HISCOX

Rapport Hiscox 2020 sur les sinistres cyber

Introduction

L'année 2020 ne ressemble à rien de ce que l'on a pu connaître récemment. Alors que le monde luttait contre le Covid-19, de nombreuses entreprises se sont mises en ligne et les risques sont passés de la sécurité physique à la cybersécurité.

Gareth Wharton
Directeur Général de la division Cyber de Hiscox

Bien que le risque cyber ne soit pas nouveau, le changement soudain des modèles d'entreprise a entraîné une demande immédiate de technologies collaboratives, d'accès à distance et la nécessité pour les entreprises de créer un site Web alors que les magasins physiques étaient fermés. Mais la rapidité de mise sur le marché et la sécurité ne vont pas souvent de pair. De nombreuses entreprises n'avaient pas l'expertise interne ou le temps nécessaire pour mettre en place une gouvernance et une surveillance de la sécurité appropriées pour leur nouvelle technologie. Le risque cyber n'a pas nécessairement augmenté du jour au lendemain, mais il s'est déplacé en fonction du rythme des besoins des entreprises, ce qui a eu des répercussions plus tard dans l'année.

Un autre changement majeur concerne les tactiques des pirates informatiques. Au début de l'année 2020, les gangs de logiciels rançon ne se contentaient plus de verrouiller les données, qui pouvaient être restaurées lorsque de bonnes pratiques de sauvegarde étaient en place. Ils ont pris la cyber extorsion et ajouté l'exfiltration de données, ainsi que les attaques par déni de service distribué (DDoS) au mélange. Pour empêcher les gangs de publier les informations personnelles des clients ou pour remettre en ligne les sites de commerce électronique, les entreprises n'avaient d'autre choix que de payer des rançons. La traditionnelle et bonne stratégie de sauvegarde n'était plus une solution infaillible contre ces pirates

Nous avons constaté une tendance continue des attaques dans la chaîne d'approvisionnement, entraînant des violations supplémentaires pour ceux qui utilisent certains fournisseurs. Les principaux organes de presse ont mis en lumière les attaques de grands fournisseurs de services comme Blackbaud et SolarWinds, illustrant l'importance de surveiller le risque cyber tout au long de votre chaîne d'approvisionnement.

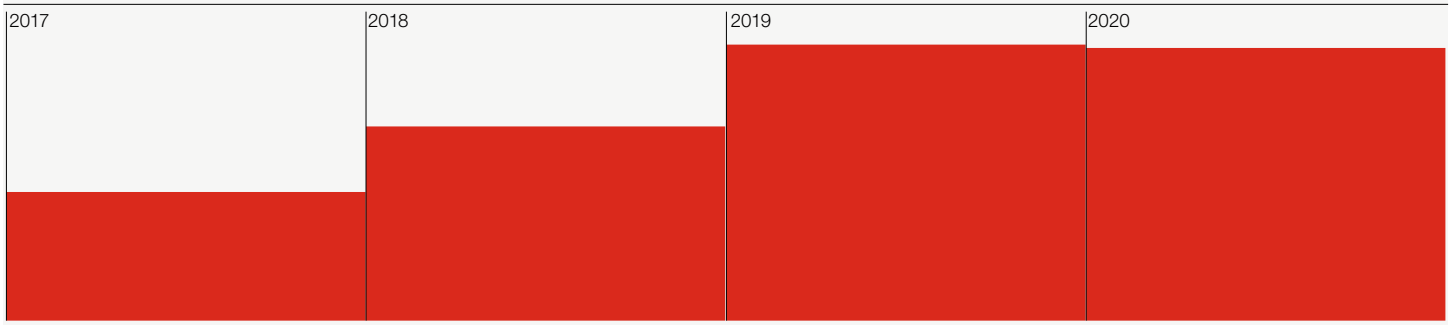
Les sinistres survenus dans nos entreprises de vente au détail Hiscox en 2020 ont reflété les impacts d'un changement du jour au lendemain vers le travail à distance, ainsi que la nécessité d'une vigilance continue contre le défi du rançongiciel. La cyberformation est plus importante que jamais étant donné que l'erreur humaine a joué un rôle dans plus de la moitié des sinistres Hiscox. L'atténuation des logiciels malveillants et l'exfiltration des données pourrait réduire la gravité des coûts et la durée de l'interruption des activités. La cybersécurité de base, comme l'authentification multifactorielle, la mise en place rapide de correctifs pour les actifs critiques et la diligence raisonnable en matière de sécurité des fournisseurs tiers, permettrait de se protéger contre les défis des risques cyber à venir.

