ANALYSE DE RISQUE

Cabinet d’expertise-comptable

Cette étude compare les probabilités des différentes attaques possibles, et des différents attaquants potentiels. Elle repose sur notre expertise de la cybersécurité, des échanges avec de nombreux clients cabinets, et l’analyse de l’actualité du piratage des cabinets d’expertise comptable. Elle ne contient malheureusement rien qu’ignorerait un pirate un peu consciencieux.

C’est un premier élément, ici commun à toute une profession, pour bâtir la politique de cybersécurité d’un cabinet.

LES TYPES D'ATTAQUE

Rançon	
L'attaque pour rançon repose sur le fait de crypter les données d'un cabinet (les rendre illisibles) puis demander au cabinet une rançon pour pouvoir les récupérer. Compte-tenu de la forte dépendance au digital des cabinets et de la pression de leurs clients et des autorités en cas de perte des données, cette attaque est très tentante pour des pirates. D'autre part les cabinets d'expertise comptable ont pour un pirate l'image d'être solvables. La rançon est calculée en fonction de la taille (entre 2 500 et 5 000 euros par employé). En cas de non-paiement de la rançon, le cabinet perd ses données et en cas de paiement il n'est pas sûr de les récupérer (environ 1/3 de non récupération suite au paiement de la rançon)	**FORT**
Vol de données pour revente à tiers concurrent	
Une telle attaque consiste à voler les données des clients d'un cabinet pour les revendre à des concurrents de ces clients. Même si les experts-comptables détiennent des données critiques concernant leurs clients (taux de marge, nature de la clientèle, prix de vente…), ceci ne s'applique qu'à une partie faible de leur clientèle. Ce n'est pas l'attaque la plus rémunératrice ni la plus simple pour un pirate.	**FAIBLE**
Vol de données pour chantage à la divulgation	
Le vol des données d'un cabinet porterait une atteinte forte à son image. Un pirate pourrait penser qu'un cabinet serait prêt à payer pour éviter cette atteinte à son image. Cependant la multiplication récente des cabinets piratés, ou immobilisés à la suite d'un piratage, rend cette attaque de moins en moins efficace. Il n'est plus vraiment honteux d'être piraté, c'est juste très gênant.	**FAIBLE**
Destruction malveillante pour désorganiser ou discréditer	
Une telle attaque suppose qu'un État veuille désorganiser une partie de l'économie ou de l'activité du pays en piratant des cabinets, directement ou via des tiers. Compte-tenu des effets potentiels d'un tel piratage sur l'économie et la perception de la TVA et de l'impôt, c'est tout à fait possible.	**MOYEN**
Attaque de prestige	
Les cabinets d'expertise comptable n'ont pas une réputation fantastique en matière de sécurité, et ne sont pas très connus du grand public. Un pirate recherchant un prestige public ou auprès des autres pirates s'attaquera à d'autres cibles pour améliorer sa réputation.	**FAIBLE**

Vol de données pour attaque par rebond sur personne physique	
Une telle attaque consiste notamment à récupérer les données sociales ou de paie traitées par un cabinet pour attaquer les employés de ses clients par un phishing hyper ciblé. C'est une stratégie très rentable pour un pirate et qui représente de gros volumes, même en piratant un petit cabinet. Ce type d'attaque se termine souvent par une escroquerie de type AMELI (qui consiste à vider le compte bancaire de la victime) ou usurpation d'identité (pour emprunt bancaire par un pirate au nom de la victime par exemple). C'est un peu long mais très rémunérateur. Le nombre de ces attaques est en très forte croissance.	**FORT**
Vol de données pour attaque par rebond sur entreprise	
Une telle attaque consiste à récupérer des données des entreprises clientes d'un cabinet pour les attaquer par un phishing hyper ciblé qui conduira le plus souvent à une attaque avec demande de rançon ou à une fraude au fournisseur. C'est une stratégie très rentable pour un pirate. Dans le cas de la fraude au fournisseur, le pirate fait effectuer les paiements du client sur un compte lui appartenant. Les dommages touchent autant le client que le fournisseur.	**FORT**
Vol de données pour revente sur le darknet	
La revente de données sur internet s'inscrit dans la logique de spécialisation des pirates, avec revente de produits intermédiaires (listes de mails, de coordonnées bancaires, d'accès,…) entre ceux qui collectent des données et ceux qui les exploitent. En l'occurrence, les données des employés des clients d'un cabinet sont faciles à revendre sur le net, surtout si elles incluent leur email. Les données revendues servent à des attaques par leur acheteur (phishing, escroquerie, …).	**FORT**
Vol de données pour usurpation d'identité	
Ce type d'attaque est commun dès lors que la structure attaquée détient des copies de pièces d'identité de personnes physiques. Elle est un peu longue mais très rentable.	**FAIBLE**

En conclusion, les cabinets sont une cible importante pour être rançonnés, mais encore plus pour rançonner leurs clients ou escroquer les employés de leurs clients.

LES TYPES D'ATTAQUANTS

Les États (et sous-traitants)	
L'attaque par un État vise à discréditer ou désorganiser un autre État. Ces attaques sont liées aux tensions géopolitiques et sont en progression régulière. La désorganisation de l'activité d'un cabinet a des effets importants sur l'économie et le fonctionnement d'un État, notamment pour la collecte de l'impôt.	**MOYEN**
Groupes de hackers, attaques en profondeur de quelques cabinets	
Ces attaques demandent des moyens importants mais sont très rémunératrices. Elles conjuguent en général le vol des données clients (entreprises et employés des clients) pour revente et pour attaque par rebond, et la rançon du cabinet dans un deuxième temps.	**FORT** **pour cabinet CA > 20 M€**
Groupes de hackers, attaques massives de multiples cabinets	
C'est le pendant en industrialisé de l'attaque en profondeur. Elle est un peu moins efficace, mais peu coûteuse du fait de l'industrialisation du process. Ce type d'attaque est très rémunératrice dans des professions ayant un fonctionnement similaire d'une structure à l'autre (comme les experts-comptables)	**FORT**
Hackers isolés	
Les pirates isolés attaquent des structures faciles à identifier et de taille (donc de niveau de sécurité grosso modo) adaptée à leurs propres compétences. De ce point de vue, les experts-comptables sont une profession facile à identifier et qu'un pirate pourrait penser solvable.	**FORT**
Hacktivistes	
Les cabinets ne sont pas dans les secteurs d'activité ciblés par ces attaques.	**FAIBLE**
Risque interne	
Ce type d'attaque est d'autant plus fort que le personnel est externe ou à fort taux de turn-over, ce qui n'est pas le cas de la plupart des cabinets.	**FAIBLE**

En conclusion, les attaquants potentiels sont multiples : pirates isolés ou groupes industriels, voire groupes experts pour les plus gros cabinets.

Quelle que soit sa taille, un cabinet peut être attaqué par des pirates avec une expertise forte.