HISCOX

Rapport cyber-sinistres 2018

Hiscox, assureur spécialiste, est une société cotée au London Stock Exchange (LSE:HSX) et dont le siège social est situé aux Bermudes. Dans le cadre de son activité de retail au Royaume-Uni, en Europe et aux États-Unis, Hiscox propose une gamme d'assurances spécialisées à destination des professionnels, entreprises et particuliers. Pour plus d'informations, rendez-nous visite à l'adresse suivante : www.hiscox.fr.

Introduction
Du ransomware au cryptojacking...

Gestion des cyber-risques
Si beaucoup voient encore la cyber-assurance comme un produit nouveau, cela fait déjà presque vingt ans qu'Hiscox propose cette garantie aux entreprises dans certains pays ; au cours des seuls 12 derniers mois, nous avons reçu à ce titre plus de 1.000 déclarations de sinistre.

La cause la plus fréquente de ces sinistres reste le ransomware – qui consiste à rendre le système informatique d'une entreprise hors d'usage jusqu'au paiement par cette dernière d'une rançon. Une analyse transversale du marché pourrait laisser penser que cette technique est sur le déclin, les particuliers comme les entreprises étant aujourd'hui mieux informés du danger qu'elle présente (surtout depuis les attaques Wannacry et Petya en 2017), mais ce type de sinistre a néanmoins donné lieu à de très nombreuses déclarations en 2018.

L'essor du cryptojacking
L'usage de ces tactiques tend à montrer que, même si la cybercriminalité est encore très portée sur le vol et l'utilisation d'informations confidentielles à des fins de gain financier, elle se développe de plus en plus sur la base d'autres méthodes, assez simples, pour atteindre ses objectifs.

Le cryptojacking, par exemple – utiliser frauduleusement la puissance de calcul des systèmes informatiques d'une entreprise pour miner des cryptomonnaies –, est une tendance émergente dont nous explorons l'impact ci-dessous, au travers d'exemples qui offrent un aperçu assez large de la variété des sinistres que nous avons eu à traiter au cours de l'année écoulée, touchant des entreprises de toutes tailles, dans toutes les industries et les zones géographiques. L'enseignement que nous en retirons est qu'aujourd'hui encore, aucune entreprise n'est à l'abri des cybermenaces, qui sont toujours en constante augmentation.

Par ailleurs, nous constatons une évolution des méthodes employées par les cybercriminels, qui associent désormais à l'assaut du périmètre relativement bien protégé des réseaux d'entreprise des attaques visant leur ventre mou sécuritaire : le personnel. L'erreur humaine émerge dès lors comme un risque majeur, comme le montrent les exemples d'attaques par phishing, mais également l'infection "à la volée" ("drive-by") sur certains sites web, la transmission non sécurisée d'informations confidentielles, ou encore la perte d'appareils non verrouillés. Les entreprises doivent donc s'assurer que leurs employés comprennent et sont capables de gérer ces risques et, à ce titre, leur formation s'avère capitale.

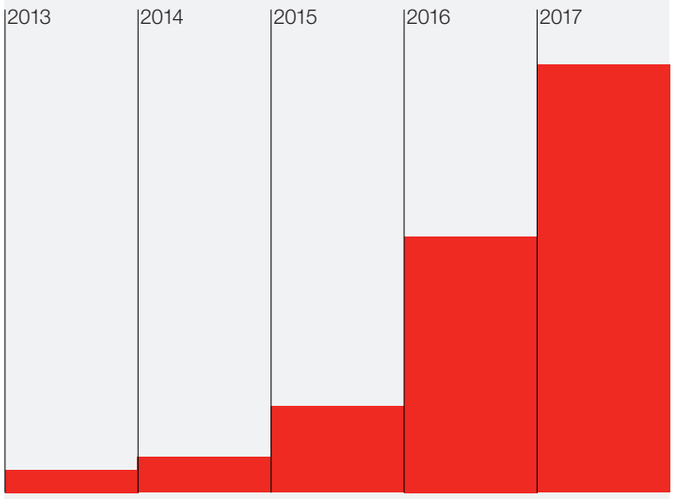
Réponse à la menace
Dans chacun des exemples détaillés ici, notre offre de cyber-assurance, loin de s'en tenir à son seul rôle d'indemnisation, a également joué un rôle crucial dans la réponse aux attaques. Les entreprises touchées ont pu rapidement avoir accès à de nombreux experts (informatiques, juridiques, communication de crise, etc.) capables de les aiguiller pendant la durée de l'incident. Notre objectif, outre la couverture des conséquences financières de l'incident, est de remettre nos assurés sur pied le plus rapidement possible.

