Comment effacer ses données personnelles sur les moteurs de recherche ?

	Comment effacer ses données personnelles sur les moteurs de recherche ?

Lorsque vous êtes sur Internet, vous êtes suivi à la trace et vos données sont transformées en outil marketing. Il faut donc penser à supprimer les données personnelles et privées, indiquées sur les moteurs de recherche pour préserver un sa vie privée.

Suite à l'arrêt de la Cour de Justice de l'Union Européenne (CJUE) en date du 13 mai 2014, vous disposez de deux moyens pour supprimer les informations vous concernant sur Internet.

Déposez une requête auprès du site d'origine
Il est possible de contacter directement le responsable du site d'origine en vous référant directement aux conditions générales du portail ou aux mentions légales. Si vous ne parvenez pas à avoir ces informations, utilisez sans tarder la base de données publique « whois ». Lorsque vous avez en main les coordonnées recherchées, il vous suffit d'adresser un courrier exposant votre souhait et l'impact de la publication de vos données personnelles sur votre vie privée.
Le site dispose d'un délai de deux mois pour vous répondre. S'il refuse ou s'il ne répond pas, vous pouvez envoyer une plainte à la CNIL avec une copie de la missive expédiée au responsable du site et sa réponse.
Même si vous avez réussi à supprimer vos données personnelles sur un site, les résultats des moteurs de recherche peuvent également conserver des traces de celles-ci durant une certaine période. Il s'agit de « caches », c'est-à-dire des copies des pages visitées par les robots d'indexations des moteurs de recherche.
Si vous tombez encore sur vos données après que le contenu jugé litigieux ait été retiré par le responsable du site d'origine, pas de raison de paniquer ! Cela vient du fait que ces robots ne parcourent les sites que toutes les deux à trois semaines environ. D'ailleurs, Google et Bing proposent des procédures pour faire disparaitre définitivement ces caches. Il suffit de suivre les procédures indiquées pour faire disparaître ces données personnelles des résultats de recherche.

Adressez-vous directement au moteur de recherche
En parallèle, il est possible pour un internaute de demander au moteur de recherche un déréférencement d'une page qui porte atteinte à sa vie privée ou à son e-réputation. Pour le cas de Google, il suffit de remplir un formulaire afin de solliciter que le géant américain supprime les résultats de recherche qui se rapportent à vos données. Il en est de même pour Bing, le moteur de recherche de Microsoft. Comme pour le cas précédent, vous pouvez saisir la CNIL en l'absence de réponse ou si vous n'êtes pas satisfait de la réponse apportée.
Bien qu'il soit possible d'effacer les données personnelles publiées en ligne, mieux vaut rester prudent et réfléchir à deux fois avant de vous identifier sur un site ou de divulguer des informations privées.

Réagissez à cet article

Source : *Comment effacer ses données personnelles sur les moteurs de recherche ?*

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:
• Téléchargement d'autres outils et logiciels malveillants pour compromettre davantage le réseau.
• 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.
• 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.
• 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 : *Comment un cybercriminel peut infiltrer votre réseau | Data Security Breach*

Que trouve-t-on dans le darknet ?

Que trouve-t-on dans le darknet ?

Sur le darknet, les pages Internet ne sont pas indexées. Vous ne pouvez donc pas les trouver via les moteurs de recherche classiques, comme Google ou Yahoo par exemple. Vous ne pouvez pas non plus y accéder par votre navigateur habituel, comme Internet Explorer ou Mozilla. Ces pages ne répondent pas au codage classique du genre « .fr » ou « .net ». Elles se terminent par « .oignon » : pour que les échanges soient anonymes sur cet Internet caché, il faut passer par une multitude de relais, comme plusieurs couches d'un oignon.

Tous ces relais expliquent pourquoi sur le darknet la connexion est plus longue. Au départ, cet Internet fantôme qui garantit l'anonymat a été créé pour aider à la liberté d'information dans des pays où tout est verrouillé, comme en Chine. Les dissidents pouvaient, via le darknet, communiquer de manière protégée. Un anonymat et une clandestinité largement détournés à des fins malhonnêtes : ventes d'armes, pédophilie ou drogues pullulent sur ce Web caché. L'un des logiciels les plus utilisés pour surfer sur le darknet s'appelle Tor (pour The Onion Router). On estime que les sites Internet sur le Web crypté sont 500 fois plus nombreux que sur le Web traditionnel.

Réagissez à cet article

Source : *Internet : que trouve-t-on dans le darknet ?*

Sputnik France visé par une cyberattaque

Sputnik France visé par une cyberattaque

Le 25 décembre, une attaque de type DDoS a fait bloquer l'accès au fil d'actualités Sputnik France. Les spécialistes techniques sont en train de régler le problème d'accès au site.

Les attaques par déni de service (Distributed Denial of Service ou DDoS) sont aujourd'hui fréquentes, notamment du fait de la relative simplicité de leur mise en exécution et de leur efficacité contre une cible non préparée. Une attaque DDoS vise à envoyer une multitude de requêtes à un serveur afin de provoquer un déni de service, c'est à dire un arrêt total du service attaqué.

Ce n'est pas la première fois que Sputnik est victime d'une telle attaque. Le 7 décembre dernier, le site de Sputnik Turquie a été attaqué par des pirates informatiques. En octobre 2015, les fils d'actualité de l'agence russe Rossiya Segodnya, et notamment ceux de Sputnik, avaient été bloqués.

Réagissez à cet article

Source : *Sputnik France à nouveau visé par une cyberattaque*

Les juges antiterroristes veulent recourir à des hackers

Les juges antiterroristes veulent recourir à des hackers

Interrogé par les sénateurs, le vice-président chargé de l'instruction à la section antiterroriste du TGI de Paris a demandé que les magistrats puissent recourir à des « experts » (comprendre des hackers) pour installer des mouchards sur les ordinateurs de suspects, puisque l'État ne veut pas fournir ses propres outils utilisés par les services de renseignement.

Interrogé par les sénateurs, le vice-président chargé de l'instruction à la section antiterroriste du TGI de Paris a demandé que les magistrats puissent recourir à des « experts » (comprendre des hackers) pour installer des mouchards sur les ordinateurs de suspects, puisque l'État ne veut pas fournir ses propres outils utilisés par les services de renseignement.
Le Sénat conduisait le 9 décembre dernier différentes auditions à huis clos dans le cadre du Comité de suivi de l'état d'urgence, mis en place pour s'assurer que l'État n'abuse pas des pouvoirs spéciaux confiés à la suite des attentats du 13 novembre 2015, et pour tirer des enseignements sur les pratiques et les obstacles rencontrés par les spécialistes de l'anti-terrorisme. Le Sénat a rendu public le compte-rendu d'audition, qui permet d'en savoir plus sur les attentes des juges.
Les sénateurs ont en effet entendu David Bénichou, le vice-président chargé de l'instruction à la section antiterroriste et atteintes à la sûreté de l'État au tribunal de grande instance de Paris. Celui-ci a vivement critiqué le manque de moyens des juges pour prévenir les actes de terrorisme, en demandant que les magistrats disposent de pouvoirs légaux et de moyens technologiques beaucoup plus proches de ceux dont disposent la police et en particulier les services de renseignement.

Une justice antiterroriste sert-elle à compter les morts ?

Alors que le rôle premier de la police est traditionnellement d'empêcher la commission des infractions, et le rôle de la justice est de les punir, M. Bénichou réfute l'opposition. « Une justice antiterroriste sert-elle à entraver des attentats ou à compter les morts en offrant à leurs auteurs une tribune, et à leur payer un avocat ? », a-t-il lancé. « Nous préférons prévenir les attentats. Pour cela, il nous faut des moyens opérationnels, performants et actualisés ».
Le magistrat a ainsi formulé deux demandes principales. Tout d'abord, il souhaite que les juges puissent saisir les e-mails archivés des suspects dans le cadre d'enquêtes préliminaires, sans que les personnes concernées soient prévenues. Actuellement les juges doivent se contenter de mettre sur écoute les boîtes emails des suspects pour collecter les correspondances reçues ou envoyées à un instant T, mais ils ne peuvent pas collecter ce qui a été émis ou reçu dans le passé (ce qu'a rappelé la cour de cassation le 8 juillet 2015). Le seul moyen d'obtenir copie des e-mails passés est de réaliser une perquisition, ce qui en droit oblige à prévenir le suspect qu'il fait l'objet d'une enquête, et à lui faire assister à la perquisition.
Ensuite, le magistrat demande à pouvoir installer des mouchards informatiques chez les suspects. En théorie cette capacité à capter à distance des données grâce à un dispositif installé localement (clé USB ou autre) ou injecté par une attaque informatique existe déjà en droit, depuis la loi Loppsi de 2011. Elle autorise les juges d'instruction à faire « mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères ».

Recourir à des hackers ou aux services de l'État

Mais dans les faits, comme nous l'avions déjà signalé en 2013, les juges n'ont pas accès aux outils théoriques. Les services de l'Agence nationale de sécurité des systèmes d'information (ANSSI) doivent en effet homologuer les outils mais selon le juge Bénichou, seuls deux outils ont été validés depuis 2011, et pour une raison inconnue, « le ministère de la justice ne les a toujours pas mis à notre disposition ».
« Les services de renseignement monopolisent les outils et ne les mettent pas à notre disposition, par crainte de les voir divulgués. Ils ont pourtant une durée de vie très courte », regrette le magistrat antiterroriste.
David Bénichou demande donc que les juges antiterroristes puissent faire appel à des « experts » extérieurs pour développer de tels outils, c'est-à-dire à des hackers à qui le magistrat passerait commande en fonction des besoins du moment. « Un amendement du Sénat autorisant le juge à commettre un expert pour développer un outil a malheureusement été retiré, le ministre de l'intérieur invoquant la sécurité du système d'information de l'administration », rappelle le juge.

Les services de renseignement monopolisent les outils

Or, « contrairement au contre-espionnage, la lutte contre le terrorisme est avant tout un problème judiciaire : nous avons un besoin opérationnel constant de ces éléments ». « C'est pourquoi je vous suggère de redéposer cet amendement », a-t-il demandé aux sénateurs.
Depuis 2014, la loi autorise potentiellement la police judiciaire à faire appel à des hackers, mais uniquement dans un cadre de perquisitions pour obtenir l'accès à des données chiffrées ou inaccessibles sur le matériel saisi. L'article 57-1 du code de procédure pénale permet en effet aux officiers de la PJ de « requérir toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition » ou pour « leur remettre les informations permettant d'accéder aux données mentionnées ».
À défaut de pouvoir avoir accès à ces mêmes personnes dans le cadre de mises sur écoute ou de piratage à distance des données, le magistrat souhaite pouvoir recourir aux services du Centre Technique d'Assistance (CTA), qui sert déjà aux magistrats dans les affaires les plus graves, lorsqu'ils doivent déchiffrer un contenu saisi par les enquêteurs. Le CTA met à la disposition de la justice ses analystes et ses supercalculateurs pour décrypter les contenus, sans que la justice ne sache quels moyens techniques ont été utilisés pour obtenir la version en clair.

Réagissez à cet article

Source : *Les juges antiterroristes veulent recourir à des hackers – Politique – Numerama*

La Turquie victime d'une grosse cyberattaque

La Turquie victime d'une grosse cyberattaque

Les serveurs internet turcs subissent depuis lundi une vaste cyberattaque qui a notamment considérablement ralenti les services bancaires, a-t-on annoncé vendredi de source proche du gouvernement turc.

L'organisation non-gouvernementale Nic.tr, chargée d'administrer les adresses des sites internet utilisant le nom de domaine «.tr» qui englobe les ministères, l'armée, les banques et de très nombreux sites commerciaux, a indiqué dans un communiqué sur son site internet que l'offensive émane de «sources organisées» en-dehors de Turquie.
Le ministre des Transports et des Communications Binali Yildirim, cité par les journaux, a évoqué une situation «préoccupante» et demandé que soient renforcées les mesures de sécurité, qui, selon lui, se sont avérées «insuffisantes».

Attaque russe?
Certains médias turcs pensent que cette attaque pourrait provenir de Russie, Moscou et Ankara traversant une grave crise diplomatique depuis qu'un bombardier russe a été abattu par la chasse turque à la frontière syrienne, le 24 novembre.
Selon la presse turque, le groupe de piratage informatique des Anonymous a de son côté déclenché une guerre numérique contre la Turquie et annoncé qu'il continuerait à perpétrer des attaques contre les systèmes informatiques en raison du «soutien de la Turquie au groupe de l'Etat islamique (EI)».

Dans un communiqué, le groupe de pirates informatiques a écrit : «La Turquie soutient Daech en lui achetant du pétrole et en soignant ses combattants (…) Si vous ne cessez pas votre soutien à Daech, nous continuerons à procéder à des cyber-attaques contre la Turquie».

Les experts ont cependant indiqué que pour le moment on ignorait l'origine de cette puissante attaque.

Réagissez à cet article

Source : *20 Minutes Online – La Turquie victime d une cyberattaque massive – Stories*

Quels sont les gadgets de la NSA utilisés par la police ?

Quels sont les gadgets de la NSA utilisés par la police ?

The Intercept a pu mettre la main sur un catalogue de périphériques utilisés par les agences américaines de renseignement pour espionner et collecter des données. Un inventaire digne de James Bond. Des questions se posent quant à la légalité de ces appareils et la nécessité d'encadrer leur utilisation par la justice.

A vos portefeuilles ! En effet, les équipements présentés par *The Intercept* et que l'on peut découvrir à cette adresse ne sont accessibles ni à toutes les bourses ni à tous les quidams. Il s'agit en effet d'appareils particulièrement sophistiqués qui permettent aux agences américaines, et tout particulièrement la NSA, de se livrer à leurs activités d'écoute et de surveillance. Certains de ces appareils sont fixes alors que d'autres peuvent être installés dans des automobiles, avions ou drones. Ces différents appareils portent des noms évocateurs comme Cyberhawk, Yellowstone, Blackfin, Maximus, Cyclone ou encore Spartacus. Selon notre confrère, un tiers de ces équipements n'auraient jamais été décrits publiquement jusqu'à présent.

Les possibilités sont différentes selon les appareils. Certains sont destinés à cibler 10000 identifiants téléphoniques différents. La plupart sont capables de géolocaliser les personnes ciblées et, selon les modèles, des fonctions plus avancées comme l'écoute des appels ou la capture des SMS sont proposées. Deux modèles permettent de récupérer les fichiers contenus sur les smartphones ainsi que les carnets d'adresses, notes ou encore récupérer les messages préalablement supprimés.

Spoofing d'adresses

L'un des appareils les plus répandus est le StingRay qui est utilisé pour récupérer les conversations en se faisant passer pour les relais officiels des opérateurs mobiles comme Verizon, AT&T et autres. Cette technique d'interception, baptisée Spoofing, est aujourd'hui largement répandue non seulement par les agences de renseignement mais également par la police fédérale ou municipale. Et c'est là que les défenseurs des libertés individuelles commencent à se faire entendre, arguant que l'utilisation de ces appareils n'est pas suffisamment encadrée et que des dizaines de milliers de personnes voient leurs conversations espionnées au seul motif qu'elles se trouvent dans une même zone géographique qu'une personne suspectée et écoutée.

Stingray I/II

Ground Based Geo-Location (Vehicular)

"Ensnares bystanders, drains batteries, blocks calls"

Review by Nathan Wessler

$134,952.00

Le 4ème amendement mis à mal

Les défenseurs de la vie privée expliquent que l'utilisation de ces appareils, dans des conditions pas ou trop peu encadrées, viole le 4ème amendement de la constitution américaine. En effet, dans un premier temps, ces différents appareils, et tout particulièrement le StingRay commercialisé par la société Harris, était essentiellement utilisé à des fins militaires ou par des agences fédérales. Cependant à partir de 2007, l'usage croissant fait par les polices municipales a commencé à poser problème car cette utilisation semble s'effectuer hors de tout cadre juridique. *The Intercept* prend l'exemple de la police de Baltimore qui a utilisé le StingRay plus de 4300 fois depuis 2007. Comme à l'habitude, la lutte contre le terrorisme sert de viatique à l'emploi de ces appareils et techniques de surveillance. Toutefois, cet argument laisse trop souvent à désirer. En effet, nos confrères citent le cas de la police de l'Etat du Michigan qui a employé 128 fois le StingRay l'année dernière dans le but d'identifier la localisation physique d'une personne suspectée de terrorisme mais l'Association de défense des libertés civiles a précisé que sur les 128 utilisations aucune n'avait un quelconque rapport avec un acte terroriste.

Des fonds douteux utilisés pour les acquérir

Plus ennuyeuses encore sont les modalités d'acquisition de ces appareils. En effet, puisqu'ils sont achetés « hors la loi », les fonds utilisés sont également hors la loi et proviendraient de saisies financières lors des découvertes de trafics en tous genres, de drogue notamment. *The Intercept* écrit que les forces de police de l'Illinois, du Michigan et du Maryland ont utilisé des fonds d'origine crapuleuse pour procéder à leurs achats. L'accusation est particulièrement grave puisque cela revient à accuser les services de police de blanchiment d'argent sale pour mener des opérations notoirement illégales.

Dans ces conditions, un certain nombre de juges américains s'alarment des dérives et souhaitent une évolution de la loi encadrant l'utilisation de ces appareils. Au mois de novembre dernier, le juge fédéral de l'Illinois, Iain Johnston a publié un mémorandum sur la manière dont avaient été utilisées ces techniques de spoofing dans une enquête autour d'un trafic de drogue. « *Un simulateur de ce type est simplement trop puissant et les informations capturées sont trop vastes pour que l'autorisation d'emploi ne soit pas délivrée par une cour dûment habilitée* ».

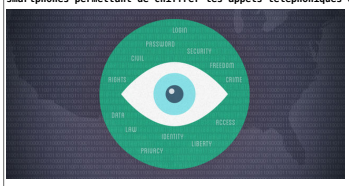
Réagissez à cet article

Source : *Les gadgets de la NSA utilisés par toute la police*

Des communications téléphoniques sécurisées avec Signal

Des communications téléphoniques sécurisées avec Signal

A 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.



À 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.

Les communications entre deux appareils équipés de Signal passent par l'Internet ouvert, mais restent indéchiffrables pour tout observateur extérieur. N'importe quel possesseur de smartphone peut ainsi disposer, sans formalités ni inscription, d'un service naguère réservé aux chefs d'Etat, aux PDG de multinationales et aux agents secrets.

La nouveauté de Signal est que l'on n'a pas besoin d'être un « geek » pour s'en servir : une fois l'application chargée, tout se fait automatiquement. « Les systèmes précédents en demandaient trop aux utilisateurs, relève Frédéric Jacobs. C'est pour ça que jusqu'à présent, le grand public a très peu utilisé le chiffrement. » Il fait allusion à PGP (Pretty Good Privacy), inventé il y a 25 ans par l'Américain Philip Zimmermann, pionner mondial du chiffrement sur Internet.

PALLIER LA DIFFICULTÉ DU CHIFFREMENT

Outre la facilité d'utilisation, l'autre objectif prioritaire de Signal était de proposer un chiffrement intégral, de bout en bout. « Le cryptage et le décryptage se font à l'intérieur de votre téléphone, explique Frederic Jacobs. Quand vous chargez l'application, elle crée automatiquement une centaine de clés de chiffrement, qui restent stockées dans l'appareil. »

Le système permet une rotation systématique : « Chaque clé servira une seule fois. Quand vous recevez un message, vous utilisez une clé qui se détruira aussitôt, et quand vous envoyez un message, l'application crée une nouvelle clé. De cette façon, si un attaquant voulait casser le chiffrement de vos communications, il serait obligé de recommencer le travail pour chaque message. Et s'il s'emparait d'une clé, il ne pourrait pas lire vos vieux messages. »

Frédéric Jacobs travaille avec deux développeurs américains installés à San Francisco : Moxie Marlinspike, un vétéran du chiffrement sur mobile qui a vendu sa première startup à Twitter, et Lilia Kai, ex-militante de l'Electronic Frontier Foundation, association de défense des libertés numériques. Au total, l'équipe permanente de Signal se compose de cinq personnes. Elle est financée par des fondations américaines engagées dans la défense des libertés sur Internet, notamment la Freedom of the Press Foundation et l'Open Technology Fund.

Le budget reste serré, et les salaires modestes. Pour gagner correctement sa vie, Frederic Jacobs travaille comme consultant informatique pour des entreprises. A court terme, cet arrangement le satisfait : « A aucun moment je n'ai pensé à m'enrichir grâce à Signal. Auparavant, j'ai travaillé dans des startups, mais j'ai vite été dégoûté par l'ambiance. Aujourd'hui, je fais partie d'une organisation libérée de l'influence perverse de l'argent. Et rassurez-vous, nous n'allons pas nous vendre à Google. »

UN LARGE PUBLIC EN ALLEMAGNE ET AUX ÉTATS-UNIS

En ces temps d'état d'urgence et de guerre contre le terrorisme, les créateurs de logiciels de chiffrement se sont fait des ennemis puissants, depuis le directeur du FBI jusqu'au premier ministre britannique. De plus en plus, les responsables politiques et policiers exigent que les développeurs créent des backdoors (portes de derrière), par exemple des systèmes permettant de récupérer les clés de chiffrement d'utilisateurs visés par des enquêtes.

Frederic Jacobs assure que Signal ne possède aucune backdoor, et qu'il peut le prouver : « Notre code est en open source, disponible librement sur Internet. Tous les experts peuvent l'analyser et le décortiquer à loisir. » Il affirme aussi qu'à ce jour, Signal n'a subi aucune pression, officielle ou autre : « Personne n'est venu nous voir, peut-être parce que nous sommes encore peu connus. »

Signal ne donne pas de chiffre précis sur son nombre d'utilisateurs, mais l'application a été chargée plusieurs millions de fois. Les plus gros contingents sont aux Etats-Unis et en Allemagne : « Signal a été adopté par des hauts fonctionnaires, y compris à Washington, mais aussi par des familles ordinaires qui veulent protéger les communications de leurs enfants, ou des jeunes couples qui s'échangent des photos intimes… »

Signal dispose de dizaines de relais sur tous les continents. Fin décembre, les principaux se trouvaient aux Etats-Unis (côte est et côte ouest), en Allemagne, en Irlande, au Brésil, en Australie et à Singapour : « Leur nombre exact varie en fonction des besoins, explique Frederic Jacobs, ce sont des serveurs ordinaires, qui se louent à la minute. Si par exemple, le trafic est important en Allemagne vers 17 heures, nous ajoutons des relais locaux, et s'il baisse à 18 heures, nous en retirons. »

Signal possède aussi un serveur central, installé aux Etats-Unis, qui envoie les notifications aux appareils avant un appel. De ce fait, le système n'est pas complètement invulnérable. Si un attaquant réussit à avoir accès à un serveur, par effraction ou lors d'une perquisition, il ne pourra pas déchiffrer le contenu des messages, mais pourra s'emparer des informations techniques dont le réseau a besoin – origine et destination des messages, date et durée des appels… En ce sens, Signal n'a pas été pensé pour les lanceurs d'alerte qui doivent rester totalement inconnus des autorités.