L'évolution générale du risque de cybersécurité et les attaques par les pirates informatiques qui ont fait la une des journaux ont fait de 2020 une année difficile ; toutefois, cette année a également permis de sensibiliser les gens à ce risque constant, mais gérable. Les mesures de base en matière de cybersécurité restent la meilleure voie vers la cyberrésilience et, associées à une police d'assurance cyber, elles aident les entreprises à atténuer, gérer et se remettre sur pied après une attaque.

Les sinistres cyber en chiffres

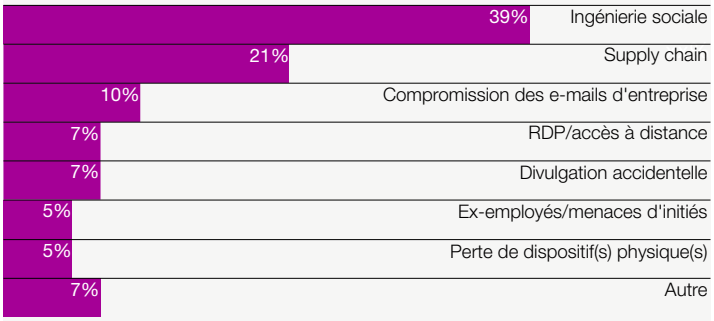
Les causes des sinistres illustrent la nécessité d'une formation continue des employés.

Croissance de la fréquence des sinistres
Tous les territoires Hiscox



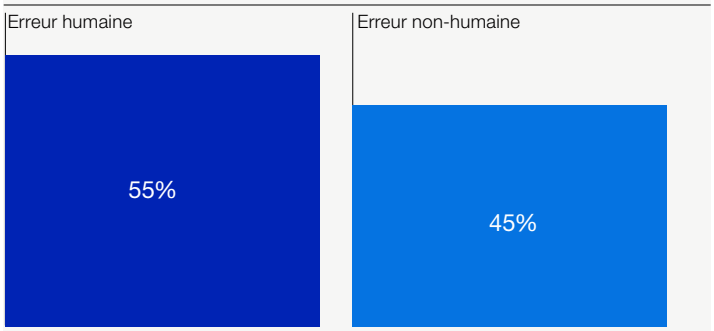
La fréquence des sinistres a presque doublé entre 2017 et 2019.

Causes des sinistres 2020
Tous les territoires Hiscox



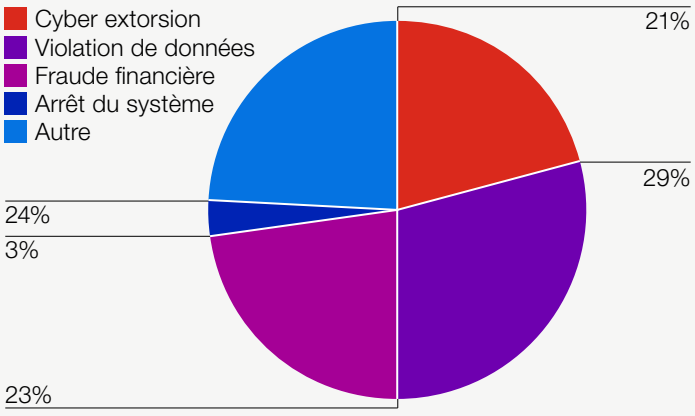
L'ingénierie sociale* et la supply chain sont arrivées en tête, soulignant l'importance de la formation des employés et de l'évaluation de la sécurité des fournisseurs, ainsi que de la sienne.

2020 facteur humain
Tous les territoires Hiscox



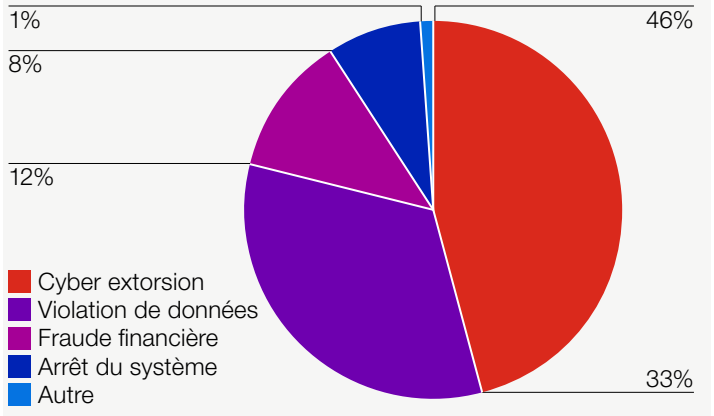
Plus de 50 % des sinistres sont dus à un accident ou à une erreur humaine. La formation des employés est le premier moyen de gérer ce facteur humain majeur.

