GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE

12 règles essentielles pour sécuriser vos équipements numériques

cpme CONFÉDÉRATION DES PME

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

La cybersécurité est un facteur de productivité, de compétitivité et donc de croissance pour les entreprises.

Quelle que soit sa taille, une PME doit prendre conscience qu'elle peut être à tout moment confrontée à la cybercriminalité. Qu'il s'agisse, par exemple, de malveillances visant à la destruction de données ou d'espionnage économique et industriel, les conséquences des attaques informatiques pour les entreprises, et plus particulièrement les TPE, sont généralement désastreuses et peuvent impacter leur pérennité.

Pour la CPME, chaque entreprise doit aujourd'hui se doter d'une politique de sécurisation des systèmes d'information inhérente à l'usage des nouvelles technologies.

Si les contraintes financières des petites structures restent un frein à la construction d'une cybersécurité optimale, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique.

Pour recenser ces usages, la Confédération, par le biais de sa Commission Economie Numérique, s'est rapprochée de l'ANSSI.

Fruit d'un partenariat constructif, un guide des bonnes pratiques informatiques a été élaboré afin de sensibiliser les PME sur cette problématique tout en leur apportant les moyens opérationnels de préserver leurs systèmes d'information.

A vous désormais, chefs d'entreprises, de devenir les acteurs de votre propre sécurité !

François Asselin
Président CPME

Qu'il s'agisse de la numérisation des dossiers de la patientèle d'un cabinet médical, des nouvelles possibilités de paiement en ligne, de la multiplication des échanges par courriel, l'usage de l'informatique s'est généralisé dans les TPE/PME. Corollaire de cette formidable évolution, de nouveaux risques ont émergé : vol de données, escroqueries financières, sabotage de sites d'e-commerce. Leurs conséquences peuvent être lourdes : indisponibilités, coût, atteinte à l'image de l'entreprise et perte de clientèle.

La complexité des menaces, le coût, le manque de personnel et de temps sont souvent autant d'arguments pour justifier un moindre intérêt porté à la sécurité informatique au sein des petites structures. Ces questions sont pourtant essentielles et relèvent souvent de réflexes simples. Il ne faut pas oublier que devoir remédier à un incident dans l'urgence peut s'avérer bien plus coûteux que leur prévention. Les mesures accessibles aux non-spécialistes décrites dans ce guide concourent à une protection globale de l'entreprise, qu'il s'agisse de ses brevets, de sa clientèle, de sa réputation et de sa compétitivité.

La sensibilisation aux enjeux de sécurité informatique de chaque acteur, notamment dans le domaine économique, est au cœur des préoccupations de l'Agence nationale de la sécurité des systèmes d'information. C'est donc tout naturellement que l'ANSSI a souhaité s'associer avec la CPME (Confédération générale du patronat des petites et moyennes entreprises) pour apporter une expertise qui coïncide avec la réalité rencontrée par les petites structures, dont je n'oublie pas qu'elles constituent 90 % des entreprises françaises. Ce partenariat fructueux nous permet de vous présenter aujourd'hui ce « Guide des bonnes pratiques informatiques » à destination des PME.

Les douze recommandations pratiques qu'il présente sont issues de l'observation directe d'attaques réussies et de leurs causes. Dirigeants et entrepreneurs, n'hésitez pas à vous les approprier pour les mettre en œuvre au sein de vos structures.

Vous souhaitant bonne lecture,

Guillaume Poupard

Directeur général – Agence nationale de la sécurité des systèmes d'information

TABLE DES MATIERES

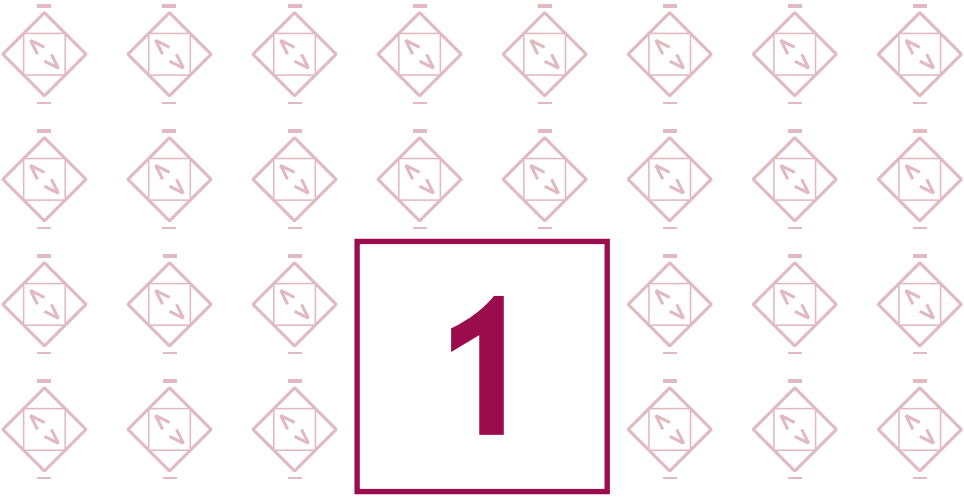
Pourquoi sécuriser son informatique ?

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages. Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les entreprises. Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours…) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable. La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau…). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise. Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre dans l'entreprise. À cet effet, la sensibilisation des collaborateurs de l'entreprise aux règles d'hygiène informatique est fondamentale et surtout très efficace pour limiter une grande partie des risques.

Réalisé par le biais d'un partenariat entre l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et la CPME, ce guide a pour objectif de vous informer sur les risques et les moyens de vous en prémunir en acquérant des réflexes simples pour sécuriser votre usage de l'informatique. Chaque règle ou « bonne pratique » est accompagnée d'un exemple inspiré de faits réels auxquels l'ANSSI a été confrontée.

*Les mots en italique marqués d'un * sont expliqués dans le glossaire situé à la fin de ce guide.*



Choisir avec soin ses mots de passe

Dans le cadre de ses fonctions de comptable, Julien va régulièrement consulter l'état des comptes de son entreprise sur le site Internet mis à disposition par l'établissement bancaire. Par simplicité, il a choisi un mot de passe faible : 123456. Ce mot de passe a très facilement été reconstitué lors d'une attaque utilisant un outil automatisé : l'entreprise s'est fait voler 10 000 euros.

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance…) et ne figurant pas dans le dictionnaire.

Deux méthodes simples peuvent vous aider à définir vos mots de passe :

- La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;
- La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » : aE2lP,lJ2Géa!

Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle…) ne doivent jamais être réutilisés pour d'autres services.

Il est préférable de ne pas recourir aux outils de stockage de mots de passe. A défaut, il faut s'en tenir à une solution ayant reçu une certification de premier niveau (CSPN)

En entreprise :

- déterminez des règles de choix et de dimensionnement (longueur) des mots de passe et faites les respecter ;
- modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box…) ;
- rappelez aux collaborateurs de ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;
- sensibilisez les collaborateurs au fait qu'ils ne doivent pas préenregistrer leurs mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements…).

