Alerte vigilance – Ransomware Lockyx

Alerte vigilance – #Ransomware Lockyx

Bonjour, Une vague d'attaques du ransomware Locky touche actuellement de nombreuses entreprises dans le monde et depuis peu en France.Voici nos conseils pour se protéger contre cette nouvelle menace :

CONSEIL N°1 : VIGILANCE UTILISATEUR

Informez vos collaborateurs de l'importance de ne pas ouvrir la pièce jointe d'un email envoyé par un expéditeur inconnu. Soyez très vigilant notamment avec les pièces jointes .zip, .doc, .xls : sources de propagation de Locky.
Les sensibiliser à l'utilisation des macros et/ou les désactiver, source de propagation de Locky.

CONSEIL N°2 : SOLUTION DE PRA

Assurez-vous que vos machines sont correctement sauvegardées, et les images externalisées pour une restauration rapide en cas d'attaque.
Les équipes ESET sont mobilisées à l'heure actuelle pour vous apporter une solution rapide et continue contre ce ransomware et ses multiples variantes quotidiennes.
Note : si vos machines sont déjà infectées, isolez-les des autres, initiez leur restauration et lancez une analyse complète de vos systèmes.
Cordialement,
L'équipe ESET
… [Lire la suite]

Réagissez à cet article

Source : *Alerte vigilance – Ransomware Lockyx*

Moyens pour les entreprises de (re)gagner la confiance des clients

Moyens pour les entreprises de (re)gagner la confiance des clients

Chaque citoyen a un rôle à jouer au niveau de la sécurité. La connaissance des fonctionnalités de sécurité, la sauvegarde de nos données et le maintien à jour des logiciels de sécurité, des systèmes d'exploitation, applications et navigateurs Internet, ne sont que quelques-unes des précautions que chacun devrait prendre sur tous ses appareils.

Lorsque ces bases ne sont pas respectées, ou si nous téléchargeons et communiquons des informations personnelles via la dernière application incontournable sans être sûrs de sa source, nous prenons simplement un énorme risque avec nos propres informations. Bien que de plus en plus de particuliers prennent conscience de ce qu'ils doivent faire pour sécuriser leurs données, comment pouvons-nous être sûrs que ces dernières sont traitées correctement lorsqu'elles sont communiquées à des entreprises? Afin de regagner la confiance de leurs clients et de l'opinion publique, les entreprises doivent travailler sur plusieurs points.

• Assurer la transparence et la confidentialité des données constamment ;
• Contrôler et chiffrer les données où qu'elles soient, stockées ou en transit;
• #GDPR : Investir pour respecter la conformité**GDPR :** (GDPR #General Data Protection Regulation / #Projet de règlement européen sur la protection des données personnelles)

Réagissez à cet article

Source : *Données personnelles: 3 moyens pour les entreprises de (re)gagner la confiance des clients | FrenchWeb.fr*

Projet de règlement européen relatif à la protection des données personnelles (en anglais GDPR General Data Protection Regulation)

Projet de règlement européen relatif à la protection des données personnelles (en anglais #GDPR #General Data Protection Regulation)

1/ Qu'est-ce que le GDPR ?
Il s'agit de l'acronyme anglais d'un nouveau règlement européen modifiant le cadre juridique relatif à la protection des données personnelles au sein de l'union européenne, effectif début 2015. Il impactera toutes les entreprises collectant, gérant, ou stockant des données et aura pour but principal de simplifier et harmoniser la protection des données dans les 28 pays de l'union européenne. En cas de non respect du règlement par les entreprises, des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial seront applicables.
L'objectif du GDPR est de faire face aux nouvelles réalités du marché, notamment en matière de protection des données liée aux réseaux sociaux ou encore au cloud computing, Les notions de transferts de fichiers sécurisés et de droit à l'oubli font également parti du GDPR.
Le développement des clouds privés, publics, ou encore de solutions hybrides a compliqué le stockage et le traitement des données au cours de ces dernières années. Le GDPR clarifiera les responsabilités de chaque entreprise en contact avec les données, facilitant ainsi la mise en conformité.

