Protection des données des entreprises v.s. combat anti-terroriste

	Protection des données des entreprises v.s. combat anti-terroriste

Critiqué par certaines forces antiterroristes, le chiffrement des messages en entreprise, aussi appelé cryptographie, reste une solution contre l'espionnage industriel.

Critiqué par certaines forces antiterroristes, le chiffrement des messages en entreprise, aussi appelé cryptographie, reste une solution contre l'espionnage industriel.

Cet été, une directrice au sein d'un grand groupe industriel s'est fait voler son ordinateur portable professionnel. Heureusement, un système de chiffrement protégeait l'accès aux informations confidentielles qui s'y trouvaient. Bilan : cet épisode n'a pas eu d'autres conséquences que l'achat d'un nouvel outil de travail pour la collaboratrice, pour 300 euros, loin du coût d'une fuite de documents sensibles que ce fleuron français a frôlé.

Le chiffrement, aussi appelé « cryptage » (un anglicisme), consiste à encoder un document ou le contenu d'un smartphone ou d'un ordinateur pour le rendre inintelligible. La lecture de ce document n'est possible que pour celui qui connaît la clef du code (souvent un mot de passe, plus rarement une empreinte digitale). Les experts considèrent que seul un ordinateur quantique pourrait tester aléatoirement toutes les combinaisons possibles d'une clef solide et reconstituer un message…

Un outil défensif

Dans un contexte de cyberinsécurité grandissante, où l'espionnage industriel n'est plus à prouver suite aux révélations d'Edward Snowden, les services secrets français (la DGSI) et l'Agence nationale de la sécurité des systèmes d'information (Anssi) encouragent les entreprises à chiffrer leurs données les plus sensibles. « C'est un outil défensif, essentiel à la protection des données numériques d'une immense majorité d'utilisateurs honnêtes ; il ne me semble pas raisonnable de l'interdire au motif que quelques individus pourraient s'en servir pour préparer des crimes ou des attentats, aussi odieux soient-ils », défend Guillaume Poupard, le directeur général de l'agence placée sous l'autorité du Premier ministre.
Cette structure est chargée de coordonner et d'aider les entreprises françaises et l'Etat à se protéger des cyberattaques. Mais son propos est quelque peu brouillé par certaines voix haut placées et un concert de discours sécuritaires. Un ancien directeur de la CIA, le procureur de la République de Paris (François Molins), le ministre de l'Intérieur (Bernard Cazeneuve) et même le chef du gouvernement britannique (David Cameron) se sont tour à tour exprimés pour demander un affaiblissement des algorithmes de chiffrement des messageries. Ce qui permettrait aux enquêteurs de police habilités de lire la correspondance protégée de certains suspects, notamment pour lutter contre le terrorisme . En octobre, le Premier ministre Manuel Valls se déclarait favorable pour les entreprises à « toutes les ressources qu'offre la cryptologie légale », une formule polémique puisque jusqu'à présent aucun mode de chiffrement, même les plus forts, n'est illégal pour elles.

« Jusqu'à une période récente, le chiffrement était considéré comme un luxe par les entreprises, mais avec la migration des messageries dans le cloud, notamment via Microsoft, les besoins dans ce domaine ont augmenté », constate Alain Bouillé, le président du Cesin, une association de responsable de la sécurité des systèmes d'information. La majorité des grandes entreprises françaises proposent des solutions de chiffrement à leurs collaborateurs. Mais peu d'entre eux les utilisent vraiment, car ces systèmes sont peu pratiques au quotidien . « Certaines briques de logiciels peuvent compléter le client-mail standard mais le chiffrement n'est pas toujours parfait avec ces modules plus simples », remarque Christophe Kiciak, le directeur audit et sécurité de Provadys, une entreprise de cybersécurité. « Apple pour les iPhones et Google pour certains smartphones Android ont des solutions qui cryptent de bout en bout certains services de messagerie, sans même que l'utilisateur s'en aperçoivent, mais elles sont menacées par les gouvernements », souligne également Gérôme Billois, consultant chez Solucom.

La seule solution de protection

Les experts sont unanimes : « Le chiffrement est la seule solution pour se protéger du vol de données suite à une attaque informatique. » Quand un smartphone est perdu, le chiffrement empêche aussi que la personne qui le retrouve en profite pour s'approprier des informations sensibles. Tout reste illisible. « Le chiffrement protège aussi de l'employé qui se trompe de destinataire pour un e-mail », note Stéphane Calé, le président de la commission « Cyber » du Club des directeurs de sécurité des entreprises.
En interne, les responsables de la protection de l'information des sociétés tentent de sensibiliser sur ces questions. « 15 à 20 % des collaborateurs sont concernés, ils travaillent dans le management, dans les bureaux d'études et les services financiers », compte Bernard Ourghanlian, le directeur technique et sécurité de Microsoft France. « Le chiffrement doit surtout protéger les données stratégiques comme les projets de rachat ou de développement à l'international », précise Christophe Kiciak. Un système de classification de données selon leur sensibilité, à la manière de la grille « secret défense » des militaires, est recommandé pour les entreprises. De tels barèmes permettent d'adapter les exigences envers chaque collaborateur, par rapport à son exposition au risque. Des formations spécifiques existent pour les assistants de direction. Le problème reste au niveau des dirigeants, souvent peu indulgents quand la sécurité vient perturber l'usage de leur smartphone dernier cri.