2

Mettre à jour régulièrement vos logiciels

Carole, administrateur du système d'information d'une PME, ne met pas toujours à jour ses logiciels. Elle a ouvert par mégarde une pièce jointe piégée. Suite à cette erreur, des attaquants ont pu utiliser une vulnérabilité logicielle et ont pénétré son ordinateur pour espionner les activités de l'entreprise.*

Dans chaque système d'exploitation* (Android, IOS, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs* des mises à jour* de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

Il convient donc, au sein de l'entreprise, de mettre en place certaines règles :

- définissez et faites appliquer une politique de mises à jour régulières :
  - » S'il existe un service informatique au sein de l'entreprise, il est chargé de la mise à jour du système d'exploitation et des logiciels ;
  - » S'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du chef d'entreprise.
- configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles ;
- utilisez exclusivement les sites Internet officiels des éditeurs.

3

Bien connaître ses utilisateurs et ses prestataires

Noémie naviguait sur Internet depuis un compte administrateur de son entreprise. Elle a cliqué par inadvertance sur un lien conçu spécifiquement pour l'attirer vers une page web infectée. Un programme malveillant s'est alors installé automatiquement sur sa machine. L'attaquant a pu désactiver l'antivirus de l'ordinateur et avoir accès à l'ensemble des données de son service, y compris à la base de données de sa clientèle.*

Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur »* et les droits dits « d'administrateur »*.

- Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels de bureautique, de jeu,…), prenez un compte utilisateur. Il répondra parfaitement à vos besoins.
- Le compte administrateur n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels,…).

Les systèmes d'exploitation récents vous permettent d'intervenir facilement sur le fonctionnement global de votre machine sans changer de compte : si vous utilisez un compte utilisateur, le mot de passe administrateur est demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur.

Au sein de l'entreprise :

- réservez l'utilisation au service informatique, si celui-ci existe ;
- dans le cas contraire, protégez-en l'accès, n'ouvrez pour les employés que des comptes utilisateur, n'utilisez pas le compte administrateur pour de la navigation sur Internet ;
- identifiez précisément les différents utilisateurs du système et les privilèges qui leur sont accordés. Tous ne peuvent pas bénéficier de droits d'administrateur ;
- supprimez les comptes anonymes et génériques (stagiaire, contact, presse, etc.). Chaque utilisateur doit être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur ;
- encadrez par des procédures déterminées les arrivées et les départs de personnel pour vous assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et surtout qu'ils sont révoqués lors du départ de la personne.

4

Effectuer des sauvegardes régulières

Patrick, commerçant, a perdu la totalité de son fichier client suite à une panne d'ordinateur. Il n'avait pas effectué de copie de sauvegarde.

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un CD ou un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports.

Avant d'effectuer des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud » ou « informatique en nuage »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques :

- » risques pour la confidentialité des données,
- » risques juridiques liés à l'incertitude sur la localisation des données,
- » risques pour la disponibilité et l'intégrité des données,
- » risques liés à l'irréversibilité des contrats.

- soyez vigilant en prenant connaissance des conditions générales d'utilisation de ces services. Les contrats proposés dans le cadre des offres génériques ne couvrent généralement pas ces risques ;
- autant que possible, n'hésitez pas à recourir à des spécialistes techniques et juridiques pour la rédaction des contrats personnalisés et appropriés aux enjeux de votre entreprise ;
- veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement* avant de les copier dans le « cloud ».

Pour en savoir plus, consultez le guide sur l'externalisation et la sécurité des systèmes d'information réalisé par l'ANSSI.

5

Sécuriser l'accès Wi-Fi de votre entreprise

La borne d'accès à Internet (box) de la boutique de Julie est configurée pour utiliser le chiffrement WEP. Sans que Julie ne s'en aperçoive, un voisin a réussi en moins de deux minutes, à l'aide d'un logiciel, à déchiffrer la clé de connexion. Il a utilisé ce point d'accès Wi-Fi pour participer à une attaque contre un site Internet gouvernemental. Désormais, Julie est mise en cause dans l'enquête de police.*

L'utilisation du Wi-Fi est une pratique attractive. Il ne faut cependant pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes malintentionnées. Pour cette raison l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise : une installation filaire reste plus sécurisée et plus performante.

Le Wi-Fi peut parfois être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre borne d'accès à Internet. Pour ce faire :

- n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès*.Les fournisseurs d'accès à Internet vous guident dans cette configuration en vous proposant différentes étapes, durant lesquelles vous appliquerez ces recommandations de sécurité:
  - » au moment de la première connexion de votre ordinateur en Wi-Fi, ouvrez votre navigateur Internet pour configurer votre borne d'accès. L'interface de configuration s'affiche dès l'ouverture du navigateur. Dans cette interface, modifiez l'identifiant de connexion et le mot de passe par défaut qui vous ont été donnés par votre fournisseur d'accès;
  - » dans cette même interface de configuration, que vous pouvez retrouver en tapant l'adresse indiquée par votre fournisseur d'accès, vérifiez que votre borne dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes) ;
  - » modifiez la clé de connexion par défaut (qui est souvent affichée sur l'étiquette de votre borne d'accès à Internet) par une clé (mot de passe) de plus de 12 caractères de types différents (cf. : 1-Choisissez des mots de passe robustes) ;
  - » ne divulguez votre clé de connexion qu'à des tiers de confiance et changez la régulièrement ;
  - » activez la fonction pare-feu de votre box ;
  - » désactivez votre borne d'accès lorsqu'elle n'est pas utilisée.

- n'utilisez pas les Wi-Fi « publics » (réseaux offerts dans les gares, les aéroports ou les hôtels) pour des raisons de sécurité et de confidentialité ;
- assurez-vous que votre ordinateur est bien protégé par un antivirus et un pare-feu. (Voir aussi Fiche 7 : Protéger ses données lors d'un déplacement). Si le recours à un service de ce type est la seule solution disponible (lors d'un déplacement, par exemple), il faut s'abstenir d'y faire transiter toute donnée personnelle ou confidentielle (en particulier messages, transactions financières). Enfin, il n'est pas recommandé de laisser vos clients, fournisseurs ou autres tiers se connecter sur votre réseau (Wi-Fi ou filaire).
- préférez avoir recours à une borne d'accès dédiée si vous devez absolument fournir un accès tiers. Ne partagez pas votre connexion.

6

Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur

Arthur possède un ordiphone qu'il utilise à titre personnel comme professionnel. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, l'éditeur de l'application peut accéder à tous les SMS présents sur son téléphone.

Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique :

- n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer ;
- en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement ;
- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;
- ne préenregistrez pas vos mots de passe (plus d'informations en fiche 1).

7

Protéger ses données lors de ses déplacements

Dans un aéroport, Charles sympathise avec un voyageur prétendant avoir des connaissances en commun. Lorsque celui-ci lui demande s'il peut utiliser son ordinateur pour recharger son ordiphone, Charles ne se méfie pas. L'inconnu en a profité pour exfiltrer les données concernant la mission professionnelle très confidentielle de Charles.