Sinistres en 2020 par impact
Tous territoires Hiscox



Les réclamations les plus fréquentes en 2020 concernaient les violations de données, autres**, et la fraude financière. Autre, qui comprend les vulnérabilités sont souvent des réclamations qui nécessitent une découverte, mais pas de coûts supplémentaires pour la notification de la violation.

Sinistres en 2020 par coût
Tous territoires Hiscox



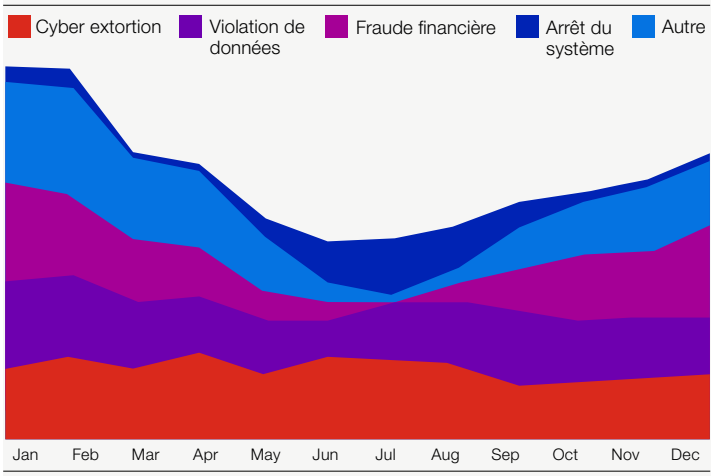
La cyber extorsion, combinée à la violation de données, fait augmenter les coûts des sinistres, en raison des rançongiciels et de l'évolution de la tendance à la divulgation de données.

*L'ingénierie sociale comprend des incidents tels que le phishing, la fraude par détournement de paiement et le pretexting.
**Autres : les piratages téléphoniques, la destruction de données, le cryptojacking et tout autre incident qui ne relève pas des autres types d'impact.

Les sinistres cyber en chiffres

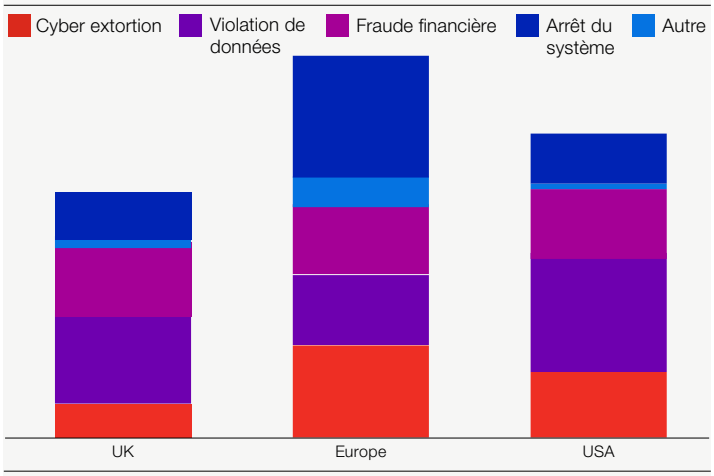
Les violations de données ont augmenté alors que les tendances en matière de rançongiciels ont évolué.

Comptage des réclamations 2020 dans le temps (impact)
Tous les territoires Hiscox



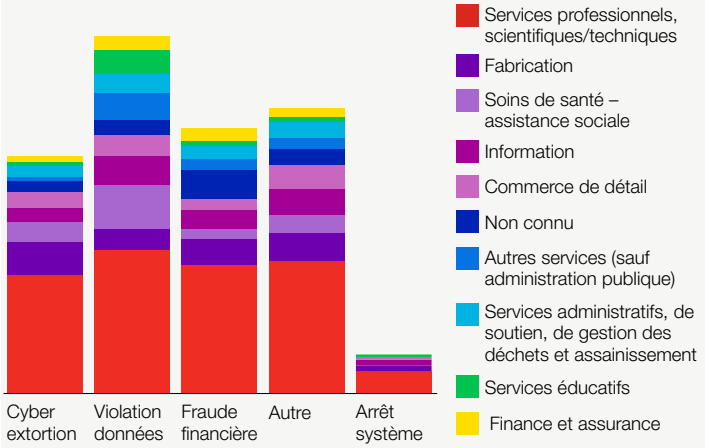
La vague de cyber extorsion de l'été a continué à représenter un défi toute l'année et devrait se poursuivre tout au long de 2021.