2/ Actuellement, comment les organisations gèrent-elles les impératifs de protection des données ? Existe-t-il des différences en fonction des pays ?
Chaque pays détient sa propre autorité de protection des données pour le moment. Puisque le GDPR est un règlement et non une directive, il s'appliquera directement à tous les pays de l'UE sans avoir besoin de changer les législations nationales.
Le GDPR aura un impact significatif sur les compagnies non-européennes opérant sur le sol européen, puisqu'il s'appliquera aussi bien aux compagnies européennes qu'aux non-européennes commerçant dans l'UE, reflétant ainsi la réalité actuelle : le business est sans frontière.

3/ Quel sera l'impact sur les entreprises ?
Les entreprises devront repenser la manière dont elles collectent, traitent et stockent les données.Il sera obligatoire de tenir à disposition des internautes dont les données sont stockées un texte clair expliquant la politique de sécurisation des données. Les entreprises devront également pouvoir leur fournir toutes leurs données personnelles dans un format simple et transférable via internet. Bien sur le droit à l'oubli devra également rendre possible la suppression rapide de toutes les données. Cette partie du règlement influence déjà certaines sociétés, comme Facebook et Google qui se préparent peu à peu au GDPR.

4/ Les entreprises sont elles prêtes pour la mise en place de ce règlement ?
Il semble que peu d'entreprises soient prêtes. Selon un sondage Ipswitch réalisé fin 2014 sur 316 entreprises européennes, 52% des sondés ont répondu ne pas être prêts. Plus grave encore 56% ne savaient pas exactement à quoi correspond le sigle GDPR.
Par ailleurs, 64 % des personnes interrogées ont reconnu n'avoir aucune idée de la date d'entrée en vigueur supposée de ce règlement. Seules 14 % des personnes interrogées ont pu indiquer clairement que le GDPR est censé entrer en vigueur début 2015.Autre point préoccupant : 79% des sondés font appel à un fournisseur cloud, mais seulement 6% ont pensé à demander à leur prestataire s'il était en règle avec le règlement européen.

5/ Que peuvent faire les entreprises pour s'assurer qu'elles sont en conformité avec le GDPR ?
Plusieurs mesures peuvent être prises pour s'assurer de la conformité de sa structure informatique. Les contrats avec tous les prestataires informatiques, notamment les fournisseurs de services cloud, doivent être passer en revue. Il faut s'assurer que, pour chaque information collectée, une demande de consentement soit effectuée et enfin il est nécessaire de savoir précisément où les données sont stockées.Une fois les processus en règle, l'entreprise pourra demander un certificat européen, valable 5 ans, attestant sa conformité au GDPR.* Enquête en ligne réalisée en octobre 2014 par Ipswitch, à laquelle ont répondu 316 professionnels de l'informatique (104 du Royaume-Uni, 101 de France et 111 d'Allemagne).

Réagissez à cet article

Source : *Projet de règlement européen (en anglais GDPR General Data Protection Regulation) – Fil d'actualité du Service Informatique et libertés du CNRS*

Safe Harbor & Privacy Shield : Comment l’entreprise peut avoir le contrôle complet de son propre cloud ?

	Safe Harbor & Privacy Shield : Comment l’entreprise peut avoir le contrôle complet de son propre cloud ?

L'invalidation de l'accord Safe Harbor a provoqué une certaine incertitude chez de nombreuses entreprises qui ne savent plus comment sauvegarder leurs données en toute sécurité et légalité – tout en les mettant à la disposition de leurs collaborateurs.

Début février, l'accord Safe Harbor 2.0 – surnommé Privacy Shield – a vu le jour, mais de nombreux doutes sur sa légitimité subsistent.
Dans ce contexte, l'incertitude demeure au sein des entreprises qui se posent de nombreuses questions autour de la conformité et ne savent pas si le Privacy Shield sera une solution sur le long terme. Il est toutefois possible de contourner les problématiques liées à l'instabilité de telles réglementations en trouvant la bonne solution – ainsi qu'un fournisseur de services adapté.

