L'ADSN FAIT TOURNER SON ATELIER GESTION DES RISQUES

Une culture de la sécurité se diffuse dans les offices, notamment sous l'impulsion de l'ADSN qui a entamé un tour de France dans un contexte de renforcement de la menace informatique. Les étapes du parcours de l'acte forment la ligne directrice de ce nouvel atelier.

Par Philippe Haumont

Pour sensibiliser offices et notaires à la gestion du risque, l'ADSN organise en liaison avec les instances notariales locales un atelier itinérant qui intéresse tous les notaires. Il multiplie ses étapes et vient souvent enrichir l'accueil des notaires nouvellement nommés. Porté par les responsables régionaux de l'ADSN – dont l'une des missions est d'accompagner sur le terrain les offices dans leurs missions régaliennes –, *« cet atelier répond à une forte demande »*, assure Anne Lenoir qui coordonne les responsables régionaux à la direction de la relation clients de l'ADSN[1].

Le sujet est sensible dans un contexte où la menace *cyber* fait peser des risques sur les systèmes informatiques des offices, même si son explosion ne touche pas les seuls notaires, loin de là. Une « culture » du risque irrigue progressivement les usages de la profession. Elle ne se limite pas à la cybersécurité. L'atelier d'une heure trente animé par l'ADSN s'attache à couvrir l'ensemble de la problématique telle qu'elle s'impose aux offices, considérant qu'une approche globale de la sécurité informatique est la meilleure protection contre les attaques.

> ***Tout ce qui est unique est stratégique***

TRANSMETTRE UNE MÉTHODE

Après une première partie consacrée au caractère stratégique de la mesure du risque pour l'office et pour le notaire, l'atelier a choisi de décortiquer le parcours de l'acte authentique, depuis le premier contact avec le client jusqu'aux formalités postérieures. Le chemin est ainsi balisé. L'exercice consiste à transmettre une méthode, à diffuser une culture et à modifier les comportements à partir du quotidien plutôt qu'à établir un questionnaire à la Prévert exhaustif, et forcément périlleux, chaque situation étant particulière. *« J'explique par exemple que dans un office, tout ce qui est unique est stratégique*, fait valoir Jean-Philippe Tolbiac, responsable régional (régions Bourgogne-Franche-Comté et Grand-Est), *aussi bien une clé Réal, une tablette de signature, une imprimante ou un notaire. »*

Comment établir un acte en toute sécurité en agissant à tous les stades de son élaboration ? Telle est la question posée aux notaires participants. L'objectif réaffirmé est d'assurer la confidentialité tout au long du parcours de l'acte, de tenir le délai et de garantir la complétude de l'information recueillie par l'office. L'enjeu, clairement exposé, est triple : assurer la validité juridique, protéger l'image de l'office et le prémunir d'un risque financier qui peut être désastreux.

Première étape, identifier les outils et les personnes qui permettent d'établir un AAE dans les règles d'authenticité requises. C'est un travail de vérification de l'aptitude du système informatique – une faille serait fatale – et de l'habilitation des différentes personnes impliquées à exécuter régulièrement les tâches qui les sollicitent. *« Les prérequis techniques et humains doivent être en place et fonctionnels »*, résume Jean-Philippe Tolbiac. Dans un deuxième temps, celui du recueil des pièces nécessaires à la constitution du dossier fournies par des tiers, vient la question de la sécurisation des échanges. Et ils sont nombreux. Les transferts de documents par courrier électronique avec les clients ou les banques feront

LES PROCHAINS ARRÊTS DE L'ATELIER

Après de premiers ateliers sur la gestion des risques organisés fin 2021 et début 2022 d'autres rendez-vous sont fixés : Pau et Valence (8 février), puis, en mars, Toulouse, Auxerre, Mâcon et Besançon.

l'objet d'une vigilance renforcée dans un contexte où le risque *cyber* frappe de plus en plus fort *(lire encadré)*. Jean-Philippe Tolbiac le rappelle : *« Les hackers ont bien compris qu'il y a des mouvements de fonds chez les notaires. »* Leurs ruses, toujours plus sophistiquées, appellent une vigilance de tous les instants pour contrer les rançongiciels, la fraude au RIB – très en vogue – ou le phishing.