Nombre de réclamations en 2020 par région (impact)
Tous les territoires Hiscox



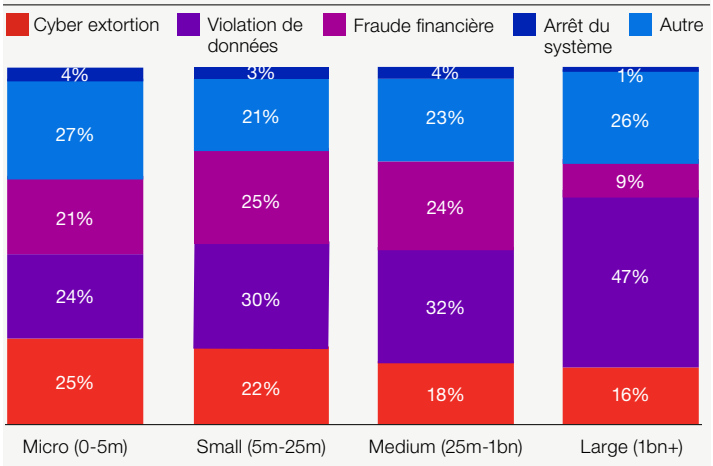
L'Europe a reçu le plus de notifications, mais les coûts étaient les plus élevés aux États-Unis. La notification précoce semble être une pratique courante en Europe, ce qui permet de réduire la durée d'interruption des activités et les coûts globaux.

Nombre de sinistres en 2020 par secteur d'activité (impact)
Tous les territoires de détail Hiscox



L'industrie professionnelle, scientifique et technique était de loin la principale suivie par l'industrie manufacturière et les soins de santé. Bien que les industries concernées reflètent les clients d'Hiscox, les soins de santé ont été particulièrement touchés par la pandémie.

Type d'impact de 2020 sur les demandes d'indemnisation par taille
Tous les territoires de détail Hiscox



Dans les micro, petites et moyennes entreprises, il y a très peu de différence entre les types d'attaques auxquelles les gens sont confrontés.

Tendances sinistres en 2020

Les tendances des demandes d'indemnisation de Hiscox sont en phase avec un grand nombre de cyber-incidents relatés dans l'actualité tout au long de 2020.

Les sinistres dans l'actualité*		Tendances sinistres Hiscox
Le ransomware Sodinokibi a publié environ 337Mo de données volées sur une plateforme russe de pirates et de logiciels malveillants d'artech information systems.	**JANVIER**	Premier exemple majeur d'exfiltration et de publication de données (doxing) après les rançongiciels. Les exploitations de réseaux privés virtuels (VPN) se produisent après les vulnérabilités publiées en janvier.
Check point, une société de cybersécurité, a signalé que les acteurs du secteur avaient enregistré des milliers de domaines zoom faux et malveillants en moins d'un mois, suite à l'augmentation du travail à distance résultant de la pandémie de Covid-19. Un certain nombre d'attaques de rançongiciels à grande échelle ont eu lieu, les acteurs du secteur profitant de la demande publique d'informations sur le Covid-19. Le géant mondial du MSP, Cognizant, a été victime d'une attaque par un logiciel malveillant de type Maze qui a perturbé ses services et ses clients.	**AVRIL**	L'hameçonnage lié au Covid-19 augmente, entraînant des taux de réussite plus élevés en matière d'hameçonnage. Les MSP sont des cibles clés pour les pirates informatiques. Les plaintes pour fraude financière augmentent en raison de la fraude par détournement de paiement (PDF). La compromission de l'email professionnel (BEC) et les courriels de phishing ont été les principales causes des violations de données de Hiscox. Les attaques contre les chaînes d'approvisionnement augmentent.
Blackbaud, un fournisseur de logiciels en nuage, subit une cyberattaque. L'entreprise fournit des services à plus de 25 000 clients dans plus de 60 pays. Microsoft corrige plus de 100 vulnérabilités pour le troisième mois consécutif. Ils demandent aux administrateurs de déployer autant de correctifs, surtout avec le nombre croissant de travailleurs à domicile, ce qui pourrait rendre les entreprises moins sûres à terme si elles ne parviennent pas à suivre le rythme.	**JUILLET**	Le "doxing" devient plus fréquent et les dommages et intérêts augmentent. Les litiges avec des tiers augmentent lorsque le logiciel rançon se transforme en violation de données.
L'Information Commissioner's office (ICO) du Royaume-Uni a infligé des amendes de 18,4 millions de livres sterling et de 1,25 million de livres sterling à Marriott et à Ticketmaster respectivement, pour avoir violé le RGPD à la suite d'incidents de violation de données survenus en 2018. SolarWinds, , un fournisseur mondial de services informatiques, a subi une violation de sécurité, certains de ses produits étant exploités par des acteurs du secteur. FireEye a confirmé avoir été attaqué suite à une attaque de la chaîne d'approvisionnement dans laquelle les acteurs du secteur ont exploité un produit SolarWinds compromis qu'ils utilisaient pour la surveillance du réseau.	**OCTOBRE**	Les attaques de la supply chain des fournisseurs de services se transforment en attaques à plusieurs niveaux. Les réclamations proviennent à la fois des fournisseurs et des clients dont les fournisseurs ont été touchés.

