AMGe
association
des médecins
du canton
de genève

DOSSIER CYBER-SÉCURITÉ

- Cyber-attaque par rançongiciel : aspects juridiques

- Comment protéger votre réseau informatique

- De l'importance des sauvegardes

- Etre prêt à gérer une cyberattaque, se préparer avant la crise

Cyber-attaque par rançongiciel : aspects juridiques

Depuis 2016, on observe une forte croissance des attaques par rançongiciel contre des PME suisses actives dans le domaine de la santé. De telles attaques visent non seulement des centres hospitaliers, mais aussi des cabinets médicaux et des médecins individuels, voire des centres de facturation. Le fait que le domaine de la santé soit une cible de choix pour les *hackers* tient en particulier au fait que les données de patients ont une valeur marchande très forte sur le *dark web*.

La présente contribution a pour but de présenter succinctement les obligations légales qui incombent au médecin, ainsi que les conséquences légales qu'il est susceptible d'encourir en cas de cyber-attaque par rançongiciel[1].

Obligations légales découlant des législations sur la protection des données

Lorsqu'on envisage le risque d'une attaque par rançongiciel, trois obligations découlant des législations de protection des données apparaissent fondamentales : l'obligation d'assurer la sécurité des données, les obligations spécifiques en matière de sous-traitance et les obligations en cas de violation de la sécurité des données.

La protection des données étant régie par de nombreuses lois[2], on se concentrera, afin de simplifier le propos, sur la nouvelle Loi fédérale sur la protection des données (nLPD) qui entrera en vigueur en septembre 2023[3].

Obligation d'assurer la sécurité des données

En amont de toute cyber-attaque, le médecin, ainsi que ses sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru[4]. Cette obligation se fonde sur une approche basée sur les risques. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées.

Pour déterminer concrètement quelles sont les mesures organisationnelles et techniques appropriées, on se référera notamment (i) aux art. 1 à 6 de la nouvelle Ordonnance sur la protection des données (nOPDo), (ii) aux publications

des autres auteurs du présent numéro, ainsi que (iii) aux recommandations publiées par le Centre national pour la cybersécurité NCSC à destination du secteur de la santé le 28 juillet 2022[5].

Cela étant, comme les technologies et les méthodes des *hackers* évoluent constamment, il est nécessaire de réévaluer régulièrement si les mesures mises en place demeurent adéquates.

Obligations en cas de sous-traitance
Il est admis que le médecin peut externaliser certaines tâches, notamment informatiques, à un ou des sous-traitants[6].

En amont de toute cyber-attaque, le médecin doit ainsi s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. En particulier, celui-là doit veiller à choisir soigneusement son mandataire, à lui donner les instructions adéquates et à exercer la surveillance nécessaire au vu des circonstances[7].

Obligation d'annoncer et documenter les violations de la sécurité des données
En cas de cyber-attaque et si la violation de la sécurité des données entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le médecin doit l'annoncer dans les meilleurs délais au Préposé fédéral à la protection des données et à la transparence (PFPDT)[8].

À notre sens, une telle annonce sera en principe toujours nécessaire pour le médecin victime d'un rançongiciel car il conviendra de partir du principe, dans le doute, que la cyber-attaque entraîne un risque élevé pour la personnalité ou les droits fondamentaux des patients. Le médecin devra également annoncer le cas aux patients concernés lorsque cela est nécessaire à leur protection ou lorsque le PFPDT l'exige[9].

« Une cyber-attaque fait peser des conséquences juridiques potentiellement très lourdes sur le médecin. Pour s'en prémunir, il lui appartient de prendre toutes les mesures nécessaires pour assurer une sécurité adéquate des données de ses patients au regard des risques encourus. »

À noter que le médecin doit également documenter les violations de la sécurité des données et conserver cette documentation pendant au moins deux ans à compter de la date d'annonce au PFPDT[10].

Risques juridiques encourus par le médecin

Sanctions en raison d'une violation du secret médical ?
Si les hackers exfiltrent les données de patients puis les publient sur Internet, il y a une divulgation d'informations couvertes par le secret médical à des tiers non autorisés. Se pose alors la question de savoir si le médecin peut se voir reprocher une éventuelle violation du secret médical.

Du point de vue du droit pénal, la violation du secret médical est réprimée par l'art. 321 du Code pénal (CP) qui prévoit une peine privative de liberté de trois ans au plus ou une peine pécuniaire.