Dans un marché de la cyber-assurance dont on estime qu'il pèsera 36 milliards de dollars en 2027 (contre 3,2 milliards aujourd'hui), ce rapport Hiscox sur les sinistres cyber – le premier d'un longue série de rapports et documents que nous produirons sur le sujet – a pour objectif de favoriser, chez nos clients, une meilleure appréhension des cyber-risques actuels et émergents, d'aider à les limiter au sein des entreprises, et enfin d'illustrer comment l'assurance peut participer d'une stratégie efficace de gestion de ces risques.

Gareth Wharton
Cyber CEO
Hiscox

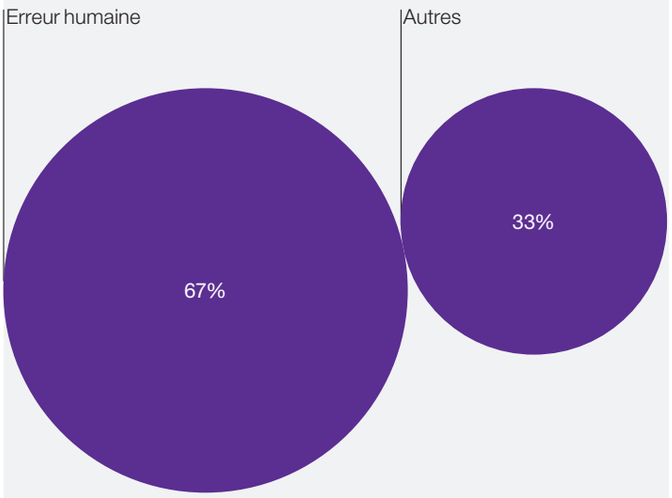
Sinistres liés à la cybercriminalité en volume
Plus de 1.000 sinistres déclarés en 2017

Hausse du nombre de sinistres
Tous territoires confondus



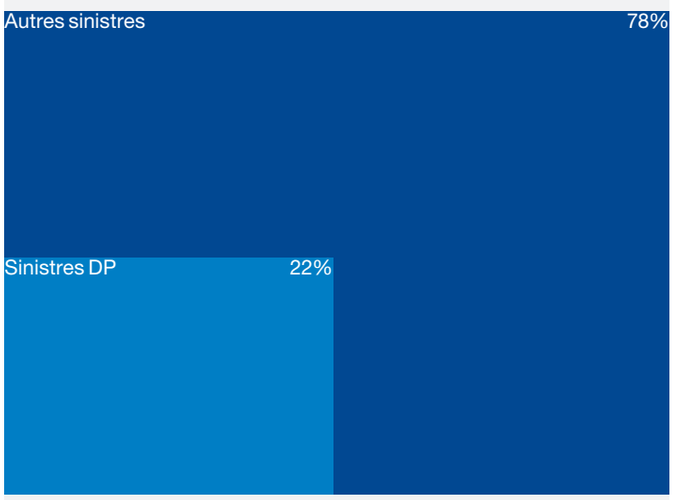
Depuis 2013, le nombre de déclarations de sinistres couverts par nos polices de cyber-assurance a augmenté de plus de 1.700%, ce qui démontre clairement que les entreprises, quelle que soient leur taille ou leur situation géographique, sont confrontées à un risque cyber bien plus intense qu'il ne l'était il y a cinq ans. Cette croissance se traduit notamment par un potentiel de pertes financières et d'atteintes à la réputation nettement aggravé.

Hiscox – sinistres 2017
Royaume-Uni



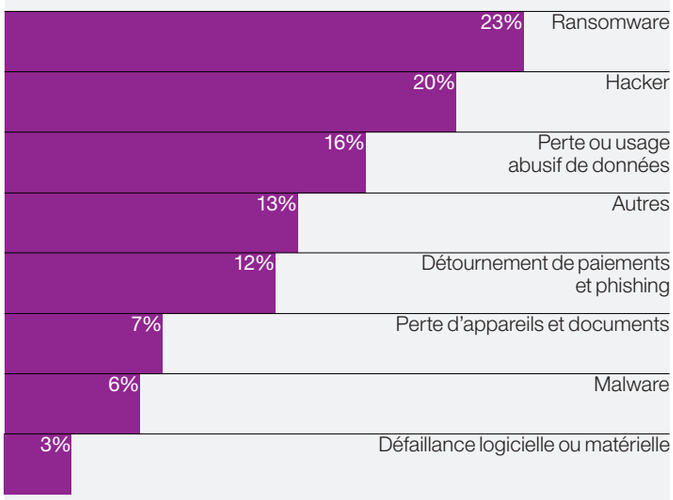
Plus des deux tiers (67%) des sinistres déclarés sont partiellement ou totalement attribuables à l'erreur d'un employé. Les erreurs les plus courantes consistent à cliquer sur un email malveillant, à visiter des sites frauduleux ou en la perte d'appareils connectés. Il est donc vital pour les entreprises d'investir non seulement dans la technologie, mais aussi dans les processus de sensibilisation aux risques, de sorte que les employés puissent former une première ligne de défense efficace.