*Notez que les incidents de sinistres dans l'actualité ne sont pas nécessairement des sinistres Hiscox mais sont fournis à titre d'exemples et d'horodatage en utilisant des informations publiques (sources diverses).

Tendances sinistres en 2020

Les principales tendances : l'exploitation des VPN, le phishing Covid-19, les risques liés à la supply chain et les rançongiciels.

Exploitation de réseaux privés virtuels (VPN)

Des chercheurs en sécurité ont signalé des failles de sécurité dans plusieurs services VPN. Les dispositifs VPN doivent être connectés à internet, ce qui permet aux attaquants de rechercher facilement ces vulnérabilités sur la toile. Ces dernières donnent aux attaquants un accès à un réseau sans identifiants de connexion. Dans tous les cas, les attaquants pouvaient alors exécuter leur propre code pour accéder aux systèmes internes, exfiltrer des données, installer un rançongiciel et/ou effacer des appareils. Au moins 15 % des demandes notifiées en janvier concernaient des vulnérabilités VPN.

Cas réel

Secteur	Transport
Chiffre d'affaires	€120-600 million
Coût du sinistre	€290,000
Incident	L'assuré est une société de transport public qui a subi une attaque par ransomware. Des pirates ont exploité une vulnérabilité récemment publiée dans Citrix Netscaler, une solution VPN bien connue. Les auteurs ont également tenté d'exfiltrer des données sensibles, mais sans succès.
Solution	L'assuré a fait appel aux services d'un fournisseur non-Hiscox et Hiscox a pris en charge la notification à l'ICO et les coûts d'interruption des activités.

Le phishing Covid-19 se poursuit

Dans le cadre des efforts visant à gérer la propagation du coronavirus (Covid-19), de nombreuses entreprises ont mandaté ou encouragé leurs employés à travailler à domicile. L'une des principales menaces auxquelles les entreprises sont confrontées lorsque leurs employés travaillent à distance sont les e-mails de phishing sur le thème du coronavirus. Les cybercriminels profitent de l'anxiété et de la soif d'informations en envoyant des emails de phishing contenant des informations sur le Covid-19, telles que vaccins, remboursements d'impôts, mesures préventives de l'OMS, etc.

Cas réel

Secteur	Industrie
Chiffre d'affaires	€1-5 million
Coût du sinistre	€10,000
Incident	L'assuré a subi une attaque de rançongiciel sur un de ses ordinateurs de la variante Ako/MedusaReborn. Malheureusement, les sauvegardes étaient datées de deux mois auparavant, suite à une panne d'électricité dans le serveur de stockage en réseau (NAS) pendant le verrouillage. La restriction en vigueur a entraîné cette panne.
Solution	Hiscox a fait appel à ses experts pour mener une enquête qui a permis de déterminer la variante du rançongiciel et le mode d'entrée. L'assuré a pu restaurer ses données à partir de sauvegardes, bien qu'il y ait eu une certaine perte de données en raison de leur ancienneté.

Attaques contre la supply chain

La tendance de ces attaques s'est poursuivie tout au long de l'année 2020. Une attaque contre un fournisseur de logiciels a entraîné 22 % des demandes d'indemnisation auprès d'Hiscox pour violation de données au troisième trimestre. Avec un nombre croissant d'attaques par rançongiciel impliquant l'exfiltration de données, les entreprises ne peuvent plus compter sur des sauvegardes efficaces pour limiter les attaques par logiciels malveillants.

En décembre, un prestataire de services informatiques a subi une violation de sécurité dans le cadre d'une vaste campagne, où ses produits ont été exploités par des acteurs du secteur. Cette situation a déclenché de nombreuses déclarations de sinistres, en particulier aux États-Unis (17 % des sinistres aux États-Unis ont eu lieu en décembre), et bien qu'aucune cyberattaque n'ait été perpétrée contre les assurés concernés, des frais d'expertise pour évaluer les dommages potentiels ont été encourus.

Cas réel

Secteur	Organisme de bienfaisance
Chiffre d'affaires	€1-6 million
Coût du sinistre	€12,000
Incident	L'assuré est une organisation caritative qui octroie de petites subventions au Royaume-Uni. L'assuré a été informé que les données relatives aux donateurs (noms, coordonnées et montants donnés) ont été touchées par une attaque de rançongiciel chez son fournisseur (processeur de données). Dans cet incident, une grande quantité de données traitées par le fournisseur pour le compte des clients a été exfiltrée par l'attaquant. Le fournisseur a payé une rançon à condition que les données exfiltrées soient détruites.
Solution	L'assuré a engagé des avocats pour le conseiller et des notifications ont été faites à environ 2 000 personnes concernées. Hiscox a couvert tous les frais de justice.

