand merci au dispositif Cybermalveillance.gouv.fr, à la Brigade d'enquêtes sur les fraudes aux technologies de l'information, à la CNIL ainsi qu'à la direction centrale de la Police judiciaire pour la richesse de leurs contributions.

Enfin et surtout, car c'est là que résident l'originalité et la force de ce document : merci à Laurent Babin, Cédric Hamelin et Jérôme Lefébure pour le récit de leur expérience. Tous étaient en première ligne quand, sans crier gare, leurs organisations ont vu leur quotidien basculer après la survenance d'une attaque par rançongiciel. Vos témoignages sont rares, précieux et contribuent sans commune mesure à la prise de conscience du risque !

« Durant la nuit du 11 au 12 octobre 2019, le groupe a fait l'objet d'une violente cyberattaque de type *ransomware*. [...] La question "Que puis-je faire sans ordinateur ?" était dans tous les esprits. En à peine deux heures, tout le monde était sur le pont ! »

Jérôme Lefébure, groupe M6

Industrie, médias, hôpitaux... Peu importe le secteur d'activité, les cyberattaques n'épargnent personne. En la matière, l'essor des rançongiciels inquiète et mobilise au plus haut niveau de l'État. En appelant à ne pas laisser impunis les auteurs de ces actes et en réunissant témoignages de victimes et bonnes pratiques de sécurité numérique, ce guide donne un coup de projecteur puissant sur cette menace et invite les organisations – du comité exécutif aux collaborateurs – à se saisir de ces questions.

Version 1.0 – Août 2020 – **ANSSI-GP-077**

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr