Pourquoi les victime de phishing, se feront encore piéger ?

	Pourquoi les victime de phishing, se feront encore piéger ?

Des chercheurs américains ont établi que les internautes se font avoir par des faux e-mails parce qu'ils ont tendance à surestimer leurs capacités à les identifier comme tels.

Un e-mail de type phishing prétendant provenir de la Société générale et incitant le destinataire à cliquer sur un lien en lui promettant un paiement.

Le phishing est peut-être une vieille arnaque par e-mail, mais elle marche encore très bien. Pas seulement parce que ces faux e-mails officiels sont de mieux en mieux faits mais aussi parce que les internautes se croient beaucoup plus forts qu'ils ne le sont en réalité pour les détecter… Trois chercheurs américains sont arrivés à cette conclusion après avoir mené une expérience assez pointue auprès de 600 personnes. Le compte rendu a été publié dans Journal of the Association for Information Systems. Et le bilan est sans appel : les internautes se surestiment largement.

L'idée était en effet de voir comment les internautes jugeaient leurs propres compétences à repérer des e-mails frauduleux, plutôt que de voir s'ils étaient capables de déjouer cette arnaque. Pour rappel, les courriers de phishing se présentent comme des courriers officiels de banque, d'assurance, de site d'e-commerce, d'opérateurs de télécommunication, parfois des impôts, avec texte à tonalité toute administrative, mentions légales et logo officiel pour les plus soignés. Ils demandent généralement au destinataire de cliquer sur un fichier attaché (en réalité un virus) ou de mettre à jour ses informations en cliquant sur un lien renvoyant vers un formulaire. L'internaute n'aura plus qu'à remplir. Le plus souvent, il est question de saisir des identifiants et des données bancaires… La force de cette arnaque réside dans le fait que c'est la victime qui a donné elle-même les informations. Il suffit pour cela que le mail soit bien fait, bien rédigé, l'adresse de l'expéditeur assez trompeuse.

Une étude en forme de sondage

Les trois chercheurs américains, issus de l'université du Texas (à Arlington et San Antonio) et de l'université Columbia, ont demandé à six cents participants de se soumettre à un sondage concernant l'examen de seize e-mails (présentés sous forme de fichier image). Tous étaient d'authentiques messages réellement envoyés, mais la moitié était du phishing, l'autre moitié de vrais e-mails d'entreprises.

De chaque message, les personnes ont dû dire si elles pensaient qu'il émanait réellement de l'entreprise censée l'avoir envoyé ou s'il était faux. Elles devaient aussi noter leur propre jugement sur une échelle de 50 à 100 : 50, si elles avaient répondu au hasard sur la fiabilité de l'e-mail, 100 si elles étaient parfaitement sûres de leur coup. Les chercheurs ont également demandé aux répondants à quel point ils étaient familiers (de « pas du tout » à « très ») de l'entreprise expéditrice et, à la fin, les participants étaient tenus d'estimer le pourcentage de bonnes réponses qu'ils pensaient avoir fournies.

Les enquêteurs ont également noté le temps mis par chaque participant à répondre à la première question (l'e-mail est-il légitime ou non), et ce pour les seize e-mails. Le tout était agrémenté de questions plus génériques sur la capacité des répondants à distinguer, dans l'absolu, des e-mails légitime d'emails de phishing, sur leurs activités en ligne, leur expérience, en tant que victime, du phishing.

Avoir été victime d'e-mails de phishing n'aide pas plus à les repérer

« *Nous avons comparé chaque jugement des répondants sur la confiance qu'ils avaient dans leurs propres réponses à la justesse effective de la réponse,* explique Jingguo Wang, de l'université du Texas à Arlington. *Nous avons découvert que 80% des participants avaient une confiance moyenne plus élevée que le taux de justesse de leurs réponses.* » Et quand il s'est agi pour les participants d'estimer combien de bonnes réponses ils avaient donné quant à la légitimité ou non des e-mails, les chercheurs se sont aperçus que 45% s'étaient surestimés.

L'enseignement de cette étude ? « *La confiance qu'ont les internautes dans leur propre jugement et dans leur efficacité à détecter du phishing n'est qu'un faible indicateur de ce qu'il en est vraiment, on ne peut pas se fier à cette confiance* » continue Jingguo Wang. Pire: même le fait que des participants aient eux-mêmes été victimes de phishing ne les aide pas à mieux reconnaître ce type d'e-mail. Le meilleur moyen d'apprendre à les détecter reste donc des séances de formation en bonne et due forme, à la fois sur la forme des messages eux-mêmes et sur la surconfiance des internautes, sur les raisons qu'ils ont de s'estimer si habiles à déceler ce genre de mails alors qu'ils ne sont pas tant que ça.

