agiris.

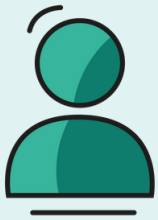
KIT DE SENSIBILISATION À LA CYBERSÉCURITÉ

POUR LES CABINETS COMPTABLES

QUI VOUS ATTAQUE ?

Les espions d'affaires

Ils cherchent à voler des informations confidentielles : résultats financiers, liste des fournisseurs, process internes, stratégies commerciales... Tout ce qui peut leur donner un avantage compétitif.

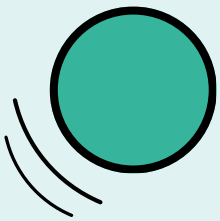


Les cybercriminels opportunistes

Ou les pirates "classiques". Ils parcourent le cyberespace à la recherche des entreprises les moins bien protégées et cherchent à gagner rapidement de l'argent le plus simplement possible.

Les États malveillants

Vous ne rêvez pas ! Certaines grandes puissances, peu démocratiques, s'intéressent aux cabinets comptables pour obtenir des informations sur les flux financiers internationaux, l'évasion fiscale ou pour surveiller des entreprises sensibles.



Les attaques par rebond

Dans cette situation vous n'êtes pas la cible du hacker, mais la porte d'entrée pour atteindre vos clients par exemple. Votre cabinet détient des informations sensibles !

Les techniques préférées des hackers

Le Social Engineering, ou manipulation humaine

Le cybercriminel va essayer de vous manipuler pour obtenir des accès. Exemple : il va essayer de vous faire peur avec un faux message d'alerte sécurité qui vous incite à cliquer sur un lien infecté. Certains se font passer pour un avocat, un banquier, ou votre propre patron !

Une technique très efficace : le spear phising. Elle consiste à personnaliser les attaques ce qui augmente leur efficacité.

41% des attaques de type spear phishing ont pour seul objectif d'établir un premier contact, pour ensuite mieux vous manipuler par la suite.

Imaginez simplement un pirate qui commence par un banal échange, avant de demander discrètement un virement urgent deux ou trois semaines plus tard.

Le Ransomware, l'attaque qui fait trembler tous les cabinets

Ou rançongiciel en français, est un virus qui va bloquer les fichiers en les cryptant. Pour récupérer vos données, le hacker va vous demander une rançon. Tout simplement ! Les conséquences peuvent être dramatiques : arrêt brutal de votre activité, pertes financières, risques juridiques, réputation du cabinet... Bref, c'est un vrai cauchemar.

80% des entreprises qui perdent leurs données à cause d'un ransomware finissent par mettre la clé sous la porte dans l'année qui suit.

PETITE INFO BONUS : le ransomware est devenu une véritable industrie disponible sur le Dark Web, accessible même aux hackers débutants sous la forme d'abonnement mensuel ! On appelle ça le Ransomware-as-a-Service.

L’attaque discrète par excellence, l’Infostealer

C’est un logiciel espion discret dont l’objectif est simple : récupérer un maximum d’informations sans attirer l’attention. L’infostealer veut avant tout consolider un maximum de données sensibles : identifiants, mots de passe, échanges confidentiels, coordonnées bancaires ou encore données fiscales sensibles de vos clients.

Le pirate récupère patiemment ces informations pour monter ensuite une attaque encore plus ciblée et efficace, comme une fraude bancaire ou une usurpation d’identité.

L’attaque par rebond, le piège ultime

L’attaque par rebond consiste à cibler un cabinet comptable pour atteindre indirectement une entreprise plus importante. Les hackers exploitent la vulnérabilité des cabinets, qui détiennent des données sensibles, pour s’infiltrer et préparer des fraudes sophistiquées.

Cette menace peut être technique (intrusion informatique) ou sociale (usurpation d’identité, fraude au président). Protéger vos systèmes, c’est aussi protéger vos clients et préserver votre réputation.

Pour en savoir plus Parole d’Expert est là pour vous !

www.agiris.fr