N°85
Mars-Avril
2021

www.village-notaires.com

Le Journal du Village des Notaires

Actualités

Enquête

Management

Associations

Gestion de patrimoine

Immobilier

Communication

Zoom sur

Veille juridique

legiteam Editions

Développer sa résilience face aux **crises cyber** *?*

La résilience prend progressivement le pas sur la sécurité comme concept central de l'informatique, afin d'appréhender les dynamiques de manière multidimensionnelle. Car la probabilité de se faire attaquer et pirater est tellement élevée que la question n'est plus seulement d'organiser la défense, mais également de minimiser l'impact d'un piratage réussi. Pour cela, il faut réagir vite et de la bonne manière.

En 2019, plus de 41% des entreprises de moins de 49 salariés avaient subi une ou plusieurs attaques ou tentatives d'attaques informatiques, qui se répartissaient ainsi pour les principaux types : 24 % de hameçonnage, 20 % *malware*, 16 % de *ransomware* (rançongiciel) et 6 % de fraude au président. En 2020, la tendance est encore plus forte puisque, selon l'éditeur de sécurité *Proofpoint*, 91 % des entreprises auraient été visées, et 65 % l'auraient été à plusieurs reprises. Nul n'est à l'abri, puisque les éditeurs de logiciels et de services numériques sont eux aussi fortement touchés, comme la française *Sopra Steria*, ou l'américaine *Solar Winds*, dont la faille de sécurité a mis en danger un grand nombre de grandes entreprises et de structures gouvernementales aux États-Unis.

Si tout le monde est concerné, le monde notarial a bien sûr ses spécificités. D'une part, il est constitué de TPE-PME, avec, d'une part, une moindre exposition médiatique que les grands groupes, et une plus grande facilité à communiquer en direct avec les autres membres de l'étude dès qu'un problème semble émerger, sans avoir à passer par les réseaux – un avantage que le télétravail pourrait venir entamer.

Les études notariales bénéficient aussi d'un avantage spécifique face au risque cyber qui est que la plupart d'entre elles ont un backup papier et une pratique encore pas totalement numérisée, qui leur permet de pouvoir continuer partiellement leur activité en cas de crise.

En revanche, les notaires traitent des données qui sont non seulement sensibles d'un point de vue financier, mais relèvent pour certaines de l'intime – testaments, contrats de mariage,… ce qui leur donne une responsabilité particulière dans la protection des données personnelles.

Les notaires sont-ils pour autant conscients du danger ? « *Malgré une prise de conscience progressive,* explique Arnaud Gressel, expert chez Resco Courtage, *il y a une erreur que j'observe de manière récurrente, qui est de croire que l'on n'est pas concerné parce qu'on n'est pas une cible. Mais c'est sous-estimer le fait qu'il n'y a pas besoin d'être une cible pour être attaqué. Les campagnes d'emailing captent très, très large, et l'on reçoit tous les jours des faux e-mails sur lesquels il suffit que quelqu'un clique une fois. Pour l'instant, je constate que ce sont surtout lorsque des structures ont été touchées ou victimes à un moment donné ou qu'elles ont vu de près une crise qu'elles sont les plus sensibilisées* ».

Comment réagir face à la crise ?

L'élément central d'une crise cyber est la perte de repères. « *Contrairement à des entreprises de grande taille,* indique Emmanuelle Hervé, experte en gestion de crise chez *EH&A, les petites structures se retrouvent seules, sans conseil d'administration derrière, sans comité d'étude des risques qui leur aurait dit, en amont, qu'il faut se préparer à ceci ou cela et comment le faire. Il y a beaucoup d'intuitu personae dans les petites structures, et la personnalité des dirigeants a beaucoup d'influence sur les décisions prises, car ils n'ont pas en interne de système expert d'aide à la décision, qui les aide à déterminer si une situation est suffisamment crisogène pour justifier l'ouverture d'une cellule de crise. Donc, quelle que soit la taille de l'entreprise, la gestion de crise ne s'improvise pas, il y a des processus et des méthodes qu'il convient de travailler en temps de paix* ».