Original de l'article mis en page : Pour détecter du phishing, l'internaute moins fort qu'il ne le croit – Sciencesetavenir.fr

---

Réagissez à cet article

Original de l'article mis en page : Pour détecter du phishing, l'internaute moins fort qu'il ne le croit – Sciencesetavenir.fr

---

Comment se protéger d'une nouvelle arnaque au phishing sur Gmail ?

Comment se protéger d'une nouvelle arnaque au phishing sur Gmail ?

Une arnaque au phishing particulièrement élaborée vise les utilisateurs de la messagerie de Google.

Crédit : Greggman

Ce mail semble contenir une pièce jointe

Une arnaque au phishing au mode opératoire à la sophistication inédite sévit depuis plusieurs semaines sur la messagerie Gmail. L'attaque, qui vise à dérober des informations personnelles afin de les réutiliser à l'insu de l'utilisateur, prend la forme d'un mail envoyé par un contact contaminé. **Il continent une pièce-jointe et un message lapidaire du type « voici le pdf demandé »**. Un clic sur la pièce-jointe renvoie l'utilisateur vers une page à l'apparence de Google Drive et lui demande de s'identifier pour la visualiser. Une fois l'opération effectuée, l'assaillant prend possession du compte de la victime, peut à son tour envoyer le mail de hameçonnage à tous ses contacts et se livrer à des usurpations d'identité ou à des escroqueries.

Crédit : Greggman

Cette page ressemble à la page d'accueil Gmail

Comme l'explique un blogueur américain qui s'est fait piéger par l'arnaque, la pièce-jointe est en fait une image intégrée dans le corps du mail associée à un lien renvoyant automatiquement vers une page web. L'url contient « https://accounts.google.com » et laisse à penser qu'il s'agit du véritable site de Google. Mais elle débute par data « :text/html » et contient un script aspirant l'identifiant et le mot de passe de la victime lorsqu'ils sont renseignés dans le formulaire.

Dans un communiqué, Google dit avoir pris connaissance du problème. « Nous continuons de renforcer nos moyens de défense contre cela. Nous faisons de notre mieux pour protéger nos utilisateurs de différentes manières, en détectant les messages de phishing grâce au deep learning, en adressant des alertes de sécurité lorsque plusieurs liens suspicieux arrivent dans les mails, en repérant des tentatives de connexion douteuses, etc. Les utilisateurs peuvent aussi activer la validation en deux étapes pour ajouter une protection supplémentaire à leur compte », écrit Google dans un communiqué.

Comment fonctionne le phishing

Contraction des mots « fishing » (pêche en français) et « phreaking » (terme désignant le piratage des lignes électroniques) – le phishing est **une technique dite de « hameçonnage » basée sur de faux mails** qui visent à collecter les données bancaires ou les mots de passe des clients. À partir de ces documents, les pirates peuvent ensuite se livrer à des usurpations d'identité et à des escroqueries.

Ces faux courriels se présentent souvent comme des courriers envoyés par une source sûre, comme le Trésor public ou les banques. Trompées par l'expéditeur supposé, les victimes fournissent souvent elles-mêmes leurs propres données personnelles. Une autre possibilité consiste à envoyer des SMS ou des mails malveillants en masse qui contiennent un lien permettant d'installer, sans le savoir, un logiciel pirate qui pourra récupérer les données personnelles des personnes ainsi trompées.

Surveiller les mails et leur orthographe

Il s'agit donc de surveiller les mails et leur contenu. Les courriels émanant d'une structure officielle (la banque, EDF, ou la caisse d'allocations familiales par exemple) ne demandent jamais à leurs clients de saisir leurs informations personnelles directement dans un mail mais depuis un site Internet crypté. Dans ce cas, **un petit cadenas apparaît systématiquement à gauche de l'URL** du site pour garantir la confidentialité des informations.

Par ailleurs, en cas d'information importante, une banque ou un opérateur contactent généralement leurs clients par courrier ou par téléphone. Les mails utilisés dans le cadre des tentatives d'escroqueries font souvent état de **situations alarmistes** et comportent des **fautes d'orthographes** ou de syntaxe laissant penser que le message a été rédigé par un logiciel de traduction automatique.

Vérifier les adresses électroniques et les URL des sites internet

Dans certains cas de phishing, les victimes sont redirigées vers un faux-site, qui ressemble comme deux gouttes d'eau au site officiel. Il faut alors vérifier que l'URL est bien la même que celle du site copié. En général, elle est beaucoup plus longue et compliquée et on peut remarquer que, dans le corps du mail, le texte affiché sous forme de lien ne correspond pas du tout au lien réel, dont l'adresse s'affiche lorsqu'on positionne le curseur dessus. Dans le cas de l'arnaque aux faux mails de la Cpam, on peut s'apercevoir que l'adresse de réclamation ne correspond pas à celle d'un organisme officiel puisqu'elle se termine en « gmail.com ».