Sinistres 2017 – Données personnelles (DP)
Royaume-Uni



Près d'un quart des sinistres déclarés au Royaume-Uni en 2017 (22%) relevaient d'un vol, perte ou utilisation abusive de données personnelles. Étant donné le renforcement récent de la réglementation européenne dans ce domaine, les incidents de ce type vont certainement devenir plus coûteux, à la fois financièrement et en matière de réputation.

2017 – Causes de sinistres
Tous territoires confondus



Même si le ransomware reste la cause de sinistre la plus fréquente en 2017, le graphique ci-dessus illustre la diversité des attaques contre lesquelles les entreprises doivent se prémunir. Certaines de ces menaces sont externes, d'autres sont internes, d'autres encore sont accidentelles. Prises ensemble, elles démontrent qu'une bonne stratégie de cyberdéfense résulte d'un effort combiné en matière de formation, de process et de technologies.

Sinistres cyber au sein des PME
Le ransomware poursuit son essor

Tout comme en 2016, le ransomware est encore la première cause des sinistres cyber déclarés en 2017, notamment du fait de la faible protection à l'entrée des systèmes informatiques pour les pirates, de la facilité de déploiement des logiciels malveillants, et du très bon retour sur investissement qu'il présente. Les attaques par ransomware passent généralement par une erreur humaine, les employés étant toujours vulnérables au phishing et aux techniques d'ingénierie sociale. Ci-dessous, quatre exemples anonymisés de sinistres que nous avons traités au cours des 12 derniers mois : dans trois d'entre eux, l'erreur humaine a été un facteur décisif.

Un cas de ransomware peu ordinaire

Secteur	Technologies
Chiffre d'affaires	€10m – €50m
Coût du sinistre	€420,000

Contexte

Notre assuré a pris conscience que ses sytèmes informatiques étaient compromis lorsqu'il s'est aperçu que certains de ses fichiers avait fait l'objet d'un chiffrement, et qu'une demande de rançon lui est parvenue. Le hacker avait réussi à obtenir l'identité de l'administrateur réseau de l'entreprise, puis avait utilisé une attaque en force brute pour trouver son mot de passe.

En utilisant les identifiants de l'administrateur pour accéder à distance aux systèmes de l'entreprise, l'attaquant a pu collecter d'autres jeux d'identifiants qui lui ont permis un accès encore plus étendu. Des données personnelles et commerciales sensibles (contrats, coordonnées bancaires, etc.) ont été compromises.

Notre réponse

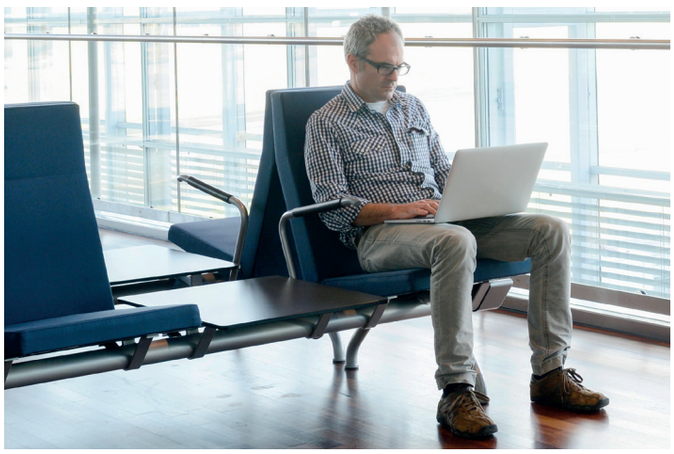
L'entreprise nous ayant contacté, nous avons immédiatement dépêché un expert et un avocat pour aider l'entreprise à gérer les conséquences de la violations de données, et pour enquêter sur la gravité de l'incident, re-sécuriser le réseau de l'entreprise et informer celle-ci de ses obligations réglementaires de notification.