PAS DE SOLUTIONS TOUTES FAITES

En suivant le parcours de l'acte, la troisième partie de l'atelier s'arrête sur l'ensemble des procédures dématérialisées qui se font *via* des connexions avec la clé Real (FCDDV, casier judiciaire, état civil). *« D'où l'importance de porter une attention particulière au respect des conditions générales d'utilisation de la clé Réal, d'envisager la possibilité d'utiliser une seconde clé dite de secours ou de révoquer des clés volées ou perdues »*, avertit Jean-Philippe Tolbiac.

Quatrième étape : la signature de l'acte et l'accomplissement des formalités postérieures achèvent le parcours. L'approche du risque est différente selon la manière dont l'acte est signé, à l'office, en mobilité ou encore à distance entre deux offices. L'atelier en évoque les différentes exigences. Quelques bonnes questions parmi d'autres qu'il conviendra de se poser : *« En cas de panne Internet à l'office, quelle solution de secours évitera l'interruption de la continuité du processus ? » « Chez le client, pour lire l'acte, un câble HDMI reliant le portable à un téléviseur ou à un moniteur permettra-t-il de satisfaire les obligations légales qui imposent que le client puisse lire l'acte qu'il devra signer ? » « À distance, la solution de visioconférence est-elle bien agréée pour assurer la sécurité et la confidentialité faute de quoi l'acte sera frappé de nullité ? »*

Dans cet office, victime d'un rançongiciel qui a crypté son serveur, *« la plus récente sauvegarde datait de six mois,* se souvient le responsable régional, *alors que pour garantir la continuité de l'exploitation, nous préconisons des sauvegardes opérationnelles régulières et des tests de restauration, hélas trop rares »*. Sensibiliser aux risques, savoir les identifier, les analyser et les hiérarchiser, créer les bons réflexes… Tout ou presque est dans le squelette de cette présentation de l'ADSN. *« Mais nous ne venons pas avec des solutions toutes faites,* précise Jean-Philippe Tolbiac, *chaque office, chaque notaire a sa problématique. »* Au bout du compte, c'est le cumul de ces nombreuses précautions et procédures qui assure la meilleure prévention.

[1] Contact : Anne Lenoir 06 87 39 97 70 ou le responsable régional ADSN rattaché à l'instance.

SUR TOUS LES FRONTS D'UNE ATTAQUE CYBER

La menace *cyber* explose dans tous les secteurs d'activité. En 2020, l'Anssi (Agence nationale de la sécurité des systèmes d'information) a relevé 2 759 signalements liés à des rançongiciels, quatre fois plus que l'année précédente. Le phénomène s'est notamment renforcé avec la crise sanitaire et l'expansion du télétravail. Près de la moitié des attaques visent les TPE/PME, souvent plus démunies. 90 % des brèches de sécurité sont causées par une erreur humaine. 94 % des attaques se déclenchent par l'intermédiaire des messageries.

La cyberattaque peut revêtir différents uniformes, quatre au total : les *malwares* (ou programme malveillant), le *phishing* (ou hameçonnage), l'immixtion dans une procédure ou encore l'attaque pure et simple du système et des réseaux (dite par « déni de service ») pour en épuiser les ressources et bloquer les serveurs.

Le *malware* exploite une vulnérabilité, soit dans le système, soit dans l'usage qui en est fait, soit dans des mails comprenant des pièces jointes ou des liens dangereux. Il peut recueillir secrètement des informations, bloquer certains accès, rendre inutilisable le système.

Le *phishing* emprunte lui aussi le chemin des messageries pour récupérer des informations personnelles, des codes et mots de passe, des références bancaires, etc. L'attaque frontale du pirate lui permet de s'immiscer dans un échange ou une transaction pour voler des informations ou modifier les contenus. Cette attaque peut survenir après l'installation d'un *malware* ou se glisser lors d'une connexion sur un wifi public non sécurisé.

L'utilisation de la messagerie devra donc faire l'objet de la plus grande attention, c'est la première porte d'entrée pour les pirates. Son usage personnel doit être limité et contrôlé, les documents confidentiels ne doivent pas y transiter, les comptes personnels seront renouvelés au rythme des mobilités, les mots de passe renforcés, etc. Ce qui est l'affaire de tous dans un office.