HISCOX

CYBERCLEAR®

Dernières tendances sinistres
Octobre à Décembre 2019

En bref

Les périodes de congés ouvrent des brèches de sécurité

La dernière partie de 2019 a vu un certain nombre de cyberattaques fleurir dans la presse – certaines ont affecté des assurés Hiscox. Les périodes de congés sont généralement propices à ce que les cybercriminels passent à l'acte. Selon le secteur d'activité, les bureaux sont plus calmes, avec moins de personnes vigilantes aux problématiques applicatives et informatiques, ou au contraire connaissent des périodes d'activité saisonnière plus importantes. le dernier trimestre de l'année n'est quoi qu'il en soit pas la bonne période pour baisser la garde de laasécurité informatique.

Chiffres sinistres clefs

Le top 3 des types de sinistres que nous avons observé : détournements financiers, cyber-extorsion et exfiltration de données.

44%

des sinistres au UK étaient des détournements financiers, via des emails professionels piratés (BEC : business email compromis) et des détournements de paiements frauduleux (PDF : payment diversion fraud) qui étaient représentés dans toutes les régions.

36%

des sinistres européens incluaient de l'exfiltration de données avec le malware Emotet souvent perçu comme un précurseur.

44%

des sinistres des Etats-Unis étaient dus à de la cyber-extorsion via ransomware, les demandes de rançon continuent de croître aux Etats-Unis.

25%

des sinistres (hors cas de ransomware) étaient le résultat d'attaques de phishing – la faille de sécurité de Microsoft Office 365 continuant d'être la source d'infiltration.

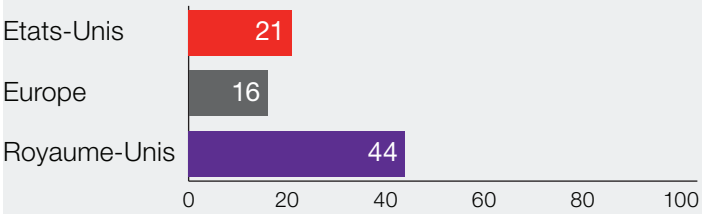
Que faire ?

Il est impératif pour toute entreprise de rester en alerte, ce qui est évidemment plus facile à dire qu'à faire. Ceci dit, réparer un système suite à une cyberattaque coûtera souvent plus en temps et en argent que de gérer et anticiper ce risque en amont, et ce sans considérer les dommages à la réputation. Certains des moyens clé pour gérer ces menaces essentielles sont :

- renforcer l'authentification multiple – c'est essentiel pour les comptes administrateurs. Pour le versement de fonds, avoir une approche d'authentification multiple systématique ;
- tester les sauvegardes et back-ups – en fonction de ce que sont vos données critiques et où elles sont stockées. Préférer les back-ups hors site et les tester régulièrement ;
- vérifier les logiciels - activer toutes les mises à jour de logiciels et les patch visant à réduire les vulnérabilités ;
- vérifier votre assurance cyber et ce qu'elle couvre – vérifier qu'elle couvre la fraude. Cette garantie est souvent à souscrire en option sur une police cyber standard ;
- la formation – former et tester vos employés à reconnaître un email de phishing ou des demandes de paiement frauduleuses.

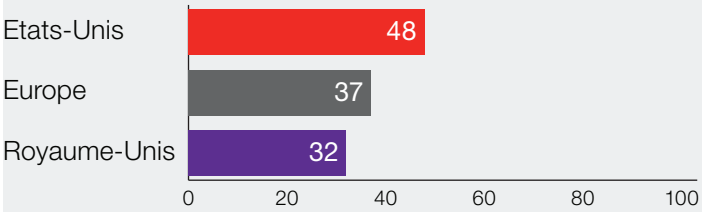
Gareth Wharton
Cyber CEO
Hiscox

Détournements financiers (%)



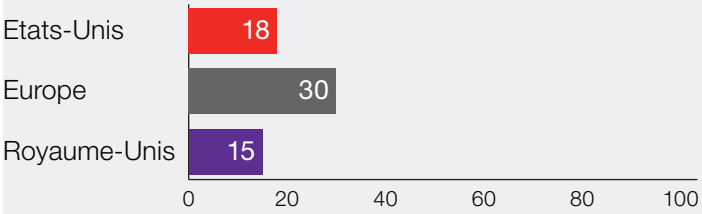
- BEC/PDF sont prédominants au UK.
- Les assurés devraient vérifier qu'ils ont bien les garanties optionnelles de couverture de la fraude dans leur police d'assurance.

Exfiltration de données (%)



- Nous observons souvent que le malware Emotet est précurseur à toute attaque par ransomware, en particulier en Allemagne.
- Nos clients devraient nous signaler dès que possible si des infections par Emotet sont détectées.