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation. Il convient de se référer au passeport de conseils aux voyageurs édité par l'ANSSI.

Avant de partir en mission

- n'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires ;
- sauvegardez ces données, pour les retrouver en cas de perte ;
- si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur ;
- apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport ;
- vérifiez que vos mots de passe ne sont pas préenregistrés.

Pendant la mission

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;
- désactivez les fonctions Wi-Fi et Bluetooth de vos appareils ;
- retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone ;

- informez votre entreprise en cas d'inspection ou de saisie de votre matériel par des autorités étrangères ;
- n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance ;
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation commerciale, utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données avec un logiciel d'effacement sécurisé ;
- refusez la connexion d'équipements appartenant à des tiers à vos propres équipements (ordiphone, clé USB, baladeur…)

Après la mission

- effacez l'historique des appels et de navigation ;
- changez les mots de passe que vous avez utilisés pendant le voyage ;
- faites analyser vos équipements après la mission, si vous le pouvez.
- n'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements (salons, réunions, voyages…) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

8

Être prudent lors de l'utilisation de sa messagerie

Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Jean-Louis a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Jean-Louis le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts;
- si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence;
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing »* ;
- n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

9

Télécharger ses programmes sur les sites officiels des éditeurs

Emma, voulant se protéger des logiciels espions (spyware), a téléchargé un logiciel spécialisé proposé par son moteur de recherche. Sans le savoir, elle a installé un cheval de Troie.*

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie*. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Dans ce contexte, afin de veiller à la sécurité de votre machine et de vos données :

- téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
- pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens ;
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

10

Être vigilant lors d'un paiement sur Internet

Céline a acheté sur Internet des fournitures de bureau pour son entreprise sans vérifier l'état de sécurité du site de commerce en ligne. Ce dernier n'était pas sécurisé. Des attaquants ont intercepté le numéro de carte bancaire de l'entreprise et ont soutiré 1 000 euros.

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordiphone (smartphone), vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet ;
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

Si possible, lors d'un achat en ligne :

- privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire ;
- n'hésitez pas à vous rapprocher votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

11

Séparer les usages personnels des usages professionnels

Paul rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels.

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette, etc.) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle pose des problèmes en matière de sécurité des données (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
- n'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
- de la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.

Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

12

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Alain reçoit un courriel lui proposant de participer à un concours pour gagner un ordinateur portable. Pour ce faire, il doit transmettre son adresse électronique. Finalement, Alain n'a pas gagné mais reçoit désormais de nombreux courriels non désirés.

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.

Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir :
  - » ne transmettez que les informations strictement nécessaires ;
  - » pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données ;
- ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ;
- pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité (Cf. Guide de la CNIL sur la sécurité des données personnelles) ;
- enfin, utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…).

En résumé …

Afin de renforcer efficacement la sécurité de vos équipements communicants et de vos données, vous pouvez compléter les douze bonnes pratiques de ce guide par les mesures suivantes :

- désignez un correspondant/référent pour la sécurité informatique dans les entreprises ;
- rédigez une charte informatique ;
- chiffrez vos données et vos échanges d'information à l'aide de logiciels de chiffrement* ;
- durcissez la configuration de votre poste et utilisez des solutions de sécurité éprouvées (pare-feux*, antivirus*) ;
- avant d'enregistrer des fichiers provenant de supports USB sur votre ordinateur, faites-les analyser par un antivirus ;
- désactivez l'exécution automatique des supports amovibles depuis votre ordinateur ;
- éteignez votre ordinateur pendant les périodes d'inactivité prolongée (nuit, week-end, vacances,…) ;
- surveillez et monitorez votre système, notamment en utilisant les journaux d'événements, pour réagir aux événements suspects (connexion d'un utilisateur hors de ses horaires habituels, transfert massif de données vers l'extérieur de l'entreprise, tentatives de connexion sur un compte non actif,…).

Pour aller plus loin

- **ANSSI** : http://www.ssi.gouv.fr
- **CNIL** : http://www.cnil.fr
- **Service de l'information stratégique et de la sécurité économiques (SISSE)** : http://www.entreprises.gouv.fr/information-strategique-sisse
- **Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Police nationale)** : https://www.internet-signalement.gouv.fr

En cas d'incident

Vous n'avez pas eu le temps de mettre en œuvre les règles décrites dans ce guide ou les attaquants ont réussi à les contourner. Ne cédez pas à la panique, et ayez les bons réflexes.

- en cas de comportement inhabituel de votre ordinateur, vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation,…) ;
- déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez-là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque ;
- prévenez votre hiérarchie, ainsi que le responsable de la sécurité, au téléphone ou de vive voix, car l'intrus peut-être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque ;
- faites faire une copie physique du disque ;
- faites rechercher les traces disponibles liées à la compromission. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.) ;
- déposez une plainte auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société, de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris et petite couronne), ou de la Direction générale de la sécurité intérieure. Retrouvez plus d'informations sur le site de l'ANSSI : *www.ssi.gouv.fr/en-cas-dincident/* ;
- après l'incident : réinstallez complètement le système d'exploitation à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information.

Glossaire

- **antivirus :** logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants ;
- **cheval de Troie :** programme qui s'installe de façon frauduleuse pour remplir une tâche hostile à l'insu de l'utilisateur (espionnage, envoi massif de spams,…) ;
- **chiffrement :** procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement ;
- **compte d'administrateur :** compte permettant d'effectuer des modifications affectant les utilisateurs (modification des paramètres de sécurité, installer des logiciels…) ;
- **logiciel espion :** logiciel malveillant qui s'installe dans un ordinateur afin de collecter et transférer des données et des informations, souvent à l'insu de l'utilisateur.
- **Fournisseur d'Accès Internet (FAI) :** organisme (entreprise ou association) offrant une connexion à Internet ;
- **mise à jour :** action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel ;
- **pare-feu (firewall) :** logiciel et/ou matériel permettant de protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet, protection d'un réseau d'entreprise,…) en filtrant les entrées et en contrôlant les sorties selon les règles définies par son utilisateur ;
- **paquet :** unité de transmission utilisée pour communiquer ;
- **phishing (hameçonnage) :** méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.
- **routeur :** élément intermédiaire dans un réseau informatique assurant la distribution des paquets de données en déterminant le prochain nœud de réseau auquel un paquet doit être envoyé ;
- **système d'exploitation :** logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels ;

- **utilisateur :** personne qui utilise un système informatique ;
- **WEP :** protocole de sécurité permettant de fournir aux utilisateurs de réseaux locaux sans fil une protection contre le piratage ;
- **Wi Fi :** connexion Internet sans fil
- **WPA 2 :** standard de sécurité protégeant les utilisateurs contre le piratage des réseaux sans fil devant se substituer au système WEP jugé insuffisant.