Nous avons également engagé une agence de relations publiques pour conseiller l'entreprise dans ses communications avec la presse et avec ses clients. Le régulateur local, les personnes dont les données personnelles ont été compromises et les clients de l'entreprise ont tous été prévenus de l'incident. Cette réaction rapide et décisive a convaincu le régulateur de ne pas prononcer de sanction.

Enseignements

Le pirate a essayé un grand nombre de combinaisons avant de trouver le mot de passe (les tentatives se comptent généralement en milliers). Pour se protéger de ce type d'attaques, une gestion sérieuse des accès aux comptes est indispensable, par exemple, en désactivant les comptes après un certain nombre d'échecs d'identification.

L'ANSSI offre de bons conseils en la matière, et recommande notamment aux entreprises d'installer les patchs de sécurité mis à disposition par Microsoft, de sauvegarder régulièrement ses données critiques, dans l'idéal quotidiennement et à l'extérieur de son système d'information, ou encore de prendre l'habitude de mettre systématiquement à jour les logiciels utilisés, que ce soit dans un cadre professionnel ou à titre privé.



Une note salée pour le restaurant

Secteur	Services de restauration
Chiffre d'affaires	€1m – €10m
Coût du sinistre	€20,000

Contexte
Une attaque par ransomware a chiffré l'intégralité du système informatique d'un restaurant, affectant jusqu'à ses caisses physiques et rendant toute transaction électronique impossible.

Notre réponse
Ayant épuisé toutes les autres options, il est apparu que le moyen le plus efficace pour rétablir les systèmes de l'établissement était de payer la rançon.

Nous avons donc pris en charge le coût de la rançon, ainsi que les coûts informatiques liés à la mise en œuvre du déchiffrement et à la restauration complète des fonctionnalités du système. Nous avons également dépêché un expert pour détecter d'éventuelles violations de données personnelles. En plus de ces coûts, nous avons compensé la perte d'activité subie par le restaurant du fait de son incapacité temporaire à traiter les transactions.

Enseignements
En aidant le personnel à reconnaître le style des potentiels emails de phishing, ou à savoir identifier dans les informations sur l'expéditeur d'un email des éléments qui le rendent suspect, les entreprises peuvent réduire de manière significative les risques d'attaque par phishing.

Il est également important de mettre en place un protocole sérieux de sauvegarde des données. Celles-ci doivent faire l'objet de tests réguliers et être stockées sur un système qui n'est pas connecté au réseau principal (par, exemple, un disque dur externe).

Vengeance par DDoS

Secteur	Services financiers
Chiffre d'affaires	€10m – €50m
Coût du sinistre	€150,000

Contexte
Une enquête de police a révélé que les attaques avaient été menées par un employé mécontent. Nous avons couvert les sommes payées par l'assuré à son sous-traitant informatique pour la restauration des systèmes. L'entreprise a également subi une interruption très préjudiciable de ses activités commerciales en raison de cette attaque.

Notre réponse
Les organisations qui dépendent de la capacité de leurs clients à accéder à des services en ligne devraient envisager l'achat d'un service de prévention des attaques DdoS. Ceux-ci filtrent le trafic et écartent les requêtes indésirables et ne transmettent au site protégé que les requêtes réputées légitimes.

Enseignements
Les organisations qui dépendent de la capacité de leurs clients à accéder à des services en ligne devraient envisager l'achat d'un service de prévention des attaques DdoS. Ceux-ci filtrent le trafic et écartent les requêtes indésirables et ne transmettent au site protégé que les requêtes réputées légitimes.

Et l'avenir ? Le cryptojacking
Plus lucratif et moins d'efforts pour les criminels

Les pirates commencent à se détourner des attaques par ransomware, invasives et très visibles, pour se consacrer sur une activité bien plus discrète : le cryptojacking. Selon Symantec, les cas de cryptojacking ont connu une hausse de 8.5% sur le dernier trimestre 2017. Une fois qu'un hacker a réussi à s'introduire dans un système informatique, plutôt que d'y charger un ransomware pour chiffrer les fichiers de la victime, l'attaque de cryptojacking va installer un logiciel de "minage". Ce dernier va tourner en arrière-plan en mobilisant la puissance de calcul non utilisée par l'ordinateur de la victime (ou les serveurs de son lieu de travail) pour miner discrètement des cryptomonnaies pour le compte du hacker. Il est probable qu'un hacker averti préfère ce mode opératoire pour passer inaperçu et accumuler des revenus supérieurs sur le long terme.

Une victime dans le secteur informatique

Secteur	Technologies
Chiffre d'affaires	€50m+
Coût du sinistre	€80,000

Contexte
Une société informatique se rend compte qu'un malware a été installé sur l'un de ses serveurs.

Notre réponse
Nous avons demandé à un expert IT d'enquêter sur les fonctions du malware et sur les circonstances de son apparition dans les systèmes de notre assuré. Nous avons examiné la possibilité d'une atteinte plus large, risquant entre autre l'intégrité des données personnelles.

Étant donné la gravité potentielle de l'intrusion, nous avons échangé un spécialiste de la protection des données de piloter l'enquête qui a confirmé que le malware était un programme de minage mais, heureusement, rien de grave : aucune fuite de données n'a été détectée.

Les publicitaires et le Bitcoin

Secteur	Marketing
Chiffre d'affaires	€0 – €1m
Coût du sinistre	€50,000

Contexte
Une société de relations publiques a remarqué un problème affectant ses courriers électroniques. Son sous-traitant informatique habituel a mené une enquête et déterminé que la cause la plus probable en était une activité malveillante. L'assuré nous a alors contacté et nous avons dépêché sur site une un expert IT, qui a confirmé que l'assuré était victime d'une attaque.

Les systèmes informatiques de la société étaient infectés par un programme de cryptojacking destiné au minage de cryptomonnaie. L'enquête a pu déterminer que les hackers qui avaient déployé ce malware étaient accédés aux systèmes de l'assuré et avaient potentiellement menacé l'intégrité de données personnelles.

Notre réponse
Après avoir enquêté pour déterminer la gravité de l'intrusion, l'équipe informatique a désinstallé le logiciel malveillant et remédié aux failles de sécurité Nous avons engagé un avocat pour informer notre client de ses obligations de notification et l'assister dans la notification du régulateur et des personnes concernées.

Enseignement
En plus des bonnes pratiques sur la bonne gestion des mots de passe et la mise à jour régulière des logiciels pour s'assurer qu'ils soient dûment "patchés" – les entreprises ont intérêt à installer des logiciels de surveillance des statistiques clés des serveurs (taux d'utilisation du processeur, de la mémoire, du réseau et du disque). Sur la durée, le logiciel de contrôle va établir un "état normal" du système, à partir duquel on peut déterminer des seuils d'alerte. Outre le fait qu'un tel logiciel peut s'avérer utile pour signaler les pannes de serveurs, il permet également d'avertir l'administrateur si un volume inhabituel de trafic est détecté, laissant ainsi soupçonner que des données sont en train d'être transmises à l'extérieur. Si le taux d'utilisation du processeur reste plus élevé qu'attendu sur une longue période, cela peut également indiquer qu'un programme malveillant de cryptojacking est à l'œuvre au sein du système.

Glossaire technique

Advanced persistent threat (APT). Attaque ciblée, c'est-à-dire dirigée contre une structure en particulier, basée sur des mécanismes plus complexes que les attaques à grandes échelles type spamming (failles 0-day, vulnérabilités spécifiques du système d'information, etc.). Elle est qualifiée de persistante car elle va en général perdurer jusqu'à ce que son objectif soit atteint. En général, ces attaques sont précédées d'une longue période de préparation, à la fois technique et relevant de l'ingénierie sociale.

Air gap. (Litt. "vide d'air") La séparation ou l'isolation physique entre un système donné et des systèmes ou réseaux tiers.

Anti-malware/anti-virus. Logiciel utilisant un analyseur qui permet d'identifier virus et autres programmes potentiellement malveillants sur une machine

Attaque par force brute. Cyber-attaque « par tâtonnement », qui vise à décoder des données cryptées en essayant toutes les combinaisons possibles ou à forcer l'accès à un système d'information jusqu' à trouver une faille qui permet d'entrer. Cette méthode prend beaucoup de temps et peut être rendue beaucoup moins efficaces par des mesures de sécurité assez basiques.

Authentification. Processus de vérification de l'identité (ou d'autres attributs) d'un individu. Peut être simple ou multi-facteurs, c'est-à-dire faire appel à plusieurs méthodes simultanément (login et mot de passe pour se connecter + code envoyé par sms, par exemple, ou mot de passe + empreinte rétinienne).

Backdoor (trojan) ou "Porte dérobée". Programme malveillant conçu pour être introduit dans un système informatique et, une fois dedans, s'exécuter pour y voler ensuite des données ou endommager l'ordinateur.

Blacklist. Liste des entités, adresses IP, etc. dont l'accès est bloqué, ou à qui certains accès ou privilèges sont refusés.

Botnet. Série d'ordinateurs compromis par un malware et contrôlés par le biais d'un réseau. Utilisé notamment dans les attaques DDoS (déni de service).