Original de l'article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s'en protéger

---

Réagissez à cet article

Original de l'article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s'en protéger

La Russie crée des unités d’élite de pirates informatiques

	La Russie crée des unités d’élite de pirates informatiques

La Russie s'appuie sur les médiaux sociaux pour appeler de jeunes recrues à intégrer des « escadrons scientifiques » capables d'accéder à des systèmes et réseaux, à l'insu des cibles. Accusée par les États-Unis d'avoir influencé l'élection américaine de novembre à travers des opérations de piratage informatique, la Russie a accéléré ses recrutements de pirates bien avant ces évènements, rapporte le *New York Times* en référence à une enquête du site d'information russophone Meduza. En plus de recruter dans les écoles d'ingénieurs, Moscou diffuse depuis plusieurs années des annonces sur les médias sociaux à l'attention d'étudiants et de programmeurs professionnels. Des hackers ayant maille à partir avec la justice sont également ciblés, selon Meduza.

L'une de ces annonces a été publiée sur le réseau social russe Vkontakte. Dans le spot vidéo ci-dessous, on devine un homme diposant d'une arme et d'un ordinateur portable. On peut y lire ce message : *« si tu es diplômé de l'enseignement supérieur, si tu es un spécialiste des technologies, nous t'offrons des opportunités, des équipements techniques de pointe, des capacités de calcul puissantes, du matériel dernier cri, un véritable entraînement au combat »*. Sans oublier le logement tout confort.

Former des « escadrons scientifiques »

Dans une autre annonce citée dans l'enquête, les autorités russes sont à la recherche d'informaticiens ayant des connaissances des *« patchs, vulnérabilités et exploits »*, explique Meduza, le site d'information russophone basé à Riga (Lettonie). La recherche de talents ne s'arrête pas là. Moscou se tournerait également vers des *« hackers ayant des problèmes avec la loi ».* Le gouvernement russe leur proposant une remise de peine en échange de leur engagement au service de la Russie…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Comment la Russie crée des unités d'élite de pirates informatiques

L’association Donne-Moi un Logement victime d’un piratage informatique

L’association Donne-Moi un Logement victime d’un piratage informatique

Fin décembre, l’association limousine Dessine-moi un logement (DML) a été victime d’un pirate informatique qui s’est attaqué à sa boîte mail.
Ce dernier a pris le contrôle de la messagerie de sa coordinatrice et a récupéré les contacts de l’association.
Des messages ont été envoyés implorant de l’aide et parlant de « situation délicate » et d’« affaire confidentielle ».
Le pirate demande d’envoyer en urgence des recharges PCS Mastercard, un moyen de paiement très prisé des escrocs. Il ne faut évidemment pas répondre à ce message.
L’association DML, spécialisée dans le logement social d’urgence, déplore cette attaque au moment des fêtes de fin d’année et doit maintenant entièrement reconstituer son carnet d’adresses électroniques.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d’audits dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : L’association Donne-Moi un Logement victime d’un piratage informatique – Limoges (87000) – Le Populaire du Centre

Tendances actuelles et émergentes pour la cybersécurité en 2017

	Tendances actuelles et émergentes pour la cybersécurité en 2017

L'année 2016 a été marquée par un grand nombre de cyberattaques très diverses, allant d'attaques de type DDoS par le bais de caméra de sécurité connectées, jusqu'au supposé piratage de partis politiques durant les élections américaines. Nous avons aussi constaté une forte augmentation des fuites de données, aussi bien au niveau des petites que des grandes organisations, avec des pertes significatives de données personnelles des utilisateurs. En cette fin d'année, nous réfléchissons donc aux directions que vont prendre ces tendances en 2017.

Les tendances actuelles et émergentes :

Les attaques destructives de type DDoS utilisant les objets connectés vont augmenter.

En 2016, Mirai a montré le potentiel destructeur important que pouvaient avoir les attaques DDoS, du fait notamment du manque de sécurité des objets connectés. Les attaques de Mirai exploitaient seulement un faible nombre d'équipements et de vulnérabilités, en utilisant des techniques simples pour deviner les mots de passe. Cependant, d'autres cybercriminels n'auront aucun mal à étendre la portée de ce type d'attaque, du fait du nombre considérable d'objets connectés contenant des codes obsolètes, ainsi que des applications et systèmes d'exploitation non mis à jour contenant souvent des vulnérabilités bien connues. Il faut s'attendre à une utilisation plus systématique des exploits présents au sein des objets connectés et de techniques avancées permettant de deviner les mots de passe, pour compromettre une plus grande variété d'objets connectés, afin de mener des attaques de type DDoS ciblant d'autres équipements connectés à votre réseau.

Les attaques ciblées d'ingénierie sociale seront plus sophistiquées.

Les cybercriminels sont de plus en plus expérimentés pour exploiter la première des vulnérabilités : l'être humain. Des attaques ciblées de plus en plus sophistiquées et convaincantes cherchent à duper et à amadouer les utilisateurs, afin de les pousser à se mettre en danger eux-mêmes. Par exemple, il est courant de voir des emails s'adressant à leurs destinataires par leurs noms et qui prétendent que ces derniers ont une dette impayée, que l'expéditeur en question serait autorisé à collecter. La peur, l'intimidation et les menaces de recouvrement au nom de la loi, sont des tactiques très utilisées et assez classiques. L'email en question vous redirige alors vers un lien malveillant, sur lequel les utilisateurs cliquent dans la panique, amorçant alors l'attaque. De telles attaques par hameçonnage (phishing), ne peuvent plus être détectées à la lecture par de simples erreurs grossières commises par les cybercriminels.

Les infrastructures financières deviendront des cibles privilégiées.

Les attaques ciblées de phishing, et particulièrement celles ciblant les dirigeants (whaling), vont continuer de croitre. Ces attaques utilisent des informations détaillées concernant les dirigeants d'entreprises, afin de duper les employés et les inciter à envoyer de l'argent à des cybercriminels, ou à compromettre certains comptes bancaires. Nous nous attendons aussi à voir davantage d'attaques ciblant des infrastructures financière sensibles, telles que l'attaque ayant pris pour cible les institutions connectées au système SWIFT, qui a coûté à la banque centrale du Bangladesh 81 millions $, en février dernier. SWIFT a récemment admis que d'autres attaques de ce type avaient eu lieu, et qu'il s'attendait à en voir davantage en déclarant, dans une lettre adressée aux clients de la banque : « La menace est très persistante, adaptative et sophistiquée. Il faut s'attendre à ce qu'elle continue de sévir. ».

L'exploitation de l'infrastructure intrinsèquement non sécurisée d'Internet va se poursuivre.

Tous les internautes font encore confiance à de vieux protocoles fondateurs, que leur omniprésence empêche de réorganiser ou de remplacer. Ces protocoles archaïques qui ont pendant longtemps été les piliers de l'Internet et des réseaux professionnels sont aujourd'hui fragilisés, parfois d'une manière surprenante. Par exemple, les attaques contre BGP (Border Gateway Protocol) auraient pu, en théorie, perturber ou même mettre hors service une bonne partie du Web. Les attaques DDoS visant Dyn en octobre dernier (lancées depuis une multitude d'objets connectés) ont mis hors service un fournisseur majeur de services DNS, et ont de ce fait rendu inaccessible une partie de l'Internet. Il s'agissait de l'un des plus importants assauts jamais observés, et ceux à l'origine de ces attaques ont déclaré qu'il s'agissait seulement d'un coup d'essai. Les fournisseurs d'accès Internet et les entreprises peuvent bien évidemment prendre des mesures pour se protéger, mais pourraient trouver difficile d'éviter tous les dégâts importants potentiellement causés par des individus ou des états qui auront choisi d'exploiter les failles de sécurité les plus profondes du Web.

La sophistication des attaques va augmenter.

Le nombre d'attaques continue à augmenter, avec une sophistication croissante des techniques et de l'ingénierie sociale, qui reflète une analyse minutieuse et répétée des organisations et des réseaux de leurs victimes. Les cybercriminels peuvent compromettre de nombreux serveurs et stations de travail bien avant de commencer à voler des données ou agir de façon plus agressive. Ces attaques, en général pilotées par des experts, sont plus stratégiques que tactiques, et peuvent au final causer des dommages considérables. Il s'agit ici d'un monde très différent des attaques par malwares programmés et automatisés dont nous avons l'habitude. C'est un monde où la stratégie et la patience jouent un rôle beaucoup plus important pour échapper aux détections.

De plus nombreuses attaques utiliseront des outils d'administration intégrés.

Nous voyons davantage d'exploits basés sur PowerShell, le langage et kit de développement de Microsoft pour l'automatisation des tâches administratives. En tant que langage de script, PowerShell contourne les détections visant les exécutables. Nous voyons également plus d'attaques utilisant des tests de pénétration et d'autres outils d'administration existants, sans qu'ils soient à priori infiltrés et en général suspectés. Ces outils puissants demandent une vigilance toute particulière et des contrôle plus robustes.

Les ransomwares vont continuer à progresser.

Comme de plus en plus d'utilisateurs sont conscients de l'existence du risque d'attaques par ransomware via les emails, les cybercriminels exploitent d'autres vecteurs. Certains expérimentent des malwares qui infectent à nouveau le système ultérieurement, longtemps après que la rançon ait été payée. D'autres commencent à utiliser des outils intégrés, à la place de malwares exécutables, afin d'éviter d'être détectés par les solutions de protection Endpoint qui se focalisent sur des fichiers exécutables. De récents exemples ont proposé de déchiffrer les fichiers de leurs victimes si elles acceptaient de diffuser le ransomware vers deux autre contacts, et que ces personnes acceptent de payer. Les ransomwares commencent également à utiliser des techniques autres que le chiffrement, par exemple en détruisant ou corrompant les en-têtes de fichiers. Qui plus est, avec le grand nombre de ransomwares qui persistent sur le Web, les utilisateurs peuvent se retrouver victimes d'attaques sans espoir de pouvoir payer en dernier recours, car le système de paiement ne fonctionne plus.

Des attaques visant des objets personnels connectés vont émerger.

Les utilisateurs d'objets connectés domestiques s'imaginent rarement que leur veilleuse écoute-bébé puisse être piratée pour attaquer des sites internet. Cependant, dès qu'un pirate contrôle un équipement connecté à un réseau domestique, il peut plus facilement pirater d'autres équipements de ce réseau, tels que des ordinateurs portables contenant des données personnelles sensibles. Nous nous attendons à voir plus d'attaques de ce genre, ainsi que des attaques impliquant des caméras vidéo ou des microphones afin d'espionner les foyers. Les cybercriminels trouvent toujours un moyen de tirer profit de leurs attaques.

Le malvertising et la corruption des écosystèmes de publicités en ligne vont s'étendre.

Le malvertising, qui fonctionne en répandant des malwares sur les réseaux publicitaires et les pages web, existe déjà depuis plusieurs années. Cependant, nous avons pu observer en 2016 une recrudescence de ce phénomène. Ces attaques mettent en évidence des problèmes plus importants au sein de l'écosystème des publicités en ligne, telle que la fraude au clic, qui génère des clics payants et ne correspondent pas en réalité aux véritables centres d'intérêts de l'internaute. Le malvertising a engendré la fraude au clic, mettant les utilisateurs en danger et abusant les annonceurs par la même occasion.

La diffusion du chiffrement entrainera des problèmes collatéraux.

Le chiffrement se diffuse très largement et il est devenu plus difficile pour les solutions de sécurité d'inspecter le trafic, facilitant ainsi la vie des cybercriminels qui cherchent à s'infiltrer sans être repérés. Sans surprise, les cybercriminels utilisent le chiffrement de manière créative. Les produits de sécurité vont devoir rapidement intégrer les protections réseaux et client afin de pouvoir détecter des évènements pouvant affecter la sécurité après que le code ait été déchiffré au niveau des systèmes Endpoint.

Les cybercriminels s'intéresseront aux exploits des systèmes virtualisés dans le Cloud.

Les attaques contre des composants physiques (exemple de Rowhammer) ouvrent la voie à de nouveaux exploits potentiellement dangereux contre des systèmes cloud virtualisés. Les cybercriminels peuvent abuser d'un hôte ou bien d'un invité sur un système hôte partagé, attaquer la gestion des privilèges et potentiellement accéder aux données de tiers. De plus, comme Docker et les écosystèmes de conteneurs logiciels (« serverless ») deviennent de plus en plus populaires, les cybercriminels vont certainement se mettre à chercher des failles à exploiter dans le cadre de cette nouvelle tendance des systèmes d'information. Nous nous attendons donc à voir des tentatives actives pour rendre de telles attaques opérationnelles.

Des attaques techniques visant les Etats et les populations apparaîtront. Les attaques technologiques sont devenues hautement politiques. Les populations doivent faire face à des risques grandissants en matière de désinformation (« les fausses nouvelles ») et concernant les systèmes de vote. Par exemple, les experts ont démontré l'existence d'attaques permettant à un électeur, au niveau local, de voter de manière répétitive sans aucune détection. Même si les Etats n'organisent jamais d'attaques contre leurs adversaires aux élections, le sentiment que ce type d'attaques puisse exister est en soi une arme puissante…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 — Global Security Mag Online

---

Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

La dernière étude dIFS sur les défis auxquels les DSI sont confrontés durant la période des fêtes de fin d'années révèle que 76% des sondés se sentent davantage préoccupés à l'approche de cette période et ce, pour plusieurs raisons : la disponibilité du personnel (41% des répondants), les risques de piratage liés à la sécurité IT (31%) ainsi que les besoins IT des collaborateurs travaillant à distance (31% également). Tout cela a un impact certain sur les processus et activités métier.

De tous, les plus inquiets quant à la disponibilité du personnel à la période des fêtes de fin d'année sont les français. 62% d'entre eux déclarent qu'il s'agit de l'une de leurs plus grandes préoccupations au cours de la saison des fêtes de fin d'année. Á l'opposé, près de la moitié des répondants américains (48%) citent le piratage informatique.

Du côté des « besoins », 42% des décideurs IT sont en demande d'un budget plus important. La migration vers le Cloud (18%) et le recrutement de personnel IT (16%) sont également cités dans le top 3 de leurs besoins. Par ailleurs, un quart des répondants américains et suédois (respectivement 26% et 25%) souhaitent, à court terme, une accélération de la migration vers le Cloud, alors qu'ils ne sont que 11% et 14% en Australie et Allemagne à privilégier cet enjeu.

