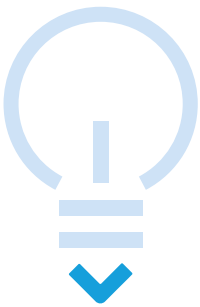
Cyberattaques : comment protéger son cabinet ?

PAR **JULIE ROMANO**, JURISTE,
& **CONSTANCE CAMILLERI**,
DIRECTRICE DE L'INNOVATION,
CONSEIL SUPÉRIEUR

Face à une recrudescence de la cybercriminalité, les cabinets d'expertise comptable doivent se prémunir contre de nouvelles menaces.

La crise sanitaire et économique liée à la pandémie de Covid-19 et l'intensification des usages numériques ont généré une augmentation des cyberattaques, exposant les cabinets d'expertise comptables à de nouveaux risques. L'année 2020 a été marquée par une recrudescence des attaques par rançongiciels. À la mi-mars 2020, près de 80 % des attaques analysées chaque jour utilisaient des thèmes liés à la Covid-19.



Aucun secteur d'activité n'est épargné selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[1], même si les victimes de rançongiciels sont principalement des collectivités territoriales, des établissements de santé et des entreprises du secteur industriel. Les cabinets d'expertise comptable ne sont donc pas à l'abri. Pour mieux s'en prémunir, ils doivent se tenir informés des menaces numériques et en alerter leurs collaborateurs.

S'INFORMER DES CYBERMENACES

Dans son rapport sur le facteur humain 2021[2], la société américaine Proofpoint, spécialisée dans la sécurité informatique, liste les techniques d'attaques les plus efficaces.

Le phishing de connexion
L'hameçonnage des identifiants de connexion représente la forme la plus courante d'attaque : plus de la moitié de toutes les menaces e-mail observées en 2020 relevaient de ce type de tentatives.
Cette technique consiste à convaincre une personne de fournir ses informations de connexion, ce qui donne aux cybercriminels accès à ses comptes bancaires, informations personnelles, comptes professionnels etc. Le phishing de connexion peut recourir à n'importe quelle technique d'ingénierie sociale, mais préfère généralement l'e-mail. Le cybercriminel se fait passer pour une plateforme à laquelle l'utilisateur est abonné, une marque réputée ou encore un collègue de la victime, et envoie un e-mail incluant un lien vers une fausse page de connexion. Dès lors que l'utilisateur fournit son nom d'utilisateur et son mot de passe, le cybercriminel utilise ces informations pour prendre le contrôle de son compte.

En 2021, une entreprise a été victime d'une attaque de phishing massif : ses collaborateurs ont reçu un e-mail contenant un lien piégé, les invitant à se reconnecter à leur compte Office 365. Trois collaborateurs ont entré leurs identifiants et mots de passe Office 365, qui étaient les mêmes que ceux leur permettant de se connecter à l'environnement Windows de l'entreprise.
Par la suite, 635 e-mails dupliqués de l'e-mail d'origine ont été envoyés aux destinataires des carnets d'adresses compromis : partenaires, clients, autres entreprises.
Alerté de la situation, l'assureur de l'entreprise a conseillé l'envoi d'un e-mail d'avertissement aux 635 adresses pour prévenir les personnes concernées de la menace constituée par ce message. Sur les conseils de son expert en cybersécurité, l'entreprise touchée a aussi changé tous les mots de passe de son environnement Windows de manière préventive. Par mesure de sécurité, aucune communication en interne n'a eu lieu à propos de ce changement de mot de passe et les salariés ont eu connaissance de la situation dès leur connexion au réseau.

En outre, le système interne utilisé par les salariés travaillant à distance pour accéder au système d'information par un site web a été désactivé pour ceux dont le mot de passe n'avait pas encore été modifié.

Ces mesures ont permis d'empêcher les cybercriminels utilisant les mots de passe compromis d'accéder directement au système d'information du client. Cette opération a perturbé le fonctionnement de ce système pendant les quelques jours de complétion de la campagne de réinitialisation des milliers de mots de passe, mais cela a permis d'éjecter les cybercriminels sans prendre le risque d'intrusion. L'impact financier total indemnisé par l'assureur lors de cette attaque s'est élevé à 130.000 €.

