Piratage d’un gros assureur-santé visant les données d’un quart des Américains

Piratage d’un gros assureur-santé visant les données d’un quart des Américains

L’un des plus gros assureurs-santé américain, Anthem, a été victime d’une attaque informatique qui visait une base de données relatives à un quart des Américains, selon le groupe.« Des cyber-pirates ont réalisé une attaque très sophistiquée pour obtenir un accès non autorisé à l’un des systèmes informatiques d’Anthem, et ont obtenu des informations personnelles sur des clients et des salariés d’Anthem », a indiqué l’assureur dans un communiqué mercredi soir.
« La base de données affectée contient des informations d’environ 80 millions de personnes et des dizaines de millions » d’entre elles ont pu être volées, a précisé une porte-parole, Cindy Wakefield, confirmant une information du Wall Street Journal.

Aucune carte de crédit affectée
Les données compromises incluent des noms, dates de naissance, numéros de sécurité sociale (qui sont un élément important d’identification aux Etats-Unis), adresses physiques ou électroniques, ainsi que des informations liées à l’emploi des personnes, y compris sur leurs revenus.
Anthem affirme en revanche qu’aucune donnée de carte de crédit n’est affectée, et dit ne pas avoir de preuve à cette date que les pirates aient accédé à des informations médicales.
Selon les experts en cyber-sécurité, les données médicales peuvent être plus lucratives pour les pirates que les cartes de crédit, parce qu’elles permettent de créer de fausses identités pour se faire prescrire des médicaments qui seront ensuite revendus, ou bien de remplir de fausses déclarations d’assurance santé.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.20minutes.fr/monde/1534579-20150205-piratage-gros-assureur-sante-visant-donnees-quart-americains

---

Avez-vous un plan pour sécuriser vos données?

05

Avez-vous un plan pour sécuriser vos données?

La 9e journée internationale de la protection des données a lieu le 28 janvier dernier. Une occasion de faire le point sur les précautions à prendre pour se protéger contre le vol de données en ligne.

David Décary-Hétu est chercheur au Centre international de criminologie comparée et professeur adjoint à l'École de criminologie de l'Université de Montréal. « Une menace courante est le cheval de Troie grâce auquel les cybercriminels peuvent prendre le contrôle d'un ordinateur à distance pour scanner vos fichiers nommés visa.txt ou passeport.jpeg, par exemple, ou passer par votre connexion pour trouver de nouvelles victime. Et tout ça se fera de façon automatisée », explique-t-il.

Le mot de passe, ce verrou numérique à ne pas négliger

« Les mots de passe sont la principale faille de protection ! », estime Carl Charest, spécialiste en nouveaux médias et co-fondateur de Letube.tv. Il ne faudrait en effet que 2 secondes à un cybercriminel pour décrypter un mot de passe reprenant un numéro de téléphone montréalais, selon howsecureismypassword.net, un site qui permet de tester l'entropie de vos mots de passe.

Entropie ? C'est la « puissance » avec laquelle votre mot de passe pourra résister aux attaques des pirates qui tenteront le plus souvent de le percer en testant, une à une, toutes les combinaisons possibles. « On peut jouer avec des minuscules, des majuscules ou des caractères spéciaux, mais la vraie force d'un mot de passe est dans sa longueur », explique M. Décary-Hétu, qui recommande d'utiliser au moins 10 caractères.

Des logiciels se chargeant de recrypter vos mots de passe, comme PasswordBox, un gestionnaire d'identité numérique développé par une start-up montréalaise et récemment rachetée par Intel, permettent aussi d'augmenter votre sécurité en ligne.

Attention à la navigation en eaux troubles

À l'image des chevaux de Troie, les hackers parsèment certains sites de programmes malveillants qui risquent de compromettre la confidentialité de vos données personnelles. Internet Explorer, Windows, Acrobat Reader, les cybercriminels s'attaquent aux logiciels les plus utilisés. Ils ont bien compris qu'à la pêche aux informations, il valait mieux planter sa ligne dans les zones où gravitent des bancs de poissons !

« Les gens ont pris l'habitude de se promener dans des coins un peu sombres d'Internet, ajoute David Décary-Hétu, ils regardent aussi beaucoup des vidéos sur des sites de streaming souvent infestés de virus qui permettront aux pirates d'infiltrer directement leur ordinateur. » Et vous pourriez bien n'y voir que du feu si votre anti-virus ne détecte pas ces virus. Mais « un signe qui ne trompe pas, c'est une machine qui commence à devenir lente et qui met du temps à démarrer », prévient M. Décary-Hétu.

Que faire une fois que l'on est infecté ? Au mieux, plusieurs logiciels de nettoyage existent, mais au pire, il faudra mettre la hache dans le système d'exploitation, tout effacer et tout réinstaller. D'où l'importance de faire régulièrement des copies de sauvegarde de ses fichiers sur des disques amovibles.

Les autres pièges de la toile

« Dès qu'on va dans un endroit public et qu'on utilise une connexion wifi qui n'est pas sécurisée, on peut se faire prendre très facilement », témoigne Carl Charest, dont une connaissance s'est fait dérober toutes ses données en se connectant à distance à son ordinateur de maison alors qu'elle assistait à une conférence. Même les dossiers médicaux seraient devenus une des cibles privilégiées par les délinquants, car ils contiennent la majorité de vos informations personnelles, mais aussi des données bancaires présentes dans les dossiers d'assurance.

Enfin, on ne clique pas sur tout ce qui surgit à l'écran ou atterrit dans sa boîte de courriels ! Les techniques d'hameçonnage grâce auxquelles les cybercriminels se font passer pour de vrais sites sont aussi courantes pour dérober des informations personnelles et financières.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesaffaires.com/mes-finances/consommation/avez-vous-un-plan-pour-securiser-vos-donnees/575727
Par Nafi ALIBERT

Quels dégâts après une attaque DDoS ?

	Quels dégâts après une attaque DDoS ?

Selon les résultats d'une étude réalisée par Kaspersky Lab et B2B International, une attaque DDoS contre les ressources en ligne d'une entreprise pourrait causer un préjudice considérable, se chiffrant en moyenne entre 52 000 et 444 000 dollars selon la taille de l'entreprise. Pour de nombreuses entreprises, ce coût a un sérieux impact sur leur bilan ainsi que sur leur réputation en raison de la perte d'accès aux ressources en ligne pour leurs partenaires et leurs clients.

Ce coût total reflète plusieurs problèmes. Selon l'étude, 61 % des victimes d'une attaque DDoS ont temporairement perdu l'accès à des informations critiques ; 38 % ont été dans l'incapacité de poursuivre leur activité principale ; 33 % font état de pertes d'opportunités et de contrats. En outre, dans 29 % des cas, le succès d'une attaque DDoS a eu un impact négatif sur la cote de crédit de l'entreprise et, dans 26 % des cas, a entraîné une augmentation de ses primes d'assurance.
Les experts incluent dans le calcul des coûts moyens la réparation des conséquences d'un incident. Par exemple, 65 % des entreprises ont consulté des spécialistes en sécurité informatique, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque. Et il ne s'agit là que des frais les plus courants.
Les informations sur les attaques DDoS et les perturbations qui en résultent pour l'entreprise sont souvent rendues publiques, ce qui accentue encore les risques. 72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d'un incident, 36 % l'ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d'une attaque DDoS et près d'une sur trois a dû demander l'aide de conseillers en image.
« Une attaque DDoS qui fait mouche peut compromettre des services critiques, avec des conséquences graves pour l'entreprise. Par exemple, les récentes attaques contre des banques scandinaves (en particulier OP Pohjola Group en Finlande) a interrompu pendant quelques jours les services en ligne ainsi que le traitement des transactions par carte, un problème fréquent en pareil cas. C'est pourquoi les entreprises doivent aujourd'hui considérer la protection DDoS comme faisant partie intégrante de leur politique globale de sécurité informatique. Cet aspect est tout aussi important que la protection contre les malwares, les attaques ciblées, les fuites de données et autres », commente Tanguy de Coatpont, Directeur Général chez Kaspersky Lab France.
La technologie de Kaspersky Lab assure la continuité d'accès aux ressources en ligne de ses clients, y compris pendant les attaques DDoS complexes, prolongées ou d'un type jusque-là inconnu. Kaspersky DDoS Protection détourne le trafic client vers les centres de nettoyage de Kaspersky Lab pendant la durée de l'attaque, filtrant le trafic malveillant de sorte que le client ne reçoive que les requêtes légitimes et que ses infrastructures et services ne soient pas saturés.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/Kaspersky-Lab-et-B2B-International,20150128,50328.html par Kaspersky

Absence d’antivirus, de mails sécurisés, budgets cybersécurité limités… les mauvais pratiques digitales des PME

03

Absence d’antivirus, de mails sécurisés, budgets cybersécurité limités… les mauvais pratiques digitales des PME

Si les PME sont hyperconnectées et semblent conscientes des risques, elles ne consacrent toutefois qu’un budget très limité pour leur sécurité informatique – moins de 50 euros par an pour plus de la moitié d’entre elles – et cumulent les mauvaises pratiques, selon les résultats d’une enquête Ipsos pour le fournisseur de solutions réseau Navista.

Si les PME françaises sont aujourd’hui hyperconnectées, elles ont encore beaucoup de progrès à faire pour assurer un minimum de sécurité informatique. C’est ce qui ressort d’une enquête réalisée par Ipsos pour le fournisseur de solutions réseau Navista et diffusée le mercredi 28 janvier.

DES PME BIEN ÉQUIPÉES ET CONSCIENTES DES RISQUES

D’après cette étude, menée auprès d’un échantillon représentatif de 300 chefs d’entreprises et responsables IT d’entreprises de 1 à 99 salariés, les PME français sont dans leur quasi-totalité équipées en informatique et 93% disposent d’un accès à internet. Elles sont également 80% à disposer de terminaux mobiles, de l’ordinateur portable au smartphone en passant par la tablette, « avec un accès au réseau de l’entreprise dans plus de 2 cas sur 3 », précise Ipsos.

Si les PME françaises ont donc bien pris le virage du numérique, elles se révèlent également conscientes des principaux risques auxquelles elles s’exposent. 9 entreprises sur 10 s’estiment ainsi exposées à une usurpation des mots de passe et à une utilisation frauduleuse ou malveillante de leurs ressources informatiques et 7 sur 10 s’estiment concernées par le piratage des données internes à la société ou de leurs clients par exemple.

DES MAUVAISES PRATIQUES EN SÉRIE

Face à ces dangers de l’économie 2.0, peu de PME prennent toutefois les mesures nécessaires. « Pour communiquer avec leurs clients ou fournisseurs, les PME françaises utilisent à 87% une messagerie qui dans 70% des cas est celui de leur fournisseur d’accès à Internet ou un générique type Google », indique Ipsos qui enfonce le clou : « plus grave encore, trois quarts d’entre elles ne savent pas où sont physiquement hébergées les pièces jointes de leurs emails ». Une aubaine pour les pirates informatiques et un problème pour les clients de ces PME, comme les grands groupes industriels.
Parmi les autres failles constatées : 26% des PME ne disposeraient pas d’un anti-virus et seules 36% ont un logiciel anti-hameçonnage (ou « antiphising ») et 52% un pare-feu (ou « firewall »). Plus de la moitié des entreprises interrogées par Ispos ne prennent en outre « aucune autre sorte de disposition pour se protéger des actes de malveillance (que ce soit l’obligation de définir des codes d’accès aux supports, la souscription d’assurances liées aux risques informatiques, le cryptage de données sur mobile, etc.) ».

UN BUDGET SÉCURITÉ INFORMATIQUE SOUVENT INFÉRIEUR À 50 EUROS

Dans ces conditions, le budget consacré à la sécurité informatique ne dépasse pas les 50 euros dans plus d’une PME sur deux ! Reste à savoir si ces négligences s’expliquent davantage par un manque de connaissance des risques – contrairement à ce que semblait montrer la première partie de l’enquête – ou à des contraintes de coûts liées notamment à la crise. Mais les économies marginales réalisées pourraient vite se retourner contre ces entreprises : le coût à supporter suite à une attaque informatique en France serait en effet de 4,8 millions d’euros en moyenne, selon une étude du Ponemon institute publiée en novembre dernier.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.usine-digitale.fr/article/absence-d-antivirus-de-mails-securises-budgets-cybersecurite-limites-les-mauvais-pratiques-digitales-des-pme.N310454
Par Julien Bonnet

Attention à vos comptes Gmail, cibles de pirates…

	Attention à vos comptes Gmail, cibles de pirates…

Un nombre croissant de comptes piratés est actuellement signalé au Luxembourg. Cela commence toujours par un vol des données de connexion. Dans certains cas, cela passe par un faux message d'erreur qui nous informe que certains e-mails n'ont pas pu être transmis. L'utilisateur est alors prié de cliquer sur un lien qui mène à une prétendue adresse web de Google. C'est ici qu'il devra saisir ses données de connexion.