Une violation de l'art. 321 CP peut être réalisée par omission notamment lorsqu'un défaut de surveillance peut être reproché au médecin[11]. Cependant, il n'y a violation du secret médical au sens de l'art. 321 CP que si le médecin agit intentionnellement ; s'il agit par négligence, il ne commet aucune infraction pénale. En matière de violation du secret médical, la frontière entre intention et négligence est parfois difficile à tracer[12]. À notre sens, une violation de l'art. 321 CP ne devrait pas pouvoir être reprochée au médecin si ce dernier a pris des mesures de sécurité informatique adéquates, mais que celles-ci n'ont pas permis d'empêcher la cyber-attaque ayant entraîné la divulgation à des tiers non autorisés d'informations couvertes par le secret médical.

Du point de vue du droit disciplinaire, la violation du secret médical est sanctionnée par un corpus de règles dispersées. On se limitera à mentionner ici l'art. 43 al. 1 de la Loi sur les professions médicales (LPMéd)[13], ainsi que les normes associatives auxquelles les médecins se soumettent, telles l'art. 34 des Statuts de l'Association des médecins du Canton de Genève[14]. Ces normes prévoient des sanctions comprenant l'avertissement, le blâme, l'amende, et une interdiction de pratiquer temporaire ou définitive. Contrairement à ce qui prévaut en droit pénal, la violation du secret médical par négligence peut conduire au prononcé de sanctions disciplinaires à l'encontre du médecin[15].

Sanction en raison d'une violation de l'obligation d'assurer la sécurité des données ?
Sont punis, sur plainte, d'une amende de 250 000 francs au plus les personnes privées qui, intentionnellement, ne respectent pas les exigences minimales en matière de sécurité des données conformément à l'art. 8 nLPD[16].

Pour les mêmes raisons qu'exposées ci-dessus en lien avec l'art. 321 CP, une condamnation pénale du médecin pour violation des exigences minimales de sécurité découlant de l'art. 8 nLPD en raison d'une attaque par rançongiciel ne devrait pas pouvoir lui être reprochée s'il a mis en place des mesures de sécurité adéquates.

Procès intenté par le patient en responsabilité civile et contractuelle du médecin ?
Plus le patient subira des atteintes graves en raison de la cyber-attaque dont son médecin aura été victime, plus il sera susceptible d'initier un procès en responsabilité civile et contractuelle contre celui-ci pour lui réclamer le paiement de dommages-intérêts.

Le montant des dommages-intérêts réclamés dépendra des circonstances du cas d'espèce, en particulier des griefs soulevés par le patient. La réparation pécuniaire réclamée sera probablement limitée si le patient se plaint d'une violation par négligence du secret médical. Le montant pourra être sensiblement plus élevé si le patient se plaint d'une erreur médicale lui ayant causé de graves séquelles. Le montant atteindra des sommets si le conjoint survivant se plaint d'une erreur médicale ayant causé le décès de son conjoint[17] et réclame le paiement d'une indemnité pour perte de soutien[18].

Conclusion

Une cyber-attaque fait peser des conséquences juridiques potentiellement très lourdes sur le médecin. Pour s'en prémunir, il lui appartient de prendre toutes les mesures nécessaires pour assurer une sécurité adéquate des données de ses patients au regard des risques encourus. Concrètement, le médecin devra démontrer avoir réfléchi à la question, avoir trouvé des solutions et avoir pris les mesures préventives nécessaires. ●

Maître Grégoire Chappuis
Etude Python Avocats (Genève) SA

Référence

1. Le rançongiciel (ou *ransomware*) est un type de logiciel malveillant qui infecte les fichiers et systèmes informatiques de la cible. Ses données sont alors cryptées et ses systèmes informatiques rendus inexploitables jusqu'au paiement de la rançon demandée par les *hackers* (cf. Rapport semestriel 2020/2 [juillet à décembre] du Centre national pour la cybersécurité NCSC du 11 mai 2021, p. 11 ss.).
2. Il peut s'agir de la Loi fédérale sur la protection des données, d'une loi cantonale telle que la Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles et/ou du Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).
3. Le lecteur est rendu attentif au fait que l'étendue des obligations décrites ci-après peut varier, en particulier si le médecin est soumis au RGPD, ce qui sera souvent le cas pour les patients domiciliés dans un pays de l'Union Européenne.
4. Art. 7 et 8 al. 1 nLPD
5. https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2022/empfehlungen-gesundheitssektor.html (consulté le 23.11.2022)
6. Art. 9 al. 1 et 2 nLPD.
7. Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, Feuille fédérale 2017 p. 6565 ss, p. 6651.
8. Art. 24 al. 1 nLPD. Les points que l'annonce doit couvrir sont prévus à l'art. 24 al. 2 nLPD, ainsi qu'à l'art. 15 nOPDo.
9. Art. 24 al. 4 nLPD.
10. Art. 15 al. 4 nOPDo.
11. Erard, Frédéric, *Le secret médical*, thèse, 2021, n. 461 et 469.
12. Si le médecin estime que la réalisation de l'infraction est possible et s'accommode de cette possibilité, il viole le secret médical par dol éventuel, ce qui constitue une forme de l'intention. En revanche, si le médecin estime que la réalisation de l'infraction est possible mais compte sur le fait qu'elle ne se produira pas, alors il agit par négligence consciente (et non intentionnellement) si la cyber-attaque qu'il a subie a entraîné la divulgation à un tiers non autorisé des données couvertes par le secret. Dans un tel cas, le médecin ne viole pas l'art. 321 CP.
13. L'art. 40 let. f LPMéd réaffirme l'obligation du médecin d'observer le secret médical.
14. Les membres de l'AMGe s'engagent à respecter notamment le Code de déontologie de la Fédération des médecins suisses (FMH), dont l'art. 11 impose aux membres de respecter le secret médical.
15. Erard, Frédéric, op. cit., n. 461, 469 et 709.
16. Art. 61 let. c nLPD.
17. À noter qu'en septembre 2022, les médias ont fait état du premier patient décédé en Europe en raison d'une cyber-attaque : https://www.sante.org/le-blog-sante.org/first-death-caused-by-cyber-attack (consulté le 23.11.2022)
18. Art. 45 al. 3 du Code des obligations.