Réagissez à cet article
Source : http://business.lesechos.fr/directions-numeriques/technologie/cybersecurite/021549442285-quand-la-protection-des-donnees-des-entreprises-percute-le-combat-anti-terroriste-205384.php
Par FL Debes

12% des attaques DDoS menées par des concurrents

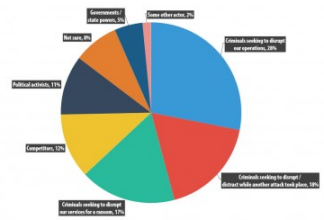
12% des attaques DDoS menées par des concurrents

Selon Kaspersky, la volonté de nuire à un concurrent serait à l'origine de plus d'une attaque DDoS sur dix dans le monde.

Demande de rançon, tentative d'arrêt de l'activité, distraction pour opérer une pénétration du réseau… Kaspersky s'est notamment penché sur les motivations qui poussent les cybercriminels à lancer des attaques DDoS (Distributed Denial of Service) contre des entreprises.
L'éditeur de sécurité a mandaté le cabinet B2B International pour y voir plus clair dans ces motivations. Non pas en demandant aux responsables des attaques eux-mêmes mais à leur victimes. Soit auprès des responsables IT et dirigeants de plus de 5 500 entreprises de toutes tailles de 26 pays dans le monde.
Selon l'étude, il ressort que près de la moitié (48 %) des victimes d'une attaque par déni de service déclarent connaître les motivations, voire les identités, de leurs assaillants ou commanditaires. Sur cet ensemble, 12% des entreprises pensent que les attaques viennent de concurrents directs qui recourent éventuellement aux services d'organisations « spécialisées » dans ce genre d'opérations. Un chiffre qui monte à 38% dans le secteur des industries de services.

5% d'attaques gouvernementales

« Les attaques DDoS ne sont plus seulement l'œuvre de cyber-criminels qui cherchent à arrêter les opérations d'une entreprise, commente Evgeny Vigovsky, responsable de la division DDoS Protection chez Kaspersky. Les entreprises sont de plus en plus méfiantes les unes des autres et il y a une réelle préoccupation pour de nombreuses entreprises – y compris les petites et moyennes – d'être touchées par les tactiques sournoises de leurs concurrents, qui commissionnent des attaques DDoS directement contre eux, endommageant leurs opérations et leur réputation. »
Autre perception, 18% des attaques seraient menées pour focaliser les équipes IT afin de mener des tentatives de pénétration du réseau en parallèle. Un chiffre proche des 17% des répondants qui déclarent que les DDoS s'accompagnent de demandes de rançons, notamment auprès des fabricants et des acteurs de l'industrie des télécoms qui s'en disent victimes à hauteur de 27% chacun. 11% seraient visés par des activistes politiques et 5% proviendrait d'agressions étatiques/gouvernementales. Mais la majorité des attaques serait menée par des criminels qui chercheraient simplement à interrompre l'activité de l'entreprise. A des fins purement gratuites ?
On en doute…



Réagissez à cet article
Source : http://www.silicon.fr/12-des-attaques-ddos-menees-par-des-concurrents-133929.html

---

Les tendances 2016 en cyber-sécurité

Les tendances 2016 en cyber-sécurité

Comme la plupart des professionnels de la sécurité informatique, je souhaite vraiment que mes prédictions ne se réalisent pas. Je préférerais que les entreprises ne soient ni piratées ni victimes de failles. Mais en prédisant la prochaine vague de menaces, nous espérons aider les entreprises à rester au fait de l'évolution des tactiques et des méthodes que les criminels vont utiliser pour les cibler. Voici dix menaces et tendances que nous devrions constater au cours de 2016 en matière de sécurité informatique.

Si une semaine peut sembler longue en politique, comme l'a observé l'ancien Premier ministre britannique Harold Wilson, une année dans le domaine de la cyber-sécurité peut ressembler à une éternité. Malgré les changements rapides, beaucoup de choses restent cependant constantes. Les trois principales menaces prévues par Check Point pour 2015 étaient la croissance rapide des logiciels malveillants inconnus, les menaces mobiles et les vulnérabilités critiques dans les plates-formes couramment utilisées (Android, iOS et autres). Ces prédictions se sont pleinement réalisées et ces menaces continueront certainement de poser nombreux problèmes. Le jeu du chat et de la souris qui a caractérisé la cyber-sécurité au cours des dernières années se poursuit. Les pirates tentent de trouver sans cesse de nouvelles manières d'attaquer les réseaux, comme le montrent les failles de cette année chez Anthem, Experian, Carphone Warehouse, Ashley Madison et TalkTalk.

Logiciels malveillants « sniper »
Les plus grandes failles de 2016 seront le résultat de logiciels malveillants conçus sur mesure pour franchir les défenses d'entreprises spécifiques, telles que lors des attaques menées contre TV5 Monde. Les attaques génériques à champ large continueront de menacer les utilisateurs individuels et les petites entreprises, et les pirates amélioreront leurs méthodes d'attaque contre les grandes entreprises qui disposent de postures de sécurité plus sophistiquées. Ils utiliseront des méthodes de phishing plus approfondies et plus sophistiquées, et d'autres astuces d'ingénierie sociale pour accéder aux systèmes et aux données qu'ils souhaitent.

Les terminaux mobiles en 1ère ligne des attaques
Le nombre d'attaques mobiles continue d'augmenter à mesure que les appareils mobiles prennent place dans l'entreprise et offrent aux pirates un accès direct et potentiellement lucratif aux données personnelles et professionnelles. D'après une étude que nous avons menée en 2015, 42% des entreprises ont subi des incidents de sécurité mobile leur coûtant plus de 200 000 €, et 82% s'attendent à une augmentation du nombre d'incidents. Cette année a également été le témoin de l'émergence de plusieurs vulnérabilités mobiles critiques, notamment Certifigate impactant des centaines de millions d'appareils Android, et XcodeGhost – première infection malveillante à grande échelle ciblant des appareils Apple iOS non jailbreakés. Nous nous attendons à d'importantes vulnérabilités mobiles similaires l'année prochaine.

La bataille contre les menaces les plus dangereuses
Dans la bataille continue entre les pirates et les professionnels de la sécurité, les agresseurs déploient des variantes personnalisées de logiciels malveillants existants et d'attaques encore inconnues (« zero-day ») de plus en plus sophistiquées, capables de contourner la technologie de sécurité traditionnelle. Ces nouveaux vecteurs d'attaque exigent des solutions plus proactives et plus avancées pour stopper ces logiciels malveillants. Des innovations comme le sandboxing au niveau du CPU, capable d'identifier les menaces les plus dangereuses avant qu'elles ne parviennent à échapper à la détection des outils traditionnels et infecter les réseaux, seront plus que jamais nécessaires en 2016 pour faire face à ces nouvelles menaces.

Les infrastructures critiques plus que jamais en ligne de mire
En décembre 2014, une aciérie en Allemagne a été frappée par des pirates qui ont réussi à accéder au réseau de production de l'usine et causer des dommages « massifs ». Le département américain de la sécurité intérieure a découvert que le Trojan « Havex » était parvenu à compromettre les systèmes de contrôle industriel de plus de 1 000 entreprises du secteur de l'énergie en Europe et en Amérique du Nord. Les cyber-attaques menées contre des services publics et des processus industriels clés se poursuivront, à l'aide de logiciels malveillants ciblant les systèmes SCADA qui contrôlent ces processus. Comme ces systèmes de contrôle sont de plus en plus connectés et offrent une surface d'attaque plus étendue, une meilleure protection sera nécessaire pour les défendre. Ces risques sur les infrastructures critiques sont particulièrement sensibles dans un contexte de menaces terroristes accrues.

Les objets connectés : futur terrain de jeu des hackers ?
L'Internet des objets en est encore à ses balbutiements, et il est peu probable qu'il ait un fort impact en 2016. Néanmoins, les entreprises doivent réfléchir à la manière dont elles peuvent protéger les appareils intelligents et se préparer à une plus vaste adoption de l'IoT. Les utilisateurs doivent se demander « où leurs données sont transmises » et « ce qui se passerait si quelqu'un mettait la main sur ces données ». L'année dernière, nous avons découvert une faille dans des routeurs équipant des TPE dans le monde entier, qui pourrait permettre à des pirates de les détourner pour lancer des attaques sur tous les appareils qui leur sont connectés. Nous nous attendons à plus de vulnérabilités similaires dans les appareils connectés.

Les wearables c'est beau … mais pas très sécurisé !
Les wearables tels que les montres intelligentes font leur entrée dans l'entreprise, présentant de nouveaux risques et défis pour la sécurité. Les données stockées dans les montres intelligentes et les autres appareils personnels intelligents sont vulnérables et pourraient même être utilisées par des pirates pour capturer de l'audio et de la vidéo via des Trojans d'accès à distance. Les entreprises qui autorisent l'utilisation de ces appareils doivent assurer leur protection via des mots de passe et des technologies de chiffrement renforcées.
Trains, avions et véhicules connectés… autant de portes d'entrée pour les hackers !

2015 est l'année de l'émergence du piratage de véhicules : leurs logiciels embarqués sont détournés afin de prendre le contrôle des véhicules. En juillet, Fiat Chrysler a rappelé 1,4 millions de véhicules Jeep Cherokee aux États-Unis après que des chercheurs aient découvert qu'ils pouvaient être piratés via le système de divertissement connecté. Avec plus de gadgets et de systèmes connectés que jamais dans les véhicules modernes, nous devons protéger ces systèmes. Il en va de même pour les systèmes complexes des avions de ligne, des trains et autres formes de transport public.

Véritable sécurité pour les environnements virtuels
La virtualisation a été rapidement adoptée par les entreprises au cours des dernières années, que ce soit via SDN, NFV ou le Cloud. Les environnements virtualisés sont complexes et créent de nouvelles couches réseau. C'est seulement maintenant que nous comprenons réellement comment protéger ces environnements. Lorsque les entreprises migrent vers des environnements virtualisés, la sécurité doit être conçue dès le départ pour offrir une protection efficace.

Nouveaux environnements, nouvelles menaces
2015 était également l'année du lancement de plusieurs nouveaux systèmes d'exploitation, tels que Windows 10 et iOS 9. La majeure partie des attaques menées contre les entreprises ces dernières années ciblaient Windows 7, en raison de la faible adoption de Windows 8. Mais avec Windows 10 et son offre de téléchargement gratuit, les cybercriminels vont donc tenter d'exploiter ce nouveau système d'exploitation. Ses mises à jour sont plus fréquentes et les utilisateurs maîtrisent moins son environnement.

La consolidation de la sécurité pour la simplifier !
Pour se protéger contre les menaces multiformes, les professionnels de la sécurité sont susceptibles de se tourner vers des solutions d'administration centralisée de la sécurité. Les grandes entreprises qui possèdent pléthore de différents produits de sécurité sur leur réseau verront la consolidation comme un moyen de réduire à la fois coût et complexité. La multitude de solutions et de produits individuels devient rapidement ingérable et peut effectivement entraver la sécurité plutôt que l'améliorer. La consolidation de la sécurité fournit un moyen efficace de réduire la complexité afin que les nouvelles menaces ne s'égarent pas entre les mailles des différents systèmes.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-cyber-securite-en-2016-Check,20151204,58072.html

---

Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs – Next INpact

Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs

Après des heures de négociations, le Parlement européen et les États membres sont arrivés lundi à un accord sur la future directive NIS (network and information security). Un texte destiné à mieux protéger les opérateurs dits critiques dans toute l'Europe.

Cette future directive sur la cybersécurité visera en effet à imposer des règles harmonisées à tout un ensemble d'opérateurs critiques. Le mouvement sera épaulé par le réseau des Computer Security Incident Response Team (CSIRT) pour discuter des incidents et identifier de possibles réponses coordonnées.

Plusieurs niveaux de reporting selon les acteurs concernés

Ce texte visera avant tout à définir des critères pour savoir qui relève de ces obligations. En tête de liste, on trouvera nécessairement les acteurs de l'énergie, du transport et de la santé. Selon l'eurodéputé Andreas Schwab (EPP), ces entreprises devront répondre à plusieurs mesures de sécurité, mais également notifier aux autorités les incidents de cybersécurité qualifiés « *d'importants.* »

Si les micro entreprises et les PME seront épargnées, les principaux acteurs du Net seront également concernés, mais avec des obligations finalement plus en retrait. Sont cités les marketplaces comme Amazon ou eBay, les moteurs de recherche mais aussi les services de cloud qui devront mettre en place de mesures de sécurité tout en rapportant aux autorités les seuls « *incidents majeurs* » qui viendraient les impacter.

Le flou règne par contre sur les autres plateformes en ligne comme les réseaux sociaux. Selon l'eurodéputé, toutefois, « *cette directive marque le début de la régulation des plateformes. Alors que la consultation de la Commission européenne sur ces acteurs est toujours en cours, les nouvelles règles prévoient déjà des définitions concrètes – une demande du Parlement européen exprimée depuis le début des négociations –*, afin de faire connaître son consentement à l'inclusion des services numériques. »

En aout dernier, l'obligation de reporter aux autorités les incidents de sécurité avait soulevé les inquiétudes des représentants du secteur. Selon l'Afdel, l'association française des éditeurs de logiciels et de solutions Internet, une obligation indifférenciée de reporting « *pourrait porter atteinte à la compétitivité des entreprises du numérique, en particulier des entreprises françaises et européennes du numérique – dont de nombreuses PME, qui n'ont pas toute la capacité d'adaptation des grands groupes internationaux –, sans atteindre les objectifs poursuivis en termes de sécurité* ». L'ASIC, l'association des services Internet communautaires, avait craint pour sa part de voir chaque État membre devenir « *le Directeur des services informatiques de l'ensemble des acteurs du numérique* », du moins si des critères trop larges étaient inscrits en dur dans le texte final.

Le projet de directive doit maintenant être approuvé formellement par la Commission au marché intérieur du Parlement européen et par le Comité des représentants permanents.

Des obligations de reporting préexistent dans certains secteurs et en France

Suite à l'adoption du Paquet Télécom en Europe, rappelons que les opérateurs télécom doivent déjà notifier les fuites de données personnelles aux autorités de contrôle des données personnelles (la CNIL, ici). En France, l'Agence nationale de la sécurité des systèmes d'information chapeaute pour le compte du premier ministre, les règles de sécurité que doivent suivre les OIV, ces opérateurs d'importance vitale dont l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Depuis la loi de programmation militaire de 2013, centrales nucléaires, hôpitaux, sociétés de transports, acteurs des télécoms, etc. ont l'obligation de fournir « *les informations nécessaires pour évaluer la sécurité de ses systèmes d'information, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que les codes sources de ces logiciels.* »

Réagissez à cet article

Source : http://www.nextinpact.com/news/97630-directive-sur-cybersecurite-amazon-ebay-google-devront-notifier-leurs-incidents-majeurs.htm

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela est une nouvelle messagerie qui prétend qu'elle peut cacher les métadonnées. Le concept est encore très expérimental, mais il est assez prometteur.

Vuvuzela est un concept de messagerie qui permet de communiquer en cachant les métadonnées. Elle est développé par David Lazar, un doctorant du MIT qui travaille sur le chiffrement et les systèmes distribués. Il a publié un papier qui décrit les principes de Vuvuzela.
Des protocoles comme TOR permettent d'avoir un certain anonymat, mais il reste vulnérable à une analyse du trafic. Avec Vuvuzela, la messagerie est spécialement conçue pour se protéger contre la surveillance gouvernementale sur les métadonnées. La NSA a admis a plusieurs reprises qu'il ne sert à rien de chiffrer les données si les métadonnées sont en clair.

Les métadonnées englobe de nombreuses informations, mais on peut les résumer par le fait qu'elle pointent vers l'identité d'une personne et les contacts de cette personne. Vuvuzela veut cacher les métadonnées, mais elle ne peut pas cacher 2 métadonnées. La première est le nombre d'utilisateurs connectés sans une conversation et la seconde concerne les utilisateurs actifs dans une conversation. Mais Vuvuzela réduit également ce problème en ajoutant des nuisances aux métadonnées.
Le concept est intéressant, mais il n'est pas prêt pour le déploiement. On peut suivre le projet sur Github.

Réagissez à cet article
Source : http://actualite.housseniawriting.com/technologie/2015/12/04/vuvuzela-une-messagerie-qui-cache-les-metadonnees/11327/

Google For Education : un attrape-données personnelles ?

Google For Education : un attrape-données personnelles ?

Pour l'Electronic Frontier Foundation, Google profite de ses services Google For Education pour collecter et exploiter les données personnelles des élèves utilisateurs à son propre bénéfice et sans rapport avec l'enseignement. Google est pourtant signataire aux US d'un traité proscrivant ces pratiques.

Comme d'autres de ses concurrents, et notamment Microsoft, Google dispose d'une offre de services Cloud destinée spécialement aux acteurs de l'enseignement : Google For Education. Ce secteur est également un des principaux débouchés, aux Etats-Unis, pour le Chromebook.
Etudiants et enseignants sont depuis toujours des cibles de choix pour les fournisseurs de technologies. Mais Google pourrait aussi avoir un autre intérêt à être présent sur ce marché, un intérêt directement lié à son cœur de métier : la collecte et l'exploitation des données personnelles.

Chrome Sync par défaut sur Chromebook

Pour l'Electronic Frontier Foundation (EFF), Google a incontestablement dépassé les bornes en matière de données personnelles et surtout renié ses propres engagements. L'organisation vient à ce titre de saisir aux Etats-Unis le régulateur, la FTC.
En cause, les pratiques de la firme de Mountain View dans le cadre de son offre Google For Education. Selon l'EFF, Google piétine le « Student Privacy Pledge », un pacte signé par 200 entreprises, dont Google et qui encadre strictement les pratiques des fournisseurs en matière de confidentialité des données dans l'univers de l'enseignement.
Le « Student Privacy Pledge » proscrit ainsi la collecte, la conservation, l'utilisation et le partage des données personnelles des élèves hors des finalités touchant à l'enseignement. Google ne suivrait pas les règles en la matière, et ce de trois façons, juge l'EFF.
D'abord, lorsque les élèves se connectent avec leur compte Google for Education, la firme collecte les données personnelles des services non liés à l'enseignement et pour des finalités ne relevant pas non plus de l'enseignement.
Deuxième infraction : les ordinateurs Chromebooks disposent d'une fonctionnalité de synchronisation activée par défaut dans Chrome. Ce paramétrage permet ainsi à Google de collecter et d'exploiter intégralement l'historique de navigation, entre autres, des étudiants utilisant Google For Education. Et une fois encore sans que ces collectes de données relèvent des finalités admises.

