Les attaques par rançongiciel : une menace pour les cabinets d'expertise comptable ?

PAR **ALEXANDRA DECAUDIN**, JURISTE, CONSEIL SUPÉRIEUR

L'année 2020 a été marquée par un record[1] d'attaques par rançongiciel (« ransomware ») : 54 incidents liés à des rançongiciels ont été signalés à l'ANSSI en 2019 ; l'Agence a enregistré une hausse de 255 % en 2020 avec 192 incidents rapportés. Les attaques par rançongiciel sont les premières menaces informatiques quotidiennes des entreprises, qui peuvent avoir des conséquences très dommageables sur la continuité de leur activité.

Dans son bilan de l'année 2020, la CNIL indique avoir reçu plus de 500 notifications liées aux rançongiciels et rappelle l'importance des mesures de sécurité à mettre en place pour protéger les données et limiter les risques de ce type d'attaque.

Qu'est-ce qu'un rançongiciel ? C'est un logiciel malveillant dont l'objectif est d'obtenir de la victime le paiement d'une rançon, qui infecte un ordinateur ou un système d'information hors d'état de fonctionner de manière réversible, après que l'utilisateur a cliqué sur un lien ou un fichier reçu en pièce jointe d'un e-mail ou en naviguant sur des sites compromis. Les criminels chiffrent par des mécanismes cryptographiques les données de l'ordinateur ou du système d'information rendant leur consultation ou leur utilisation impossible. Le pirate demande alors une rançon en échange de la ou des clés de déchiffrement des fichiers corrompus[2].

Dans la plupart des cas, les entreprises parviennent à reconstituer leurs données grâce à des copies de sauvegarde sur un support déconnecté (comme par exemple, un disque dur externe amovible) sans avoir à payer la rançon. Mais il faut savoir que les sauvegardes peuvent aussi être affectées par un rançongiciel.

Dans tous les cas, comme on le verra ci-après les sauvegardes doivent être déconnectées du système d'information pour prévenir le risque de chiffrement.

> Les cabinets d'expertise comptable peuvent eux aussi être les victimes de rançongiciels. Ces derniers mois ont d'ailleurs été marqués par plusieurs attaques à l'encontre d'experts-comptables.

L'année dernière, un cabinet a vu ses 4 serveurs infectés par un rançongiciel. L'auteur 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 pu vendre à d'autres sociétés contre paiement d'une rançon, ce qui a permis au cabinet de ne pas payer les rançons.

Un autre cabinet a subi ce même type d'attaque dans le cadre d'une opération de rachat d'un autre

1. Rapport de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur www.cert.ssi.gouv.fr.
2. La rançon est souvent réclamée en Bitcoin.

cabinet d'expertise comptable. Les ordinateurs infectés ont été débranchés pour éviter que l'attaque ne se propage au sein du groupe. L'auteur de l'attaque avait déverrouillé toutes les sauvegardes automatiques et les alertes d'intrusion dans le système d'information.

Les assureurs des cabinets d'expertise comptable ne sont que rarement amenés à payer les rançons demandées dès lors que la restitution des données est possible et que son coût est inférieur au montant de la rançon.

Ce n'est que dans de rares cas qu'un cabinet est contraint de payer la rançon pour éviter par exemple des pénalités qui seraient imposées à son client du fait de l'absence de transmission de certaines données à l'administration lorsqu'il n'a pas le temps imparti pour la reconstitution des données ou qu'elle est impossible, et à condition que le montant des pénalités soit supérieur au montant de la rançon.

> Le mot de Gilles Dauriac, président du comité des assurances du Conseil supérieur de l'ordre des experts-comptables, « *Dans certains pays étrangers, les assureurs ont une politique de refus systématique de paiement des rançons, ce qui a fait cesser ces tentatives d'extorsion d'argent.* »

QUELS RISQUES POUR LES CABINETS ?

Le cabinet peut subir des pertes financières, faute de pouvoir accéder aux données. L'image du cabinet va en pâtir et cela pourra entrainer une perte de confiance des clients.

Les violations de données ont aussi des conséquences directes sur les personnes physiques, dont les données sont compromises, puisqu'elles peuvent conduire à des usurpations d'identité.

Les rançongiciels peuvent également conduire à une sanction financière prononcée par la CNIL, dans l'hypothèse où le cabinet n'a pas mis en place les mesures de sécurité informatiques suffisantes pour protéger les données de ses clients.

COMMENT LIMITER LES RISQUES ?

Les cabinets doivent vérifier qu'ils ont bien souscrit une assurance cybersécurité qui pourra les accompagner dans ce type d'attaque. La majorité des assureurs en France en proposent une permettant de garantir le risque lié aux rançongiciels. Il est à noter cependant que certains d'entre eux depuis le début de la pandémie et l'accélération du télétravail dans les entreprises ne souhaitent plus assurer ce risque ou revoient les conditions de couverture.

Les cabinets doivent également sécuriser les données qu'ils détiennent. Ils doivent donc mettre en place plusieurs mesures préventives :

- utiliser et maintenir à jour les logiciels antivirus ;
- effectuer des copies de sauvegarde régulières des données dans un lieu différent de l'environnement de production hors réseau internet afin de pouvoir rapidement constituer les données en cas d'attaque ;
- sensibiliser les collaborateurs à l'importance de détecter les attaques de rançongiciels en les informant des bonnes pratiques à suivre telles que :
  - ne pas cliquer sur les liens dans les e-mails ou les pièces jointes en provenance de sources inconnues ou d'un expéditeur connu et les supprimer de votre messagerie (et également de la corbeille),
  - ne pas télécharger d'application ou de logiciels libres sur internet, sans l'autorisation du service informatique,
  - mettre à jour l'antivirus et configurer le pare-feu,
  - utiliser des mots de passe[3] suffisamment complexes et les changer régulièrement.
- analyser les systèmes et effectuer des audits et des contrôles de vulnérabilité pour détecter les points d'entrée potentiels sur leur système d'exploitation ;
- mettre en place un mécanisme de détection de l'altération des fichiers permettant notamment d'empêcher le chiffrement des serveurs de fichiers par un rançongiciel.

COMMENT RÉAGIR EN CAS D'ATTAQUE ?

Il faut débrancher l'ensemble des ordinateurs et alerter immédiatement l'assureur et le prestataire informatique.

Il ne faut pas se précipiter pour payer la rançon réclamée dès lors qu'il n'existe aucune garantie que les données soient restituées ou que de nouvelles attaques n'interviennent pas à nouveau : il faut rapidement faire le point avec son assureur pour évaluer la possibilité ou non de reconstituer les données bloquées, le coût de cette reconstitution et décider ensemble de la décision à prendre concernant le paiement de la rançon.

Il est indispensable de conserver les preuves de l'attaque (les fichiers de journalisation du pare-feu, les copies physiques des postes ou serveurs touchés, les fichiers chiffrés, etc.).

Il est également nécessaire de porter plainte auprès des services de police.

POUR EN SAVOIR PLUS

Consultez le guide de ANSSI « Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ? » sur www.ssi.gouv.fr

3. Authentification par mot de passe : les mesures de sécurité élémentaires préconisées par la CNIL. Plus d'informations sur : https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires).