Un tiers des salariés communiquent des informations liées à son entreprise

Un tiers des salariés communiquent des informations liées à son entreprise

Les salariés prennent de plus en plus d'importance dans l'e-réputation RH de leur entreprise ! C'est ce que révèle l'infographie « Marque employeur : il est temps d'e-penser », produite par l'agence de marketing digital et éditorial Parlons RH, à partir de données croisées de différentes études.

33 % des salariés communiquent des informations liées à leur entreprise sur les réseaux sociaux.

Ce qui constitue une augmentation de 608 % en deux ans ! En tête des prises de parole par les salariés, 43 % des sondés communiquent des appréciations sur le management (+ 344 % en deux ans), 40 % discutent des appréciations sur la stratégie de l'entreprise (+ 640 % en deux ans) et 37 % portent des appréciations sur certains de leur collègues. Si les sentiments des salariés sont positifs ou neutres à 14 %, 6 % publient des avis négatifs sur l'entreprise.

Comment expliquer cette augmentation ? Les salariés possèdent une vie sociale virtuelle de plus en plus abondante. Surtout, seulement 29 % des salariés affirment qu'il existe une charte ou des règles internes sur l'usage des réseaux sociaux. 39 % des salariés affirment à l'inverse qu'il n'existe pas de charte ou de règles internes sur les réseaux sociaux, ou ne connaissent pas leur existence (34 %).

Pour plus de la moitié des sondés (60 %), les managers n'ont proposé aucune action concernant l'usage des réseaux sociaux. Seuls 21 % des managers ont proposé des formations, 9 % des réunions d'information, 6 % ont remis aux salariés un guide des bonnes pratiques et 4 % ont informé les salariés des risques pour l'entreprise.

Les avis influencent fortement les employés potentiels

Ces avis ont pourtant un fort impact sur la marque employeur, qui désigne la situation générale de l'e-réputation de l'entreprise pour ses salariés actuels, futurs et aux yeux de toutes les parties prenantes de l'entreprise. La marque employeur permet de rendre l'entreprise plus attrayante aux yeux de tous, et permet notamment de faciliter l'embauche.

Ainsi :

95 % des candidats se renseignent sur les entreprises avant de postuler.

4/5 des salariés ont déjà postulé après avoir lu des commentaires positifs en ligne sur une entreprise

1/3 des candidats refuserait un poste dans une entreprise à mauvaise réputation employeur.

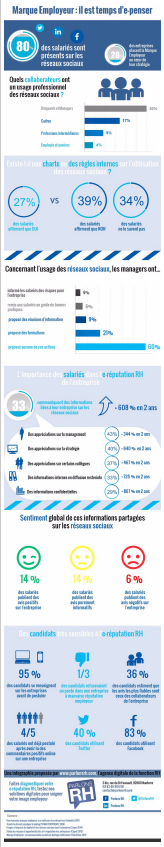
36 % des candidats estiment que les avis les plus fiables sur l'entreprise sont ceux des collaborateurs

Définir son identité et la diffuser efficacement sur lnternet permettraient ainsi d'embaucher plus facilement et d'avoir des salariés plus efficaces. Ce qui est important quand on sait qu'un recrutement raté coûterait entre 40 000 euros et 100 000 euros, selon Gwenaëlle Quénaon-Hervé, directrice générale adjointe du site Regionsjob.

Des outils et des méthodes existent pour l'utilisation des réseaux sociaux par les salariés

Même si des posts spontanés n'ont pas forcément objectif de nuire aux entreprises, les maitriser est aujourd'hui un enjeu de taille pour les sociétés afin d'éviter un bad buzz redoutable qui pourrait éloigner les meilleurs talents. Un point d'autant plus important que l'infographie explique que 80 % des salariés sont présents sur les réseaux sociaux.

D'où l'intérêt de sensibiliser et responsabiliser les employés pour en faire de véritables ambassadeurs pour les entreprises. Aux Etats-Unis, des programmes de sensibilisation des salariés se sont par exemple développés avec des fournisseurs de services et de logiciels qui aident les marques à responsabiliser les salariés dans les médias sociaux. Au programme : écoute ou surveillance des salariés, ou encore collaboration sociale, comme celle proposée par la société Jive.



Réagissez à cet article

Source : http://www.reputationvip.com/fr/blog/reseaux-sociaux-1-salarie-sur-3-communique-des-informations-liees-a-son-entreprise

Un pirate soupçonné du piratage de VTech arrêté

Un pirate soupçonné du piratage de VTech arrêté

Un jeune homme de 21 ans soupçonné d'être à l'origine du piratage des 6,4 millions de comptes d'enfants et 4,9 millions de comptes d'adultes, clients du fabricant de jouets VTech a été interpellé par la police britannique.

Suite au piratage des données personnelles de 11,3 millions de comptes clients du fabricant de jouet VTech, le plus grand vol de données concernant des enfants, la police anglaise indique avoir procédé à l'arrestation d'un jeune homme de 21 ans, soupçonné d'être à l'origine du délit. L'unité de cybercriminalité régionale du sud-est du Royaume-Uni a en effet indiqué dans un communiqué de presse ce mardi qu'elle avait arrêté un homme dans la ville de Bracknell, soupçonné d'avoir accédé sans autorisation aux serveurs et aux données de VTech. La ville, située à l'ouest de Londres, est un vivier pour les entreprises de haute technologie.
« Nous en sommes encore aux premiers stades de l'enquête et il y a encore beaucoup de travail à faire », indique Craig Jones, chef de l'unité de cybercriminalité régionale. Plusieurs équipements informatiques ont été saisis par la police.
Basée à Hong Kong, la société VTech est spécialisée dans les jeux ludo-éducatifs et propose depuis plusieurs années des tablettes tactiles adaptées aux enfants. Début décembre, elle avait été obligée de révéler que les données personnelles stockées dans les comptes de 6,4 millions d'enfants et 4,9 millions adultes avaient été copiées. Près de la moitié des victimes vivent en Europe.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-la-police-britannique-a-arrete-le-hacker-presume-des-clients-vtech-63293.html

Safe Harbor : les CNIL

européennes doivent choisir entre force ou faiblesse

Safe Harbor : les CNIL européennes doivent choisir entre force ou faiblesse

Sans base légale mais en acceptant de prendre « un risque », les CNIL européennes ont donné jusqu'à fin janvier à l'Union européenne et aux États-Unis pour s'accorder sur un autre cadre permettant l'export de données personnelles vers les USA. Mais l'ultimatum ne sera visiblement pas respecté, et les autorités administratives hésitent sur l'attitude à adopter, entre diplomatie, force ou faiblesse.

C'est dans une position délicate que la Cour de justice de l'Union européenne (CJUE) a plongé la CNIL et ses homologues du G29, lorsqu'elle a décidé le 6 octobre dernier d'invalider le Safe Harbor, qui permettait aux entreprises américaines comme Facebook d'importer chez elles les données des internautes européens. La plus haute juridiction de l'Union a de fait obligé les autorités de protection des données à choisir entre leur mission officielle de protection de la vie privée des citoyens, et leur contrainte officieuse de ne pas bloquer l'activité économique liée à l'exploitation des données personnelles.
Dans un arrêt protecteur des droits de l'homme tel que la CJUE les multiplie ces dernières années concernant Internet, la Cour a en effet jugé que les conditions n'étaient plus réunies pour être certain que les États-Unis respectent en droit et en fait la bonne protection des données personnelles des internautes européens traitées sur le sol américain. Elle a donc invalidé avec effet immédiat le Safe Habor qu'utilisaient des milliers d'entreprises américaines, dont Facebook, Google, ou Microsoft, ce qui aurait dû conduire à bloquer immédiatement tous les transferts de données vers les États-Unis, au moins le temps que les dossiers fondés sur d'autres mécanismes juridiques soient vérifiés et validés.

Or la CNIL et ses homologues ont décidé, sans aucune logique juridique mais par choix politique et pragmatique, d'octroyer aux États-Unis et à la Commission européenne un ultimatum fixé au 31 janvier 2016 pour négocier un nouveau Safe Harbor 2.0 assorti de nouvelles législations protectrices aux USA. « Quand nous avons appelé à une période de transition jusqu'en janvier, c'était un risque que nous avons pris ensemble. (…) Nous avons décidé de cette phase de transition afin de permettre à tous les acteurs du secteur de prendre leurs responsabilités », reconnaît aujourd'hui la présidente de la CNIL Isabelle Falque-Pierrotin, dans une interview à Euroactiv.

« Les transferts de données ne continueront pas à n'importe quel prix »

Mais les négociations traînent, et les États-Unis n'ont toujours pas proposé de législation qui permettrait notamment aux Européens de faire valoir leurs droits contre la NSA, lorsque celle-ci accède à leur données sans contrôle judiciaire. En principe, le Safe Harbor 2.0 (s'il aboutit) ne devrait donc pas être plus sécurisant que l'ancien, et n'aura aucune validité pour légaliser les transferts des données.

Interdire les transferts ? L'arme atomique

La menace de l'arme atomique de la suspension des transferts de données, brandie notamment en Allemagne, est donc théoriquement existante. Mais la CNIL peine à (se) convaincre d'une intention de l'utiliser, tant les enjeux économiques sont forts. « Nous souhaitons tous que les transferts de données continuent, parce qu'ils sont associés à des intérêts économiques et politiques très importants. Mais ils ne continueront pas à n'importe quel prix », prévient ainsi Mme Falque-Pierrotin.

Alors que le G29 avait demandé que des solutions juridiques soient trouvées avant la fin janvier 2016, le groupe se contente désormais d'exiger « un geste politique ».
« Je ne sais pas s'il sera possible de finaliser tout cela avant fin janvier, mais nous devons au moins recevoir un signe qu'ils ont compris le message des juges. Il ne s'agit pas de produire un Safe Harbor numéro deux. Il faut réellement tenir compte des arguments du juge, qui s'inquiète de la protection des données des citoyens européens aux États-Unis, quand les services de renseignement y ont accès », prévient la présidente du groupe des CNIL européennes.
Rendez-vous fin janvier pour voir quelles mesures seront effectivement prises.

Réagissez à cet article
Source : http://www.numerama.com/politique/134571-cnil-europeennes-safe-harbor-diplomatie-faiblesse.html

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

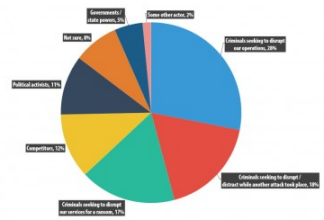
12% des attaques DDoS menées par des concurrents

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

Quelques pistes en prévention ou en curation d'attaque par

ransomwares

Quelques pistes en prévention ou en curation d'attaque par ransomwares

Un de vos clients est victime d'un ransomware. Cryptolocker, Cryptowall, Supercrypt, TeslaCrypt, … Peut importe le malware, le résultat est à peu prêt le même. Ses fichiers sont cryptés, et l'impact est énorme. Dans l'urgence, il convient de procéder correctement, en prenant certaines précautions. Je vais donc ici vous donner quelques pistes (un peu en vrac) afin de traiter au mieux le problème.

Sauvegarde
J'imagine que si vous consultez cet article, aucune sauvegarde de votre client n'est exploitable. Sinon, vous l'auriez remontée.
Cependant, avant d'envisager toute action sur le/les systèmes infectés, pensez à procéder à une sauvegarde. Je recommande d'arrêter immédiatement ces systèmes infectés. Ensuite, qu'il s'agisse d'un serveur, ou d'un simple client, clonez le disque dur.
Pour cela, effectuez un clone en mode hors ligne, avec un de ces outils par exemple : Acronis, Veeam, AOMEI.
Ca vous permettra d'effectuer les tests que vous voulez sur le clone, sans aucun risque.

Lister les fichiers cryptés
Un outil bien pratique permet de lister les fichiers cryptés par Cryptowall. En effet, cette infection stocke la liste des fichiers qu'elle crypte dans le registre. L'outil ListCWall permet de localiser et utiliser ces infos afin de vous sortir une liste des fichiers, et permet aussi de les exporter afin de les stocker par exemple sur un média externe avant de formater la machine si besoin.

Utilitaires de décryptage
Ce qu'il faut retenir de ce paragraphe, ce n'est pas autant la liste des outils (non exhaustive) que je vous propose, mais que de tels outils voient le jour périodiquement. Pensez à regarder du côté des éditeurs d'antivirus (ou sur Tech2Tech!!), si un nouvel outil existe concernant l'infection que vous avez à traiter en particulier. En effet, suite à des enquêtes internationales, parfois, des réseaux tombent. Et lorsque les services en charge de ces enquêtes découvrent un lot de clés de cryptages, les éditeurs d'antivirus peuvent les exploiter afin de les intégrer dans des outils de décryptage. Pas sur que ca fonctionne donc (si la clé utilisée ne fait pas partie de celles qui ont été découvertes) mais vous pouvez le tenter…
On peut lister par exemple :
RectorDecryptor chez Kaspersky (pour le ransomware Rector)
XoristDecryptor chez Kaspersky (pour le ransomware Xorist/Vandev)
ScatterDecryptor chez Kaspersky (pour le ransomware Scatter)
ScraperDecryptor chez Kaspersky (pour le ransomware Scraper)
RakhniDecryptor chez Kaspersky (pour le ransomware Rakhni)
Ransomware Decryptor chez Kaspersky (pour le ransomware Coinvault/Bitcryptor)
Decryptor 0-1.3 chez Bitdefender (pour le ransomware Linux.Encoder.1)
DecryptCryptoLocker par FireEye et Fox IT (pour le ransomware CryptoLocker)
TeslaDecrypt par Cisco Talos Security Intelligence (pour le ransomware TeslaCrypt)

Récupérer les fichiers
A ma connaissance, si vous n'avez pas de sauvegardes, et que le ransomware n'a pas d'outil de décryptage dédié ayant été élaboré, il y a peu de chances de retrouver les fichiers.
Cependant, deux pistes peuvent s'avérer intéressantes :

Shadow Volume Copies
Les shadow copies (service de clichés instantanés), peuvent s'avérer utiles dans le cas d'un ransomware. Cependant, il faut déjà que le service soit activé et configurée correctement. Ensuite, la majorité des ransomware un peu élaborés et récents désactivent ce service, et vont effacer les snapshots déjà présents. S'ils s'avèrent utilisables, le logiciel Shadow Explorer sera pratique pour récupérer les fichiers.

Récupération de données
Il semblerait que, dans le cas de certains ransomware, les fichiers soient copiés, cryptés, puis supprimés. Il serait alors envisageable, si la machine est arrêtée au plus vite, de récupérer des fichiers à l'aide d'un utilitaire de récupération de données.
Pour cela, clonez d'abord le disque par précaution, en mode hors ligne (Live CD).

Se protéger des ransomwares
Plusieurs éditeurs de solutions de sécurité proposent des utilitaires plus ou moins élaborés afin de se protéger contre un cryptage de données.
Il y a d'abord une approche qui consiste à interdire le lancement d'exécutables situés dans %APPDATA%. C'est en effet un mode de fonctionnement courant de ce type de malwares. Cette fonction est proposée par Bitdefender à travers son outil gratuit Anti-Cryptowall. Personnellement cet utilitaire ne m'a pas vraiment convaincu lorsque je l'ai essayé, puisque j'ai pu lancé des exe situés dans %APPDATA%…
CryptoPrevent, utilitaire développé par Foolish IT permet de se prémunir d'une attaque par un CryptoLocker. Cependant, la version gratuite nécessite des mises à jours manuelles visiblement. Voyez plutôt vos besoins sur les différentes versions commerciales.
BitDefender a intégré dans sa version grand public 2016 un moteur d'analyse de cryptage. Le but est d'analyser en temps réel une éventuelle activité de cryptage sur la machine, et de la stopper. Cette fonction sera intégrée dans les antivirus pro maximum en début d'année 2017.
Pour ma part, je suis distributeur des solutions Panda Security Cloud. Et un outil a été mis au point durant l'été : Adaptive Defense 360. Venant en renfort de n'importe quel antivirus, ce produit permet de bloquer tous les logiciels que l'entreprise n'a pas décidé explicitement de laisser fonctionner sur son parc. Il en résulte une protection quasi parfaite, même si ca a un coût. Et comme il faut bien manger, je me fais au passage une petite pub : n'hésitez pas à me contacter si vous désirez vous équiper de cette solution!
Ce ne sont évidement que des exemples, non exhaustifs. Mais ils traduisent la diversité des solutions élaborées afin de contrer les ransomwares et cryptolockers, qui sévissent actuellement de manière dramatique.

Réagissez à cet article
Source : http://www.tech2tech.fr/ransomware-avec-cryptage-quelques-pistes/

Comment un cybercriminel peut infiltrer votre réseau

Comment un cybercriminel peut infiltrer votre réseau

La sécurité est plus que jamais une priorité pour les entreprises, contribuant activement à sa réussite. Les RSSI doivent désormais s'assurer que leurs projets en matière de sécurité IT sont en phase avec les objectifs de l'entreprise.

Nous sommes tous connectés à Internet, ce qui est très positif. Mais ce lien permanent implique que nous sommes tous au cœur d'un écosystème de grande envergure. Il est essentiel de comprendre que tout ce qui touche une organisation impactera également de nombreuses autres entreprises, et notamment ses partenaires. Ainsi, en cas de piratage d'une entreprise, ce sont des données personnelles identifiables qui sont détournées. Ces données peuvent être revendues à des spécialistes de l'usurpation d'identité ou constituer un terreau favorable aux attaques de phishing. Plus l'assaillant disposera d'informations sur vous, plus l'email qu'il vous enverra apparaîtra comme légitime et vous incitera à cliquer sur un lien malveillant.

Notons que les tactiques d'attaques actuelles sont similaires à celles d'il y a quelques années : récupération de mots de passe faibles, attaques de type phishing et téléchargement de logiciels malveillants à partir de sites web infectés ou de publicités malveillantes. Sauf qu'aujourd'hui, l'assaillant a gagné en furtivité et en efficacité lorsqu'il mène son attaque.

Penchons-nous, par exemple, sur les réseaux sociaux et les services en ligne. Nous sommes très nombreux à les utiliser, qu'il s'agisse de Facebook, de LinkedIn, ou encore des sites de rencontres en ligne. Les assaillants l'ont parfaitement compris et capitalisent sur la fibre émotionnelle de chacun. Ils établissent ainsi leur passerelle d'entrée vers les dispositifs des utilisateurs en s'aidant de ces sites et de techniques d'ingénierie sociale. Ainsi, si les méthodes d'ingénierie sociale restent les mêmes, les vecteurs et la surface d'attaque ont, en revanche, progressé. Parallèlement, ce sont les techniques de furtivité qui ont gagné en précision, avec des assaillants toujours plus aptes à se dissimuler. Se contenter d'utiliser les antivirus traditionnels n'est donc tout simplement plus suffisant.
Parmi les techniques utilisées, l'attaque de type phishing est la méthode principale pour s'immiscer au sein des réseaux d'entreprise.
Un email de phishing, conçu pour paraître le plus légitime possible, est envoyé avec un fichier joint ou une URL malveillante, et incitant l'utilisateur à ouvrir le fichier ou à cliquer sur l'URL.
L'attaque par téléchargement furtif (ou drive–by attack) est une autre technique utilisée par les assaillants. Ces derniers piratent un site Web et y installent un script java malveillant qui redirigera l'utilisateur vers un autre site hébergeant un logiciel malveillant téléchargé en arrière-plan vers l'équipement de l'utilisateur. Dans le cas d'une attaque ciblée, les assaillants peuvent passer des mois à identifier les sites Web les plus consultées par les organisations ciblées, pour ensuite les infecter.
Le malvertising (publicité malveillante) compte également parmi les techniques utilisées. Cette attaque emprunte les codes des attaques drive-by, mais l'assaillant se focalisera sur l'infection des sites de publicités. Il devient possible d'infecter un seul de ces sites qui, à son tour, pourra infecter jusqu'à 1 000 autres sites Web. Ou l'art d'industrialiser son attaque.
Enfin, n'oublions pas l'attaque mobile. Nombre de ces attaques sont similaires à celles mentionnées plus haut, mais elles ciblent les dispositifs mobiles. Notons qu'il est possible d'infecter un dispositif mobile via un message SMS, ou à l'aide d'un logiciel malveillant qui se présente en tant qu'application ludique ou de contenu pour adultes.
Lorsque l'assaillant est rentré dans un réseau et qu'il réside sur le dispositif d'un utilisateur (ordinateur de bureau ou portable, équipement mobile), il doit désormais injecter de nouveaux logiciels malveillants et outils pour mener à bien sa mission. Généralement, les informations de valeur ne sont pas stockées sur les postes de travail, mais plutôt sur les serveurs et des bases de données. Voici donc un aperçu des étapes supplémentaires pouvant être mises en œuvre par un cybercriminel déjà présent dans le réseau :

1. Téléchargement d'autres outils et logiciels malveillants pour compromettre davantage le réseau.
2. Exploration du réseau pour identifier les serveurs hébergeant les données ciblées. Recherche du serveur Active Directory contenant tous les identifiants d'authentification, dans l'objectif de pirater ces données, véritable sésame pour le cybercriminel.
3. Une fois les données ciblées identifiées, recherche d'un serveur provisoire pour y copier ces données. Le serveur idéal est un serveur stable, à savoir toujours disponible, et disposant d'un accès sortant vers Internet.
4. Exfiltration furtive et lente de ces données vers les serveurs des assaillants, généralement déployés dans le cloud, ce qui rend la neutralisation des communications plus complexe.

Les cybercriminels présents au sein du réseau sur une longue durée pourront obtenir tous types d'informations disponibles puisque les données d'entreprise, dans leur grande majorité, sont archivées sous format électronique. Plus le cybercriminel est présent sur le réseau, plus il en apprend sur les processus et les flux de données de votre entreprise. L'attaque Carbanak qui a ciblé de nombreuses banques dans le monde en est la parfaite illustration. Lors de cette exaction, les cybercriminels sont remontés jusqu'aux ordinateurs des administrateurs ayant accès aux caméras de vidéosurveillance. Ils ont ainsi pu surveiller de près le fonctionnement du personnel bancaire et enregistrer tous les processus dans le détail. Ces processus ont été reproduits par les cybercriminels pour transférer des fonds vers leurs propres systèmes.

Comme déjà souligné, une brèche dans le réseau s'initie généralement par un simple clic d'un utilisateur sur un lien malveillant. Après avoir investi le poste de l'utilisateur piraté, l'assaillant commence à explorer le réseau et à identifier les données qu'il souhaite détourner. C'est dans ce contexte que la notion de segmentation de réseau devient essentielle. Cette segmentation permet de maîtriser l'impact d'un piratage puisque l'entreprise victime peut isoler la faille et éviter tout impact sur le reste du réseau. D'autre part, elle permet de cloisonner les données sensibles au sein d'une zone hyper-sécurisée qui rendra la tâche bien plus complexe pour ceux qui souhaitent les exfiltrer.

Pour conclure, gardons à l'esprit qu'il est impossible de protéger et de surveiller le réseau dans sa totalité, compte tenu de son périmètre étendu et de sa complexité. Il s'agit donc d'identifier les données les plus sensibles, de les isoler et de porter son attention sur les chemins d'accès vers ces données.

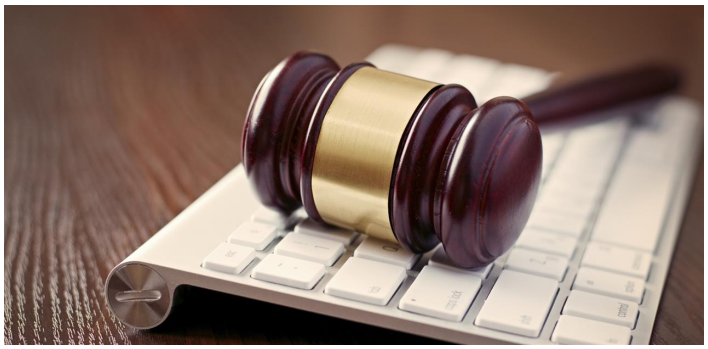
Réagissez à cet article
Source : http://www.globalsecuritymag.fr/Comment-un-cybercriminel-peut,20151209,58191.html

---

Ne pas avertir son employeur de propos injurieux sur Facebook devient une faute grave

Ne pas avertir son employeur de propos injurieux sur Facebook devient une faute grave

La cour d'appel de Lyon a confirmé le mois dernier le licenciement d'une salariée accusée d'avoir tenu sur Facebook des propos dégradants et injurieux à l'égard de ses collègues de travail. L'employeur n'a pourtant pas réussi à prouver que la personne mise en cause était bien l'auteur des messages délivrés sur un groupe spécialement créé à cet effet. Explications.



Travaillant en tant que sellière maroquinière depuis 2002 chez Hermès, Madame X est licenciée en décembre 2011 pour faute grave. C'est-à-dire sans préavis ni aucune indemnité. Il faut dire que les reproches formulés par son employeur sont relativement sérieux.

La salariée est en effet accusée d'avoir ouvert en octobre 2011 un groupe Facebook intitulé « Les potins d'Hermès », sur lequel étaient relatées des « *situations tenant à la vie privée de certains collaborateurs nommément désignés* », « *sous forme de messages et anecdotes* ». C'est suite à des remontées internes que la direction a eu vent de ces commentaires jugés « *profondément dégradants et injurieux* » à l'égard des employés concernés, ce qui a poussé les responsables de l'entreprise à chercher à remonter jusqu'à leur auteur.

Problème : l'administrateur de ce groupe dispose d'un compte Facebook au nom de « Jules César ». Autrement dit, il s'agit d'un beau pseudonyme… Après enquête, l'employeur affirme que l'adresse IP de l'auteur de ces messages correspond à celle du domicile de Madame X. Dans un premier temps, la salariée reconnaît avoir eu connaissance de ce groupe, tout en niant en être à l'origine. Mais dans un second temps, elle finit par admettre que le compte « Jules César » et le groupe « Les potins d'Hermès » ont bien été crées depuis son ordinateur, mais par sa sœur…

« *Même dans le cas où les déclarations de votre soeur (par ailleurs très limitées quant à son hypothétique implication personnelle) [seraient] avérées, et dans la mesure où vous nous avez déclaré avoir eu connaissance de la création de la page et de son contenu dès sa mise en ligne, vous auriez dû à tout le moins nous alerter au sujet d'une telle initiative dont la teneur et la portée ne pouvaient rester sans conséquence vis-à-vis de l'entreprise et de ses collaborateurs* » retient ainsi l'employeur dans sa lettre de licenciement.

Impossible d'identifier le créateur du groupe

Sauf que l'ex-salariée estime avoir été remerciée à tort. Elle a donc tout d'abord saisi le conseil des prud'hommes de Lyon, lequel a confirmé le licenciement pour faute grave en novembre 2013. Madame X a ensuite saisi la cour d'appel de Lyon, qui a justement rendu sa décision le 20 octobre dernier.

Les magistrats se sont intéressés en particulier aux adresses IP fournies par Hermès. Ils ont cependant constaté que la connexion ayant servi à créer le profil Jules César et à alimenter « *la plupart* » des messages litigieux correspondait en fait à « *une adresse IP algérienne dont l'employeur n'a pu identifier le titulaire* ». En clair, il était impossible de prouver en l'état qu'il s'agissait de Madame X ou même de sa soeur.

Mais cela n'a pas empêché la cour d'appel de considérer qu'il y avait malgré tout eu faute grave de la part de la salariée. Cette faute ? Savoir que le groupe « Les potins d'Hermès » existait et n'avoir rien signalé. La décision, que nous avons pu consulter, retient en ce sens que « *la faute commise par Mme X en n'alertant pas sa direction sur la création de ce groupe de discussion alors qu'à partir de son propre ordinateur étaient mis en ligne des propos déshonorants pour ses collègues de travail (…) est d'une gravité suffisante pour rendre impossible le maintien de cette salariée dans l'entreprise pendant la durée limitée du préavis* ».

La cour d'appel n'a donc pas donné suite aux demandes de l'ex-salariée, qui réclamait plus de 40 000 euros d'indemnités.

Réagissez à cet article

Source : http://www.nextinpact.com/news/91031-propos-injurieux-sur-facebook-ne-pas-avertir-son-employeur-peut-etre-faute-grave.htm

Les opérateurs satellitaires européens nient leur rôle dans la fourniture d’Internet à Daesh

Les opérateurs satellitaires européens nient leur rôle dans la fourniture d’Internet à Daesh

Outil central dans la machine de propagande de Daesh, Internet permet de recruter au-delà des frontières. Pour se connecter, les terroristes utiliseraient les capacités de satellites européens.

Dans une enquête publiée le week-end dernier, le journal allemand Spiegel Online pointe du doigt plusieurs acteurs de l'Internet satellitaire européens (SES, Avanti et le français Eutelsat) pour leur rôle supposé dans la fourniture d'une connexion au Web à Daesh. Alors que les géants du Net Google, Facebook ou Twitter sont appelés à contenir la propagande de l'organisation terroriste, se pose ici la question de son accès au réseau.

Et cette question est centrale dans la lutte contre le terrorisme, car Internet est l'un des vecteurs principaux utilisés par Daesh pour embrigader ses futures recrues. L'organisation diffuse sur les réseaux sociaux grand public ses messages de propagande, qu'elle adapte dans les langues locales, afin de toucher le plus de gens.

Des paraboles turques

Selon le Spiegel, l'organisation terroriste contourne le mauvais état des infrastructures Internet des zones qu'elle contrôle – en Syrie et en Irak – en se connectant par satellite, au moyen de paraboles achetées dans des pays frontaliers, dont la Turquie. En tant que prestataires techniques situés en amont de la chaîne, les opérateurs satellitaires se sont défendus de connaître les clients finaux, voire d'avoir pris des précautions.

C'est le cas d'Eutelsat, seul à avoir réagi publiquement

Le français, contrôlé à 26 % par l'État via la Caisse des dépôts, apporte dans un communiqué deux « clarifications ». Premièrement, il « n'a pas de contact avec des utilisateurs finaux », deuxièmement, « son réseau de distribution n'inclut aucun fournisseur de services en Syrie ». Eutelsat souligne qu'en 2013, il a interdit aux distributeurs de fournir des services Internet en Syrie.

Coordonnées GPS

Pourtant, lorsque les équipements fournis par les FAI se connectent aux satellites, ces derniers reçoivent des coordonnées GPS. Des informations censées permettre, en théorie, de pouvoir remonter la piste. Ainsi selon le Spiegel, de telles connexions sont bel et bien réalisées depuis le territoire de Daesh, dont Raqqa, la capitale autoproclamée, ou encore la ville de Mossoul, en Irak. Mais du côté des opérateurs satellitaires, aucun signal.

L'opérateur luxembourgeois SES a déclaré ne « pas (avoir) connaissance que ses satellites sont utilisés par l'EI ou dans des zones syriennes contrôlées par l'EI » et que si tel était le cas, il mettrait « tout en œuvre pour y mettre fin ». Eutelsat, lui, dit « n'avoir aucune connaissance d'utilisation de ses ressources par Daesh ». Si l'Internet satellitaire était coupé, il enrayerait la propagande, mais aussi les efforts de résistance des civils.

Réagissez à cet article

Source : http://pro.clubic.com/actualite-e-business/actualite-789264-eutelsat-daesh.html

Le blog du journal The Independent victime de malvertising, la faute à Flash

Le blog du journal The Independent victime de malvertising, la faute à Flash

L'un des blogs du quotidien britannique The Independent a été victime d'un piratage et l'un de ses encarts publicitaires redirigeait les utilisateurs vers un logiciel malveillant. La meilleure parade pour l'internaute lambda ? Tenir Adobe Flash à jour.

La société Trend Micro alerte sur son blog d'une attaque visant l'un des blogs du quotidien britannique The Independent. Dans un post daté de mercredi, la société de cybersécurité fait état d'une cyberattaque ayant visé le blog du quotidien américain britannique The Independent. La source de l'infection provient selon Trend Micro de l'un des blogs WordPress du quotidien : les chercheurs de Trend Micro ont ainsi remarqué que celui-ci redirigeait les utilisateurs vers une page de l'Angler Exploit Kit. Celui-ci tentait par la suite d'exploiter une vulnérabilité au sein d'Adobe Flash afin d'installer un logiciel de type rançongiciel sur la machine des utilisateurs affectés.
Selon un porte-parole de The Independent interrogé par la BBC, l'infection était causée par une opération de malvertising : en conséquence, les administrateurs du site ont donc bloqué l'affichage de publicité sur la page incriminée en attendant que le problème soit résolu. Le quotidien britannique précise que rien ne laisse entendre que des utilisateurs du site ont pu être affectés par l'attaque.

Adobe Flash : usual suspect

L'attaque n'a rien d'inhabituel : au contraire, on a plutôt affaire à un cas d'école assez représentatif des nouveaux moyens d'infections utilisés par les cybercriminels. D'une part, la technique du malvertising se démocratise : cette méthode consiste pour les cybercriminels à se faire passer pour des régies d'annonceurs publicitaires afin de pouvoir exploiter les outils de marketing programmatique pour faire apparaître leurs pages web malveillantes sur des sites à forte audience.
Dailymotion a ainsi été récemment victime de ce type d'attaque, qui gagne en popularité ces derniers mois. Les attaquants ont également eu recours à l'Angler Exploit Kit, le kit d'exploit le plus populaire actuellement parmi les cybercriminels. Véritables couteaux suisses des pirates, ces outils se présentent sous la forme de plateformes mises à jour afin d'exploiter facilement les vulnérabilités récemment découvertes dans les programmes populaires, Adobe Flash étant l'une des cibles favorites.
Enfin, le malware distribué appartient à la catégorie des ransomware, ou rançongiciel en français : le bien connu Cryptolocker. Celui-ci permet à l'attaquant de chiffrer l'ensemble des données sur le disque de la victime, données qui ne seront déchiffrées qu'en l'échange d'une rançon de 499$.
Pour l'utilisateur, la meilleure protection possible reste de veiller à conserver son navigateur et ses différents programmes à jour. Tout particulièrement Flash : on en profite pour signaler qu'une nouvelle mise à jour a été publiée par Adobe et corrige un peu plus de 70 failles de sécurités affectant le logiciel d'Adobe. Celui-ci étant la cible de choix des cybercriminels, on peut également envisager la suppression pure et simple du logiciel pour les plus paranoïaques.
Adobe annonçait d'ailleurs récemment amorcer la mise à la retraite de sa technologie, qui semble de moins en moins pertinente à l'heure de HTML5. Pour les victimes de ransomwares tels que cryptolocker, certaines sociétés de cybersécurité proposent des utilitaires permettant de decrypter les fichiers chiffrés par le logiciel malveillant, mais le fonctionnement n'est pas garanti.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/le-blog-du-journal
-the-independent-vi
ctime-de-malvertising-la-faute-a-flash-39829632.htm