Secret et cybersécurité

Cyberrisques sur les données numériques

Myriam Quéméner , avocat général honoraire, Docteur en droit

Les cybermenaces constituent désormais un véritable fléau qui vise tous les secteurs d'activités économiques, en particulier les professions détentrices de données numériques sensibles qui représentent de la valeur et qui sont ensuite négociables et revendables . Tel est le cas des professions du chiffre et du droit comme par exemple les avocats dont les données sensibles doivent rester normalement secrètes mais qui sont très convoitées en raison de la valeur qu'elles représentent .

En effet , les cabinets d'avocats sont souvent la cible de cyberattaques réalisées par des cybercriminels variés . L'exposition des cabinets d'avocats à la menace informatique s'explique notamment par leur accès à des données sensibles, mais également en raison de leurs clients que certains cybercriminels veulent viser . L'ANSSI relève dans un rapport récent[1] que la surface d'attaque des cabinets d'avocats ne cesse de s'étendre, notamment du fait de la numérisation croissante de la profession et des procédures judiciaires. Or, les cyberattaques informatiques peuvent avoir de graves conséquences dans le domaine financier et réputationnel.Après avoir présenter les modes opératoires utilisés contre les cabinets d'avocats et leur conséquences souvent désastreuses , il conviendra d'envisager comment anticiper et remédier à ces attaques numériques.

1.-Le constat : des rançongiciels à l'espionnage économique et stratégique

Depuis plusieurs années, l'ANSSI constate une forte augmentation du nombre de cyberattaques par le recours à des rançongiciels[2] . Ce moyen conduit à l'exfiltration de données que les cybercriminels menacent de rendre publiques si la rançon n'est pas payée

Les cyberattaques s'accroissent constamment en raison notamment de nouvelles innovations numériques . Par exemple le déploiement du cloud computing a généré de réelles vulnérabilités pour les données hébergées par les cabinets d'avocats. Le cloud complexifie la localisation exacte du stockage des données, dont la confidentialité peut notamment être menacée par l'extraterritorialité de certaines législations . La fuite de données à caractère personnel peut également porter atteinte

[1] Etat de la menace informatique contre les cabinets d'avocats https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-004.pdf

[2] Codes malveillants déployés par des cybercriminels pour chiffrer les données d'un système d'information. Les attaquants contactent ensuite les victimes pour leur demander une rançon en échange de la clé de déchiffrement.

au secret professionnel et engager la responsabilité des avocats au regard de la loi Informatique et Libertés et du Règlement général sur la protection des données (RGPD) européen

Les données sensibles détenues par les cabinets d'avocats en font également des cibles de choix pour des attaquants cherchant à surveiller les activités d'avocats ou de leurs clients. Depuis au moins la fin des années 2000, des acteurs présumés étatiques ont compromis des cabinets dans le but de collecter des informations utiles à des missions d'espionnage économique ou stratégique. Ce type d'acteur s'intéresse particulièrement aux brevets, aux dossiers de fusion-acquisition, aux procédures judiciaires ou d'arbitrage, ou encore à l'application de sanctions et d'embargos internationaux. L'ANSSI relève dans son rapport[3] une hausse du nombre d'attaques conduites contre le secteur par des entreprises privées et des mercenaires possédant des capacités de lutte informatique offensive. Ces organisations, dotées pour certaines de compétences avancées, proposent leurs services à de nombreux États à travers le monde, mais également à des particuliers. Plusieurs cabinets d'avocats ont été la cible d'attaquants recrutés par des enquêteurs privés, des entrepreneurs ou des personnalités politiques pour surveiller la partie adverse.

D'autres groupes de cybercriminels se spécialisent sur le vol de technologies des clients des cabinets d'avocats. En 2017, le groupe APT10 7 aurait compromis un cabinet américain spécialisé en droit de la propriété intellectuelle . Le cabinet conseillait par ailleurs des entreprises chinoises préparant leur entrée sur le marché américain. Les attaquants se seraient introduits dans les systèmes d'information en utilisant des identifiants probablement dérobés durant de précédentes attaques, puis auraient exfiltré de grandes quantités de données via le service de partage de fichiers Dropbox. Le groupe APT10 est accusé publiquement d'opérer pour le compte du ministère chinois de la Sécurité d'État (MSE) par l'Australie, le Canada, les États-Unis, la Nouvelle-Zélande et le Royaume-Uni .

Des cabinets d'avocats sont parfois la cible d'attaques opportunistes ou ciblées ayant eu pour conséquence de déstabiliser leurs activités ou visant directement à intimider leurs clients. Ces opérations consistent essentiellement en la divulgation d'informations exfiltrées que les attaquants jugent compromettantes pour les cabinets et/ou leurs clients ou à rendre indisponibles leur système d'information en chiffrant leurs données. Ce type d'attaque est notamment le fait de groupes hacktivistes cherchant à dénoncer les pratiques de certains cabinets ou leur soutien à des gouvernements étrangers, par exemple dans le contexte de tensions internationales. Néanmoins, des acteurs

[3]Rapport «Etat de la menace informatique contre les cabinets d'avocats 2023 », https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-004.pdf

présumés étatiques emploieraient également ce mode d'action en représailles à des politiques jugées agressives ou pour décrédibiliser des dissidents réfugiés à l'étranger.Certaines cyberattaques peuvent conduire à la disparition de certains cabinets.

Exemples de cyberattaques

En 2021 , lors d'une cyberattaque visant un cabinet d'avocats, des fichiers avaient été piratés dont certains relatifs à l'attentat de Charlie Hebdo et l'assassinat du professeur Samuel Paty. Des éléments de cette procédure judiciaire avaient été publiés sur le darknet en novembre 2021. Plus de 13 millions de documents avaient été proposés à la vente pour 30 000 dollars sur le réseau Tor. Les enquêteurs avaient rapidement déterminé que le cabinet *avait été victime du rançongiciel Everes[4]t*.

Un hacker se prétendant éthique[5] s'était positionné comme négociateur dans l'affaire dite Everest, qui avait conduit en 2021 à une fuite de données liées à l'instruction de l'attentat de « Charlie Hebdo ». Il a été reconnu coupable d'association de malfaiteurs et de complicité de tentative d'extorsion[6].Il est aussi interdit d'exercer dans le domaine de la cybersécurité pendant cinq ans, dont quatre avec sursis. Il doit enfin s'acquitter d'une amende de 13 000 euros et verser, au total, 39 000 euros de préjudice aux différentes parties civiles.

Récemment, le cabinet Williams & Connolly[7], a informé ses clients qu'une partie limitée des comptes de messagerie d'avocats avait été piratée à l'aide d'une faille "zero-day[8]",

---

[4] https://www.solutions-numeriques.com/proces-requis-pour-le-complice-presume-dun-groupe-de-hackers-ayant-vise-un-cabinet-davocats-parisien

[5] Florent Curtet

[6] s://www.lemonde.fr/pixels/article/2024/12/16/le-hackeur-florent-curtet-condamne-a-deux-ans-de-prison-avec-sursis_6452291_4408996.html

[7] https://www.lexpress.fr/monde/des-cabinets-davocats-americains-pris-pour-cibles-par-des-hackers-chinois-BQEFDFXNQFHU3C7Y4SP3WR63IE/

[8] vulnérabilité inconnue des concepteurs du logiciel

c’est-à-dire une. ces attaques viseraient à recueillir des renseignements stratégiques dans le cadre de la compétition géopolitique et stratégique entre la Chine et les Etats-Unis.

Les cyberconseils

Le rapport de l’Anssi précité fait une série de recommandations afin d’anticiper ces menaces numériques étant précisé qu’il convient aussi de suivre désormais au vu de l’instabilité du monde les enjeux et les évolutions géopolitiques dès lors que les cabinets d’avocats ont des activités à l’international.

Afin de réduire les cyberrisques ,il convient de cartographier les menaces possibles , cartographier les risques comme par exemple l’externalisation de certaines tâches qui peut être sources de vulnérabilités.Il est nécessaire de lister les contrats de ces prestataires (hébergeurs, intégrateurs, mainteneurs, éditeurs de solutions, etc)., et les impacts sur le secret de l’instruction, le secret professionnel ou le secret des affaires. Cette réflexion doit intégrer les menaces décrites dans ce document. Pour chaque utilisation d’un service numérique (échange de fichiers, messagerie, etc.), toujours s’interroger sur le niveau de confiance à accorder à ce service pour protéger les informations traitées au bon niveau, notamment sur l’origine du fournisseur du service, la localisation du service ou encore son niveau de protection (HTTPS, authentification, traçabilité, etc.). Il faut aussi faire un inventaire des données métier Il est primordial de réaliser un inventaire des données métier : format, emplacement, sensibilité, responsabilité, besoin d’en connaître, etc. Il est pertinent aussi de faire régulièrement une sauvegarde hors-ligne et de stocker celle-ci dans un lieu physique sécurisé (export sur un disque externe USB et stockage dans un coffre par exemple). On doit aussi prévoir à l'avance un mode d'organisation dégradé Il est important d’organiser à l’avance un mode d’organisation dégradé dans le cas où le système d’information est indisponible à la suite d’une attaque : canal de communication de secours, récupération des données depuis la sauvegarde sur un poste de travail ou un serveur isolé,. Enfin , il faut prévoir un poste de travail de secours, ou un moyen de se doter d’un nouveau matériel, et une procédure de restauration des données en cas de compromission des postes

Enfin , il faut prévoir un poste de travail de secours, ou un moyen de se doter d’un nouveau matériel, et une procédure de restauration des données en cas de compromission des postes