Comment protéger votre réseau informatique ?

Toutes les entreprises, aussi petites soient-elles, sont la cible des criminels informatiques. Les menaces sont quotidiennes, non discriminantes et les conséquences souvent dramatiques.

Il est malheureusement illusoire de chercher la sécurité définitive et absolue : vous ne pouvez que compliquer la tâche des criminels, leur demander plus d'efforts qu'ils ne tireront peut-être de bénéfice et les inciter ainsi à aller voir ailleurs. La bonne nouvelle, c'est que c'est souvent largement suffisant !

Les menaces sont de plus en plus sophistiquées

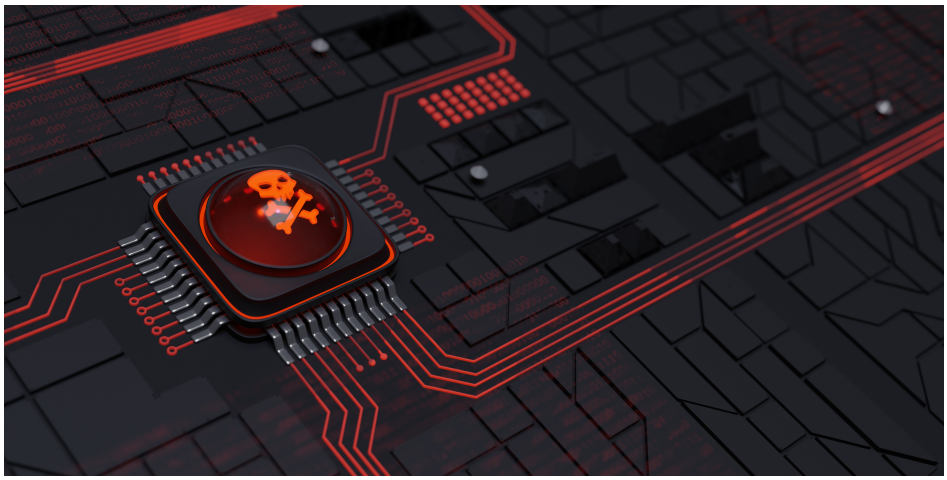
Les menaces auxquelles nous sommes tous confrontés sont de plus en nombreuses mais surtout de plus en plus convaincantes. L'époque des courriels rédigés dans un français très approximatif qui vous demandent le numéro de votre carte de crédit est définitivement révolue.

Les criminels ont désormais à leur disposition des outils sophistiqués et des talents particulièrement aiguisés qu'ils recrutent à grand renfort d'offres publiques d'emploi.

La survie de chaque entreprise, quelle que soit sa taille, passe nécessairement par une profonde prise de conscience des risques et la mise en place de mesures de sécurité essentielles

Protéger votre exposition sur internet

Votre réseau informatique est une cible de choix pour les criminels lorsqu'ils s'intéressent à vous.
Ainsi, les outils que vous utilisez quotidiennement, mais aussi ceux qui ont été mis en place dans l'urgence début 2020 avec le début de la pandémie, peuvent constituer une porte d'entrée facile d'accès :
-la manière dont vos collaborateurs travaillent depuis leurs domiciles respectifs
-votre messagerie professionnelle (Exchange?)
-vos caméras de surveillance,
-etc.