Une situation de crise cyber est donc marquée par la confusion : les ordinateurs ne marchent plus, les mails ne passent plus, l'activité est interrompue. Le dirigeant se retrouve très démuni car il ne sait pas quelle est l'étendue des dégâts : est-ce qu'il y a des *data* volées ? Sont-elles juste cryptées ? Quels types de *data* sont concernées ? Quel volume ? Il est normal d'être déboussolé mais il faut d'abord être clair sur les priorités : redémarrer le plus tôt possible tout en préservant le capital confiance de l'étude. Pour cela, il est indispensable de se faire aider.

« *Le but,* souligne Delphine Mercelat, Directrice des assurances du notariat chez *LSN assurances*, *est que l'étude contacte au plus vite l'assurance afin que le sinistre soit géré en un minimum de temps et que l'activité soit interrompue le moins possible. Plus le notaire réagit vite, plus il nous déclare le sinistre vite, plus ça peut être réglé vite. S'il tarde un peu, le virus peut alors se diffuser et atteindre tout le réseau informatique de l'étude* ».

Un réflexe récurrent mais qui n'est pas pertinent est d'appeler le prestataire informatique habituel, parce que, d'une part, celui-ci n'a peut-être pas forcément le même temps de réactivité ni la même disponibilité que les experts de l'assurance et, d'autre part, le côté cyber peut être quelque chose de nouveau et de compliqué à gérer pour lui. Il n'aura peut-être pas le réflexe de gérer l'incident avec une approche d'expert qui consiste à sauvegarder les preuves pour l'indemnisation et le recours, ou pourrait avoir tendance à débrancher le système informatique alors que certains éléments peuvent encore être sauvés.

Aux côtés de la réponse informatique, les autres pans de la réponse à la crise sont, d'une part juridique, et d'autre part communicationnel. Dans tous ces domaines, la bonne démarche consiste à recourir aux experts mis à disposition par les assurances.

Si le notaire n'a pas la main sur les aspects informatique et juridique, il doit néanmoins concentrer toute son énergie sur la gestion de crise et sur la communication. Une difficulté principale dans une telle situation est qu'il est presque impossible de savoir combien de temps les opérations en cours – déchiffrage, négociation – vont durer : quelques heures, quelques jours ou quelques semaines.

Pour organiser ces aspects, une réunion de crise doit être organisée au plus vite. Elle peut ne prendre que quelques heures, et permet de clarifier les priorités pour cette situation exceptionnelle : « *pour bien analyser tous les scénarios d'évolution,* indique Emmanuelle Hervé, *il faut partir de l'événement et se demander : comment cela peut-il empirer ? Même si*

Que faire en cas de demande de rançon ?

S'ils sont à la recherche de rançons importantes, les hackers ne vont pas viser de notaires, mais des grandes structures. Toutefois, les *ransomwares* génériques circulent, et fonctionnent, puisqu'un certain nombre d'entreprises se font piéger et finissent par payer. S'il faut savoir que la recommandation classique en France, en cas de *ransomware*, est de ne surtout pas payer, une observation essentielle est que « *les entreprises assurées contre le cyber payent beaucoup moins de rançons que les sociétés qui ne sont pas assurées*, précise Arnaud Gressel, expert chez *Resco Courtage*, *du simple fait qu'elles ont une assistance immédiate dès les premières heures. Tout va plus vite, les données vont être mieux préservées, et la pression est moindre. Quand une entreprise est livrée à elle-même, elle va plus facilement se dire qu'il vaut mieux payer pour survivre* ».

l'on a envie de se dire que ça va s'arranger, il faut faire cet effort intellectuel. Si toute l'informatique est bloquée pendant des mois, quelle continuité d'activité est possible ? Si des datas sensibles sont dehors, quels sont les impact côtés clients et employés ? et côté CNIL ? Que faire si nous prenons une amende de 4 % du CA et une procédure au pénal ? il faut balayer toutes les grandes dimensions de la crise par catégorie, business, financier, juridique, humain, réputationnel et dérouler les scénarios d'évolution défavorables jusqu'au bout. C'est ça qui est difficile en général, c'est de le faire jusqu'au bout et, ensuite, de remonter dans l'autre sens en se demandant ce qu'on peut faire pour, soit baisser la probabilité d'occurrence des scénarios qu'on vient de développer, soit diminuer l'impact si jamais ça arrive quand même. Et donc, ça, c'est vraiment un travail à faire en démarrage de gestion de crise ».