Contacts

CPME

Amélie JUGAN

ajugan@cpme.fr

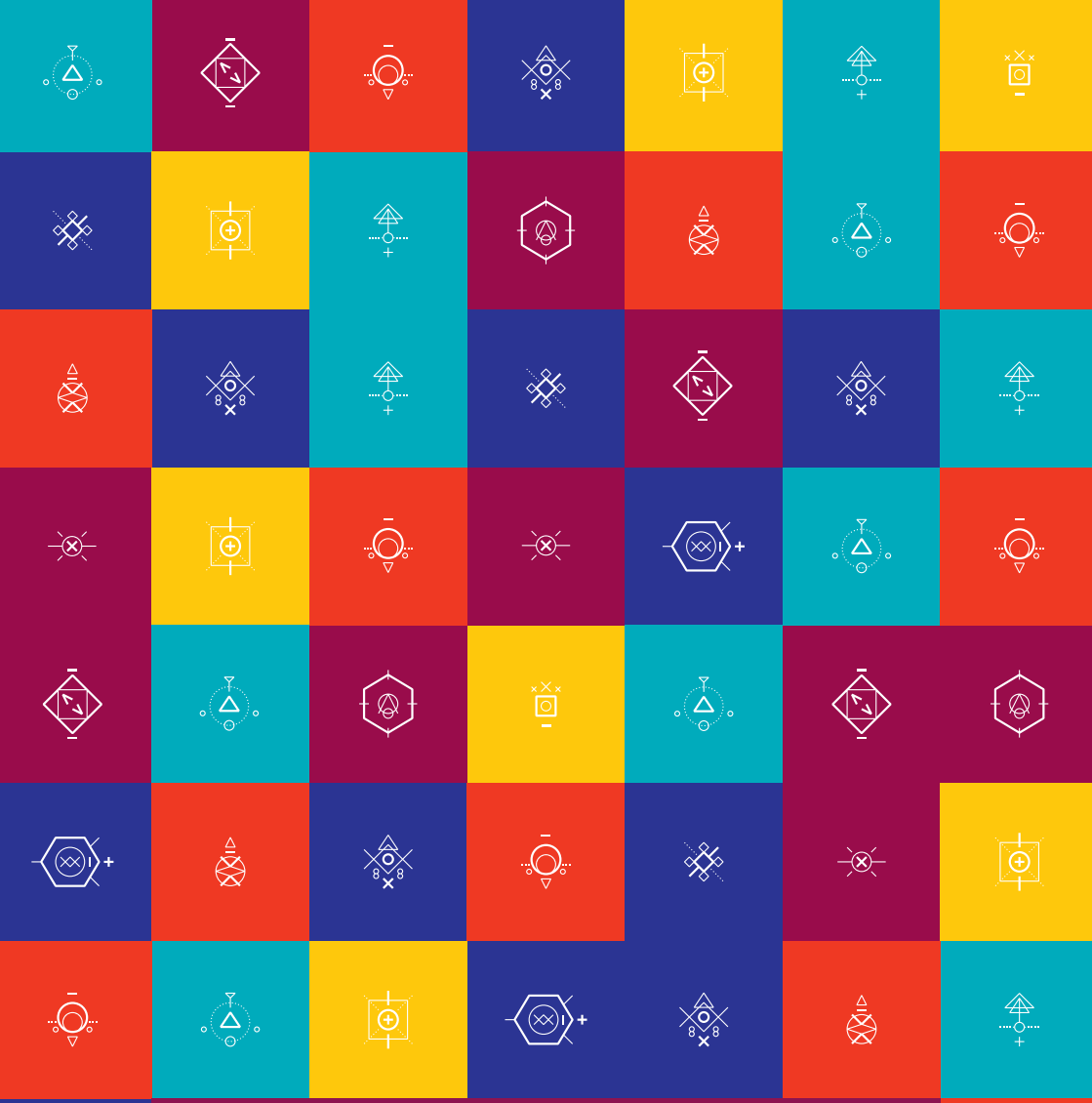
ANSSI

communication@ssi.gouv.fr

Guide téléchargeable sur les sites :

www.cpme.fr

www.ssi.gouv.fr



Version 1.1.1 - Septembre 2017
20170901-1801

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
www.ssi.gouv.fr / communication@ssi.gouv.fr / twitter.com/ANSSI_FR

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%A7o-nigiciels.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**

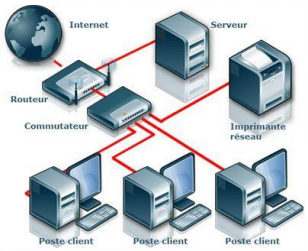
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr

Gendarmerie nationale

Région de gendarmerie de Nouvelle-Aquitaine et gendarmerie pour la zone de défense et de sécurité Sud-Ouest

Information Cyber et Covid-19

La situation particulière que nous vivons actuellement est **propice aux attaques cyber.**
Opportunistes, les pirates informatiques exploitent notre besoin d'information, nos demandes, l'utilisation accrue du réseau informatique et les conditions de télétravail...



I/ Protection du réseau informatique d'une structure

@ Prévenez les menaces

*****Profitez du ralentissement de l'activité pour faire un bilan informatique complet ;**

*****Procédez à des sauvegardes régulières et hors ligne des données, sans oublier de déconnecter à l'issue, votre support de sauvegarde.**

@ Sensibilisez vos salariés/employés

*****Assurez vous de connaître les personnes à contacter ;**

*****Utilisez un Réseau Privé Sécurisé (VPN) de confiance, un antivirus mis à jour…**

*****Rappelez les règles d'utilisation du réseau informatique de votre structure ;**

*****Séparez vos données personnelles de l'activité professionnelle ;**

*****Vérifiez par un contre-appel l'identité d'un interlocuteur ;**

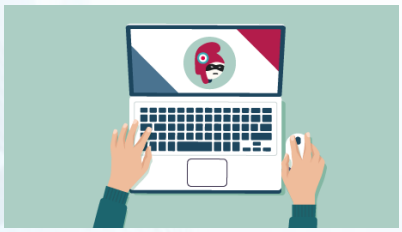
*****Assurez vous de connaître les consignes et personnes à contacter en cas d'incident.**

II/ L'actualité des cybercriminels

Faux sites internet de vente en ligne de produits sanitaires (masques, gel hydroalcoolique, médicaments) : ***Rendez-vous*** sur les sites officiels.

Fausse commande et faux ordres de virement : ***Vérifiez*** les demandes de virement ou un changement de RIB d'une facture, d'un salaire.

L'hameçonnage, le phishing : ***Méfiez-vous*** des mails, SMS et appels téléphoniques non identifiés qui ont pour but de vous soustraire des informations personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.



Dons frauduleux : ***Évitez*** de cliquer sur les liens des appels aux dons et rendez vous directement sur les sites officiels.

Rançongiciel, Ransomware : Attaque empêchant l'accès aux données de l'entreprise et réclamant une rançon pour les libérer. Elle peut s'accompagner d'un vol de données et d'une destruction préalable des sauvegardes.