Il faut disposer d'un parefeu (firewall) qui protège votre réseau informatique, vos infrastructures et tous les équipements électroniques de votre cabinet. C'est lui qui est responsable de ce qui peut être utilisé de l'extérieur mais aussi de ce qui peut être réalisé de l'intérieur du cabinet directement.
Rien de ce qui se trouve dans votre cabinet ne doit être visible depuis internet sans avoir été préalablement identifié par votre propre serveur VPN (Virtual Private Network). Si par exemple vous utilisez régulièrement des services de "Bureau à distance" sur votre serveur Windows au cabinet, la connexion préalable à votre propre serveur VPN doit être obligatoire.
Les journaux d'activités devraient être activés partout où c'est possible afin de conserver le maximum de traces et d'éléments en cas d'incident ou d'intrusion.

Ce sont eux qui permettront de comprendre ce que les criminels ont pu faire et ce qu'ils ont potentiellement exfiltré.

Ce ne sont que les tous premiers gestes de survie qu'il faut effectuer. Ces actions sont toujours l'affaire de professionnels très spécialisés car le domaine est extrêmement complexe.

Protéger vos postes de travail

L'une des premières règles concernant les postes de travail est de les tenir aussi à jour que possible. Que ce soit Windows ou MacOS, installez toujours les dernières versions, puis toutes les mises à jour qui sont rendues disponibles par la suite.
Installez/activez un antivirus et un parefeu sur chaque poste de travail (Windows & Mac). Pour Windows, le produit "Defender" qui est intégré à Windows 10/11 est parfaitement suffisant. Efficace et discret, le produit a fait d'importants progrès ces dernières années et il est une excellente alternative aux grands noms du marché (Kaspersky, McAfee, Sophos, BitDefender, etc).

Sur Mac, le parefeu intégré doit être activé et un antivirus de votre choix ajouté (BitDefender, ClamXAV, etc). Les virus sont certes moins nombreux sur Mac mais ils sont de plus en plus fréquents. Avec les parts de marché grandissantes d'Apple, la tendance va s'accélerer. Un antivirus a toujours été indispensable, maintenant plus que jamais.

N'utilisez/n'installez aucun programme qui ne soit pas indispensable pour votre pratique ou celle de votre secrétariat. N'utilisez pas de logiciel gratuit aux usages multiples, pour vous aider à optimiser votre PC (CCleaner par exemple) ou pour ajouter de nouvelles émoticones à votre messagerie. Ce ne sont que deux cas parmi d'autres pour rappeler que les logiciels gratuits ne sont jamais gratuits et vos données médicales sont trop précieuses pour être partagées en échange de cette gratuité. Moins il y a de logiciels installés sur vos postes de travail, plus la surface d'attaque est réduite pour le criminel.

Evitez d'utiliser les clés USB pour échanger des documents, que ce soit entre vos propres PC ou de l'extérieur (fiduciaire, patients, confrères). Elles constituent l'un des vecteurs importants de la transmission des virus informatiques. Préférez des services d'échange de données mieux sécurisés comme Swisstransfer (https://swisstransfer.com) ou votre messagerie @amge.ch par exemple.

Enfin, appliquez une séparation stricte entre la sphère professionnelle et la sphère privée. Il ne faut pas consulter vos courriels privés sur les PC du cabinet, et cela vaut aussi pour votre secrétariat. Consulter sa messagerie privée dans l'environnement sécurisé de votre cabinet médical revient à inviter un criminel chez vous : vous pouvez avoir le meilleur système d'alarme disponible, il ne sert à rien lorsque c'est vous qui leur ouvrez la porte.

Accompagnement, sensibilisation des collaborateurs

Vos collaborateurs se trouvent en première ligne et c'est eux que les criminels contacteront par courriel ou par téléphone. C'est l'un des passages obligés pour pénétrer votre réseau et prendre possession de vos infrastructures.

On lit encore trop souvent que les collaborateurs sont le maillon faible de la cybersécurité. C'est non seulement faux mais c'est tout le contraire car un collaborateur sensibilisé, formé, accompagné, sera le meilleur atout possible à votre disposition. Bien sûr, il ne s'agit pas de les transformer en spécialistes de cybersécurité, mais lorsqu'ils ont été sensibilisés, lorsqu'ils ont vu comment les criminels travaillent et leurs méthodes pour convaincre ou mettre la pression, vos collaborateurs deviennent alors infiniment plus vigilants. Et plus leur vigilance augmente, plus votre sécurité s'améliore.