Une autre démarche indispensable à réaliser, qu'il aurait même été préférable de réaliser en amont, est la cartographie de toutes les parties prenantes de l'étude. En externe : identifier les clients importants qui vont particulièrement s'inquiéter d'un éventuel vol de données et les appeler directement pour leur assurer que le maximum est fait. En interne : aller parler aux employés qui peuvent craindre pour la perte de leur emploi, ou qui se sont fait voler des photos compromettantes qu'ils gardaient sur l'ordinateur de bureau, et qui peuvent avoir peur qu'elles fuitent. S'il est encore temps, c'est l'occasion de mettre sur papier l'ensemble des contacts pour pouvoir communiquer avec ces personnes même si toutes les données ont été perdues ou bloquées.

Jordan Belgrave

Jean-Marc Couret, notaire à Toulon : « *Je suis très attentif à la protection informatique* »

J'ai mis en place un système automatique de sauvegarde toutes les six heures, que je contrôle régulièrement : trois sauvegardes sur place sur trois serveurs différents plus une sauvegarde en extérieur, donc quatre sauvegardes redondantes. Le backup des bases de données a lieu la nuit et est répercuté sur mes différentes sauvegardes. Je réalise également une copie des images virtuelles de mes serveurs et de mes postes clients une fois par mois. C'est une opération manuelle que j'ai quand même grandement automatisée, mais je dois arrêter moi-même les machines pour éviter que le processus ne démarre alors qu'elles sont en cours de fonctionnement. De la sorte, j'ai une redondance d'informations et je peux réinstaller les postes en partant de zéro et redémarrer l'activité très facilement. À ce niveau-là, on peut difficilement faire plus.

Les ordinateurs de notre étude font tourner des machines virtuelles Windows sous Linux, car je trouve que Linux a une plateforme stable et sécurisée, notamment pour les serveurs (ne pas oublier que plus de 60 % des serveurs servant d'infrastructure d'internet sont des machines Unix (Linux ou BSD)... C'était encore plus vrai avant Windows 10. Sous Linux, les machines sont, par défaut, en mode utilisateur et, quand vous avez de l'administration à faire, vous entrez seulement à ce moment-là en mode administrateur. La base de la sécurité informatique est que seuls l'informaticien ou le dirigeant aient le statut administrateur. Sans quoi, tout le monde peut s'installer des logiciels sur sa machine et risquer d'infecter des postes. Dans le même esprit, les ports USB sont désactivés par défaut.

Il est certain que la virtualisation ralentit un petit peu les machines par rapport à une machine exécutant en direct Windows, mais on est sur un niveau de sécurité supplémentaire parce que, si la machine Windows est piratée, les machines sous Linux, et notamment les serveurs, sont mieux protégées. La sécurité informatique absolue n'existe pas, mais mon système permet au moins de limiter les risques et de traquer d'où a pu partir la fuite.

J'ai déjà eu une attaque au crypto-virus sur un serveur Windows. J'ai interrompu toutes les machines de l'office, étant sensibilisé aux principes de sécurité informatique et d'isolation des postes. Une fois que tous les ordinateurs étaient éteints, j'ai pu les vérifier chacun indépendamment sans connexion avec le réseau, puis réinstaller une image virtuelle de sauvegarde sur les postes contaminés, déterminer le serveur et restaurer les données corrompues. Tout cela m'a pris quatre heures et, le lendemain, toute l'informatique était opérationnelle sur l'étude. Pour le même problème, un confrère a eu 15 jours d'immobilisation de son étude.