Elles sont possibles par une intrusion sur le réseau de l'entreprise, un accès à distance (notamment en cette période les accès distant doivent être sécurisés), par la compromission de l'équipement d'un collaborateur ou un défaut de mise à jour du matériel informatique (pièces jointes ou liens présents dans les courriers électroniques).

En cas de doute, la gendarmerie est à vos côtés

En cas d'urgence, contactez le 17

Pour toute question :

cyber-vigilance-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

Région de gendarmerie de Nouvelle-Aquitaine
Division des opérations/Bureau renseignements – Section de recherches/Pôle cybercriminalité

CONSEILS AUX ENTREPRISES : PRÉPARER LA REPRISE D'ACTIVITÉ AU DÉCONFINEMENT

L'annonce du début du déconfinement va vous permettre d'envisager une reprise au moins partielle et progressive de votre activité.
Si, dans une première étape, le recours au tététravail reste toujours à privilégier partout où c'est possible,vous devez vous préparer à cette reprise, tant au plan sanitaire que pour reprendre le contrôle de votre sécurité numérique.

Les 10 mesures suivantes visent à vous aider dans la réalisation de votre plan d'action cybersécurité de déconfinement.

1. Recenser et analyser les incidents de sécurité
exemples : hameçonnage de mot de passe, document suspect reçu en pièce-jointe d'un message…, pour cerner le plus précisément possible les incidents survenus.

2. S'assurer du bon fonctionnement de ses outils de protection
antivirus, pare-feu, systèmes de détection d'intrusion…

3. Rechercher les indices de compromission
comme des connexions inhabituelles, les annuaires de comptes pour déceler toute création de nouveau compte suspect, des règles de transferts de messages vers des comptes externes illégitimes.

4. Contrôler et tester les sauvegardes
Avant de reprendre l'activité de l'organisation, il est particulièrement important de vérifier leur bon fonctionnement, notamment en procédant à des tests de restauration et de s'assurer de disposer d'une copie récente des données qui soit déconnectée du réseau afin de pouvoir faire face à une attaque par rançongiciel.

5. Réaliser les mises à jour de sécurité
Si durant le confinement certains systèmes n'ont pas pu recevoir leurs mises à jour de sécurité, il convient de mettre en œuvre un plan de rattrapage cohérent et sans précipitation pour éviter tout effet de bord sur l'activité opérationnelle. La priorité sera donnée aux systèmes de sécurité, puis aux systèmes ou serveurs critiques exposés directement ou indirectement sur Internet, et enfin aux postes de travail des collaborateurs.

6. Recentraliser les données

Durant le confinement, des données de l'organisation ont pu être dispersées sur les postes des télétravailleurs ou de manière temporaire sur certains services de d'hébergement externes (cloud). Il convient donc de les recentraliser au sein de l'organisation pour s'assurer de leurs sauvegardes et de les supprimer dans les règles de l'art sur les stockages inappropriés pour limiter tout risque d'atteinte en matière de confidentialité.

7. Contrôler les équipements nomades avant de les reconnecter au réseau de l'entreprise

Avant d'en ré-autoriser la connexion au système d'information de l'entreprise, tous les équipements nomades utilisés durant le confinement (ordinateurs portables, téléphones mobiles, tablettes) doivent faire l'objet d'un contrôle strict pour s'assurer qu'ils n'ont pas été compromis, et idéalement faire l'objet d'une réinstallation complète depuis une matrice maîtrisée, sécurisée et convenablement mise à jour par l'organisation.

8. Refermer les accès externes devenus inutiles

L'organisation doit s'attacher à réduire son exposition, et donc sa surface d'attaque, en refermant tous les accès externes ouverts qui seraient devenus inutiles. Il peut s'agir d'accès externes à fermer au niveau des pare-feux mais aussi de comptes avec droits privilégiés ouverts à titre exceptionnel sur certains systèmes de l'organisation qu'il faudra clôturer.

9. Mettre fin aux usages à risques dérogatoires

Pour faire face au confinement, de nombreux usages d'applications, de services ou de pratiques ont pu être autorisés à titre exceptionnel mais peuvent présenter un risque de sécurité pour l'organisation. Il convient donc de communiquer avec pédagogie et transparence sur l'arrêt d'autorisation de ces pratiques dérogatoires.

10. Tirer rapidement les enseignements du confinement pour traiter tout ce qui doit l'être

L'organisation doit savoir tirer les enseignements de la crise pour se préparer à être en capacité de mieux l'affronter en cas de résurgence. Cela peut concerner sa politique d'équipement matériel en postes nomades professionnels maîtrisés pour les télétravailleurs, en équipements logiciels ou outils de travail à distance (visioconférence, téléconférence, hébergements de données…), en outils et procédures sécurisées de télétravail ou de télé-administration de ses systèmes, en infrastructures de sécurisation de ses systèmes, en formation et sensibilisation de ses collaborateurs, etc.

Nous contacter ⇨

securite-economique-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

EN CAS D'URGENCE, APPELEZ LE 17 OU LE 112

VOUS ÊTES VICTIMES ?

Une question ?
Besoin d'aide ?

On vous accueille en ligne

Scanner le QR Code et dialoguer par tchat

BRIGADE numérique Gendarmerie

LES ACTEURS

VOUS SOUHAITEZ SÉCURISER VOS MARCHÉS ET VOTRE SAVOIR-FAIRE EN FRANCE ET À L'INTERNATIONAL ?

LA DIRECTION GÉNÉRALE DES DOUANES

- prévient les pratiques agressives et déloyales ;
- préserve les intérêts français à l'étranger via son réseau international d'attachés douaniers ;
- participe au contrôle des investissements étrangers en France ;
- promeut l'agrément Opérateur Economique Agréé (OEA), label de confiance douanier européen.

Contact
+33 (0) 9 70 27 55 80
pae-bordeaux@douane.finances.gouv.fr
Outil
www.douane.gouv.fr

L'ASSOCIATION FRANÇAISE DE NORMALISATION (AFNOR)

- propose des solutions fondées sur les normes volontaires, documents consensuels reflétant les bonnes pratiques les plus reconnues au niveau européen et international.

Contact
+33 (0) 5 57 29 14 33
delegation.bordeaux@afnor.org
Outil
https://normalisation.afnor.org/thematiques/numerique/

L'INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE (INPI)

- accompagne les entreprises, sur le territoire et à l'export, en matière de propriété industrielle pour protéger le savoir-faire des acteurs économiques en France.

Contact
0820 210 211
nouvelleaquitaine@inpi.fr
Outil
www.inpi.fr

VOUS SOUHAITEZ PROTÉGER VOS INFORMATIONS STRATÉGIQUES, VOS LOCAUX, SENSIBILISER VOS SALARIÉS, FAIRE UN DIAGNOSTIC ?

