Alerte presse

Ransomwares :

Plus de 4 entreprises sur 10 ne récupèrent pas toutes leurs données après le versement d'une rançon

- **Plus d'un tiers (36 %) des entreprises ayant payé une rançon ont été visées une seconde fois par des cybercriminels.**
- **Plus de quatre entreprises sur dix (41 %) ayant payé une rançon n'ont pas récupéré toutes leurs données.**
- **Plus d'un quart (26 %) ont estimé qu'une attaque par ransomware menaçait sérieusement la solvabilité et la viabilité de leur entreprise.**
- **Les courriels de phishing restent le point d'infiltration le plus courant pour les gangs de ransomware.**

Paris le 15 novembre 2022 – **En complément de son Rapport 2022 sur la gestion des cyber risques, Hiscox, assureur spécialiste de la protection cyber pour les petites et moyennes entreprises, dévoile un nouveau focus dédié aux ransomwares, qui bénéficie d'éclairages actualisés s'appuyant notamment sur deux tests de phishing menés pendant l'été avec cinq auprès de cinq entreprises.**

Le rapport met en évidence les limites du paiement des rançons par les entreprises : 59% des entreprises ayant payé une rançon à des cybercriminels n'ont pas réussi à récupérer toutes leurs données.

Outre la perte de données, une part significative des entreprises ayant payé les rançons a été confrontée d'autres problèmes :

- 43 % ont dû reconstruire leurs systèmes, alors même qu'elles avaient reçu la clé de déchiffrement
- 36 % ont subi une autre attaque par la suite
- 29 % ont vu leurs données divulguées
- Dans 19 % des cas, le pirate a ensuite exigé plus d'argent
- Dans 15 % des cas, la clé de déchiffrement n'a pas fonctionné

Plus d'un quart (26 %) a estimé que l'attaque avait eu un impact financier important, menaçant la solvabilité et la viabilité de leur entreprise.

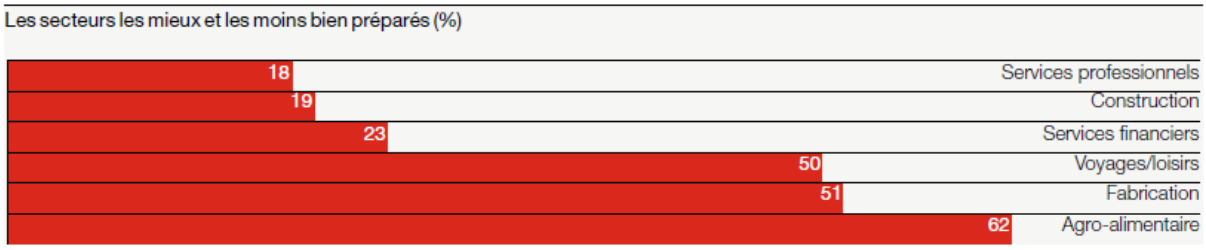
« *Les statistiques montrent que le paiement des rançons ne résout pas toujours tous les problèmes. Il n'est, par exemple, souvent pas possible de restaurer pleinement son système informatique ou d'éviter une fuite des données. Notre rapport montre qu'il est plus efficace d'investir dans la mise en œuvre d'une cyber défense solide – en maintenant les logiciels à jours, en organisant des formations internes régulières, en sauvegardant fréquemment ses données – ainsi que dans la préparation d'une réponse appropriée en cas d'attaque, plutôt que de payer systématiquement les cybercriminels. Un chiffre est particulièrement éloquent : plus d'un quart (26%) des entreprises qui ont payé une rançon dans l'espoir de récupérer leurs données l'ont fait parce qu'elles n'avaient pas de sauvegardes* », commente **Nicolas Kaddeche, Directeur technique d'Hiscox France**.

Le phishing : une menace pour tous les échelons de l'entreprise

Les e-mails de phishing sont les modes d'intrusion les plus communs des ransomwares, constaté par 62 % des entreprises sondées par Hiscox, devant le vol d'identifiants (44 %) et l'intrusion par un tiers fournisseur (40 %).