D'après les chiffres du gouvernement américain, les attaques par rançongiciels ont augmenté de 300 % l'année dernière.

Comme le rappelle le groupement d'intérêt public « Actions contre la cybermalveillance » (ACYMA)[3], les campagnes d'hameçonnage par SMS se sont également considérablement développées en 2020. Les SMS permettent aujourd'hui des interactions directes avec Internet et ce mode de communication est de plus en plus utilisé par les différentes plateformes pour communiquer directement avec leurs usagers. L'utilisation du SMS comme support d'hameçonnage semble être une tendance forte qui se confirmera certainement dans les prochaines années. Il convient donc d'être également vigilants à la réception des SMS et non uniquement des e-mails !

Les attaques par rançongiciels

Ces attaques consistent à prendre en otage les données des victimes en les chiffrant, puis à exiger le paiement d'une rançon pour les déverrouiller. D'après les chiffres du gouvernement américain, les attaques par rançongiciels ont augmenté de 300% l'année dernière. La tendance actuelle des cybercriminels est de privilégier l'attaque des entreprises de grande taille plutôt que les campagnes de grande envergure mais peu lucratives.

Toutefois, les cabinets d'expertise comptable peuvent eux aussi être les victimes de rançongiciels.

En effet, en 2020, un cabinet a vu ses 4 serveurs infectés par un rançongiciel. Le cybercriminel a demandé le paiement de 4 rançons pour obtenir les clés de déchiffrement de chacun des serveurs. Les experts en assurance ont pu retrouver les clés de déchiffrement que les criminels avaient vendus à d'autres sociétés contre le paiement d'une rançon, ce qui a permis au cabinet attaqué de ne pas payer les rançons[4].

La stéganographie

Cette technique qui consiste à dissimuler du code malveillant dans des images et d'autres types de fichiers, a été utilisée dans des campagnes de cyberattaques très ciblées en 2020. Différente de la cryptographie qui consiste à rendre illisible un fichier sans l'aide de la clé de déchiffrement, la stéganographie a pour objectif de cacher un fichier dans un autre fichier et est aujourd'hui utilisée pour infecter les ordinateurs. En général, pour que l'attaque fonctionne, il faut que l'ordinateur soit déjà infecté par un logiciel malveillant, qui exécute ensuite les commandes intégrées dans l'image. Par exemple, avec la commande « print », le logiciel malveillant imprime ce qu'il y a sur l'écran et vole des informations confidentielles. Les attaques stéganographiques fonctionnent parce qu'elles sont difficiles à repérer : là où la cryptographie cache le contenu d'un message, la stéganographie cache le message lui-même, ce qui attire beaucoup moins l'attention. L'analyse de tous les fichiers média pour trouver une information précise est long et complexe ; les logiciels de sécurité informatique actuels sont donc généralement impuissants.

Il existe des techniques spécialement conçues pour lutter contre la stéganographie, comme la méthode de l'histogramme, mais elles ne sont pas au point à ce jour.
En janvier 2019, les utilisateurs de Mac ont été visés par une campagne de publicité malveillante utilisant la stéganographie. La publicité contenait, dans ses images, du code JavaScript ultraléger et indétectable. Son rôle était de rediriger les utilisateurs vers des sites proposant de fausses mises à jour d'Adobe Flash, qui étaient en réalité des logiciels malveillants.

Les techniques CAPTCHA

Ces attaques utilisent les tests visuels servant à distinguer les personnes des machines, généralement utilisées sur des sites Internet légitimes pour vérifier qu'un visiteur est un humain et non un robot. La plupart du temps, la victime reçoit un e-mail l'invitant à cliquer sur un lien ou à ouvrir une pièce jointe puis à passer un test CAPTCHA afin d'accéder à ladite page ou pièce jointe. Une fois qu'il a réussi le test CAPTCHA, l'utilisateur est alors renvoyé vers une page contenant un logiciel malveillant.

Les CAPTCHA malveillants ont affiché en 2020 un nombre de clics 50 fois supérieur à celui de l'année précédente.

Il est difficile de savoir pourquoi : il est possible que les collaborateurs aient été plus distraits et plus disposés à se laisser prendre au piège en raison des nouveaux contrôles mis en place pour le télétravail et à considérer le code CAPTCHA comme une mesure de sécurité normale.