Des pratiques trompeuses pour l'EFF

Enfin, Google a prévu dans les paramétrages d'administration de sa suite de services des paramètres autorisant sur les Chromebooks le partage des données des étudiants avec Google ainsi que des tiers. Or, le « Student Privacy Pledge » n'autorise pas un tel partage et une telle option n'aurait donc pas même dû être prévue à cet effet.
L'EFF demande donc au régulateur américain d'ouvrir une enquête sur les « agissements ou pratiques injustes et trompeurs » de Google, mais aussi d'exiger de la firme de détruire toutes les données des étudiants collectées jusqu'à présent en violation du « Student Privacy Pledge ».
Et cela pourrait faire beaucoup de données personnelles. Comme le rappelle ComputerWorld, Google revendiquait en octobre plus de 50 millions d'utilisateurs (élèves et enseignants) de Google For Education et 10 millions d'étudiants sur Chromebook.
Contacté par ComputerWorld, Google esquive les accusations formulées par l'EFF. La firme se déclare confiante dans le fait que ses outils respectent à la fois la loi et ses promesses, dont le Student Privacy Pledge.
Mais comme le signale l'EFF, Google a déjà reconnu au moins une mauvaise pratique et s'est engagé auprès de l'association à retirer l'activation par défaut de Chrome Sync sur les Chromebooks vendus aux établissements scolaires.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/google-for-education-un-attrape-donnees-personnelles-39829148.htm

Les solutions VPN touchées par une faille sur la redirection de ports

Les solutions VPN touchées par une faille sur la redirection de ports

Suivre
nVpn.net @nVpnNet
Fixed a possibility to exploit a VPNs PF feature revealing a user’s real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy
01:07 – 27 Nov 2015
4 4 Retweets 2 2 j’aime

La société de sécurité Perfect Privacy a averti hier dans un billet de blog que bon nombre de solutions VPN étaient vulnérables à des attaques par redirection de port. De fait, un grand nombre d'utilisateurs pourraient voir leurs adresses IP réelles être dévoilées par des pirates utilisant les mêmes réseaux.

Les VPN, ou réseaux privés virtuels, sont conçus pour permettre laccès à des ordinateurs distants. Ils sont également souvent utilisés pour masquer les adresses IP dorigine. Mais il n'est finalement pas très compliqué d'obtenir quand même cette information, surtout quand les solutions existantes autorisent la redirection de port et qu'elles ne sont protégées contre des attaques utilisant cette fonctionnalité.

La faille « #VPN Fail »

Hier, la société Perfect Privacy a averti qu'un grand nombre de solutions VPN pouvaient révéler ces adresses IP si un pirate savait où chercher.

Pour que l'attaque fonctionne, il doit se trouver sur le même réseau virtuel que sa victime et connaître son adresse IP de sortie.

Comme l'indique The Hacker News, cette étape est assez simple puisqu'il suffit d'attirer l'utilisateur sur un site évidemment contrôlé par le pirate. Si la redirection de port est activée, le pirate pourra obtenir l'adresse IP réelle de la victime en l'amenant à ouvrir par exemple une image. À partir de là, il devient possible de rediriger le trafic vers un port là encore contrôlé par le pirate, d'où le nom de l'attaque.

Cette faille de sécurité, nommée « VPN Fail » par Perfect Privacy, a donné lieu à un avertissement lancé à de nombreux éditeurs. La plupart sont donc informés et le tir a été corrigé pour des solutions comme Private Internet Access, Ovpn.to et nVPN. Ce dernier est pour le moment le seul à avoir confirmé officiellement que cétait le cas, comme en atteste le tweet ci-dessous.

Perfect Privacy indique cependant que toutes les solutions n'ont pas été testées et que le nombre de produits vulnérables est donc sans doute important.

Clients VPN, systèmes dexploitation, BitTorrentLa faille pose évidemment un vrai problème de sécurité et de vie privée. Les VPN sont très utilisés dans les pays par exemple où la censure est importante, notamment parce qu'ils bloquent le repérage de la géolocalisation.

En conséquence, une faille qui laisserait apparaître la véritable adresse IP ne peut que briser tout l'intérêt de ces solutions et on peut espérer que des correctifs seront rapidement déployés.

La dangerosité de la faille est grande selon Perfect Privacy, puisqu'à cause de la nature même de la faille, on risque de la retrouver dans un très nombre de produits, dont les systèmes d'exploitation.

Elle peut également être utilisée pour piéger des internautes qui se serviraient de BitTorrent. La technique s'exploite d'ailleurs plus rapidement puisque le pirate n'a pas besoin d'amener l'utilisateur sur un site. Il doit simplement se trouver sur le même VPN et avoir activé la redirection de port.

nVpn.net @nVpnNet

Fixed a possibility to exploit a VPNs PF feature revealing a user's real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy

01:07 – 27 Nov 2015

4 4 Retweets 2 2 j'aime

Rien à faire pour linstant du côté de lutilisateur

Dans tous les cas, la victime n'a pas besoin d'avoir l'option activée, et il n'y a donc rien qu'elle puisse faire de son côté. Tous les protocoles liés au VPN, comme OpenVPN et IPSec, sont également concernés. La seule solution est actuellement d'attendre, jusqu'à recevoir une notification de son fournisseur de solution VPN, si bien entendu ce dernier prend la peine de communiquer.