Pour le reste, les cryptologues célèbres qui ont audité le code de Signal se sont dit impressionnés par sa qualité. La consécration la plus éclatante vient de Philip Zimmermann qui travaille aujourd'hui pour Silent Circle, société américaine offrant un service payant de chiffrement des communications, dont le siège social est en Suisse depuis 2014. Créée par des anciens membres des commandos d'élite de l'US Navy et visant une clientèle haut de gamme, ainsi que les militaires et les humanitaires en mission, Silent Circle, pour les messages-texte, a abandonné son ancien protocole de chiffrement, et a adopté celui de Signal.

Réagissez à cet article

Source : *Signal, une application pour téléphoner de manière sécurisée*

Comment gérer une crise e-réputation en 5 étapes

Comment gérer une crise e-réputation en 5 étapes

Tout le monde fait des erreurs. Malheureusement, certaines de ces erreurs sont plus mauvaises que d'autres. Dans le monde professionnel, peu importe votre expérience ou bien le sérieux de votre travail effectué, vous connaîtrez sans doute dans votre carrière au moins une de ces cinq erreurs de niveau de crise présenté dans cet article.

On retrouve souvent des fautes de frappes comme des coquilles lors d'envoi de courriers électroniques ainsi que des malentendus qui sont rarement une cause de préoccupation majeure pour l'entreprise, ce qui est bien sure néfaste afin de garder une bonne réputation.
Lorsque vos erreurs provoquent une échéance manquée, engendrant un coût important pour la société, ou bien d'une mauvaise relation établie avec un client, il est normal de paniquer. Après une telle erreur, en fonction de votre histoire et de la culture de votre entreprise, l'ensemble de votre travail pourrait être remis en cause.
Cependant, paniquer est la pire chose que vous pouvez faire. Toutes les erreurs ne sont immédiatement pas réparables suivant leur seuil de gravité, mais elles peuvent être toutes récupérables grâce à plusieurs solutions adaptables à chaque problème précis.
La prochaine fois que vous vous trouvez dans une situation professionnelle embarrassante à cause d'une des erreurs de niveau de crise citée plus bas, prenez le temps d'analyser ces cinq étapes essentielles:

1 ATTÉNUEZ UN NIVEAU DE CRISE EN RÉAGISSANT RAPIDEMENT
Il est nécessaire de réagir vite lorsqu'un niveau de crise fait son apparition, en effet, dans toutes les situations le temps de réaction est décisif afin de faire face de manière efficace.
Par exemple, si vous avez une fuite au niveau de votre tuyauterie, il est préférable de contacter un plombier dans les meilleurs délais avant que ce problème s'accentue et devienne par conséquent plus difficile à réparer, et donc plus coûteux.
De même si vous avez envoyé des emails par erreur comprenant des informations erronées par exemple, ou bien qu'une pièce soit défectueuse dans votre machine production, le premier réflexe à avoir serait d'éviter de nouveaux dégâts en cessant la production afin de réparer la pièce en question.
Il est également possible de réparer provisoirement une pièce abîmée afin de gagner du temps pour s'équiper de solutions plus coûteuses, mais ce procédé aboutit rarement à une réparation à long terme significative. Elles aideront à réduire les dégâts que vous devrez réparer.