Il faut aussi rappeler de favoriser et encourager la communication de toutes les façons possibles. En cas de doute, vos collaborateurs doivent pouvoir s'adresser à un point de contact clairement identifié. S'ils pensent avoir fait une fausse manipulation ou cliqué sur un lien suspect, ils doivent pouvoir en informer leur contact sans délai et surtout sans crainte ; il est encore trop souvent pratiqué la "formation obligatoire en cybersécurité" en représailles d'un clic inattentif. Tout le monde (et, nous, professionnels aguerris compris!) peut avoir quelques secondes d'inattention, de baisse de vigilance ; il suffit du bon message, au bon moment, avec le bon contexte et la bonne coïncidence, et nous cliquerons tous, cela ne fait aucun doute.

Lorsque cela arrivera, la communication et sa spontanéité seront les éléments déterminants pour maîtriser et atténuer les conséquences. Il faut les entraîner, les faciliter, les développer et les inciter.

L'entreprise doit également fournir les outils indispensables pour que ses collaborateurs puissent exercer dans les meilleurs conditions possibles. Il n'est par exemple pas raisonnable de demander d'utiliser des mots de passe compliqués, longs et systématiquement différents pour chaque service sans leur fournir un gestionnaire de mots de passe (1Password, DashLane, Biltwarden, etc).

Et c'est bien sûr valable pour toutes les autres contraintes que vous jugerez pertinentes pour la sécurité de vos données : il faut les accompagner de solutions et d'outils pour qu'elles ne deviennent pas des obstacles. Sans cela, nous observons qu'elles finissent toujours par être contournées. Pas systématiquement par lassitude mais parce qu'elles deviennent un frein à l'efficacité du travail de vos équipes.

Conclusion

Si vous parvenez à mettre en place ces premières recommandations, vous aurez déjà fait un pas significatif vers la sécurité. Comme nous l'avons dit en ouverture de cet article, la sécurité absolue n'existe pas mais tous ces petits pas décrits plus haut sont autant d'obstacles à surmonter pour les criminels. Et comme tout le monde, ils n'apprécient pas les efforts inutiles. Alors ennuyez-les autant que possible.

IT-Awareness Sàrl
Fabian Lucchi
Spécialiste IT

Comment s'assurer qu'elles soient disponibles

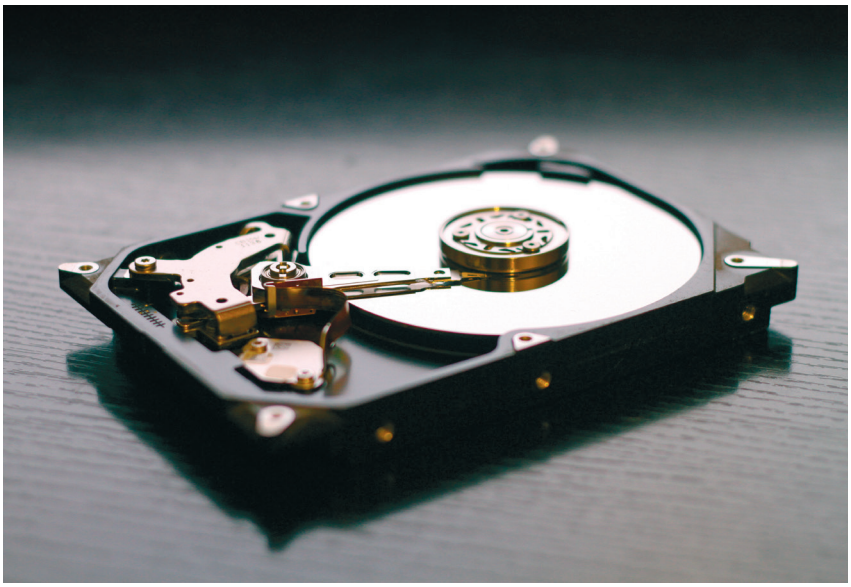
De l'importance des sauvegardes

Nous présentons ici quelques règles élémentaires de bonne pratique qui vous assurent la disponibilité et l'integrité de vos données, en toute circonstance.

Pouvoir disposer de sauvegardes fiables et à jour nécessite de suivre quelques principes de base simples :

- l'anticipation
- sauvegardes à l'abri des rançongiciels et des virus
- le chiffrement
- au moins une copie dans un autre lieu
- une sauvegarde qui n'est pas testée n'existe pas.

Si vous les appliquez assidûment, vous ne vous trouverez jamais démuni après un incident informatique, quel qu'il soit, et vos données seront toujours disponibles.



Disque dur mécanique interne.

L'anticipation

La première règle ne souffre aucune exception : vous devez mettre en place un plan de sauvegarde approprié en amont de tout incident.

Nous faisons tous confiance aux installations en place car elles fonctionnent bien tout au long de l'année. Si bien qu'on en oublie même leur présence. Jusqu'au moment où un rouage se grippe (p. ex. un rançongiciel ou une panne).