Bug. Erreur, défaut, lacune ou imperfection imprévue et relativement mineure au sein d'un système, d'un logiciel ou d'un appareil.

Chiffrement. Processus par lequel une information ou donnée est convertie en un code, de sorte qu'elle soit illisible par toute personne ou appareil ne disposant pas d'une clé chiffrée idoine.

Conseil des normes de sécurité de l'industrie des cartes de paiement (PCI-SSC). Organe dirigeant du PCI. Le Conseil des normes de sécurité PCI (PCI SSC) a été formé en septembre 2006 par American Express, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide et Visa International. Le site du Conseil des normes de sécurité PCI répertorie environ 700 membres / adhérents.

Contrôle d'accès. Processus au terme duquel sont acceptées ou rejetées les requêtes spécifiques, les tentatives d'obtenir et d'utiliser certaines données et services associés de traitement de l'information, mais aussi les demandes d'accès à des installations physiques.

Cookie. Fichier stocké sur un ordinateur qui permet aux sites web de se souvenir d'un utilisateur.

Cryptographie. Méthodes consistant à protéger des informations en les convertissant dans un format illisible pour tout individu ne disposant pas de la clé de décryptage. Il existe différentes formes de chiffrement, le format le plus largement répandu étant le PGP (Pretty Good Privacy).

Cryptojacking. Utilisation non autorisée d'un ordinateur-cible pour le minage de cryptomonnaie.

Data loss prevention (DLP). Ensemble de procédures et d'outils logiciels visant à assurer que des données sensibles ne puissent pas sortir d'un réseau prédefini.

Distributed denial-of-service attack (DDoS). Attaque visant à empêcher l'accès d'utilisateurs légitimes à un ordinateur ou à un site internet ciblé en submergeant ce dernier de requêtes et/ou d'instructions ; elles sont le plus souvent menées au moyen d'un botnet.

Domain name system (DNS) ("Système de noms de domaine"). L'annuaire du web. Permet aux ordinateurs de traduire les noms de domaine, par exemple hiscox.com, en adresses IP, et donc d'établir une connection entre ordinateurs distants.

DNS hijacking, ou "manipulation de l'espace des noms de domaine". Attaque qui modifie les réglages d'un ordinateur pour qu'il ignore le DNS, ou bien se connecte à un serveur DNS contrôlé par des pirates malveillants. Les attaquants peuvent alors rediriger ses communications vers un site frauduleux.

Drive-by download. Infection d'un ordinateur par un malware lorsqu'un utilisateur visite un site malveillant,même en l'absence d'action particulière de l'utilisateur pour initier le téléchargement.

Exploit. Élément de programme permettant d'exploiter une faille de sécurité (généralement un défaut de programmation d'un logiciel) afin d'infecter ou d'accéder à la mémoire d'un ordinateur.

Faille 0-Day. Exploit qui tire parti d'une faille de sécurité le jour même où la vulnérabilité est connue du public. Ces exploits sont en principe bloqués ultérieurement par des patchs de sécurité/ des mises à jour fournies par l'éditeur du logiciel.

Firewall, ou pare-feu. Barrière logicielle entre divers réseaux, ou parties d'un réseau, visant à bloquer le traffic malveillant, ou à prévenir les tentatives de piratage. Le pare-feu inspecte l'ensemble du traffic à la fois entrant et sortant et vérifie qu'il répond à certains critères. Dans le cas contraire, le pare-feu bloque l'accès.

Hacktivisme. Désigne les activités de piratage menées à des fins politiques, éthiques, ou sociétales (les attaques d'Anonymous en sont un bon exemple).

Hameçonnage / phishing. Technique par laquelle des cyber-pirates se font passer pour des interlocuteurs de confiance (grandes sociétés, organismes financiers) familiers de leurs cibles, et leur demandent par email des informations confidentielles (type mots de passe, numéros de comptes bancaires, etc) ou des transferts de fonds, ou encore les incitent à se connecter sur une page web corrompue. C'est une méthode qui relève de l'ingénierie sociale (exploitation d'une faille humaine plutôt que technique). de la banque choisie, par exemple), certains iront quand même jusqu'à lire le mail et ouvrir la pièce jointe / cliquer sur le lien. Se rattachent aussi au hameçonnage le spear-phishing,

ou harponnage (se concentrer sur un seul utilisateur ou service) ou le whale-phishing / hameçonnage ciblé (se concentrer sur des personnes à haut revenu).