Une fois qu'ils ont mis la main sur les données de connexion, les criminels convertissent le compte en arabe. Ensuite, une nouvelle adresse e-mail est créée sur Yahoo, très semblable à l'adresse originale (par exemple: pit.luxi@yahoo.com à la place de pit.luxi@gmail.com).
Tout le courrier entrant sur l'adresse gmail est ensuite redirigé vers la nouvelle adresse e-mail contrôlée par les criminels. L'adresse de réponse des e-mails sortants est également sur le compte Yahoo, de sorte que la victime ne se rend pas compte de ce qui se passe. En outre, les criminels copient la liste entière des contacts de la victime et les suppriment du compte Gmail, pour empêcher la victime de communiquer. Ils vident aussi toute la boîte de réception, ainsi que tous les contenus des différents dossiers.

Une fraude perfide
Pendant que la victime se débat avec le rétablissement de la langue d'origine, les escrocs peuvent tranquillement commencer à envoyer des e-mails de phishing ou des demandes d'argent à la liste de contacts des victimes. Si la victime insouciante réinitialise son compte dans les 7 jours, dans sa langue, il verra une notification lui indiquant que tous ses messages sont transférés à l'adresse xxx@yahoo.com. Passé ce délai de 7 jours, la notification disparaît.
Si votre compte Gmail se retrouve subitement dans une autre langue, c'est le signe indubitable qu'il a été piraté et que votre identité à été usurpée.

Les bons réflexes
La police, Bee Secure et CASES vous conseillent de réagir de la manière suivante:
• faites repasser votre compte dans la langue d'origine ;
• désactivez la redirection automatique de vos e-mails ;
• ensuite, modifiez votre mot de passe sans attendre. Un mot de passe solide doit comporter 10 caractères au minimum, avec des caractères spéciaux, des majuscules, des minuscules et des chiffres, de manière à ce qu'il ne figure dans aucun dictionnaire ;
• restaurez vos listes de contacts;
• récupérez vos e-mails disparus (suivez le tutoriel vidéo de la police);
• prévenez vos contacts que votre compte à été piraté et qu'ils ne doivent en aucun cas répondre aux e-mails provenant d'une autre adresse (Yahoo en l'occurrence). Dans la mesure du possible, cette adresse doit être signalée et bloquée par le fournisseur.

☞ La police a réalisé un tutoriel video qui vous guide pour les étapes 1 à 5:

D'un point de vue préventif, les mesures suivantes sont toujours valables:
activez la double authentification sur vos comptes e-mail;
ne saisissez jamais de données personnelles (login, mot de passe, numéro de carte de crédit..) sur une page web que vous avez ouverte en cliquant sur un lien dans un e-mail ;
suivez les bonnes pratiques e-mail (https://www.cases.lu/fr/e-mail-bonnes-pratiques.html).
suivez les conseils donnés dans l'article clever clicks for safer business (https://www.cases.lu/arnaques.html)
Si un ami ou une connaissance vous demande de lui envoyer de l'argent pour l'aider à se sortir d'une situation difficile, il s'agit très probablement d'une arnaque. En cas de doute, appelez votre ami pour prendre de ses nouvelles.
Si vous pensez que le compte e-mail d'un de vos contacts a été piraté, prévenez-le.
Cette vague de phishing vise pour l'instant les comptes Gmail, mais elle pourrait se produire avec tout autre fournisseur de messagerie. Ouvrez l'oeil!
Pour plus d'information, consultez la chaîne TV de la Police. Bee Secure y a participé à l'émission du 15 janvier sur la Cybercriminalité:

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://www.cases.lu/fr/comptes-gmail-pirates-copies-et-convertis-en-arabe.html

Sommes-nous invisibles sur les réseaux sociaux anonymes ? Denis JACOPINI répond à une journaliste de l'émission « On n'est plus des pigeons » sur France 4

	Sommes-nous invisibles sur les réseaux sociaux anonymes ? Denis JACOPINI répond à une journaliste de l'émission « On n'est plus des pigeons » sur France 4

Denis JACOPINI interviewé par une journaliste de l'émission « On n'est plus des pigeons » a répondu à la question « Sommes-nous invisibles sur les réseaux sociaux anonymes ? »Secret, Whisper ou Yik Yak… Ces nouveaux réseaux sociaux promettent l'anonymat à leurs utilisateurs. Sauf que rien n'est invisible sur le net.Rumeurs, mots doux, coup de gueule… Publier tout ce qui vous passe par la tête sans dévoiler sa véritable identité, c'est la promesse des réseaux sociaux anonymes comme Whisper.sh, chuchotement en français, Secret.ly, Rumr ou encore Yik Yak, une sorte de Twitter. Conçues essentiellement pour les smartphones, ces plates-formes gratuites incitent leurs membres à se lâcher sans compromettre leur e-réputation. Elles disent garantir des discussions avec des amis ou de parfaits inconnus sans qu'on puisse, dans certains cas, retrouver l'identité de l'émetteur, ou bien, les messages envoyés.

Doit-on féliciter ces applications en matière de protection de la confidentialité de ses utilisateurs ?
Mouais. Avant tout, à donner la possibilité de tout dire sous couvert d'anonymat, ces réseaux se livrent aux dérives de racisme, d'harcèlement et de diffamation. Au niveau technique, quelques incohérences. En octobre dernier, le quotidien britannique The Guardian, sur le point à l'époque de conclure un partenariat média avec Whisper, a eu accès aux coulisses de l'éditeur. Le journal a accusé l'application de collecter des données personnelles et de géolocalisation de ses utilisateurs. D'après The Guardian, Whisper gardait un œil sur les publications et les localisations de ses utilisateurs pour sa collaboration avec les médias. Le but : recouper le contenu des messages pour vérifier si une information était avérée.

Un réseau social qui ne laisse pas de traces, impossible ?
Pour Denis Jacopini, expert judiciaire en informatique, Whisper, comme les autres réseaux sociaux anonymes « se revendiquent dans leur communication comme une forme de réseau social anonyme. Sauf que la souscription n'est pas anonyme. Tous les éléments pour identifier une personne sont là au moment de l'inscription via son smartphone. »
Même si ce type d'applications ne donne pas directement accès à l'identité d'une personne, l'adresse IP du terminal utilisé pour la connexion Internet permet de récolter les informations du téléphone.
Pourtant, la garantie de l'impossibilité de « tracer » les utilisateurs a été mise en avant notamment par le réseau Whisper. Sur Twitter, son éditeur Neetzan Zimmerman garantissait mi-octobre 2014 qu'il est techniquement impossible de déterminer la localisation des utilisateurs qui n'activaient pas leur localisation GPS. Pour l'expert en informatique Denis Jacopini, « désactiver la localisation GPS est inutile » pour éviter tout traçage. En effet, l'adresse IP du téléphone permet de remonter au fournisseur d'accès à Internet puis de déterminer la localisation de l'utilisateur.
Des informations que les fournisseurs peuvent communiquer aux autorités sur demande. D'autant que le droit applicable en matière de protection des données est celui du pays du propriétaire des plates-formes, souvent américaines. « L'anonymat n'est pas garanti vis-à-vis des autorités, c'est bien pour les copains », conclut Denis Jacopini. Et encore. Alors, pour vider son sac en public sans problème, parlez-en à une proche. Tout s'arrange avec l'écoute et la parole.
Marie Dagman

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.france4.fr/emissions/on-n-est-plus-des-pigeons/enquete/sommes-nous-invisibles-sur-les-reseaux-sociaux-anonymes_294315
Par Marie Dagman

Des failles de sécurité aussi dans les drones ?

28

Des failles de sécurité aussi dans les drones ?

Un chercheur indien croit avoir décelé une faille de sécurité lui permettant de prendre le contrôle d'un drone Parrot. Il a mis au point un malware capable de prendre le contrôle de l'appareil à distance et de modifier les instructions de vol.

Les drones, comme à peu près tout ce qui repose de près ou de loin sur les technologies numériques, ne sont pas exemptés de failles de sécurité. Le chercheur indien Rahul Sasi s'est lancé le défi de prendre le contrôle à distance d'un drone fabriqué par Parrot et pense y être parvenu, à l'aide d'un malware conçu par ses soins et sobrement baptisé Maldrone.
Rahul Sasi n'a pas encore publié de prototype détaillé de sa méthode, mais explique sur une page web la façon dont il a procédé et accompagne le tout d'une petite vidéo de son programme en action.
La faille trouvée par le chercheur indien lui permet de prendre dans une certaine mesure le contrôle de l'appareil en profitant d'une faille de sécurité du programme d'autopilotage du drone. En jouant avec les processus d'échanges d'informations entre les différents capteurs du drone et le programme d'autopilote, le pirate est capable de prendre la main sur un drone, et ce à distance.

Nos drones sont-ils dignes de confiance ?
Selon Rahul Sasi, la backdoor ainsi mise en place est du genre tenace et un simple reboot du drone ne suffit pas à s'en débarrasser, conférant à l'attaquant un accès persistant au système de contrôle du drone. Rahul Sasi explique que son malware est également capable de s'auto-répliquer et de se propager à d'autres drones.
Potentiellement inquiétant, le malware développé par le chercheur ne cherche néanmoins pas à nuire particulièrement aux utilisateurs mais a été crée dans un simple but de recherche et par pure curiosité selon Rahul Sasi. On peut donc écarter pour le moment la possibilité de voir un groupe de cybercriminels pirater à distance une armée de drones civils afin de faire passer de la drogue en douce à la frontière à l'insu de leurs propriétaires.
Mais pour l'instant, on prendra quelques pincettes : il faudra attendre le 7 février pour disposer de plus d'informations techniques sur le sujet, date à laquelle Rahul Sasi prévoit de revenir plus en profondeur sur son hack à l'occasion de la conférence Nullcon. Nous avons contacté Parrot à ce sujet et nous mettrons à jour cet article si la société souhaite réagir à cette annonce.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/les-drones-aussi-ont-des-failles-de-securite-39813694.htm
Par Louis Adam

Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

L'éditeur Qualys a mis la main sur une vulnérabilité importante qui permettrait de prendre le contrôle à distance de la plupart des distributions Linux. Les appareils de type routeurs-modems ou NAS sont également concernés.

Les chercheurs en sécurité de la société Qualys ont mis la main sur une faille critique (CVE-2015-0235) qui touche tous les systèmes Linux. Baptisée « Ghost », elle permettrait aux pirates de prendre le contrôle à distance « de tout un système, en se passant totalement des identifiants système », explique l'entreprise dans un communiqué. Un patch a été développé en concertation avec les éditeurs Linux. Il est en cours de diffusion et d'ores et déjà disponible sur certaines distributions, telles de Debian, Red Hat ou Ubuntu.
Cette terrible faille est logée dans une librairie GNU/Linux baptisée« glibc », qui est intégrée dans toutes les distributions Linux et qui permet de gérer les appels système de bas niveau, comme l'allocation d'espace mémoire, l'ouverture de fichiers, etc. Seules les versions antérieures à glibc 2.18 sont vulnérables. « Malheureusement, très de peu distributions Linux ont intégrés les versions récentes de glibc, pour des raisons de compatibilité. C'est pourquoi la plupart sont vulnérables », explique Wolfgang Kandek, directeur technique de Qualys.

Quid des routeurs ou des NAS ?
Comment fonctionne Ghost ? Cette vulnérabilité se caractérise par un dépassement de mémoire tampon (buffer overflow) dans les fonctions gesthostbyname et gethostbyaddr. Ces fonctions sont appelées par les applications Linux quand elles doivent gérer des connexions Internet, comme par exemple les serveurs de messagerie. C'est d'ailleurs la cible sur laquelle se sont penchés les chercheurs de Qualys pour développer un exemple de code d'exploitation : ils ont conçu une attaque dans laquelle il suffit d'envoyer un email vers le serveur pour accéder à l'interface ligne de commande (shell). C'est aussi simple que ça !
Qualys recommande aux administrateurs de mettre à jour leurs systèmes Linux aussi rapidement que possible. Mais une question reste en suspens : quid des nombreux objets connectés que nous possédons tous à la maison, tels que les routeurs-modems ou les disques durs en réseau (NAS) ? « Ils intègrent tous la librairie glibc. Mais pour créer une attaque, il faut également que ces appareils utilisent les fonctions vulnérables. Il faut ensuite trouver le bon vecteur d'attaque. Ce n'est pas évident à priori », souligne Wolfgang Kandek. En somme : pas la peine de paniquer tout de suite. Les pirates vont certainement se pencher sur la question, mais ils vont mettre du temps à développer leurs attaques. Pour réduire le risque, il est conseillé de mettre à jour les firmwares des appareils dès qu'ils seront disponibles.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/643126/ghost-la-faille-critique-qui-permet-de-prendre-le-controle-des-systemes-linux/
Par Gilbert Kallenborn