LA DIRECTION ZONALE DE SÉCURITÉ INTÉRIEURE (DZSI)

- participe à la protection du patrimoine scientifique et technique de la nation (PPST) ;
- apporte son expertise en matière de sécurité économique ;
- accompagne les entreprises dans leurs démarches de protection des informations stratégiques et sensibles.

Contact
securite-economique-bordeaux@interieur.gouv.fr
Outil
La lettre d'information « Flash Ingérence » disponible sur abonnement, à solliciter par écrit à l'adresse ci-dessus.

L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

- apporte son expertise et son assistance technique aux administrations et aux entreprises dans leur développement numérique ;
- assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

Contact
nouvelle-aquitaine@ssi.gouv.fr
Outils
www.ssi.gouv.fr
https://secnumacademie.gouv.fr/ (formation à distance)

LES DÉLÉGUÉS À L'INFORMATION STRATÉGIQUE ET À LA SÉCURITÉ ÉCONOMIQUES (DISSE)

- informent, orientent et conseillent les acteurs économiques en matière de sécurité économique.

Contact
na.disse@direccte.gouv.fr
Outils
Guide des 26 fiches de sécurité économique et DIESE (diagnostic d'intelligence économique et de sécurité économique) sur : https://sisse.entreprises.gouv.fr

GENDARMERIE : LES RÉFÉRENTS SÉCURITÉ ÉCONOMIQUE ET PROTECTION DES ENTREPRISES (SÉcoPE)

- aident à l'identification des risques et à l'adaption des dispositifs de protection ;
- organisent des actions de sensibilisation et de prévention au profit de différents acteurs (entreprises, associations, facultés...).

Contact
securite-economique-nouvelleaquitaine@gendarmerie.interieur.gouv.fr
Outil
Jeu des 8 familles d'atteintes à la sécurité économique sur **www.gendarmerie.interieur.gouv.fr**

LE SERVICE ZONAL DU RENSEIGNEMENT TERRITORIAL (SZRT 33)

- assure le suivi économique et social des entreprises dans les départements ;
- exerce des fonctions de capteur dans la mise en œuvre globale de la politique publique d'intelligence économique ;
- détecte les vulnérabilités et les atteintes aux entreprises.

LA DÉLÉGATION RÉGIONALE À LA RECHERCHE ET À LA TECHNOLOGIE (DRRT)

- participe à la sensibilisation des établissements d'enseignement supérieur, des organismes publics et privés de recherche, des centres de ressources technologiques (CRT) ainsi que des jeunes entreprises innovantes (JEI), en matière de sécurité économique.

Contact
drrt.nouvelle-aquitaine@recherche.gouv.fr

VOUS ÊTES UNE ENTREPRISE ACTIVE SUR LES MARCHÉS DÉFENSE, OU INTÉRESSÉE PAR CES OPPORTUNITÉS ?

LA DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE (DRSD)

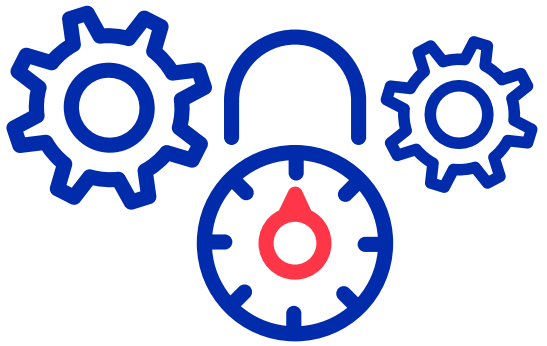
- décèle et neutralise toute menace contre les intérêts nationaux et la souveraineté nationale, touchant la sphère défense ;
- assure le suivi, la sensibilisation, le conseil des industries et instituts de formation ou de recherche en lien avec la défense dans sa mission de contre-ingérence économique (incluant la cyber défense).

Contact
+33 (0) 5 57 85 10 22
drsd-bordeaux-cie.contact.fct@intradef.gouv.fr
Outils
www.drsd.defense.gouv.fr

LA DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

- accompagne les PME de la base industrielle et technologique de défense (BITD) dans leur projet de développement (innovation, exportation, accès au marché) ;
- contribue à la sensibilisation des PME et ETI à la sécurité économique et à la cybersécurité.

Outils
www.achats.defense.gouv.fr (espace PME)
www.ixarm.com



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE

SISSE Commissaire et Service de l'Information Stratégique et de la Sécurité Économiques

www.prefectures-regions.gouv.fr/nouvelle-aquitaine
@PrefAquitaine33 @PrefetNouvelleAquitaine33

ENTREPRISES ET LABORATOIRES
EN NOUVELLE-AQUITAINE

PROTÉGEZ VOS INFORMATIONS STRATÉGIQUES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE

SÉCURISEZ L'AVENIR DE VOTRE ENTREPRISE !

Chaque année, un nombre croissant d'entreprises et de laboratoires de recherche sont victimes de captations d'informations stratégiques ou sensibles.

Ces actes ciblés peuvent entraîner une perte de compétitivité importante pour l'établissement et altérer son image, voire mettre en péril son existence.

Certains savoir-faire peuvent également être détournés à des fins malveillantes.

Dans un monde où la concurrence est exacerbée, la compétitivité conditionne la survie de l'entreprise.

La protection des savoir-faire et des informations devient alors un enjeu vital pour sa pérennité.

Du chef d'entreprise à l'ouvrier, du cadre supérieur au chargé de communication, du directeur de laboratoire au chercheur, chacun est concerné par la sécurité économique.

LES RISQUES DE SÉCURITÉ

LES ATTEINTES PHYSIQUES SUR SITE

Intrusions dans un bâtiment (public ou privé) pour dérober des informations stratégiques non-protégées.

LA FRAGILISATION, LA DÉSORGANISATION D'ENTREPRISES

Manœuvres pour déstabiliser un établissement sous plusieurs formes : parasitisme, dénigrement, débauchage de personnel, détournement de clientèle, etc.

LES ATTEINTES AU SAVOIR-FAIRE

Perte de compétence clé, captation de brevet, contrefaçon de produits, concurrence déloyale, espionnage.

LES INTRUSIONS CONSENTIES

Captations d'informations stratégiques via les conférences, séminaires, visites de délégations étrangères, entrisme, stagiaires, intérimaires, etc.

LES RISQUES FINANCIERS

Dépendance vis-à-vis d'un client,d'un fournisseur prédominant, injection, de capitaux par fonds activiste, escroquerie financière, sanctions de partenaires étrangers.

LES ATTEINTES À LA RÉPUTATION

Attaque informationnelle sur l'identité et la situation de l'entreprise, qui porte préjudice à son image et à sa réputation.

LES FRAGILITÉS HUMAINES

Vol à distance d'informations stratégiques dans l'entreprise par des personnes extérieures via l'ingénierie sociale, par exemple en usurpant l'identité d'un salarié, d'un client ou d'un fournisseur.

LES RISQUES INFORMATIQUES

Destruction ou chiffrement de données, vols d'ordinateurs et de supports de stockage, atteintes aux traitements et systèmes automatisés de données, attaques par déni de service distribué.