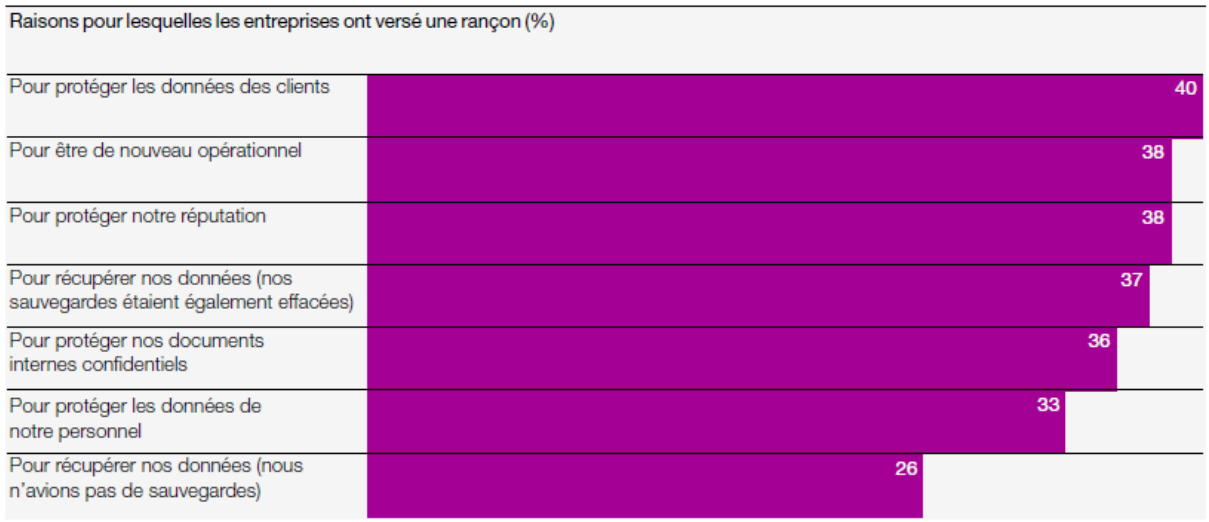
Deux tests réalisés à l'été 2022 par Hiscox auprès de 5 entreprises montrent que tous les échelons de l'entreprise sont concernés : dans une première simulation s'appuyant sur des leurres génériques envoyés en masse (colis Amazon, alerte LinkedIn, etc.), le taux de clic global était de 9 %. Dans le cadre d'une deuxième simulation avec des e-mails ciblés conçus spécifiquement pour chaque entreprise et ciblant des membres de la direction, le taux de clics a été multiplié par quatre, atteignant 36 %. Ces résultats alertent sur la nécessité d'un effort de formation et de sensibilisation très soutenu au sein des entreprises.

Les services professionnels et financiers, et le secteur de la construction mieux préparés aux ransomwares



Pourcentage d'entreprises touchées par un ransomware ayant versé une rançon, par secteur d'activité

La protection des données clients : 1ère raison du versement d'une rançon



Pour accéder au Rapport Hiscox 2022 complet sur la gestion des cyber-risques : ici

Pour accéder au focus actualisé sur les ransomwares : ici

À propos de l'étude

Hiscox a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5 181 professionnels en charge de la stratégie de cybersécurité de leur entreprise ont été sondés (plus de 900 personnes par pays pour les États-Unis, le Royaume-Uni, la France et l'Allemagne, plus de 400 pour la Belgique, l'Espagne et les Pays-Bas et plus de 200 pour la République d'Irlande). Les participants ont rempli le questionnaire en ligne entre le mardi 30 novembre 2021 et le vendredi 21 janvier 2022.

Pendant l'été 2022, Hiscox a mené une analyse complémentaire sur la menace du phishing en réalisant deux simulations auprès de cinq entreprises, afin de mesurer les taux de clics dans différentes configurations.

A propos d'Hiscox en France

Hiscox, assureur spécialiste depuis 1901, est établi en France depuis 25 ans où il assure près de 100 000 particuliers et professionnels. Assureur historique de l'Art et des biens d'exception pour la clientèle privée, Hiscox a su ensuite développer son expertise dans le domaine des assurances professionnelles avec une gamme spécialisée couvrant aujourd'hui près de 500 métiers de services. Distribué via des courtiers spécialisés, des partenaires banquiers ou assureurs, Hiscox a été pionnier de l'assurance en ligne et via conseillers pour les entrepreneurs et indépendants. Hiscox est aujourd'hui leader de l'assurance des métiers de l'informatique et du digital et a développé une offre cyber parmi les plus complètes du marché. C'est la connaissance et la compréhension des métiers de ses clients et de leurs risques, la mobilisation des meilleurs experts avant, pendant et après les sinistres qui permettent à Hiscox de construire des couvertures adaptées à leurs besoins. Hiscox a l'ambition de changer l'expérience de l'assurance pour ses clients et l'objectif de protéger au mieux ce qui compte pour eux. https://www.hiscox.fr

Contact presse
Weber Shandwick : hiscox@webershandwick.com
Romain MERLE – 06 60 35 18 43