La cybercriminalité à l’encontre des entreprises s’industrialise

	La cybercriminalité à l’encontre des entreprises s’industrialise

Un écosystème professionnalisé de cybercriminels mène la danse.
Pas d'électrochoc dans les entreprises après l'affaire Sony : les investissements restent insuffisants.
Sony débordé par les cybercriminels
Phishing, escroquerie, espionnage, vol de secrets industriels… Si ces phénomènes ne sont pas nouveaux, la cybercriminalité ne s'est jamais aussi bien portée.
Bernard Cazeneuve n'a pas manqué de rappeler la réalité de cette menace au Forum international de la cybersécurité, qui s'est tenu à Lille la semaine dernière. « Des attaques de plus en plus sophistiquées touchent principalement les entreprises et visent à leur voler des données stratégiques, parfois en très grande quantité », a fait valoir le ministre de l'Intérieur. Si le phénomène est difficile à chiffrer, il connaît une montée en puissance. Pourquoi ? « La technologie explose. Il y a de plus en plus d'applications. Plus on développe vite, plus le risque de bugs augmente», explique Jean-Michel Orozco, président de CyberSecurity chez Airbus Group (ex-Cassidian).
Au quotidien, les entreprises doivent lutter contre la petite délinquance, peu sophistiquée mais rentable. « Les entreprises ont été fortement touchées par les "cryptolockers" », explique Eric Freyssinet, chef de la division de lutte contre la cybercriminalité de la Gendarmerie nationale. Des pirates bloquent des PC, et exigent des rançons pour les débloquer. Bien sûr, celui qui paie ne récupère pas pour autant ses données.
« Les anciennes menaces s'industrialisent. Les banques, par exemple, souffrent beaucoup d'attaques en déni de service [rafale d'attaques dont le but est de bloquer les systèmes] ou de phishing », explique Michel Van Der Berghe, à la tête d'Orange Cyberdefense. Plus élaboré, « le "spearphishing" permet d'envoyer des e-mails ultraciblés personnalisés par secteur identifié, l'armement, le transport… » dit Eric Freyssinet. C'est grâce à un e-mail très bien personnalisé que la Syrian Electronic Army a réussi, ces derniers jours, à pirater « Le Monde ».

Des PME très exposées
Les PME sont particulièrement exposées aux faux placements, où la victime verse de l'argent à un tiers soi-disant spécialisé dans les placements à haut rendement. Selon la gendarmerie, ce type d'attaque représente les « trois quarts des escroqueries » qui concernent les entreprises. Plus connue, « l'arnaque au président » consiste à extorquer de l'argent à une entreprise en se faisant passer pour son dirigeant. Parmi les victimes, Michelin, qui a perdu 1,6 million d'euros.
L'espionnage – de secrets industriels ou commerciaux –, un fléau auquel font face les entreprises depuis deux ou trois ans, ne requiert pas non plus de techniques ultrasophistiquées. « Un mot de passe faible, type 1 2 3 4 5 6, sur un équipement de réseau ou une application peut suffire », estime Stanislas de Maupeou, directeur-conseil cybersécurité chez Thales. Dans ce cas-là, la difficulté consiste surtout à identifier les intrusions.

Cellules « N-Tech » : la gendarmerie aussi s'arme face à la cybercriminalité

Pas facile de lutter contre ces attaques à grande échelle. Car, en face, on a affaire, non pas à des groupements organisés, mais à un écosystème criminel. « Sur le "dark Web", on trouve des publicités pour des attaques en kit. Il y a même des réductions ! » explique Michel Van Der Berghe. « Ceux qui vendent les virus ne sont pas ceux qui les collectent. Deux personnes différentes à deux bouts de la France peuvent se mettre d'accord pour développer un virus. Elles communiquent sur Tor, sur certains forums ou sur des messageries instantanées comme Jabber », explique le lieutenant-colonel.
De leur côté, les entreprises restent insuffisamment armées. Le piratage massif de Sony, victime d'un vol à grande échelle de données, n'a pas créé d'électrochoc. Chez Thales, un seul client exerçant dans le même domaine que Sony, et expliquant qu'il ne pourrait supporter une attaque d'une telle ampleur, a appelé, chez Airbus aucun.