Quand un incident surviendra pour vous (il ne s'agit pas de savoir "si" mais bien "quand"), vous aurez besoin de vos sauvegardes pour remettre votre cabinet en état de fonctionner.

À défaut de les avoir à disposition et pleinement fonctionnelles, vous n'aurez plus aucune donnée, plus de dossiers patients (par exemple pour Mediway, Achille, PSIpi, etc), plus de comptabilité, plus d'agenda, plus de courriers, plus de liens avec les laboratoires. Exactement comme si on emportait vos PC et vos serveurs pendant la nuit et qu'on vous laissait, en échange, un bloc de papier et quelques crayons.

Sauvegardes à l'abri des rançongiciels et des virus

Nous devons préciser avant toute chose que si vous faites déjà des sauvegardes avec un disque externe que vous branchez avec un cable sur votre serveur, c'est très bien. Et si vous utilisez plusieurs disques différents que vous remplacez peut-être tous les jours, c'est encore mieux.

Malheureusement, **cela revient parfois au même que ne pas avoir de sauvegarde** du tout !

Si vos serveurs voient ce disque externe, le rançongiciel aussi. Il prendra possession de vos sauvegardes, au même titre que toutes les autres données, et il les chiffrera avec sa propre clé. Elles seront sous le contrôle exclusif des criminels et vous n'aurez d'autre choix que de négocier avec eux pour obtenir la clé qui vous permettra **peut-être** de les récupérer.

Bien que la décision de négocier ou non avec un acteur malveillant soit individuelle et dépendante de chaque situation particulière, vous n'aurez aucune garantie d'obtenir une clé fonctionnelle de leur part. Certains rançongiciels

Enigma, machine à chiffrer/déchiffrer.

comportent des défauts de conception qui rendent tout déchiffrage impossible, même avec la bonne clé.

Et il faut garder à l'esprit qu'il s'agit de criminels : le respect et l'éthique ne font pas partie de leurs valeurs.

Pour corser le tout, certains virus sont conçus pour détruire vos données, sans récupération possible. Parmi eux, quelques variantes agissent très lentement pour passer inaperçues le plus longtemps possible. Elles détruisent quelques mots/phrases dans des documents pris au hasard, petit à petit sur plusieurs semaines/mois. Il vous faudra «par chance» ouvrir l'un de ces documents altérés pour réaliser ce qu'il est en train de se passer. Et le jour où vous vous en rendrez compte, le virus aura déjà endommagé des milliers de documents.

L'utilisation de disques externes pour vos sauvegardes permet généralement de revenir en arrière de quelques jours mais ce sera insuffisant pour retrouver vos données. Les recommandations courantes quant à la durée de conservation des sauvegardes vont de 2 à 13 mois.

Il est crucial d'utiliser un système de sauvegarde qui les place hors de portée des rançongiciels et permette en plus de les conserver sur une longue période.

Vous ne devriez ainsi pas utiliser un disque externe directement branché sur le serveur (disques USB à proscrire) ni un dossier partagé sur votre réseau. Il faut privilégier un moyen qui ne soit pas directement visible par Windows ou MacOS. Les «petits» serveurs de fichiers qu'on appelle «NAS» (pour Network Attached Storage) sont par exemple une bonne solution (Synology, QNAP, etc), mais un fournisseur d'espace de sauvegarde "Cloud" situé en Suisse est tout aussi bon (Exoscale, infomaniak, etc).

Le chiffrement

Vos sauvegardes doivent toujours être chiffrées afin de les protéger des regards non autorisés. Si quelqu'un peut voir les fichiers de votre dernière sauvegarde, il ne doit pas pouvoir en comprendre le contenu. C'est valable pour celles que vous confiez à un service Cloud, mais aussi pour celles que vous faites sur place dans votre cabinet (en cas de cambriolage).

Veillez toutefois à garder la clé de chiffrement en totale sécurité et toujours disponible : si elle protège vos données des regards non autorisés, elle vous en interdit aussi l'accès si vous l'égarez.

Au moins une copie dans un autre lieu

Les solutions spécialisées que vous installez dans votre cabinet garantissent une résilience optimale de vos données en cas d'incident, mais elles ne vous protègent pas des dégâts physiques (incendie, panne, cambriolage).

La seule garantie fiable de la disponibilité de vos sauvegardes est une copie automatique dans un autre lieu :

- si vous faites des sauvegardes sur place au cabinet, il faut conserver une copie automatique à l'extérieur
- si vous avez confié vos sauvegardes à un prestataire informatique, il faut qu'il dispose d'une copie automatique dans un second emplacement.

Et non, emporter les disques externes USB à l'extérieur du cabinet ne constitue pas une copie dans un second emplacement!

