L’étude d’avocats victime d’une cyberattaque

Célian Hirsch, le 21 avril 2022

Une cyberattaque réussie contre une étude d’avocats peut attirer l’attention de l’autorité compétente que la confidentialité des données n’est pas respectée.

Information Commissioner’s Office, Tuckers Solicitors LLP Monetary penalty notice, 10 mars 2022

Le 24 août 2020, l’Étude d’avocats anglaise Tuckers Solicitors LLP découvre être la cible d’une cyberattaque par *ransomware*. Les hackers réussissent à crypter 972’191 fichiers informatiques archivés, dont 24’712 se rapportent à des dossiers de procédures judiciaires ; parmi les dossiers cryptés, 60 sont exfiltrés par les hackers et publiés sur le *darkweb.*

Ces données piratées comprennent notamment des dossiers médicaux, des déclarations de témoins, le nom et l’adresse des témoins et des victimes, ainsi que les infractions présumées des prévenus.

Le 25 août 2020, Tuckers informe l’*Information Commissioner’s Office* (ICO, l’autorité anglaise de protection des données) de cette fuite des données.

Le 27 août 2020, Tuckers mandate un expert externe afin de recevoir un *Cyber Security Incident Response Report*. Ce rapport ne permet néanmoins pas de découvrir comment les pirates ont accédé au réseau informatique de Tuckers. Cela étant, le rapport indique qu’une vulnérabilité connue n’avait pas été corrigée immédiatement en janvier 2020, mais uniquement en juin 2020.

Tuckers notifie ensuite les personnes concernées de la fuite des données et communique également à ce sujet via son site web.

Bien que l’ICO admette que la fuite des données est attribuable aux *hackers*, elle considère que Tuckers n’a pas suffisamment protégé ses données. Le 10 mai 2022, l’autorité anglaise prononce ainsi une amende contre l’Étude d’avocats en raison d’une violation de la confidentialité des données (art. 5 par. 1 let. f RGPD).

Premièrement, l’ICO souligne que Tuckers n’utilisait pas l’authentification multi-facteurs pour

accéder à distance à son réseau informatique. Or ce système est recommandé depuis plusieurs années par le *National Cyber Security Centre* (NCSC) et permet de réduire drastiquement les risques de cyberattaques.

Deuxièmement, Tuckers n'a mis en place un correctif de sécurité (*patch*) qu'en juin 2020, alors que celui-ci était connu depuis janvier 2020. Or la NCSC avait précisément publié un communiqué en janvier 2020 informant de cette faille de sécurité et que celle-ci était exploitée par des acteurs malveillants. Ce correctif était en plus gratuit.

En raison de la nature très sensible des données traitées par l'étude d'avocats et du faible coût de la mise en place du correctif de sécurité, l'ICO considère que Tuckers n'a pas traité ses données « de façon à garantir une sécurité appropriée » (art. 5 par. 1 let. f RGPD).

L'ICO en profite pour souligner que la *Privacy Policy* de l'Etude prévoyait précisément que « *all software, operating system and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities* ».

Enfin, l'ICO reproche également à Tuckers de ne pas avoir crypté ses données. Or il existe des logiciels gratuits en *open-source* qui permettent un tel cryptage. L'ICO relève que le cryptage des données constitue même la norme pour les études d'avocats.

En raison de ce triple manquement à l'obligation de garantir une sécurité appropriée des données, l'ICO décide de sanctionner Tuckers d'une amende (art. 83 RGPD). Afin de déterminer son montant, l'ICO prend notamment en considération que les données ont été publiées sur le *darkweb*, qu'elles étaient protégées par le secret professionnel et qu'elles étaient particulièrement sensibles (des dossiers comprenant les données de victimes et de prévenus). L'autorité anglaise arrive à la conclusion que le montant de £ 98'000.- constitue une amende appropriée.

Quid si une étude d'avocats suisse devait être victime d'une telle cyberattaque ?

Tant l'actuel LPD que la nLPD imposent aux responsables du traitement de protéger leurs données de manière appropriée au risque (art. 7 LPD et art. 8 nLPD). Selon nous, cette norme légale impose également aux études d'avocats d'installer rapidement les correctifs de sécurités (*patch*) lorsqu'ils sont connus et exploités par des acteurs malveillants.

En particulier, la *Computer Emergency Response Team* de la Confédération aurait même informé directement des études d'avocats en mars 2021 d'une vulnérabilité de Microsoft

Exchange. La faille de sécurité Log4j a également attiré l'attention médiatique en fin d'année 2021. À notre avis, une étude d'avocats qui n'a pas corrigé ces failles de sécurité viole l'art. 7 LPD, notamment en raison des données sensibles qu'elle traite.

Le droit actuel ne prévoit néanmoins pas d'amende administrative pour une telle violation. Au contraire, l'art. 61 let. c nLPD prévoit une amende pénale pour la violation intentionnelle des exigences minimales en matière de sécurité des données édictées par le Conseil fédéral selon l'art. 8 al. 3 LPD. Il faut cependant encore patienter avant de découvrir la version définitive de ces « exigences minimales en matière de sécurité des données » dans la future ordonnance (cf. P-OLPD). Il ne nous semble pas exclu de retenir qu'une personne directement informée d'une faille importante de sécurité et qui ne met pas en place son correctif puisse tomber sous le coup de cette disposition pénale.

Proposition de citation : Célian Hirsch, L'étude d'avocats victime d'une cyberattaque , 21 avril 2022 *in* www.swissprivacy.law/137