Réagissez à cet article

Source : http://www.nextinpact.com/news/97495-vpn-fail-solutions-vpn-touchees-par-faille-sur-redirection-ports.htm

Objets connectés, des cadeaux aussi pour les pirates informatiques

Objets connectés, des cadeaux aussi pour les pirates informatiques

Les pirates informatiques pourraient se frotter les mains avec l'arrivée des fêtes de fin d'année et parmi les cadeaux, des millions de nouveaux et potentiellement vulnérables appareils connectés à internet.

Drones, bracelets de fitness, montres et appareils électroménager « intelligents »… n'importe quel appareil connecté « peut être un point d'entrée pour accéder à votre réseau informatique.
Même si s'introduire dans un accessoire vestimentaire connecté ou un drone ne semble pas apporter grand chose aux pirates, cela peut ensuite servir de porte d'entrée à un smartphone et aux appareils auxquels il se connecte…
Une fois l'accès ouvert aux ordiphones, ordinateurs ou smartphones, les pirates pourraient facilement y installer des virus qui aspirent tous les mots de passe qui transitent sur votre réseau et les renvoient directement au pirate…
Beaucoup des gadgets électroniques proposés aux consommateurs , lorsque les sécurités sont activées, utilisent malheureusement des connexions peu sécurisées et recourent souvent de manière minimale à des mots de passe ou autres moyens d'authentification peu difficiles à percer.
Quand on reçoit ces nouveaux jouets qui brillent pour Noël, on veut juste commencer à s'en servir.
Avec la frontière de plus en plus floue entre travail et loisirs, les salariés risquent davantage de ramener des documents d'entreprise sensibles chez eux et que parfois, rien qu'en se connectant au réseau wifi de la maison, ils exposent des documents sur tout internet.
Le cabinet de recherche Gartner estime que 6,4 milliard d'objets connectés seront utilisés dans le monde en 2016, soit 30% de plus que cette année, et que leur nombre grimpera à 20,8 milliards d'ici 2020.
Juniper Research prédit pour sa part que les ventes de « jouets intelligents » atteindront 2,8 milliards de dollars cette année, tout en notant que « les vendeurs se reposeront probablement sur l'expertise de fournisseurs extérieurs de logiciels pour éviter des désastres en termes de relations publiques causés par des pirates ».

Alors, avant de profiter de votre nouveau joujou, prenez un peu de temps et assurez-vous d'avoir suffisament de sécurité en place sur votre appareil, vos communications, votre réseau… car une fois que vous aurez mis en route l'appareil et commencé à échanger des données, il sera trop tard pour faire marche arrière. Vous vous serez plutôt concerntré sur son utilisation.

Réagissez à cet article
Source : Denis JACOPINI

https://www.lesnewseco.fr/2015/11/21/science-high-tech/les-pirates-informatiques-pourraient-sinviter-pour-noel-5359.html

Comment protéger au mieux les données clients des cyberattaques ?

Comment protéger au mieux les données clients des cyberattaques ?

Les derniers piratages des données bancaires de plus de 1,3 millions de clients Orange, les 83 millions de données de clients volées à la banque américaine JP Morgan Chase ou les menaces d'hackers de divulguer l'identité de 36 millions d'utilisateurs du site de rencontres canadien Ashley Madison… Tous ces épisodes démontrent que les cyber-attaques menacent aujourd'hui fortement la liberté individuelle et les données personnelles.