Cela peut sembler excessif mais il faut rappeler l'omniprésence de la Loi de Murphy qui dit :

« Si quelque chose peu mal tourner, ça tournera mal. Mais au pire moment. »

Porte de coffre fort historique

Une sauvegarde qui n'est pas testée n'existe pas

Voici une situation vécue par une société qui ne disposait pas de prestataire informatique : les collaborateurs avaient pour consigne de remplacer un disque dur branché directement sur le serveur tous les jours et de faire une rotation avec 10 disques différents, un pour chaque jour de la semaine sur deux semaines. Le disque était emporté à l'extérieur des locaux chaque jour et remplacé par le suivant le lendemain.

Par chance, la société s'est dit qu'il était temps de faire contrôler son installation. Il a été découvert que le logiciel de sauvegarde **n'enregistrait plus rien sur les disques depuis plusieurs mois.** Les collaborateurs transportaient ainsi des disques vides pour les mettre à l'abri. Sans ce regard extérieur, la société ne s'en serait rendu compte que le jour où une sauvegarde aurait été nécessaire après un incident.

Il est **essentiel de vérifier très régulièrement** que les sauvegardes contiennent bien ce que l'on pense qu'elles contiennent. Et plus on le fait souvent, plus le temps de travail potentiellement perdu en cas de problème sera réduit car on a l'assurance qu'elles sont à jour.

Il faut aussi régulièrement lire la dernière sauvegarde intégralement, comparer ce qui est récupéré avec ce qui est en ce moment sur le serveur, chercher à identifier les différences, les dossiers oubliés. Sans cette étape, vous ne saurez si vos sauvegardes sont fonctionnelles que le jour où vous en aurez besoin.

Si vous confiez déjà vos sauvegardes à votre prestataire informatique, il doit vous informer spontanément de tous les tests qui sont effectués, des divergences potentielles entre votre serveur et ce qui est sauvegardé, des ajustements qu'il applique pour y remédier. Bref, il doit vous tenir au courant tout au long de l'année. Si vous n'avez jamais de retour de sa part au niveau du contrôle des sauvegardes, appelez-le dès maintenant pour que que cela change. La transparence est la seule garantie éprouvée.

Les services de professionnels sont nécessaires

Gérer efficacement des sauvegardes est pratiquement un métier à part entière. Et bien que vous puissiez le faire vous-même (avec le bon logiciel, le bon service Cloud, la bonne combinaison d'outils et le bon accompagnement), l'expérience du terrain montre que vos sauvegardes ne seront au bout du compte et dans la plupart des cas :

- pas à jour ; il faut du temps pour surveiller leur bon déroulement, chaque jour
- pas contrôlées en détail ; il faut du temps, ponctuellement tout au long de l'année
- probablement jamais testées ; il faut du temps et des ressources.

Pouvoir disposer de sauvegardes de données efficaces demande de l'expérience et des compétences spécifiques, mais aussi et surtout du temps pour l'entretien et le suivi.

Il convient de mettre en balance d'une part le budget demandé par les prestataires spécialisés pour assumer cette charge pour vous, et d'autre part les conséquences d'un retour au bloc-notes et aux crayons si lors de votre arrivée au cabinet un matin vous constatiez la disparition de votre matériel informatique ou de vos données. ●

IT-Awareness Sàrl
Fabian Lucchi
Spécialiste IT

Être prêt à gérer une cyberattaque, se préparer avant la crise

"Il y a 2 types d'entreprises celles qui SONT en crise et celles qui le SERONT"(Didier Heiderich)

Votre organisation est-elle résiliente? Notre définition de la résilience: «Une organisation résiliente est une organisation consciente, qui maîtrise ses risques, est organisée en cas de crise et a prévu des plans de secours pour assurer la continuité de ses activités.»

Ces quatre facteurs sont souvent appréhendés par les sociétés de manière individuelle, alors que c'est seulement en les associant que la résilience est possible et devient instinctive.

Les dirigeants de toutes organisations doivent pouvoir répondre à ces quatre questions.

Maîtrisez-vous vos risques?

Les entreprises et gouvernements sont mal ou pas préparés à réagir à un choc extrême. Il est pourtant de la responsabilité de chaque dirigeant de prévoir la survie de son entreprise et de ses activités.

L'acronyme VICA pour volatile, incertain, complexe et ambigu, caractérise parfaitement l'environnement dans lequel évoluent les entreprises. La volatilité se caractérise par une forte instabilité de l'environnement qui peut se manifester par des changements brusques, parfois violents, sans que ceux-ci soient prévisibles et sans que ces changements permettent

«Gouverner, c'est prévoir»

Emile de Girardin

Gestion des risques
- Entreprise
- Humains
- Système d'information

Gestion de crise
- Organisation de la cellule
- Logistique & matériel
- Procédures, chaîne de décisions et suivi

Gestion de la continuité
- Activités
- Ressources
  - IT
  - RH
  - Logistique
  - Fournisseurs

nécessairement de retrouver une quelconque stabilité nouvelle.