Tendance sinistres 2020

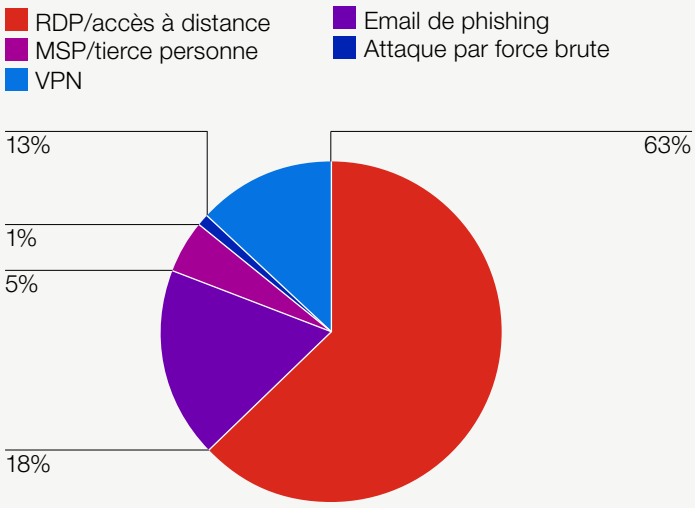
Evolution des rançongiciels

L'année 2020 a vu une augmentation des attaques de rançongiciels couplées à l'exfiltration de données. De nombreux rançonneurs ont lancé des sites web pour afficher les données volées afin de nuire à la réputation des victimes, ou de mettre aux enchères les données. Cela s'est également reflété chez Hiscox, où les cas de piratage ont évolué d'une interruption d'activité à des incidents de violation de données. Hiscox a également vu de nombreux cas où les fournisseurs de l'assuré sont victimes de rançongiciels, affectant ainsi les données de l'assuré.

Cas réel

Secteur	Media
Chiffre d'affaires	€100-500 million
Claim cost	€500,000
Incident	L'assuré est une agence de presse qui a subi une attaque par rançongiciel. Les rançonneurs ont exfiltré les données de l'assuré, y compris celles des 800 employés (noms, adresses personnelles, dates de naissance, numéros de permis de conduire et de sécurité sociale).
Solution	Les cyber criminels ont demandé une rançon de 1,2 million de dollars. Elle a été négociée pour les empêcher de publier les données volées.

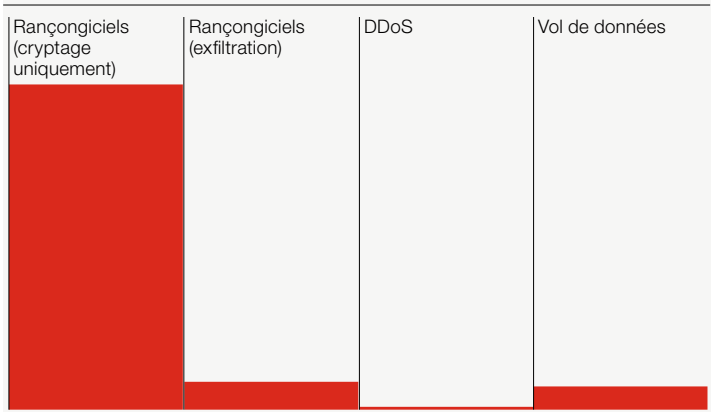
2020 mode d'entrée de la cyber extorsion
Tous les territoires Hiscox



Le portail de bureau à distance (RDP)* reste le point d'entrée commun des attaques de rançongiciels. 63% de tous les sinistres liés à ces attaques se sont produits via un RDP ouvert à Internet. Pour beaucoup, les incidents liés aux rançongiciels ont évolué pour inclure l'exfiltration de données, augmentant le coût des sinistres, tenant compte de la notification aux autorités de réglementation, de la surveillance du crédit, etc.

*Il s'agit d'un échantillon de 39 % des cas de rançongiciels sur la période d'octobre 2019 à septembre 2020 pour lesquels le point d'entrée a pu être confirmé.

Type de cyber extorsion en 2020
Tous les territoires Hiscox



Vue du marché londonien

Bien que ce rapport soit axé sur les petites entreprises au Royaume-Uni, aux États-Unis et en Europe, l'évolution des rançongiciels a également touché les marchés de Londres. Pour les entreprises de plus d'1 milliard d'euros de CA, la fréquence et la gravité des sinistres liés aux rançongiciels ont fortement augmenté en 2020. La tactique du doxing a augmenté le temps et le coût de la gestion des sinistres.