Hashing (ou hachage). Processus utilisant un algorithme de chiffrement irréversible pour convertir une information en une valeur alphanumérique aléatoire. Typiquement utilisé pour protéger l'intégrité des mots de passe au cas où un acteur malveillant parviendrait à accéder à la base de données où ceux-ci sont stockés. Souvent associé à un "salage" des données (v. infra).

Ingénierie sociale. Techniques de manipulation psychologique utilisées par un attaquant pour pousser sa victime à certaines actions, souvent par le biais d'un phishing, mais aussi au moyen d'appels téléphoniques, de faux comptes LinkedIn, etc. Les actions visées sont généralement la connexion à un site malveillant, ou l'exécution non-désirée d'un fichier joint.

Injection SQL. Le SQL est un langage informatique normalisé servant à l'exploitation des bases de données. Une injection SQL consiste en une manipulation de ce langage instruisant à la base de données visée d'effectuer des tâches différentes de sa fonction attendue.

ISO27001. Norme internationale établissant les bonnes pratiques en terme de gestion de la sécurité de l'information.

Keylogger. Type de logiciel malveillant capable d'enregistrer furtivement les frappes de clavier d'un utilisateur et de les communiquer à un tiers.

Malware. Abréviation de « malicious software », terme commun désignant l'ensemble des logiciels malveillants, dont les virus, vers informatiques, trojans et logiciels espions. Dans le langage courant, les termes malware et virus sont souvent utilisés de manière interchangeable.

Menace interne. Personne ou groupe de personnes au sein d'une entreprise qui présente potentiellement, soit par négligence, soit par malveillance, un risque de violation des politiques de sécurité. Network access control (NAC). Un contrôleur d'accès au réseau est une méthode permettant de réserver l'accès d'un réseau aux appareils qui se conforment à une politique de sécurité prédéfinie.

NIST cyber security framework. (États-Unis) Cadre général de normes, bonnes pratiques et recommandations destiné à promouvoir la sécurité informatique. Visant à la neutralité industrielle, géographique et normative, il s'intéresse moins aux mesures à prendre qu'aux résultats attendus.

Norme PCI-DSS (norme de sécurité de l'industrie des cartes de paiement). Un standard de sécurité des données, établi à l'initiative du PCI, qui gouverne la manière dont les entreprises qui perçoivent des paiements par carte de crédit ou débit doivent traiter et protéger les données concernées. On distingue quatre niveaux de gouvernance selon le volume de transactions traitées, du niveau quatre pour les plus modestes, au niveau un pour les plus importants. Les limites précises de ces niveaux sont décidées par chaque marque individuellement. Informations supplémentaires disponibles ici : www.pcisecuritystandards.org.

Patch, ou correctif. Extension logicielle et/ou du firmware destinée à corriger les bogues et vulnérabilités.

Phreaking. Utilisation d'un ordinateur ou autre appareil pour tromper un système téléphonique. Le phreaking est souvent utilisé pour passer des appels gratuitement, ou bien les faire facturer au compte d'un tiers.

Plan de réponse aux incidents (IRP). Ensemble prédéterminé et documenté de procédures visant à détecter et à réagir aux incidents de cybersécurité.

Point d'extrémité. Un appareil connecté à internet. Le terme peut désigner des ordinateurs de bureau, portables, smartphones, tablettes, clients légers, imprimantes, etc.

Protocole RDP (Remote Desktop Protocol). Protocole qui permet à un utilisateur de se connecter à un système informatique par le biais d'internet.

Qualified security assessor (QSA). Fournisseur de services d'évaluation certifié PCI-DSS pour l'audit de conformité des marchands partenaires.

Questionnaire d'auto-évaluation (SAQ). Formulaire d'auto-évaluation utilisé par les plus petits commerçants pour vérifier leur conformité avec la norme PCI DSS.

Ramscraping. Technique utilisée par certains malwares afin d'extraire les informations carte de paiement de la mémoire d'une machine avant qu'elles ne soient cryptées.

Ransomware. Logiciel malveillant qui chiffre ou bloque l'accès à des données et/ou systèmes et soumet la remise de la clé de chiffrement utilisée au paiement d'une rançon.

Rapport de conformité (RoC). Délivré par un QSA lorsque les systèmes informatiques d'un commerçant sont en conformité avec la norme PCI-DSS.

Red team exercise. Exercice mené en conditions réelles consistant à simuler une attaque de hacker, ou une tentative d'exploiter une vulnérabilité d'un réseau d'entreprise.

Redondances. Systèmes supplémentaires ou alternatifs, sous-systèmes, ressources ou processus permettant de garantir un certain degré de fonctionnalité en cas de défaillance d'un autre système, sous-système, ressource ou processus.