*Les nouveautés de l'*archivage notarial *?*

L'archivage fait partie de l'ADN des notaires : préserver le passé pour assurer leur mission aujourd'hui et préparer la transmission en bon ordre à ceux qui viendront après. Pour autant, les choix sont nombreux et variés, et font jouer tout autant des aspects financiers, organisationnels, que culturels, entre partisans du zéro papier et sceptiques du numérique, ainsi que dans l'appréhension des diverses technologies disponibles.

L'archivage est d'abord une question d'organisation : « *Je me suis rendu compte,* souligne Françoise Cohen-Cassuto, dirigeante d'*Un dossier Une place*, *que la plupart des gens ne savent pas contextualiser, titrer ou simplement classer comme les normes professionnelles d'archivistique le recommandent. C'est bien normal : bien classer, bien nommer, ce n'est pas le cœur de l'activité des professionnels ! Pour cette raison, une fois que le paramétrage des délais d'archivage est déterminé et que l'arborescence est en place, il est beaucoup plus pertinent de confier ces tâches à un logiciel* ». Un tel logiciel intègre donc le cycle de vie des dossiers et documents dans leur intégralité, pour les dossiers papier comme numériques, depuis leur création, leur nommage, en passant par la gestion des emprunts et des retours. Un tel suivi logiciel permet de déterminer, par exemple, qui est la dernière personne qui a recherché ce dossier que l'on ne retrouve plus, « *parce qu'il est très probable que ce soit chez cette personne que se trouve le dossier* ». Quel que soit le niveau d'ordre et de désordre d'où l'on parte, aucune situation n'est désespérée ! Un *process* de réorganisation bien rôdé peut rapidement venir à bout de tous les chaos, qu'ils soient physiques ou numériques.

Pour mettre en place un stockage papier, différentes options sont envisageables, qui ont toutes un coût. Stocker au sein de l'étude est onéreux quand le foncier est cher, faire stocker par un prestataire représente une dépense récurrente, mais stocker loin de l'étude où le foncier est plus accessible montre vite ses limites : « *nous avons travaillé,* indique Laurent Biet, directeur commercial du pôle Notaires chez *Xelians*, *avec des notaires dont les archives étaient à quelques kilomètres de chez eux. Puisqu'il y a presque autant d'actes recherchés que d'actes créés, ils doivent y envoyer des collaborateurs ou faire ce déplacement eux-mêmes, ce qui représente autant de temps perdu et donc un coût caché* ».

Le choix porte aussi sur la forme que prend la conservation. Elle peut se faire en conteneurs ou en linéaires, le premier étant moins cher à stocker mais plus coûteux pour chaque consultation, « *parce que,* explique Erwan Vilain, responsable commercial chez *Novarchive*, *il y a sept conteneurs les uns sur les autres avec chacun l'équivalent de 50 cm d'archives, donc l'archiviste, pour consulter un seul document, peut avoir à manutentionner un certain nombre de conteneurs avant de trouver ce qu'il cherche, ça n'est pas fait pour être consulté*

tous les jours ». Le linéaire est donc intéressant dès lors qu'il y a des insertions ou consultations récurrentes à faire dans un dossier.

Une autre option plutôt raffinée consiste à relier ses archives pour en faire des livres, avec évidemment un coût supérieur aux autres solutions, mais beaucoup d'avantages : « *d'une part,* précise Laurent Biet, *on n'a jamais mieux fait que des livres pour conserver du papier en bon état et de manière pérenne, d'autre part, il y a un souci d'élégance parce que les études choisissent la toile, la couleur et personnalisent ainsi des livres avec tous leurs actes originaux dedans, qu'ils n'auront d'ailleurs pas à utiliser, puisque, par ailleurs, tout est numérisé* ». Donc, pour les nombreux notaires qui n'aiment pas se dessaisir de leurs archives papier, il est possible d'aller gagner de la place dans l'étude tout en conservant ses minutes.