« Ce qui ressort clairement de notre étude est que de nombreux décideurs IT ont des craintes légitimes pour la période des fêtes de fin d'année : disponibilité du personnel, risque de piratage informatique, commente Mark Boulton, CMO d'IFS. Il est essentiel que toutes les entreprises, quelle que soit leur taille, se préparent à affronter les problèmes qui pourraient survenir et soient en mesure d'accompagner, à distance, leurs collaborateurs ». L'IoT et la migration vers le Cloud faisant partie des solutions possibles.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

En 2017, les pirates informatiques vont mettre les bouchées doubles

En 2017, les pirates informatiques vont mettre les bouchées doubles

Les hackers vont notamment chercher à ébranler la confiance que l'on porte aux données, annonce un rapport de CyberArkBy SHOSHANNA SOLOMON

Les cyber-criminels du monde entier devraient intensifier leur activité l'année prochaine en utilisant l'intelligence artificielle et la manipulation des sources d'information pour créer des attaques plus fortes et plus dévastatrices, mettent en garde les experts de CyberArk.
En infiltrant et en manipulant les sources d'information, les pirates s'efforceront de saper la confiance des gens dans l'intégrité des données qu'ils reçoivent, utiliseront l'intelligence artificielle pour mener des cyber-attaques plus sophistiquées et augmenteront la collaboration entre eux pour déclencher un plus grand désordre, selon les prévisions cybersécuritaires pour 2017.
« L'intégrité de l'information sera l'un des plus grands défis auxquels les consommateurs, les entreprises et les gouvernements du monde devront faire face en 2017, où les informations venant de sources vénérées ne seront plus dignes de confiance », ont déclaré les experts.
« Les cyber-attaques ne se concentreront pas seulement sur une entreprise spécifique, il y aura des attaques contre la société visant à éliminer la confiance elle-même ».
Les attaquants ne se contentent pas d'accéder à l'information : ils « contrôlent les moyens de changer l'information là où elle réside et la manipulent pour les aider à atteindre leurs objectifs », affirment les auteurs.
Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)
Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)
Manipuler l'information – dans une campagne électorale par exemple – peut être un outil puissant. L'altération de contenus inédits, comme les fichiers audio, pourrait conduire à une augmentation des tentatives d'extorsion, en utilisant des informations qui peuvent ne pas être réelles ou prises hors de leur contexte.
« Il sera plus facile que jamais de rassembler des informations réelles volées dans une brèche avec des informations fabriquées, pour créer un déséquilibre ce qui rendra plus difficile pour les gens de déterminer ce qui est réel et ce qui ne l'est pas ».
L'augmentation de l'utilisation mobile, du web et des médias sociaux sont parmi les facteurs clés contribuant à l'augmentation explosive des cyber-menaces, a déclaré MarketsandMarkets, une firme de recherche basée au Texas, dans un rapport. La semaine dernière, Yahoo a subi le plus grand piratage au monde connu à ce jour, dans lequel la société a découvert une violation de sécurité vielle de 3 ans qui a permis à un pirate de compromettre plus d'un milliard de comptes d'utilisateurs.
Le marché mondial de la cyber-sécurité atteindra plus de 170 milliards de dollars d'ici 2020, selon une estimation de MarketsandMarkets, avec des entreprises qui se concentrent globalement sur les solutions de sécurité mais aussi sur les services…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Les pirates informatiques vont mettre les bouchées doubles en 2017 | The Times of Israël

---

Que nous réserve la CyberSécurité en 2017 ?

Que nous réserve la CyberSécurité en 2017 ?

La fin de l'année c'est aussi et surtout la période des bilans. Dans cet article, nous mettrons en évidence les cinq tendances les plus importantes tendances à venir. Qu'elles se maintiennent ou évoluent durant l'année 2017, une chose est sûre, elles risquent de donner du fil à retordre aux professionnels de la cybersécurité.

1 : intensification de la guerre de l'information
S'il y a bien une chose que la cybersécurité nous a apprise en 2016, c'est que désormais, les fuites de données peuvent être motivées aussi bien par la recherche d'un gain financier ou l'obtention d'un avantage concurrentiel que pour simplement causer des dommages dus à la divulgation d'informations privées. À titre d'exemples, le piratage du système de messagerie électronique du Comité National Démocrate (DNC) américain qui a conduit à la démission de Debbie Wassermann Schultz de son poste de présidente ; ou encore, la sécurité des serveurs de messagerie qui a miné la campagne présidentielle américaine de la candidate Hillary Clinton dans sa dernière ligne droite. Il est également inexcusable d'oublier que Sigmundur Davíð Gunnlaugsson, le Premier ministre islandais, a été contraint de démissionner en raison du scandale des Panama Papers.
Les évènements de ce type, qui rendent publiques de grandes quantités de données dans le cadre d'une campagne de dénonciation ou pour porter publiquement atteinte à un opposant quelconque d'un gouvernement ou d'une entreprise, seront de plus en plus fréquents. Ils continueront de perturber grandement le fonctionnement de nos institutions et ceux qui détiennent actuellement le pouvoir.