Elles viennent également rappeler qu'aucune entreprise, même bien protégée, n'est aujourd'hui en mesure de garantir à 100% la sécurité des données qu'elle manipule. Face à ce constat, les entreprises doivent changer la façon dont elles peuvent rapidement détecter et répondre en utilisant de nouvelles solutions plus précises, plus actionnables pour les équipes de sécurité.
C'est un véritable enjeu pour les entreprises d'assurer à leurs clients la protection la plus fiable possible.
Voici 4 conseils aux entreprises pour protéger au mieux les données sensibles de leurs clients et les actions à mettre en place lors d'une attaque :
• Toute organisation chargée de la gestion des données personnelles très sensibles de leurs clients doit prendre ses responsabilités très au sérieux et protéger ainsi les données contre les accès non autorisés indésirables. Cela impliquerait de multiples niveaux de contrôles de sécurité au niveau de l'IT, peut-être en commençant par le cryptage des données personnelles alors qu'elles sont actives et en cours d'utilisation. Cette approche peut être efficace à la protection des données hautement sensibles, même si le réseau dans lequel elles résident est compromis. Cela peut paraître couteux à mettre en œuvre mais c'est une méthode de protection efficace.
• Il est capital d'avoir des processus et procédures internes qui garantissent l'accès physique aux centres de stockage de données sécurisées y compris de CLOUD. Les comptes d'utilisateurs inutilisés devraient être supprimés rapidement et les restrictions d'accès gérés de façon stricte pour s'assurer que tous les employés n'aient pas accès aux données de n'importe quel autre utilisateur.
• Nous pouvons également parler d'une nouvelle génération, solide dans son approche, permettant d'atténuer les menaces (en constante évolution) d'attaques malveillantes des réseaux d'entreprise provenant de l'extérieur. Les organisations "pirates" peuvent percevoir cela comme une énorme opportunité financière à voler les données personnelles détenues par quelque organisme que ce soit. Le fait d'avoir des défenses périmétriques fortes mises en place comme un pare-feu, des anti-virus sur toutes les stations de travail , d'une solution de filtrage d'e-mail, ou encore d'une solution IPS / IDS et un SIEM offrant la possibilité de surveiller les événements de toutes ces technologies en un seul endroit, ne restent malheureusement pas les plus fiables et beaucoup de sociétés ayant mis en place ces solutions ont quand même été attaquées, des brèches ont été exploitées car toutes ces solutions ne permettent pas d'arrêter tous les logiciels malveillants persistants qui vont compromettre un réseau en offrant la possibilité de se déplacer librement afin de trouver des données ciblées à voler.
• Là où les entreprises doivent se focaliser (en plus d'autres options internes déjà mentionnées), c'est de déployer une solution de détection des menaces plus intégrée qui peut extraire des informations à partir de plusieurs points dans le réseau, d'analyser ce qui se passe en temps réel (sur les stations de travail et sur le réseau) et défendre activement les réseaux d'entreprise avec la possibilité d'automatiser les réponses défensives générées en temps réel et 24 heures sur 24. Il y a encore à ce jour une réticence au niveau des comités exécutifs des entreprises de reconnaître la nécessité d'avoir un budget propre à la « Cyber Sécurité » mais qui permettrait de continuer à investir sur les dernières générations de solutions qui sont adaptées aux nouvelles menaces. Jusqu'à ce que cela change ; les cyber attaques vont continuer, les hackers utilisant des outils automatisés de pointe. Et nous continuerons de découvrir de nouvelles attaques de grandes ampleurs, quasiment tous les jours !

Réagissez à cet article
Source : http://www.infodsi.com/articles/157575/proteger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html

---

Le nombre d’attaques sur Mac a considérablement augmenté en 2015

Le nombre d’attaques sur Mac a considérablement augmenté en 2015

Selon l’étude d’un spécialiste de la sécurité, il y a eu plus d’attaques sur Mac en 2015 que durant ces cinq dernières années cumulées.

Jusqu’a présent, il s’agissait d’un archétype assez clair : les PC étaient plus vulnérables aux attaques que les Mac. Les détenteurs des ordinateurs Apple pouvaient alors se targuer de posséder un objet protégé des virus et autres logiciels malveillants.
Mais, selon une étude de Bit9 + CarbonBlack , spécialiste en sécurité informatique, cette idée est désormais mise à mal : « Jusqu’à présent, on a longtemps cru que les Mac faisaient face à beaucoup moins de risques de cyber-attaques que les PC et, jusqu’à très récemment, ce sentiment était plutôt correct. Les utilisateurs de Mac ont été, la plupart du temps, plus à l’abri que les utilisateurs Windows. Mais le vent est en train de tourner », indique la société qui affirme que le nombre de malwares ayant ciblé le système OS X d’Apple a bondit cette année.
En 2015, il y a même eu plus d’attaques sur OS X que durant les cinq dernières années cumulées.
948 malwares en 2015 Entre 2010 et 2014, l’OS d’Apple a été la cible de 180 logiciels malveillants, Bit9 + CarbonBlack indique qu’il y en a eu près de 948 cette année, soit « l’année la plus prolifique de toute l’histoire de l’OS X d’Apple ».
Si les attaques sont plus nombreuses sur le système Apple, c’est aussi parce qu’il y a de plus en plus de personnes qui ont acheté des Macs ces dernières années. Un revers de médaille en quelque sorte : ces engins sont devenus « mainstream » et se sont fortement implantés dans les entreprises.
Par exemple, le marché des OS sur desktop est certes dominé par Windows, mais Apple s’affiche désormais en 3e place parmi les systèmes les plus utilisés, avec 14,46% de parts de marché en 2015, contre 12,46% en 2014.
Si ces logiciels malveillants sont souvent découverts à temps par les entreprises et les chercheurs, il convient malgré tout aux utilisateurs de vérifier s’ils disposent d’un logiciel antivirus à jour, qu’ils soient des afficionados du PC ou du Mac.

Réagissez à cet article
Source : http://www.lesechos.fr/tech-medias/hightech/021447295747-le-nombre-dattaques-sur-mac-a-considerablement-augmente-en-2015-1171406.php