Avant novembre 2019, lorsque les rançongiciels étaient à leur début, le cycle de vie d'un sinistre ne dépendait réellement que de la rapidité avec laquelle l'assuré notifiait un sinistre d'interruption d'activité (IE), en plus de tout ajustement ou négociation autour de l'IE par la suite. La récupération complète pouvait prendre un an ou moins.

Lorsque le doxing et l'exfiltration de données sont arrivés, les frais de notification de la violation et d'interaction réglementaire se sont ajoutés, et le potentiel de litige avec des tiers a augmenté. Que le litige découle d'un rançongiciel ou d'une simple violation de données, le délai de clôture de la réclamation peut désormais être de deux à trois ans, et ce, si le litige ne va jamais jusqu'au procès.

La fréquence des sinistres et l'évolution des rançongiciels en doxing ont augmenté la gravité et les pertes pour les entreprises de plus d'1 milliard d'euros de CA.

Atténuer les risques

Les cyber risques doivent être maîtrisés. Contribuez à les réduire en mettant en œuvre certaines mesures de réduction essentielles.

Construire un pare-feu humain

Formez les employés à repérer et à gérer les courriels de phishing, ainsi qu'à comprendre les autres cyber risques. Les employés sont la première ligne de défense contre une cyberattaque. Hiscox propose actuellement la Hiscox CyberClear Academy, une plateforme de formation gratuite à la cyber conscience, à tous ses clients de cyber assurance.

Activer l'authentification multifactorielle

Les failles dans Microsoft Office 365 (O365) continuent d'être à l'origine de nombreuses fraudes concernant des email compromis (BEC) ou détournements de fonds frauduleux (PDF) pour Hiscox aux États-Unis et en Europe. Sur tous les comptes d'utilisateurs, mais surtout sur les comptes d'administrateurs, l'authentification multifactorielle est une première étape simple vers la sécurité.

Testez votre stratégie de sauvegarde

Il ne suffit pas d'avoir des sauvegardes fréquentes, en ligne et hors ligne. Vous devez vous assurer que votre plan de sauvegarde a été testé et approuvé. En Allemagne, pendant plusieurs mois, Hiscox n'a payé aucune rançon grâce à des sauvegardes adéquates.

Patch et mises à jour fréquentes

Le VPN reste un point d'entrée courant dans les attaques de rançongiciels. Ce sont des technologies sur lesquelles on compte beaucoup, notamment pour le travail à distance. De tels incidents peuvent être évités par l'application systématique de correctifs. Assurez-vous que les logiciels anti-malware, les IDS/IPS (logiciels de détection/prévention des intrusions), etc. sont à jour. Si vous utilisez de tels services et qu'ils n'ont pas encore été corrigés, veuillez les désactiver pour éviter qu'ils ne soient détectés par les scans Internet. Réinitialisez également les informations d'authentification de tous les VPN concernés.

Fermez tous les ports ouverts inutiles

L'accès à distance (ou (Remote desktop protocol – RDP) reste le principal point d'entrée des attaques de rançongiciels et, au final, de l'exfiltration de données. Lorsque ces ports sont exposés à Internet, ils offrent un moyen relativement facile pour les criminels de pénétrer dans un réseau. De tels incidents peuvent être évités en appliquant des correctifs, en désactivant les ports (sauf si nécessaire) et en limitant leur exposition à Internet. Les ports qui doivent rester ouverts doivent être régulièrement surveillés.

Informez rapidement votre assureur

Les logiciels malveillants peuvent être la première étape d'attaques plus importantes entraînant des coûts accrus. Plus tôt vous notifiez un sinistre potentiel ou réel, plus vite votre entreprise pourra reprendre ses activités. Selon le Rapport sur la gestion des risques cyber HIscox 2020, qu'une rançon ait été payée ou non, les pertes moyennes pour toutes les entreprises soumises à une attaque par rançongiciel étaient presque deux fois plus élevées que celles qui n'ont eu à lutter que contre un logiciel malveillant seul – 927 000 dollars contre 492 000 dollars. Alors que les cas d'exfiltration de données continuent d'augmenter, la détection précoce des logiciels malveillants est plus importante que jamais pour prévenir une attaque par rançongiciel et un éventuel doxing.

Exigez que vos fournisseur se protègent

La vigilance à l'égard des fournisseurs de la chaîne d'approvisionnement est essentielle, surtout s'ils traitent les données des assurés. Le " doxing " lors d'attaques rançongiciel est désormais monnaie courante et ne fera qu'augmenter le nombre de réclamations pour violation de données.