2 : l'ingérence de l'État-nation
Nous avons assisté cette année à une augmentation des accusations de violations de données orchestrées par des États-nations. À l'été 2015, l'administration Obama a décidé d'user de représailles contre la Chine pour le vol d'informations personnelles relatives à plus de 20 millions d'Américains lors du piratage des bases de données de l'Office of Personnel Management. Cette année, le sénateur américain Marco Rubio (républicain, État de Floride) a mis en garde la Russie contre les conséquences inévitables d'une ingérence de sa part dans les élections présidentielles.
Il s'agit là d'une autre tendance qui se maintiendra.
Les entreprises doivent donc comprendre que si elles exercent ou sont liées de par leur activité à des secteurs dont les infrastructures sont critiques (santé, finance, énergie, industrie, etc.), elles risquent d'être prises dans les tirs croisés de ces conflits.

3 : la fraude est morte, longue vie à la fraude au crédit !
Avec l'adoption des cartes à puces – notamment EMV (Europay Mastercard Visa) – qui a tendance à se généraliser, et les portefeuilles numériques tels que l'Apple Pay ou le Google Wallet qui sont de plus en plus utilisés, les fraudes directes dans les points de vente ont chuté, et cette tendance devrait se poursuivre. En revanche, si la fraude liée à des paiements à distance sans carte ne représentait que de 9 milliards d'euros en 2014, elle devrait dépasser les 18 milliards d'ici 2018.
Selon l'article New Trends in Credit Card Fraud publié en 2015, les usurpateurs d'identité ont délaissé le clonage de fausses cartes de crédit associées à des comptes existants, pour se consacrer à la création de nouveaux comptes frauduleux par l'usurpation d'identité. Cette tendance devrait se poursuivre, et la fraude en ligne augmenter.
Le cybercrime ne disparaît jamais, il se déplace simplement vers les voies qui lui opposent le moins de résistance. Cela signifie, et que les fraudeurs s'attaqueront directement aux systèmes de paiement des sites Web.

4 : l'Internet des objets (IdO)
Cela fait maintenant deux ans que les experts prédisent l'émergence d'un ensemble de risques inhérents à l'Internet des objets. Les prédictions sur la cybersécurité de l'IdO ont déjà commencé à se réaliser en 2016. Cela est en grande partie dû à l'adoption massive des appareils connectés d'une part par les consommateurs, mais aussi par les entreprises. En effet, d'après l'enquête internationale portant sur les décideurs et l'IdO conduite par IDC, environ 31 % des entreprises ont lancé une initiative relative à l'IdO, et 43 % d'entre elles prévoient le déploiement d'appareils connectés dans les douze prochains mois. La plupart des entreprises ne considèrent pas ces initiatives comme des essais, mais bien comme faisant partie d'un déploiement stratégique à part entière.
Cette situation va considérablement empirer. L'un des principaux défis de l'IdO n'est pas lié à la sécurisation de ces appareils par les entreprises, mais plutôt au fait que les fabricants livrent des appareils intrinsèquement vulnérables : soit ils sont trop souvent livrés avec des mots de passe par défaut qui n'ont pas besoin d'être modifiés par les utilisateurs, soit la communication avec les appareils ne requiert pas une authentification de niveau suffisant ; ou encore, les mises à jour des firmwares s'exécutent sans vérification adéquate des signatures. Et la liste des défauts de ces appareils n'en finit pas de s'allonger.
Les entreprises continueront d'être touchées par des attaques directement imputables aux vulnérabilités de l'IdO, que ce soit par des attaques par déni de service distribué (attaques DDoS), ou par le biais d'intrusions sur leurs réseaux, rendues possibles par les « faiblesses » inhérentes de l'IdO.

5 : bouleversements de la réglementation…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Les grandes tendances 2017 de la cybersécurité, Le Cercle

---

Victime de Ransomware ? Payer ou ne pas payer ?

Victime de Ransomware ? Payer ou ne pas payer ?

Selon une étude d'IBM, près de 70% des entreprises victimes d'un ransomware acceptent de payer les cybercriminels pour récupérer leurs données. 50% de celles-ci ont versé plus de 10.000 dollars. Pourquoi payer ? Pour récupérer l'accès à leurs données critiques.

« On ne paie pas, ce n'est pas une solution raisonnable » jugeait en début d'année le patron de l'agence de sécurité de l'Etat (Anssi). Pour Guillaume Poupard, verser des rançons aux auteurs de ransomware n'est pas la solution.

Pourquoi ? Car, entre autres, « cela contribue uniquement à soutenir financièrement les développeurs du malware » justifie Catalin Cosoi, responsable de la stratégie sécurité de BitDefender. Mais voilà, faute de sauvegarde et compte tenu de l'importance des données, des entreprises se résignent à payer.