Gérer les archives numériques

La numérisation des pratiques du notariat est un acquis depuis de nombreuses années, mais l'archivage numérique reste un enjeu qui soulève de nombreuses questions. Si le choix est fait de numériser les archives papier, comment opérer ?

Préférez-vous qu'une équipe vienne numériser sur place, ou envoyer vos archives être numérisées chez le prestataire ?

Souhaitez-vous une numérisation dite « *fidèle* » conforme à la norme NF Z42-026 qui permettra de se débarrasser de l'original papier d'un grand nombre de documents justificatifs, notamment pour les dossiers d'annexes ?

Souhaitez-vous récupérer vos archives papier ou les laisser en dépôt ?

Souhaitez-vous une numérisation immédiate ou une option « *scan on demand* » ? « *Lorsque l'on est pas certain,* souligne Erwan Vilain, *que l'ensemble du fonds va être consulté dans les 10 ans ou 20 ans à venir, la solution scan on demand peut avoir beaucoup de sens* ». Dans ce cas, les documents sont stockés chez votre prestataire qui numérise les documents en fonction de vos besoins, et chaque demande de numérisation que réalise l'étude est ainsi l'occasion d'enrichir progressivement les archives numériques. C'est notamment utile lorsque les autres études font des demandes de documents, et la facturation de cette demande permet de couvrir les frais de numérisation sans faire l'avance des fonds. « *Les notaires reçoivent le document numérisé et n'ont alors plus qu'à transférer le mail à l'étude qui en a fait la demande* ».

La numérisation des archives papier est la première brique, car elle permet l'indexation de tous les documents par titulature mais aussi par contenu au moyen de processus OCR, quelle que soit la diversité des supports, puisque les classeurs d'actes papier des années 70 peuvent côtoyer le cartulaire des années 60 et les boîtes d'archives plus contemporaines réalisées dans les années récentes. Tout ceci est numérisé, indexé et intégré à la base documentaire de l'office. « *C'est le passé papier,* indique Laurent Biet, *puis viennent les actes électroniques réalisés par les notaires depuis la mise en place des logiciels métier. Ils vont être extraits, indexés et versés dans la base documentaire. Puis vient ce que j'appelle 'le fil de l'eau', à savoir les AAE produits au fur et à mesure par l'étude, et ceux-ci vont, soit être versés directement par l'étude dans la base documentaire, soit être gérés par un opérateur qui vient à l'étude de manière régulière pour les extraire et les indexer* ».

L'accès à cette base de données est bien sûr sécurisé et requiert identifiant et mot de passe, et la possibilité existe, surtout avec le développement du télétravail, de relever la sécurisation de l'accès en requérant un code unique envoyé par SMS. Le plan de classement mis en place lors de la numérisation est également très important puisqu'il va déterminer un accès sécurisé aux archives. En effet, la personne désignée comme administrateur du système d'archivage donne des droits d'accès afin que chacun n'ait accès qu'aux archives qui le concernent : quelqu'un qui gère, par exemple, la comptabilité fournisseur, n'aura pas accès aux minutes, et ne pourra ni verser un nouveau document ni détruire des archives.

Où se trouvent vos données une fois numérisées ? Dans une base de données installée à l'étude pour y accéder via votre interface. Et si vous souhaitez des archivages extérieurs ? Ils sont installés, avec une double écriture, et pas une simple réplication, sur des serveurs situés en France, et non sur un *cloud* à la localisation ambiguë. Quand un document de type Word, Excel, Jpeg est versé sur l'archivage électronique, si la durée utile de conservation est de moins de dix ans, l'image est transformée au moment du versement pour créer un PDF. Au-delà des dix ans, il est préconisé de créer ce qu'on appelle un PDF/A. Pour assurer une sécurité maximale, des tests de lecture récurrents sont effectués pour vérifier l'état des archives : « *nous contrôlons les archives électroniques chaque année,* souligne Erwan Vilain*, pour vérifier, au travers des scellés, que les documents n'ont pas été altérés, et pour vérifier l'intégrité de la lecture* ».

Jordan Belgrave