CONSEILS POUR VOTRE STRATÉGIE D'ENTREPRISE

Identifier son information stratégique

- réaliser un classement des informations détenues par votre entreprise ;
- se questionner sur l'impact qu'engendrerait la perte, la destruction ou la divulgation de ces informations ;
- identifier les informations sensibles, stratégiques et les lieux sensibles de votre entreprise.

Identifier les risques, menaces et vulnérabilités

- réaliser un diagnostic ;
- évaluer les forces et faiblesses de votre entreprise et sa progression dans le temps à l'aide d'outils informatiques (ex : logiciel DIESE via le site du SISSE).

Prendre des mesures de protection

- sensibiliser vos salariés aux risques ;
- encadrer l'accueil des personnes externes à votre entreprise ;
- protéger votre savoir-faire ;
- savoir bien communiquer sans divulguer vos informations stratégiques ;
- élaborer un plan de continuité et de reprise d'activité en cas de crise.

Assurer une veille

- surveiller l'évolution des réglementations qui affectent l'activité de votre établissement ;
- identifier les innovations ;
- surveiller la concurrence, votre image et son impact.

Mener des actions d'influence

- participer à l'élaboration des normes ;
- valoriser votre réseau, votre image.

Cybermenaces et Covid-19

Recommandations pour les entreprises et les salariés en télétravail

Faux sites liés au COVID19

• Prenez garde aux faux sites Internet relatifs aux ventes en ligne de masques, gel hydroalcoolique.

Fausses commandes et faux ordre de virement

• Vérifiez la signature de documents ou les tentatives de récupération des mots de passe de vos données d'entreprise.

• Vérifiez les demandes d'un virement exceptionnel ou un changement de RIB d'une facture ou d'un salaire faite par un dirigeant, d'un fournisseur, d'un prestataire, voire d'un collaborateur, pour demander un virement exceptionnel ou un changement de RIB d'une facture ou d'un salaire. Son identité a pu être usurpée suite au piratage d'un compte de messagerie, par message et même téléphone.

L'hameçonnage / Phishing

• méfiez-vous des mails, SMS, chat (réseaux sociaux, messageries instantanées type Whatsapp) et appels téléphoniques non identifiés. Cette technique soustrait des informations personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.

Portails d'information

www.contacterlagendarmerie.fr
www.cybermalveillance.gouv.fr
www.ssi.gouv.fr
www.cnil.fr

Dons frauduleux

• Évitez de cliquer sur les liens des appels aux dons et rendez vous directement sur le site officiel.

Rançongiciel / Ransomware

Cette attaque consiste à empêcher l'accès aux données de l'entreprise et à réclamer une rançon pour les libérer. Elle s'accompagne d'un vol de données et d'une destruction préalable des sauvegardes.

Elles sont possibles par une intrusion sur le réseau de l'entreprise, un accès à distance, par la compromission de l'équipement d'un collaborateur ou un défaut de mise à jour du matériel informatique (pièces jointes ou liens présents dans les courriers électroniques).

Pensez à :

Bilan sécurité et sauvegarde des données

• Profitez du ralentissement de l'activité, faites un bilan complet avec votre responsable informatique ou une entreprise cybersécurité.

• Procédez à des sauvegardes régulières et hors ligne des données. Déconnectez votre support de sauvegarde à l'issue.

Attestation de travail

• Facilitez la mobilité de vos salariés en éditant des attestations de déplacement dérogatoire avec le timbre officiel de l'entreprise.

Déplacements / Télétravail

• Vos collaborateurs et salariés doivent renforcer leur vigilance lors de leurs trajets domicile/lieu de travail, en particulier leurs équipements mobiles.

• Mettez à disposition des solutions de sécurité (VPN, antivirus) et assurez-vous qu'ils connaissent les règles de mise en œuvre et de mise à jour.

• Proscrivez à vos collaborateurs l'emploi d'espaces de partage personnel des documents.

• Rappelez les consignes et contacts en cas d'incident.

Charte informatique

• Faites un rappel sur les droits et devoirs de chacun sur les règles d'utilisation du réseau informatique de l'entreprise.

• Si nécessaire, mettez à jour les consignes et les nouveaux outils du travail à distance.

Conception graphique Sirpa-gendarmerie C 8889 - 2020

#RÉPONDREPRÉSENT

GENDARMERIE
NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

Opération tranquillité Entreprise et Commerce

La gendarmerie peut surveiller votre commerce, entreprise ou son périmètre
Signalez vous auprès de votre brigade pour en bénéficier

Votre commerce/ entreprise est fermé

- **Fermez** bien tous les accès de votre commerce ou entreprise.
- Dans la mesure du possible, limitez les stocks et **ne conservez pas** d'argent liquide.
- **Activez** vos systèmes de protection : éclairage, alarme, vidéo. Vérifiez régulièrement leur bon fonctionnement.
- En l'absence de client et d'employé **vous pouvez installer** un dispositif de vidéosurveillance sans formalité particulière.

Votre commerce/ entreprise est ouvert

- **Soyez attentif à votre environnement,** détectez les comportements inhabituels et signalez-les nous.
- **Vérifiez régulièrement le bon fonctionnement** de vos équipements de protection déjà en place : éclairage, système d'alarme et vidéo le cas échéant.
- Si possible, ouvrez et quittez à plusieurs les locaux.
- **Ne stockez pas** vos produits à la vue des clients.
- **Limitez, si possible,** les stocks de produits de grande valeur.
- **Rappelez** à vos collaborateurs et/ou employés les mesures élémentaires de sûreté (fermetures effectives des ouvrants, activation des alarmes…).

Prévention Cyber

Plus de conseils sur www.cybermalveillance.gouv.fr

- Attention aux cyberattaques, aux escroqueries ou aux démarchages directs, notamment si vous fonctionnez en télétravail : ne relâchez pas votre vigilance et sensibilisez vos collaborateurs !
- Maîtrisez la communication de vos activités et l'utilisation des réseaux sociaux pour ne pas susciter l'intérêt d'un délinquant.