A surveiller 2021

Que va-t-il se passer ? Certaines tendances sont là pour rester et les entreprises de toutes tailles doivent se protéger, rester vigilantes et renforcer leur résilience.

1

Les retombées de SolarWinds

Les impacts immédiats et les larges ramifications sont encore inconnus. Il est probable que les attaques se multiplient et que les chaînes d'approvisionnement en logiciels deviennent des cibles. Les services de construction et de déploiement ont toujours été conçus pour la vitesse et la commodité, et non pour la sécurité. Se méfier de l'exploitation des vulnérabilités critiques des produits Microsoft.

2

Evolution des rançongiciels

Les criminels sont créatifs et innovants lorsqu'il s'agit de faire pression sur les victimes pour qu'elles paient. Différents modes d'attaque seront utilisés conjointement pour provoquer des perturbations supplémentaires - DDoS et doxing en plus des rançongiciels. Les ports d'accès à distance RDP ouverts et l'exploitation des vulnérabilités de l'accès à distance resteront les principales voies d'entrée des cybercriminels. Le doxing constitue une menace majeure pour toutes les entreprises et le secteur de la cyberassurance en général.

3

La menace perpétuelle du Covid-19

Les campagnes de phishing passeront de la diffusion du Covid-19 aux informations sur les vaccins et à l'inscription. Les attaques cibleront probablement l'effort de réponse au Covid-19 et les industries et services correspondants - soins de santé, gouvernement local, distributeurs de vaccins, etc.

4

Le paysage juridique évolue

Les actions en justice intentées par des tiers et les recours collectifs vont augmenter, tout comme les amendes liées au RGPD, car les violations de données se multiplient en raison du doxing et des violations de la supply chain. Compte tenu de la pression exercée sur les rançongiciels, nous verrons probablement d'autres interventions gouvernementales et des changements de politique entourant les paiements et les exigences de prévention des rançongiciels.

5

Nouveau vecteurs d'attaque

Nous devons faire preuve d'autant de créativité que les cybercriminels, en anticipant leurs mouvements. Parmi les zones de vigilance potentielles, citons les attaques de logiciels malveillants sur les points de vente, les tempêtes géomagnétiques et autres armes électromagnétiques, les attaques sur les protocoles temporels et les kits d'exploitation armés des États-nations.

Glossaire

Business email compromise (BEC).
L'accès et le contrôle non autorisés d'un compte de messagerie professionnelle, qui peuvent conduire à une violation des données ou à une fraude par détournement de paiement.

Cyber extorsion.
Les cybercriminels cryptent les données/systèmes d'une victime (rançongiciels), menacent de publier les données volées, prennent en otage les données/systèmes, etc. jusqu'à ce que la victime réponde à leurs demandes de paiement.

Violation de données.
Accès non autorisé à des données et, dans la plupart des cas, suppression ou copie de ces données du réseau de la victime.

Doxing.
Il s'agit de l'acte de divulguer ou de publier publiquement des données appartenant à quelqu'un d'autre sans son autorisation.

Ex-employés/menaces d'initiés.
Il peut s'agir d'ex-employés mécontents ou d'employés mal intentionnés.

Fraude financière.
Cybercriminalité impliquant le vol d'argent.

Impact humain.
Les actions ou inactions involontaires des employés qui peuvent entraîner un cyber incident. Il s'agit notamment des courriels usurpés, du hameçonnage, de la fraude par détournement de paiement (PDF), de la divulgation accidentelle, etc.

Perte ou vol du dispositif physique.
Perte d'un dispositif physique contenant les données de l'assuré.

Fournisseurs de services gérés (MSP)/tiers.
Cyber incidents résultant d'un tiers ou d'un fournisseur.

Mauvaise configuration.
Configuration incorrecte de certaines technologies conduisant à un cyber incident.

Payment diversion fraud (PDF) – Détournement de fonds frauduleux.
Les cybercriminels redirigent le(s) paiement(s) vers un compte frauduleux.

Remote desktop protocol (RDP) – accès à distance.
Un outil propriétaire développé par Microsoft qui fournit à un utilisateur une interface pour se connecter à un autre ordinateur via une connexion réseau.

Virtual private network (VPN).
Couramment utilisé pour permettre aux travailleurs à distance qui ne font pas partie du réseau de l'entreprise d'accéder en toute sécurité aux services de l'entreprise depuis leur domicile ou lors de leurs déplacements.

Hiscox Assurances
38 avenue de l'Opéra
75002 Paris France

T +33 (0)1 53 21 82 82
E info.france@hiscox.com
Pour en savoir plus sur nos solutions CyberClear
hiscox.fr/courtage/toutes-assurances-hiscox/cyberclear

21444 04/21