Il existe deux alternatives pour sauvegarder et utiliser ses données en toute sécurité dans le cloud sans se soucier de problématiques de conformité.
D'une part, l'entreprise peut rechercher un fournisseur de cloud computing exploitant ses Data Centers dans un pays européen. D'autre part, les entreprises sont tout à fait capables de constituer leur propre cloud et d'y mettre leurs données, ressources informatiques et applications à la disposition de leurs collaborateurs. Le marché du stockage externe offre de nombreuses solutions pour ces deux approches. Le rôle, pour tous les grands acteurs sur le marché, étant d'offrir aux clients une sauvegarde et un partage parfaitement sûrs de leurs données dans le cloud.

Les utilisateurs du cloud doivent pouvoir faire entièrement confiance à leur fournisseur de services
Dès qu'une entreprise prend la décision d'utiliser une architecture cloud public pour stocker une partie de ses informations, elle doit trouver un fournisseur adapté à ses exigences mais également irréprochable en termes de fiabilité.
La priorité dans cette démarche, lorsque l'on souhaite éviter des soucis de conformité, est de s'assurer que le fournisseur mette à disposition ses centres de données en Europe. En outre, l'entreprise est parfaitement en droit de demander si la sauvegarde de données de son fournisseur est effectuée exclusivement dans ses propres centres de données ou s'il en fournit une copie à d'autres centres de données d'un pays tiers. L'évaluation des accords de niveau de service (SLA), de la méthode et de la chronologie de sauvegarde appliquée pour telles ou telles données mais aussi des conditions de leur récupération sont des points à examiner lors du choix du fournisseur.
Cela permet d'établir une solution de confiance entre l'utilisateur et son service cloud. C'est sur la base de cette confiance et de la garantie que leurs données ne quittent pas l'Europe que les utilisateurs peuvent opter pour différents services de cloud.
D'autre part, l'utilisateur doit impérativement veiller à ce que le fournisseur utilise un encodage afin d'écarter tout risque d'utilisation abusive (intentionnelle ou aléatoire) de ses données.

L'entreprise peut avoir le contrôle complet de son propre cloud
La deuxième option garantie une sauvegarde et un partage des données parfaitement sûrs dans une architecture cloud, et confère donc à l'entreprise le plein contrôle sur ses informations et services numériques. Légèrement plus complexe, cette option consiste à créer sa propre architecture cloud privée.
L'entreprise devra certes gérer davantage de ressources, mais elle pourra puiser pleinement dans les services mis à disposition, les droits d'accès, la sélection des applications et l'assistance technique. Ces avantages garantiront une meilleure flexibilité aux collaborateurs de l'entreprise, ainsi que des outils nécessaires pertinents pour faciliter leurs tâches et les mêmes droits d'utilisation que s'ils travaillaient dans un cloud public. La sécurité des données et des appareils sera également garantie conformément aux mesures internes prises par l'entreprise.
Un cloud privé n'est pas concerné par les effets de Privacy Shield et permet d'utiliser différents services basés sur le cloud computing. En effet, les applications telles que « Box » ou « Dropbox » ne devraient plus être utilisées dans un environnement influé par de telles réglementations.

La pratique BYOD est une tendance très actuelle dans le monde de l'entreprise, mais elle complique l'intégration des terminaux dans les procédures de sauvegarde et rend difficile un contrôle complet sur toutes les informations de l'entreprise. L'utilisation combinée d'un cloud privé et de solutions d'accès, de synchronisation et de partage des fichiers est susceptible de remédier à cela. Les collaborateurs pourront ainsi accéder en toute sécurité aux données depuis n'importe quel terminal, les synchroniser et les partager avec leurs collègues, clients, partenaires et fournisseurs.
Un tel logiciel peut remplacer le serveur FTP et permet, par exemple, le libre-service en créant différents comptes utilisateurs tout en déchargeant les tâches de l'administrateur. L'intégration de solutions MDM facilite la gestion des appareils portables et assure un contrôle souple des données et des comptes.
Via l'utilisation d'une bonne solution d'accès, de synchronisation et de partage, le responsable informatique peut mettre en place une meilleure gouvernance des données en établissant des droits d'accès mais peut aussi retracer le transfert ou le partage éventuels des données concernées.
Les entreprises désireuses d'utiliser un cloud parfaitement sûr et de conserver le plein contrôle de leurs ressources et données opteront donc pour un cloud privé et des applications adaptées aux besoins de leurs collaborateurs et personnel informatique.

La sécurité doit être la priorité absolue
La débâcle provoquée par l'invalidation du Safe Harbor a permis de tirer une leçon très importante. La sécurité et la confidentialité des données doivent être des priorités absolues, quelle que soit la solution choisie par une entreprise, qu'il s'agisse d'un cloud privé ou public. Les informations numériques doivent donc impérativement être encodées avant de quitter l'entreprise ou – mieux – le réseau protégé. Une procédure de sauvegarde, par exemple, offre déjà une certaine protection, mais pour toutes les entreprises désireuses d'empêcher définitivement tout accès illicite à leurs données personnelles ou d'entreprise, l'encodage est une priorité absolue. Seul un encodage efficace est apte à garantir la protection et la sécurité des données … [Lire la suite]

Réagissez à cet article

Source : *Safe Harbor & Privacy Shield : comment assurer la conformité ? – JDN*

Stocker des données pendant des milliards d’années est désormais possible

Stocker des données pendant des milliards d’années est désormais possible

---

Des chercheurs de l'université de Southampton ont annoncé avoir créé une technologie permettant « d'enregistrer des données en cinq dimensions et de les stocker pendant des milliards d'années ».

Les données sont sauvegardées sous forme de « nanostructures » gravées sur un disque de verre à l'aide d'un laser ultrarapide, dit « laser femtoseconde ». Le procédé permet d'encoder des informations en cinq dimensions: les trois coordonnées spatiales, la taille et l'orientation des nanostructures. Ces dernières modifient le trajet de la lumière à travers le verre et sa polarisation, ce qui permet ensuite de lire les données sauvegardées en utilisant à cet effet un microscope optique et un polariseur.

© FLICKR/ A HEALTH BLOG

Les pensées humaines dévoilées en temps réel par un ordinateur

Le support, dit « disque 5D », est capable de stocker jusqu'à 360 téraoctets d'information et ce, à des températures allant jusqu'à 1.000°C. Selon les inventeurs de cette technologie, il peut également rester opérationnel pendant 13,8 milliards d'années à une température ambiante.

Les scientifiques de Southampton avaient déjà présenté leur innovation en 2013, mais ils n'avaient à l'époque réussi à enregistrer qu'un fichier texte de 300 kilooctets. Depuis, ce mode de stockage a considérablement évolué, ce qui a permis d'enregistrer en 5D la Déclaration universelle des droits de l'homme, l'Optique de Newton, la Magna Carta et la Bible.

« Il est fascinant de penser que nous avons créé une technologie permettant de sauvegarder et de stocker des documents et des informations pour les générations futures. Grâce à cette technologie nous pouvons être sûrs que notre civilisation, tout ce que nous avons appris ne sera pas oublié », a déclaré le professeur Peter Kazansky, du Centre de recherche en optoélectronique (ORC) de Southampton… [Lire la suite]

Réagissez à cet article

Source : *Stocker des données pendant des milliards d'années*

est désormais possible

Apple condamné à créer un firmware spécial pour le FBI

Apple condamné à créer un firmware spécial pour le FBI

Le tribunal de Californie a ordonné à Apple de fournir au FBI les moyens technologiques pour accéder au contenu en clair d'un téléphone utilisé par l'auteur de la tuerie de San Bernardino. Apple ne devra pas déchiffrer lui-même, mais supprimer une protection d'iOS 8 qui permet d'éviter les tentatives d'accès par force brute.

À la demande du FBI, un tribunal de Californie a ordonné mardi à Apple de fournir une « assistance technique raisonnable » aux enquêteurs de la police fédérale, qui cherchent à accéder au contenu en clair du téléphone de l'auteur de la tuerie de San Bernardino, Syed Rizwan Farook. Cette attaque terroriste avait fait 14 morts le 2 décembre 2015.

Estimant que ses principes de protection de la confidentialité des données de ses clients étaient indérogeables, Apple avait refusé d'apporter son concours actif au déchiffrement de l'iPhone 5C du suspect, dont le contenu est illisible tant qu'il n'est pas débloqué. La firme de Cupertino se dit de toute façon incapable de déchiffrer le contenu, puisque la clé est générée et stockée sur le téléphone lui-même, et qu'il n'a donc pas davantage la main que les experts en cryptologie des services de renseignement américains.

FAIRE SAUTER LA PROTECTION APRÈS 10 TENTATIVES INFRUCTUEUSES

Mais le FBI a obtenu de la justice qu'Apple l'aide autrement. L'entreprise dirigée par Tim Cook devra fournir une mise à jour du firmware, qui fasse sauter la protection du téléphone contre les tentatives abusives d'accès (il n'est pas précisé comment une telle mise à jour pourrait être installée). En effet le suspect avait activé sur son smartphone la fonctionnalité de sécurité d'iOS qui fait qu'après 10 saisies erronées de codes PIN, le contenu du téléphone est automatiquement effacé.

Apple devra fournir au FBI le moyen de modifier le système iOS sur l'iPhone 5c de Farook, pour que la fonction d'effacement du contenu du téléphone ne soit pas activée. Le FBI espère ainsi opérer par force brute pour deviner le mot de passe à force de tentatives répétées, et ainsi gagner l'accès au contenu en clair du téléphone.

APPLE DEVRAIT FAIRE APPEL

Par ailleurs, toujours dans le même objectif, Apple devra fournir au FBI le moyen de tester rapidement plusieurs combinaisons, pour éviter d'avoir à construire un robot qui tape lui-même lentement les codes les uns après les autres. Avec quatre chiffres pour le code PIN, 10 000 combinaisons sont possibles.

Selon la BBC, Apple devrait toutefois faire appel de la décision. L'entreprise craint certainement que sa coopération soit interprétée comme la fourniture d'un backdoor à l'administration américaine, qui minerait la confiance qu'ont les clients dans la protection apportée par Apple.

« Apple n'a jamais collaboré avec une quelconque autorité publique, de quelque pays que ce soit, afin de créer une « porte dérobée » dans ses produits ou services », peut-on lire sur le site officiel d'Apple. « Sur les appareils sous iOS 8 ou ultérieur, vos données personnelles sont protégées par votre code. En effet, pour ces appareils, Apple ne peut répondre aux demandes d'extraction de données iOS émanant des autorités : les fichiers à extraire sont protégés par une clé de chiffrement liée au code de l'utilisateur, auquel Apple n'a pas accès ».

… [Lire la suite]

Réagissez à cet article

Source : *Apple condamné à créer un firmware spécial pour le FBI – Politique – Numerama*

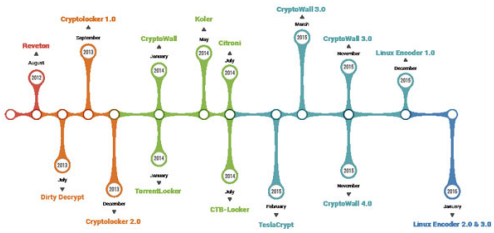
Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données

Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données

---

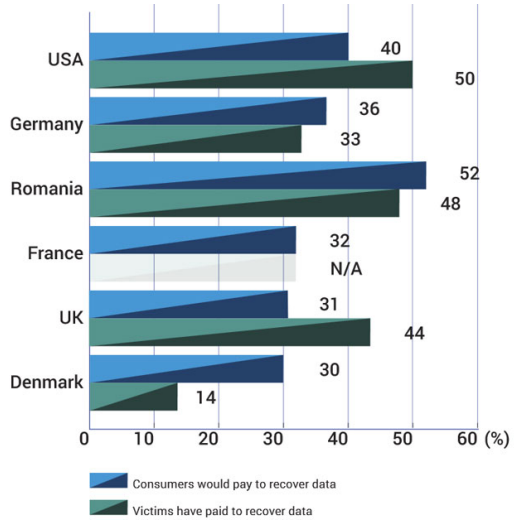
Le ransomware est une catégorie de programme malveillant qui une fois installé chiffre les données du PC et exige de son propriétaire qu'il paie une rançon pour les récupérer. Et les victimes seraient, pour une bonne partie d'entre eux, disposées à payer cette rançon.
Si vous étiez victime d'un ransomware (ou rançongiciel), paieriez-vous la rançon exigée pour récupérer vos fichiers ou enverriez-vous les cybercriminels promener ? Le fait que vous soyez au travail ou à votre domicile ferait-il une différence ?

Selon une étude, le comportement des victimes de ransomware pourrait bien dépendre du lieu où celles-ci se trouvent lorsque la demande de rançon leur parvient. Ce qui varierait également, c'est le montant de cette rançon.



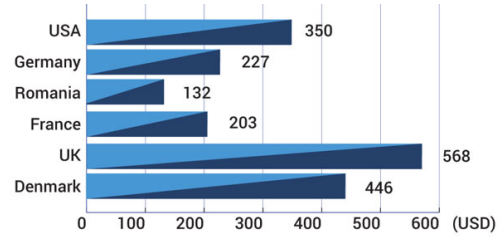
32% des sondés français paieraient pour leurs fichiers.
Comme son nom le suggère, le ransomware va chiffrer les fichiers enregistrés sur l'ordinateur compromis. Menaçant les utilisateurs de l'impossibilité de récupérer ces documents, les cybercriminels exigent le versement d'une rançon. Une fois celle-ci versée, promesse serait faite de déchiffrer les données des victimes.

Et d'après une étude de l'éditeur de sécurité Bitdefender, tous les internautes, en fonction de leur nationalité, ne sont pas égaux face à ces logiciels malveillants. Ainsi aux Etats-Unis, 50% des victimes de ransomware ont accepté de payer.
En France ? Cette donnée n'est pas disponible. En revanche, 32% des internautes français interrogés déclarent qu'ils paieraient en cas d'infection. Cette part dépend aussi, très logiquement, de l'importance accordée aux fichiers devenus inaccessibles en raison du chiffrement.



Par exemple, 18% des répondants du Royaume-Uni paieraient pour les documents personnels, 17% pour les photos personnelles et seulement 10% pour les documents liés au travail » détaille BitDefender.

Accepter de payer est une chose, mais quel montant ? Sur ce point aussi, les sommes varient très significativement d'un pays à un autre. Au Royaume-Uni, une victime accepterait de verser jusqu'à 568 dollars, contre 203 dollars en France.



Payer la rançon aide juste les cybercriminels
Un tel comportement consistant à céder aux cybercriminels est-il cependant recommandé ? Catalin Cosoi, responsable de la stratégie sécurité de BitDefender, déconseille de payer. « Alors que les victimes sont généralement enclines à payer la rançon, nous les encourageons à ne pas à se livrer à de telles actions, car cela contribue uniquement à soutenir financièrement les développeurs du malware. »
En janvier, à l'occasion du FIC 2016, le directeur de l'Anssi a évoqué l'infection du ministère des Transports par un ransomware. Et Guillaume Poupard était formel : « On ne paie pas, ce n'est pas une solution raisonnable. »
Pourquoi ? Notamment, car le cybercriminel peut tout à fait choisir de ne pas livrer les clefs nécessaires au déchiffrement des fichiers, et rien ne garantit non plus qu'il ne relancera pas une nouvelle attaque ultérieurement. Les sauvegardes restent donc la meilleure parade face à ces malwares, préconise l'Anssi … ***[Lire la suite]***

Réagissez à cet article

Source : *Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données*

Un ransomware paralyse un hôpital américain

Un #ransomware paralyse un hôpital américain

La France n’est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d’une attaque similaire à celle relayée dans la presse au ministère des Transports en début d’année.

La France n’est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d’une attaque similaire à celle relayée dans la presse au ministère des Transports en début d’année.

Le système informatique de l’hôpital a été infecté par des cyberattaquants ayant recours à un malware de type ransomware (ou rançongiciel) : celui-ci chiffre les données contenues sur la machine et les rend inaccessibles à l’utilisateur, qui se voit contraint de verser une rançon afin d’espérer récupérer l’accès à ses fichiers. Sans système de sauvegarde fonctionnel, la situation peut rapidement devenir critique et cela semble être le cas de cet hôpital, dont les services administratifs se retrouvent paralysés depuis une semaine comme le relatent les médias locaux.