#RÉPONDREPRÉSENT

Vous êtes victime

- **En cas d'urgence,** appelez le 17 ou 112
- **En cas de cambriolage,** ne touchez à rien et composez le 17
- Pour les vols, dégradations, escroqueries : **www.pre-plainte-en-ligne.gouv.fr**
- Votre sûreté a des vulnérabilités fortes, les référents et correspondants sûreté de la gendarmerie peuvent vous conseiller. **Adressez-vous** à votre brigade de gendarmerie : **www.interieur.gouv.fr/Contact/Contacter-une-brigade-de-gendarmerie-ou-un-commissariat-de-police**

Conception graphique Sirpa-gendarmerie C 891 - 2020

GENDARMERIE NATIONALE

La sécurité numérique à la maison pendant la crise du Coronavirus

LES CYBERCRIMINELS

LES PIÈGES

- Escroqueries et hameçonnages liés aux produits sanitaires (masques, gel hydroalcoolique, médicaments)
- Logiciels malveillants et autres virus informatiques
- Application Coronavirus détournées
- Ne cliquez pas sur des liens de sources inconnues
- Méfiez-vous des publicités alléchantes
- Vérifiez à deux fois l'origine des appels aux dons
- Ne donnez pas vos coordonnées bancaires sur des sites inconnus
- Vérifiez les mises à jour de vos systèmes d'exploitation et antivirus
- Sauvegardez régulièrement vos données

En cas de fraude à la carte bancaire, signalez-le à votre banque et sur la plateforme PERCEVAL sur

Service-Public.fr
Le site officiel de l'administration française

ATTENTION FAUSSES INFORMATIONS

Beaucoup d'informations circulent, douter permet d'éviter de propager soi-même de fausses informations :

- Qui est l'auteur ? Quelle est son intention ?
- Quelle est la nature du site ? Qui est son éditeur ?
- Quelle est la source de l'information ? A-t-elle été publiée sur d'autres sources de confiance ?
- De quand date l'information ? Est-ce que l'information est cohérente (lieux, dates, personnes) ?
- Que disent les commentaires sur le site et sur les réseaux sociaux qui reprennent cette information ?

INFORMEZ-VOUS AUPRÈS DES SOURCES OFFICIELLES :
https://www.gouvernement.fr/info-coronavirus

information
CORONAVIRUS COVID-19

TÉLÉTRAVAIL

- Respectez les règles de sécurité numérique et les procédures auxquelles vous êtes habitué ; restez attentif et n'hésitez pas à vérifier par un contre-appel l'identité d'un interlocuteur
- Séparez autant que possible vos activités et données personnelles ou professionnelles ; interdisez l'accès de vos équipements professionnels à vos proches
- Utilisez le VPN (réseau privé sécurisé) fourni par votre employeur
- Assurez-vous de connaître les personnes à contacter et rendez-compte de tout incident

POUR PLUS DE CONSEILS ET VOUS FAIRE ASSISTER EN CAS D'INCIDENT, RENDEZ-VOUS SUR LE SITE DE NOTRE PARTENAIRE :

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

DES ENFANTS + CONNECTÉS

- Parlez avec vos enfants **DES RISQUES SUR INTERNET** et soyez toujours à leur écoute.
- Pour l'école à la maison, n'utilisez que les plateformes officielles et évitez les réseaux sociaux réservés aux plus grands.
- Pour les plus jeunes, rappelez-leur de ne jamais discuter avec des inconnus et utilisez des outils de contrôle parental.
- Comme pour les logiciels et matériels des plus grands, changez les mots de passe par défaut, vérifiez les configurations de sécurité et les mises à jour.

BRIGADE numérique
Gendarmerie

Pour toute question, 24h/24, 7j/7 :
www.contacterlagendarmerie.fr

En cas d'urgence, contactez le 17

CYBERGEND
INVESTIGATION & CRIMINALISTIQUE

MINISTÈRE DE L'INTÉRIEUR

Gendarmerie nationale

L'INTELLIGENCE ÉCONOMIQUE... OBJECTIF COMPÉTITIVITÉ !

• L'intelligence économique est la gestion de l'information stratégique utile aux acteurs économiques dans un objectif d'accroissement de compétitivité.

• L'intelligence économique est aussi un mode de gouvernance fondé sur la maîtrise et l'exploitation de l'information stratégique pour créer de la valeur durable pour une entité.

• Anticiper les changements à venir dans l'environnement de l'entreprise par la maîtrise de l'information, c'est faire de l'intelligence économique !

L'INTELLIGENCE ÉCONOMIQUE C'EST AUSSI UNE POLITIQUE PUBLIQUE

• Pilotée par le Service de l'information stratégique et de la sécurité économiques (SISSE), elle est placée, au niveau territorial, sous la houlette du préfet de région.

• De l'échelon national à l'échelon territorial, la gendarmerie est un acteur de cette politique publique.

• Au fait des nombreuses atteintes qui touchent chaque jour le tissu entrepreneurial, la gendarmerie agit tout particulièrement dans le domaine de la sécurité économique et la protection des entreprises.

SENSIBILISER & ALERTER

• L'environnement des entreprises peut parfois leur être hostile. La maîtrise de cet environnement réduit considérablement les risques.

• C'est en ce sens que s'inscrit l'action de la gendarmerie en matière de sécurité économique.

• Les référents sécurité économique et protection des entreprises réalisent des actions de sensibilisation et de prévention au profit des acteurs économiques. Ils collaborent étroitement avec d'autres services de l'État pour répondre au mieux aux besoins des entreprises.

CONTACT

Les référents sécurité économique et protection des entreprises de la gendarmerie sont à votre écoute.

securite-economique@gendarmerie.interieur.gouv.fr

www.gendarmerie.interieur.gouv.fr

GENDARMERIE NATIONALE

SÉCURITÉ ÉCONOMIQUE & PROTECTION DES ENTREPRISES

La Gendarmerie nationale, acteur de la politique publique d'intelligence économique

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

LE DISPOSITIF TERRITORIAL DES RÉFÉRENTS SECOPE

• La Gendarmerie nationale dispose d'un réseau de référents Sécurité Économique et Protection des Entreprises (SEcoPE) disséminés sur toute l'étendue du territoire.

• Présents jusqu'au niveau départemental, ces référents agissent pour prévenir les atteintes à la sécurité économique et sensibiliser les acteurs territoriaux dans une dynamique de réseau et de partenariat.

LES PRINCIPALES MISSIONS DES RÉFÉRENTS SECOPE

Nos référents agissent dans la perspective de vous permettre:

- de mieux identifier les risques et menaces auxquels vous êtes exposés ;

- d'adapter vos dispositifs de protection ;

- de diffuser une culture de sécurité du patrimoine informationnel.

Le patrimoine de l'entreprise est matériel (locaux, outils de production...) et aussi immatériel (savoir-faire, données, réputation...). L'un et l'autre doivent être protégés. Un auto diagnostic a été réalisé par les services de l'État. Nos référents sont là pour vous accompagner dans sa mise en œuvre.

LE DISPOSITIF DES RÉFÉRENTS SÉCURITÉ ÉCONOMIQUE ET PROTECTION DES ENTREPRISES DE LA GENDARMERIE NATIONALE

securite-economique-gair@gendarmerie.interieur.gouv.fr
Gendarmerie de l'Air

securite-economique-gmar@gendarmerie.interieur.gouv.fr
Gendarmerie Maritime

securite-economique-gta@gendarmerie.interieur.gouv.fr
Gendarmerie des Transports Aériens

securite-economique-garm@gendarmerie.interieur.gouv.fr
Gendarmerie de l'Armement

securite-economique-cgom@gendarmerie.interieur.gouv.fr
Commandement de la gendarmerie de l'Outre-Mer

securite-economique-gsan@gendarmerie.interieur.gouv.fr
Commandement de la sécurité des armements nucléaires