Les entreprises sont donc seules et doivent être autonomes en termes de gestion de crise et de continuité.

Êtes-vous prêts à gérer une situation de crise ?

Un événement **soudain**, souvent très **brutal, imprévu,** ayant des **conséquences importantes, graves** pour le service et pour lequel les procédures et organisations habituelles sont dépassées, inadaptées. La crise dépasse l'organisation et les processus standards.

Les causes peuvent être variées, naturelles (inondations, tempêtes, tremblements de terre, épidémies, etc.), environnementales (incendies, explosions liées à des infrastructures ou site à risque, etc.), humaines (défaillances de processus, erreurs humaines, malveillances, attentats, etc.), technologiques (pannes, défaillance matérielle, virus, **cyber-attaque**, etc.).

Il s'agit donc de gérer la survenance d'un événement extraordinaire malgré un certain nombre de facteurs aggravants, tels que le stress, la pression (politique, média, interne, etc.) et le cumul des événements en cascade (systémique).

Il faut donc s'appuyer sur une méthode approuvée et entraînée avec des individus (cellule de crise), une logistique (salle de crise), des formulaires et procédures (journaux d'appels, de décision, main courante, suivi des actions, étude de scénarios, etc.) pour pouvoir justifier par la suite, les décisions, les actions et les mesures prises devant un conseil d'administration, des actionnaires ou la justice.

Le challenge est donc d'avoir les outils et indicateurs pertinents et permettant une lecture rapide de la situation afin de prendre les décisions adéquates. Il est nécessaire d'avoir une vision dynamique des risques et menaces, d'évaluer l'impact et probabilité, notamment avec une menace immatérielle.

La cellule de crise doit pouvoir actionner des mesures pour sauver l'entreprise, réduire les impacts et assurer la poursuite de ses activités.

Avez-vous des plans de secours pour assurer la continuité de votre activité ?

« Ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes de l'entreprise puis la reprise planifiée des activités »

Cf. Règlement 97-02 du Comité de réglementations bancaire et financière

Ainsi, la continuité d'activité est un ensemble de mesures permettant à une entreprise d'anticiper et maîtriser ses risques opérationnels, en réduisant les impacts potentiels d'une interruption. On appelle Gestion de la Continuité d'Activité (BCM pour Business Continuity Management) la mise en place de procédures opérationnelles permettant de maintenir les activités, même en mode dégradé, en cas de sinistre, et de revenir à une situation normale le plus rapidement possible.

Quatre ressources principales maintiennent l'activité d'une entreprise :

- L'IT (Informatique, data center, communication)
- Les RH (Compétences clés, employés, direction)
- La logistique (Bâtiments, transport, chaîne de production)
- Les fournisseurs (Matière première, produits, services)

Ces quatre ressources, de manière individuelle ou cumulée, doivent être confrontées à vos risques et à des scénarios de catastrophes. Lorsque l'activité de ses ressources sont couvertes, nous parlons de continuité.

L'entreprise est ainsi capable de reprendre son activité après un sinistre, et de capitaliser sur les expériences vécues, afin de se maintenir dans un processus d'amélioration continue et de performance.

La continuité est une démarche qui s'anticipe. Lorsqu'une crise survient, il est trop tard pour s'y préparer.

Un proverbe chinois l'énonce comme ça : « Les tuiles qui vous protègent de la pluie ont été posées par beau temps ».

Vos collaborateurs sont-ils conscients des comportements à adopter et des enjeux de la continuité ?

La sensibilisation des collaborateurs est une des clés de la résilience. En effet, lorsque chaque collaborateur mesure les enjeux, tant pour l'entreprise qu'au niveau personnel (perte d'emploi, diminution de salaire pour chômage technique, etc.), il devient acteur du processus de continuité en proposant des solutions, en demandant et en participant aux tests et exercices.

La direction de l'entreprise doit porter la culture de la continuité en sensibilisant l'ensemble du personnel, en formant les responsables d'activités, en exerçant continuellement les procédures de secours ou de contournement et en cherchant constamment à vérifier et à améliorer les plans de secours.

Pour preuve, les organismes comme l'armée, les services de secours (police, sanitaire, feu), sont tous dans un processus d'entraînement et de répétition afin d'être prêts et efficaces lors de la survenance d'un sinistre. ●

Charly Delay
PragmaTIC-Consulting