Si l’attaque n’a pas entièrement bloqué le traitement des patients, mais environ 900 nouveaux entrants ont été redirigés vers d’autres hôpitaux en attendant que le problème soit résolu.

L’attaque n’est, selon les déclarations du directeur de l’établissement, pas directement ciblée contre l’hôpital. Il s’agirait plutôt d’une attaque classique, issue d’un utilisateur peu précautionneux ou d’une politique de sécurité informatique défaillante.

Néanmoins, plusieurs sources expliquent que les cybercriminels exigent le versement de 9000 bitcoins afin de déchiffrer les données retenues par le malware.

Un plan sans accroc?

Et on avoue être un peu surpris : effectivement, les ransomwares sont une menace en pleine expansion et le ministère des Transports a récemment été victime d’une attaque de ce type. En revanche, le succès de ce nouveau type de menace tient à un modèle économique bien rodé. Les auteurs d’attaques par ransomware visent généralement un large panel de cibles et demandent des rançons relativement modérées, afin de s’assurer que les victimes pourront les payer.

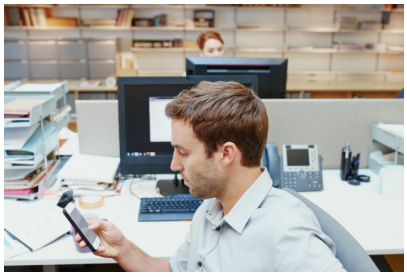
9000 bitcoins, même pour un hôpital de grande taille, paraissent être une somme inhabituelle pour une demande de rançon. Cela ne représente pas moins de 3,6 millions de dollars. L’information n’a pas été confirmée par les sources officielles en charge du dossier ou par la communication de l’hôpital, prudence donc avant de tirer des conclusions hâtives. Gageons que si cette information venait à se vérifier, le FBI ne conseillera pas de simplement payer la rançon pour résoudre le problème.

Rançon extravagante ou non, les dégâts sont réels pour l’hôpital : le directeur explique ainsi que les formalités administratives et le renseignement des dossiers médicaux se fait maintenant à la main en attendant que le système informatique soit rétabli… [Lire la suite]

Réagissez à cet article

Source : *Quand un ransomware paralyse un hôpital américain*

Comment motiver vos salariés par l’e-réputation ?



Comment motiver vos salariés par l'e-réputation ?

La marque employeur n'est pas un concept tout nouveau mais il serait bien dommageable de la négliger pour autant. Avec l'apparition et la démocratisation des réseaux sociaux, il est nécessaire aujourd'hui d'envisager une numérisation de cette marque employeur si l'on ne veut pas se laisser dépasser et garder la main sur son « e-réputation ».

Parmi les canaux de communication autour de la marque employeur, il y a ceux que l'entreprise peut directement maîtriser (le site web, le profil LinkedIn, etc.) et ceux sur lesquels elle n'a pas la main (les comptes personnels des collaborateurs sur les réseaux sociaux). Or, les avis des collaborateurs sont considérés comme plus fiables que la communication officielle. Il est plus naturel de faire confiance à des témoignages individuels qui seront, à tort ou à raison, considérés comme plus authentiques.
En dépit de ce constat, beaucoup d'entreprises tardent à « numériser » leur marque employeur et subissent leur e-réputation plus qu'ils ne la construisent. Seules 28 % des entreprises (enquête StepStone) donnent une place centrale à la communication numérique au cœur de leur stratégie. Pourtant, beaucoup ont conscience de l'importance de celle-ci sur le recrutement puisque 79 % des employeurs prévoient de s'investir dans cette direction.
Pour commencer, il serait judicieux d'identifier, en interne, les collaborateurs engagés et volontaires et de les inviter à participer à la communication numérique sur la marque employeur. Il convient aussi d'encourager, former et conseiller les moins sensibilisés à la question.

