MEDIA ALERT

LES 10 CYBERATTAQUES QUI ONT MARQUE L'ANNEE 2019

Le 19 décembre 2019 – ***A l'approche de la fin d'année, Hiscox, spécialiste de l'assurance cyber, revient sur les failles de cyber sécurité les plus frappantes de 2019.***

La menace cyber ne concerne pas uniquement les entreprises : aujourd'hui les centres hospitaliers, les villes, ou même les pays en sont les cibles directes. La diversité des secteurs attaqués cette année, comme des modes opératoires démontre qu'aucune organisation n'est à l'abri d'un cyber incident.

Selon le *rapport Hiscox sur la gestion des cyber risques 2019*, *« 81% des entreprises ne sont pas assez armées contre la menace cyber. La nécessité de se protéger contre ces risques est d'autant plus importante que le nombre de cyberattaques continue d'augmenter »* **commente Astrid-Marie Pirson, Directrice Technique de la souscription chez Hiscox France.**

1. Altran - Janvier 2019

En début d'année, le géant français du conseil en technologie a été victime d'une cyberattaque qui a temporairement interrompu son activité en Europe. A l'aide d'un virus cryptolocker, le hacker a réussi à pénétrer dans le système informatique de l'entreprise et à chiffrer un à un ses fichiers. Pour limiter la propagation du virus, le groupe a dû déconnecter son système informatique et mettre en place un protocole de restauration inédit pour que l'activité reprenne son cours. Les perturbations se sont prolongées jusqu'en février, soit plus d'un mois après le début de l'attaque, et l'entreprise a notamment payé une rançon de 300 bitcoins, soit 1 million d'euros, sans avoir jamais reçu la clé de décryptage. Le coût financier de cette cyberattaque est estimé à 20 millions d'euros.

2. Airbus – Janvier 2019

Après Altran, c'est à Airbus, le groupe d'aéronautique, d'être la cible des hackers. Si l'attaque n'a pas eu de conséquences sur les opérations commerciales, des données personnelles ont toutefois été consultées par les pirates (coordonnées professionnelles, identité de collaborateurs…).

3. ICANN – Février 2019

L'annuaire central de l'internet, l'ICANN, situé en Californie, a été victime d'une cyberattaque inédite à la fois par sa taille et son mode opératoire : un piratage à grande échelle qui consistait à modifier les adresses de sites internet pour donner aux utilisateurs l'illusion d'être sur un site sécurisé et récupérer leurs données personnelles (mots de passe, identifiants, adresses email, …).

4. Equateur / Julian Assange – Avril 2019

Après avoir retiré son droit d'asile à l'informaticien australien Julian Assange, les services publics et administrations de l'Equateur ont subi une série de cyberattaques. Par exemple, la page d'accueil du site de la municipalité de La Mana, dans le centre du pays, a arboré pendant quelques heures, la photographie de l'interpellation du célèbre fondateur de Wikileaks, en guise de protestation.

5. Baltimore (USA) – Mai 2019

Des hackers ont infiltré le réseau informatique de la ville de Baltimore et neutralisé les données de 10 000 ordinateurs municipaux pendant plus de trois semaines. Une attaque qui a eu des conséquences importantes : impossibilité pour les habitants de payer en ligne leurs impôts et taxes, images de caméras de surveillance corrompues, incapacité des services municipaux à générer des factures. Les hackers se sont servis d'un outil de piratage initialement développé par la NSA, et ont exigé le versement d'une rançon de 89 000 euros en bitcoins. Selon les dernières évaluations, le préjudice financier pour la mairie s'élève à 16 millions d'euros : 9 millions d'euros pour la remise en état du système informatique (dont le rachat de milliers d'ordinateurs), et 7,1 millions d'euros de perte de revenus. S'y ajoute bien sûr le préjudice subi par les citoyens de Baltimore dont les données personnelles, notamment bancaires, ont été dérobées.

6. Eurofins – Juin 2019

Au mois de Juin dernier, Eurofins, leader mondial de l'analyse biologique, a été victime d'un ransomware qui a perturbé ses systèmes informatiques et exposé les données de santé de centaines de milliers de Français. La répercussion de cette attaque informatique a été considérable, puisque la perte est estimée à 35% sur les bénéfices semestriels du groupe. Au-delà des conséquences financières, l'impact se mesure également en terme de confiance et de réputation : certains clients, britanniques notamment, ont suspendu les contrats d'Eurofins jusqu'à ce qu'ils obtiennent la garantie que leurs données n'ont pas été compromises.