Résilience. Capacité d'un réseau à maintenir ses fonctions opérationnelles (résistance aux perturbations et capacité à opérer des fonctions de base même en cas d'atteinte grave), à se rétablir efficacement en cas de défaillance avérée et à adapter rapidement sa capacité pour répondre à des requêtes imprévisibles ou à leur soudaine multiplication (comme dans les attaques DDoS).

Rootkit. Un élément logiciel qui permet de dissimuler des programmes ou processus en cours d'exécution sur un ordinateur.

Salage. L'ajout d'une suite aléatoire de caractères à un mot de passe avant hashing afin de rendre son décryptage plus difficile.

Secure file transfer protocol (SFTP). Protocole pour la transmission de fichiers chiffrés par internet.

Secure sockets layer (SSL). Protocole obsolète (remplacé par le TLS) pour la transmission de données privées reposant sur des systèmes cryptographiques utilisant deux clés symétriques pour le chiffrement des données. Les navigateurs web indiquent qu'une connexion est protégée par protocole SSL en affichant un cadenas ou un certificat de sécurité près du champ URL.

Security information and event management (SIEM). Une solution de sécurité qui améliore la visibilité de la cybersécurité au sein des entreprises en procédant à l'aggrégation et à la corrélation des alertes et logs générés par de multiples sources et logiciels de sécurité (IPS, IDS, AV, etc).

Serveur de commande et contrôle. Ordinateur qui émet des instructions aux appareils formant un botnet.

Spoofing. Falsification de l'adresse expéditeur d'un courrier électronique à des fins de phishing ou d'ingénierie sociale.

Spyware. Logiciel qui collecte les informations d'un système d'information ou d'une interface web à l'insu de l'utilisateur, souvent à des fins publicitaires ou d'espionnage industriel.

Surface d'attaque. L'ensemble des ressources matérielles et logicielles connectées à internet au sein d'une organisation. Plus ces ressources sont nombreuses, plus il existe de vulnerabilités potentielles pouvant être utilisées par un adversaire pour attaquer l'organisation.

Système de détection des intrusions (IDS). Appareil ou application logicielle destinée à la surveillance de réseaux ou systèmes et permettant de détecter les activités malveillantes ou les violations de politiques d'utilisation en signalant toute activité inhabituelle aux administrateurs.

Système de prévention des intrusions (IPS). Version proactive de l'IDS pouvant automatiquement procéder au blocage d'utilisateurs ayant des comportements suspects.

Test d'intrusion ou de pénétration. Processus d'évaluation qui consiste à rechercher des vunérabilités et à tenter de contourner les éléments de sécurité d'un réseau ou d'un système informatique.

Threat actor (cyber délinquant). Individu, groupe, organisation, ou gouvernementqui perpètre ou a l'intention de perpétrer des actions préjudiciables (autrement dit, un hacker).

Threat vector (vecteur de menace). Méthode utilisée par un cyber délinquant pour accéder à un réseau.

Transport layer security (TLS). Successeur du SSL, il s'agit également d'un protocole de sécurisation des échanges sur internet utilisant des clés symétriques pour le chiffrement des données. De nombreux navigateurs internet indiquent qu'une connexion est sécurisée par TLS en affichant un cadenas ou un certificat de sécurité à côté du champ d'adresse. On parle encore souvent de protocole SSL en langage courant.

Trojan, ou cheval de Troie. Programme malveillant conçu pour imiter l'apparence d'un logiciel légitime, mais qui exécute en réalité des fonctions nuisibles et cachées.

Ver informatique. Forme de malware qui peut se dupliquer et se propager sans qu'une interaction humaine ou système soit nécessaire. Un malware en pilote automatique, en quelque sorte.

Virtual private network (VPN). Système permettant de connecter des ordinateurs distants à un réseau central, qui offre aux utilisateurs la possibilité de communiquer entre eux ou d'accéder aux serveurs de l'organisation par le biais d'internet, et de manière sécurisée.

Virus. Programmes malveillants capables de se propager à d'autres fichiers.

Vulnérabilité. Bug logiciel exploité par un hacker pour pirater un ordinateur.

Whitelist. Une liste d'entités, adresses IP, applications, etc. réputées de confiance pour qui l'accès et/ou certains privilèges sont garantis.

Zombie (aussi appelé bot). Un ordinateur infecté qui est contrôlé à distance par un hacker. Il fait généralement partie d'un botnet.

Hiscox

19 rue Louis Legrand
75002 Paris

hiscox.fr

19264 8/18