Pas seulement des moyens
Beaucoup de dirigeants n'ont pas encore fait grand-chose. « Les moyens seuls ne suffisent pas. Il faut aussi un plan, avec une gouvernance qui sait quoi faire en cas de problème », détaille Jean-Michel Orozco, d'Airbus CyberSecurity, qui estime qu'un grand groupe devrait dépenser entre 8 et 11 % de son budget informatique en sécurité. On est loin du compte. « Aujourd'hui, on est à 3 ou 4 %. Or, en cas de problème, si l'on doit remonter entièrement un système, cela peut coûter 20 % du budget IT », estime Stanislas de Maupeou, qui rappelle qu'au regard des outils existants, la lutte contre le fléau est à la portée de tous.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesechos.fr/tech-medias/hightech/0204110358637-la-cybercriminalite-a-lencontre-des-entreprises-sindustrialise-1087050.php
Par Sandrine Cassini

Le danger de la société du Big Data

Le danger de la société du Big Data

Pour comprendre le monde de demain, il faut garder en tête une seule date : l'année 2002 ! C'est durant l'année 2002 que nos sociétés ont produit pour la première fois plus de données que l'humanité depuis sa création.

C'est fou mais aujourd'hui et demain davantage encore, tous les objets qui nous entourent communiqueront entre eux et donneront une foule d'informations numériques sur nous. Il y aura des puces insérées dans nos matelas qui mesureront nos cycles de sommeil, nos frigos qui nous alerteront sur les produits périmés ou les courses à faire, sans oublier nos puces bancaires qui sont déjà dans nos smartphones et qui mesureront le moindre achat ou paiement, que ce soit pour s'alimenter ou payer un parking. Bref, toutes ces données numériques, ces datas comme disent les professionnels, rendront notre vie transparente et nous serons nus comme des vers pour ceux ou celles qui détiendront ces informations, ces fameuses datas.

Tous les objets qui nous entourent communiqueront entre eux et donneront une foule d'informations numériques sur nous.

Aujourd'hui, personne n'en a cure, car bien souvent, on se dit que les informations qui sont données (ou seront données demain) sont inoffensives, voire même nous aident à vivre mieux. C'est vrai, par exemple, quand c'est une brosse à dents qui nous avertit que notre hygiène buccale laisse à désirer, c'est vrai aussi lorsqu'une puce, glissée sous notre peau, nous donnera de précieuses indications sur notre état de santé.
Tout cela et bien d'autres choses encore sont vraies mais pour autant, ce business du Big Data est également porteur de dangers… Et là, visiblement à part quelques intellectuels, personne ne semble s'en soucier. Qui peut dire si demain, notre mutuelle, notre banquier ou notre assureur ne regardera pas toutes ces données sur notre santé pour traquer les mauvaises habitudes des fumeurs, des buveurs, de ceux et celles qui mangent trop gras, ou trop salé ou qui ne sont pas abonnés à une salle de sport ou que sais-je encore.
Il ne faut pas se leurrer, la tentation sera trop grande pour ces assureurs ou ces banquiers de nous appliquer un tarif individualisé, un tarif en fonction de notre profil de risque exact. Si c'est le cas, c'est un changement de société radical qui s'annonce ! Cela serait la fin de la mutualisation des risques comme l'indique le journal Les Echos. En clair, les moins chanceux seront laissés au bord du chemin, sans couverture d'assurance ou alors à un tarif impayable.
Le danger de cette société du Big Data, c'est que si demain tout le monde se sent épié, plus personne n'osera prendre des risques… Cela sera une société immobile, que nous fabriquerons sans le savoir. C'est la raison pour laquelle, je le dis souvent, nous ne sommes pas seulement en crise, nous sommes dans une société en pleine mutation. Et nous percevons pour le moment qu'une petite partie de ces changements… C'est interpellant mais aussi très passionnant à comprendre.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://trends.levif.be/economie/politique-economique/le-danger-de-la-societe-du-big-data/article-opinion-362781.html
Par Amid Faljaoui