7. L'agglomération Grand Cognac – Octobre 2019

Via un simple cryptovirus qui a infecté le système de messagerie puis touché 400 ordinateurs, toutes les données informatiques de l'agglomération de Grand Cognac en Charentes ont été rendues illisibles, et une demande de rançon s'élevant à 180 000 euros a été faite par le hacker. Les dégâts ont par ailleurs été évalués par la commune aux alentours de 150 000 euros

8. M6 – Octobre 2019

Le groupe de médias français a été victime d'une attaque informatique, a priori via un rançongiciel. Si le groupe a pu continuer à assurer la bonne diffusion des programmes sur l'ensemble des antennes TV et radio, cette attaque rappelle la grande vulnérabilité des médias aux risques cyber. La dernière cyberattaque d'ampleur signalée contre un média en France était celle de TV5 Monde en 2015. Le groupe avait alors perdu le contrôle de ses sites internet, de ses comptes sur les réseaux sociaux, et avait dû couper pendant plusieurs heures les programmes de ses 11 chaînes.

9. EDENRED – Novembre 2019

Edenred, leader mondial des solutions de paiement dans le monde du travail a été ciblé par un virus, heureusement rapidement identifié, ce qui a permis de limiter sa propagation. Le retour à la normale des activités d'Edenred a été rendu possible grâce aux mesures de précaution prises immédiatement après l'attaque, notamment la déconnexion des systèmes afin de protéger les activités commerciales et les opérations des clients. Aucune donnée personnelle n'a été volée ou consultée et aucune contamination ou propagation auprès des clients d'Edenred n'a été constatée.

10. CHU de Rouen – Novembre 2019

Une importante cyberattaque a visé le centre hospitalier universitaire (CHU) de Rouen : le pirate a bloqué les machines et exigé une rançon pour les redémarrer. L'attaque a provoqué un arrêt général des équipements touchant à l'informatique, aux ascenseurs, à l'imagerie médicale, aux systèmes d'analyses… La remise en route du système a mobilisé au total une cinquantaine de personnes.

Astrid-Marie Pirson se tient à votre disposition pour tout complément d'information.

A propos d'Hiscox Groupe

Hiscox est un groupe international d'assurances spécialisées. Son ADN de spécialiste en fait un référent pour la protection des œuvres d'art et patrimoines d'exception mais aussi pour les risques informatique et cyber.
Le Groupe Hiscox emploie plus de 3 300 collaborateurs dans 14 pays et 34 bureaux pour répondre aux besoins de ses clients.
https://www.hiscoxgroup.com/

A propos d'Hiscox en France

En France, Hiscox Assurances s'appuie sur l'expertise de 135 collaborateurs pour proposer ses produits d'assurances spécialisés à travers 3 canaux de distribution (Courtage, Direct et Partenariats). Cette organisation reflète la volonté d'Hiscox de placer les besoins du client au centre de son développement en lui offrant une approche multicanale.
Par le biais de son réseau de courtiers spécialisés, l'assureur propose une large gamme d'assurances pour la clientèle privée, les professionnels et les collectivités.
Parallèlement, la distribution via des partenariats noués avec des banc-assureurs ou des mutualistes offre une approche complémentaire.
Pleinement investi sur le digital, Hiscox est également le 1er assureur RC Pro 100 % en ligne pour les TPE. Ce canal de vente directe (via le site www.hiscox.fr et des conseillers) permet une assurance simplifiée en phase avec les besoins spécifiques des entrepreneurs.
L'agilité et les valeurs d'Hiscox définissent son activité, avec un accent sur l'humain, le courage et l'excellence dans l'exécution au service de ses clients. Sa nouvelle signature de marque « Penser à tout, et surtout à vous » en est l'illustration.
Plus d'informations : http://www.hiscox.fr

Contacts presse

Weber Shandwick hiscox@werbershandwick.com
Alix LAGERSIE – 07 61 44 68 42
Julie FONTAINE - 07 63 10 69 21