Cyber extortion (%)



- Les demandes de Ransom aux USA sont plus élevées que dans les autres régions, mais nous commençons à observer une hausse en Europe.
- Nous continuons à indiquer que les backs-ups sont indispensables pour prévenir d'une extortion ou d'un ransomware. Hausse significative des cas de ransomware au UK.
- Ruyuk et Sodinokibi sont plus les ransomeware identifiés les plus fréquents, notamment aux Etats-Unis.

Exemples d'attaques dans la vrai vie

Une entreprise de formation a besoin de leçons sur l'authentification à deux facteurs
Secteur : formation, éducation
CA : 7,3 m€
Coût du sinistre : 22 000€

Un employé reçoit un email d'une personne prétendant être le PDG et demandant un virement à un compte de banque de détail. L'employé prépare et effectue le paiement le jour même. Ce n'est que quand d'autres demandes du même type ont été formulées que l'activité frauduleuse a été découverte. Hiscox a payé le montant des transferts au compte frauduleux ainsi que les coûts d'experts pour confirmer la cause de la fraude. On a ainsi confirmé que la perte était bien une fraude de type ingénierie sociale provenant d'un email identifié comme frauduleux.

Fuite de données dans une entreprise dans l'IT
Secteur : informatique
CA : 31,2 m€
Coût du sinistre : 182 000€

Un certain nombre d'ordinateurs portables ont été volés sur le site de l'entreprise. Ces ordinateurs n'étaient pas cryptés et contenaient des données client confidentielles. Le service sinistre Hiscox a dépêché un expert et instruit l'analyse. Celle-ci a démontré que presque 900 individus devaient être notifiés et qu'il fallait initier un service de crédit monitoring pour éviter tout risque de dérives de l'incident.

Un hacker peu charitable
Secteur : caritatif
CA : 5,6 m€
Coût du sinistre : 283 000€

Une ONG faisant de la recherche et développement a vu 39 de ses serveurs cryptés. L'établissement n'a pas répondu à la demande de rançon et 60 employés se sont retrouvés incapables d'utiliser leurs postes de travail. Hiscox a accompagné son client pour migrer vers une nouvelle infrastructure IT a payé la reconstitution et le montant de la perte d'exploitation.

Glossaire

Vous avez dit... ?

Les termes liés au cyber attaques ressemblent souvent à des acronymes barbares. Nous allons ici vous aider à vous familiariser avec eux.

Authentification multiple

Mécanisme de sécurité impliquant d'utiliser plusieurs méthodes d'authentification pour mieux vérifier l'identité d'un utilisateur avant de lui donner l'accès à un système ou une transaction.

BEC : business email compromise
Email professionnels piratés

Accès et contrôle non autorisés à un compte email professionnel pouvant conduire à un accès non autorisé à des données ou à un paiement frauduleux.

Cyber-extorsion

Cyber-pirates cryptant les données/les systèmes de leur victime (rançongiciel - ransomware), et menaçant de divulguer les données volées, prenant en otage les données ou systèmes, etc... jusqu'à ce que les victimes satisfassent leurs demandes de paiement.

Détournements financiers

Cybercriminalité incluant le détournement de fonds.

Fuite de données

Accès non autorisé aux données et dans la plupart des cas, extraction ou copie de ces données hors du réseau de la victime.

PDF : payment diversion fraud
Fraude par détournement de fonds

Cybercriminels redirigeant des paiements vers un compte frauduleux.

Rançongiciel – ransomware

Catégorie de logiciel malveillant qui encrypte ou bloque l'accès à des données ou système, avec une clef de désencryptage fournie seulement contre paiement d'une rançon.

Sauvegarde off line/duplication – redondance

Systèmes additionnels ou alternatifs, sous-systèmes, actifs ou procédés qui permettent de maintenir le niveau de fonctionnalités globale en cas de perte ou de défaillance d'un autre système, sous-système actif ou procédé.

Vulnérabilité

Bugs dans un logiciel que les hackers exploitent pour compromettre les ordinateurs.

Hiscox France
19 rue Louis le Grand
75002 Paris

T +33 (0) 1 53 21 83 12
E hiscox.communication@hiscox.fr
www.hiscox.fr

Hiscox, assureur spécialiste international, est une société cotée au London Stock Exchange (LSE:HSX), dont le siège social est situé aux Bermudes. Notre ambition est d'être un assureur spécialiste reconnu, disposant d'un portefeuille diversifié par produit et zone géographique. Dans le cadre de notre activité de retail au Royaume-Uni, en Europe, en Asie et aux États-Unis, nous proposons une gamme d'assurances spécialisées pour les professionnels, entreprises et particuliers. Les activités relatives aux contrats internationaux, grands comptes et à la réassurance sont gérées par nos divisions Hiscox Marché de Londres et Hiscox Re & ILS. Nos valeurs définissent notre entreprise, qui attache la plus grande importance aux personnes, à la qualité, au courage et à l'excellence dans la réalisation. Nous sommes fidèles à nos engagements et notre service de gestion de sinistres plusieurs fois récompensé en est la preuve. Pour de plus amples informations, rendez-vous sur www.hiscoxgroup.com.

20538c 04/20