Ransomware : des attaques à large spectre

C'est ce qu'observe IBM Security dans une étude. D'après Big Blue, les entreprises sont de plus en plus victimes de ransomware. Mais d'abord par opportunisme. Ces attaques sont désormais bien moins ciblées et affectent des victimes plus que des cibles.

L'attaque fin novembre contre le système de transport de San Francisco en est une illustration. Les pirates expliquaient ainsi automatiser l'infection par un ransomware après détection de vulnérabilités. La municipalité avait cependant refusé de payer la rançon de 100 bitcoins (alors plus de 70.000 dollars).

Selon IBM, la rentabilité du ransomware encourage à la multiplication des attaques. Près de 40% des emails de spam contiendraient désormais un tel programme malveillant. Cela se traduit mécaniquement par une hausse du nombre de victimes.

Et les entreprises victimes auraient donc majoritairement tendance, à près de 70%, à payer la rançon pour récupérer leurs données, chiffrées par les cybercriminels et donc inexploitables. Le préjudice financier dépasserait les 10.000 dollars pour 50% de ces sociétés.

Payer ou renoncer à ses données critiques

Les 20% restants auraient versé plus de 40.000 dollars, estime IBM. Au total, Big Bue évalue à 1 milliard de dollars, le montant ainsi extorqué aux entreprises grâce à un ransomware…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Ransomware – Payer ou ne pas payer ? Une large majorité d'entreprises a choisi – ZDNet

Six secondes suffisent pour pirater une carte bancaire

	Six secondes suffisent pour pirater une carte bancaire

En multipliant les tentatives sur différents sites, des chercheurs sont parvenus à contourner facilement les systèmes de paiement sécurisés mis en place et ce sans même posséder la carte bancaire physique utilisée.

Votre carte bleue n'est en sécurité nulle part. Sans connaître aucun détail de celle-ci, des pirates peuvent facilement pirater un compte en banque. Il leur suffit simplement d'un ordinateur, d'un accès à Internet et de six secondes, révèlent les chercheurs de l'université de Newcastle, au Royaume-Uni, dans une étude publiée dans le journal académique *IEEE Security & Privacy*(IEEE signifiant Institute of Electrical and Electronics Engineer).
Dans la pratique, les chercheurs ont utilisé une attaque par force brute pour contourner les mesures de sécurité visant à protéger le système de paiement en ligne des fraude. Connectée sur différents sites, l'équipe de chercheurs a généré de façon répétée et continue des variations des différentes informations sécurisés de cartes de paiement (numéro de carte, date d'expiration et cryptogramme visuel) jusqu'à obtenir un résultat favorable. D'après l'étude, c'est vraisemblablement une attaque du genre qui était au cœur de l'attaque informatique contre la filiale bancaire du géant britannique de la distribution Tesco, dont 20.000 clients ont été victimes.

Deux petites faiblesses qui en font une grosse

Si l'attaque parvient à réussir, c'est parce que le système ne détecte en effet pas les échecs répétés sur une même carte si cela se produit sur différents sites, d'autre part, tous les sites ne demandent pas les mêmes informations au même moment, ce qui permet de deviner un champ à la fois.

« Ce type d'attaque exploite deux faiblesses qui ne sont pas trop graves d'elles-même mais lorsque utilisées simultanément présentent un sérieux risque pour l'ensemble du système de paiement », explique dans le communiqué Mohammed Ali, étudiant en doctorat à l'école d'informatique de l'université de Newcastle et auteur principal de l'étude.

Simplement en partant des six premiers numéros de la carte de paiement, qui servent à indiquer la banque et le type de carte et sont donc identiques pour chaque fournisseur unique, *« un pirate peut obtenir les trois informations essentielles pour réaliser un achat en ligne en tout juste six secondes »*. Le délai peut être extrêmement réduit dans les cas où le pirate dispose des numéros de cartes, ce qui risque d'arriver de plus en plus souvent au vue de la récente vague d'intrusions informatiques survenues dans les plus grandes entreprises. Il leur suffit dans ce cas de deviner la date d'expiration – moins de 60 essais puisque la plupart des cartes de crédit sont valides cinq an au maximum -, puis le cryptogramme visuel composé de trois chiffres – ce qui prend dans le pire des cas 1.000 essais.
Mohammed Ali souligne toutefois que cette technique d'attaque par force brute ne marche qu'avec le réseau VISA, *« le réseau centralisé de MasterCard a été capable de détecter l'attaque après moins de 10 essais – même lorsque les paiements étaient répartis sur différentes réseaux »*. Autre point faible de la technique : la confirmation par SMS, que demandent bon nombre de sites d'e-commerce en France…[lire la suite]

Rapport 2015 de l'Observatoire de la sécurité des cartes de paiement
Original de l'article mis en page : Il suffit de six secondes pour pirater une carte bancaire

---

Réagissez à cet article