L'usage des réseaux sociaux par les employés

En 2014, encore 20 % des salariés français n'étaient pas présents sur les réseaux sociaux selon l'étude Cegos sur l'impact du digital dans l'entreprise. Soit par manque d'intérêt, soit par crainte de divulguer leurs informations personnelles.
Si les 80 % restants eux, utilisent les réseaux sociaux, beaucoup en ont avant tout un usage personnel et peu y voient une utilité professionnelle. Parmi ceux qui ont décidé d'en faire un outil de travail cependant, on retrouve en grande majorité des cadres, des dirigeants et des managers. Les raisons d'utiliser les réseaux sociaux dans un but professionnel sont pourtant multiples :
• Entretenir et agrandir son réseau professionnel
• Exercer une veille professionnelle
• Rechercher un emploi / recruter de nouveaux collaborateurs
• Etc.
30 % des directeurs et managers s'en serviraient même pour « véhiculer une image positive de leur entreprise » !
Malgré cette tendance à communiquer sur leur entreprise, les salariés sont méfiants : 38 % craignent des répercussions de la part de leur employeur. Et pour cause, nous avons tous entendu parler de cas de licenciements, abusifs ou non, suite à des messages publiés par des usagers imprudents…
Paradoxalement, les salariés acceptent de plus en plus d'être en relation avec leur hiérarchie et leurs collègues sur les réseaux sociaux. 46 % d'entre eux seraient « amis » avec leur patron ou certains membres de la direction !

L'importance d'un accompagnement

Plus d'un salarié sur trois publierait des informations à propos de son entreprise sur les réseaux sociaux. Ces messages vont de simples appréciations sur les produits ou services proposés par l'entreprise à la diffusion d'informations confidentielles, en passant par des avis donnés sur la stratégie, le cadre de vie, l'ambiance, etc. Les salariés s'expriment de plus en plus au sujet de leur entreprise sur internet et cela peut être une force autant qu'une faiblesse pour la réputation de l'employeur.
Les conséquences sur l'e-réputation peuvent être importantes si des dispositifs d'accompagnement ne sont pas mis instaurés. Dans les faits, seuls 6 % des entreprises ont remis un guide de bonnes pratiques sur les réseaux sociaux et 9 % auraient organisé des réunions d'information sur le sujet.

Il serait pourtant temps d'y penser ! On identifie **3 conséquences majeures d'une mauvaise e-réputation** sur la marque employeur :
• Un problème de recrutement (une entreprise dont l'image est mauvaise sur Internet n'apparaît pas comme attractive)
• Une démotivation du personnel
• Une augmentation des coûts due à la création d'un poste spécifique de chargé de veille et e-réputation

Une bonne e-réputation apporte de bons candidats

Dans leur recherche d'emploi, les candidats se renseignent sur la réputation de l'entreprise avant de postuler. Ils se rendent sur les sites web et les comptes officiels des entreprises sur les réseaux sociaux en premier lieu.
L'une des premières conséquences d'une mauvaise réputation pour une entreprise est économique. Pour travailler dans une société à la réputation "peu séduisante", les candidats réclament un supplément salariat minimum de 5 %, selon une étude de LinkedIn sur la marque employeur, publiée en septembre dernier.
Par ailleurs, plus d'un tiers des candidats français refuseraient catégoriquement un poste dans une entreprise affligée d'une mauvaise réputation employeur, quel que soit le supplément salarial proposé.
60 % des salariés à plein temps affirment que la perception d'une entreprise qu'ils connaissent peut s'améliorer s'ils entendent ou lisent des commentaires positifs de la part de personnes travaillant dans leur secteur d'activité. De quoi confirmer que les collaborateurs sont bel et bien les meilleurs ambassadeurs de la marque employeur… [Lire la suite]

Réagissez à cet article

Source : *L'importance de l'e-réputation pour motiver vos salariés | Mieux*

Un site Internet pour le règlement en ligne des litiges

Si vous avez un problème concernant un achat en ligne, vous pouvez utiliser ce site pour essayer d'obtenir un règlement extrajudiciaire.
Pour l'utiliser, vous devez vivre dans l'Union Européenne et le professionnel concerné doit y être établi
Les professionnels de certains pays peuvent également utiliser ce site pour déposer plainte contre un consommateur concernant un bien ou service vendu en ligne. … [Lien vers le site https://webgate.ec.europa.eu]

Réagissez à cet article

Source : *Accueil – Règlement en ligne des litiges*