Le piratage de messagerie
Dans ce type d'attaque, le cybercriminel se fait passer pour un collègue, un dirigeant ou un fournisseur à l'aide d'un large choix de techniques d'usurpation d'identité. L'expéditeur peut demander au destinataire de transférer des fonds, de faire un paiement, de détourner des salaires, de modifier des informations bancaires ou d'envoyer des informations sensibles.
Les attaques BEC (Business Email Compromise) sont difficiles à détecter, car elles n'ont pas recours à des URL malveillantes ou à des logiciels malveillants susceptibles d'être analysés et identifiés par des cyberdéfenses traditionnelles.
Elles reposent plutôt sur l'usurpation d'identité et d'autres techniques d'ingénierie sociale pour inciter les victimes à exécuter des actions pour le compte du cybercriminel.

RENFORCER SA CYBERVIGILANCE

Face à l'explosion des opérations malveillantes, il est recommandé aux experts-comptables et à leurs collaborateurs de redoubler d'attention :

- Vérifiez la fiabilité et la réputation des sites que vous visitez et que vous relayez. Évitez certains sites dangereux (sites de téléchargements, vidéos en ligne…).
- Soyez vigilants aux fausses informations ; pour rester informé sur la situation sanitaire et économique, référez-vous au site dédié du gouvernement ou au site privé de l'Ordre.
- Méfiez-vous des mails sur le thème Covid-19 : ne cliquez pas sur les liens et n'ouvrez pas les pièces-jointes.
- En cas d'expéditeurs inconnus ou de messages (ou SMS) inhabituels : ne répondez pas, ne cliquez pas sur les liens, n'ouvrez pas les pièces-jointes, ne transmettez pas vos numéros bancaires.
- Masquez votre webcam.
- Téléchargez vos applications uniquement sur les sites officiels des éditeurs et ne téléchargez jamais de programmes depuis un mail si vous n'êtes pas absolument certain de son origine.
- Faites régulièrement des sauvegardes de vos données et gardez une copie déconnectée.
- Appliquez les mises à jour de sécurité sur vos équipements connectés (serveurs, ordinateurs, téléphones, tablettes…) dès qu'elles sont disponibles et à partir des sites officiels.
- Utilisez des mots de passe uniques et solides, ne les communiquez jamais (qu'elle qu'en soit la raison) et activez la double authentification chaque fois que possible.
- Munissez-vous d'antivirus et d'antispam et vérifiez que les mises à jour sont faites sur les sites officiels.
- Pour les réunions en distanciel, privilégiez des solutions qui protègent la vie privée (telles que Tixeo - certifié par l'ANSSI - ou Livestorm) et lisez attentivement les conditions qui informent de l'usage fait des données collectées
- Soyez vigilants aux changements de RIB de vos fournisseurs et faites un contre-appel à un numéro déjà référencé en cas de doute.
- Tenez-vous régulièrement au courant des campagnes de cyberattaques liées à la crise en vous rendant sur le site cyber malveillance du gouvernement.

Et surtout, faites preuve de bons sens, gardez un esprit critique, ne vous précipitez pas, prenez toujours le temps de la réflexion.

POUR ALLER PLUS LOIN

- **Consultez régulièrement le site du gouvernement dédié à la cyber malveillance** https://www.cybermalveillance.gouv.fr
- **Téléchargez sur le site privé du Conseil supérieur les 11 commandements** essentiels pour assurer votre cybersécurité.
- **Le guide de la cybersécurité** pour les experts-comptables.
- **Le kit mission** « Diagnostic/ évaluation des risques cybersécurité »

1. Rapport d'activité 2020 de l'ANSSI : https://www.ssi.gouv.fr/agence/missions/rapport-dactivite-2020/
2. https://www.proofpoint.com/fr/resources/threat-reports/human-factor
3. Rapport d'activité 2020 d'ACYMA : https://www.cybermalveillance.gouv.fr/medias/2021/04/Rapport-activite-cybermalveillancegouvfr-2020.pdf
4. Article page 40 du SIC Mag n°406, juillet-août 2021, *Les attaques par rançongiciel : une menace pour les cabinets d'expertise comptable.*