2 FAITES UNE ÉVALUATION DES DÉGÂTS RECENSÉS
Ensuite, faites de votre mieux afin de faire un inventaire de toutes vos erreurs causées avec minutie. Cela évitera que vous vous retrouviez dans une situation stressante à causes des répercussions qu'une erreur peut provoquer lorsque son niveau de complexité n'est pas bien analysé.
Écrivez une liste de tous les domaines affectés par l'erreur et attribuez un classement ou une valeur au degré de dégâts commis, ainsi que le coût éventuelle d'une réparation. Par ce biais, vous serez dans de meilleures conditions pour gérer aux mieux les erreurs rencontrées, tandis que le système de classement vous donnera une indication claire et précise sur les problèmes à traiter en priorité.

3 INFORMEZ LES SERVICES CONCERNÉS
Dissimuler toute erreur serait une mauvaise idée. En effet, prendre en charge une problématique à l'avance serait plus respectable et bénéfique à votre réputation.
Tenez informé dès que possible des problèmes rencontrés à votre patron, votre superviseur, votre client, ou vos partenaires afin d'éviter toute répercussion aggravée.
Il ne suffit pas simplement d'admettre que vous avez fait une erreur. Vous devrez aussi expliquer que vous êtes dans le processus de réunir un plan d'action afin de résoudre une erreur rencontrée. Si vous avez besoin de plus de détails pour finaliser votre tâche, ou bien que vous ayez besoin de conseils précis émis d'un de vos supérieurs.
L'étape suivante est peut-être la plus importante, bien qu'elle soit l'avant dernière à lire.

4 INVENTEZ UN PLAN D'ACTION EN TENANT INFORMÉS VOS INTERLOCUTEURS
Votre plan d'action ne devrait pas être réactionnaire, en effet la seule mesure réactionnaire que vous devez prendre est celle qui atténue ou empêche de nouveaux dégâts. Votre plan d'action se doit d'être soigneusement réfléchi sérieusement. Votre but est de rectifier chaque erreur causée, il préférable également d'y inclure des excuses pour le coût estimé des options de rétablissement entreprises amputés à la société, ainsi qu'envers les clients, fournisseurs et tout autres personnes qui auraient été affectés par votre erreur.
Commencez à exécuter votre plan d'action aussi rapidement et efficacement que possible sans mettre en péril la force ou l'intégrité de votre plan.
Il est également une bonne idée de remonter vers les services concernés en leur faisant savoir que vous êtes officiellement dans le processus de rectifier l'erreur. Une telle mise à jour de statut peut apaiser de nombreuses préoccupations, tout en disant long sur votre aptitude à la récupération d'une crise, ce qui est excellent pour la suite de votre carrière.

5 APPRENEZ À PRENDRE DES MESURES DE PRÉCAUTION
Enfin, une fois que votre plan d'action est finalisé ou bien qu'il se trouve dans les étapes finales d'exécution, il est nécessaire de prendre du temps pour apprendre de votre erreur. Pourquoi est-ce arrivé ? Ce qui vous a poussé à prendre cette décision et quelles circonstances l'ont motivée ?
Ces types de questions vous aideront à identifier la cause de l'erreur, ce qui vous aidera à comprendre la nature du problème dans son ensemble afin d'éviter d'autres erreurs semblables qui pourraient refaire surface à l'avenir.
À moins que vous n'ayez fait quelque chose de vraiment grave, une erreur ne vous coûtera pas votre carrière ni votre réputation si cela ne devient pas répétitif.
Essayez de ne pas trop vous soucier des conséquences que pourrait apportée une erreur, mais dirigez tous vos efforts à améliorer vos performances pour ne plus que ça se reproduise. Vos actions entrepris pour corriger l'erreur sont plus éloquents que vos erreurs commises, il est donc primordial de faire preuve de prudence et de faire tout en votre pouvoir afin de corriger efficacement une erreur de niveau de crise.

Réagissez à cet article

Source : *Comment gérer une crise e-réputation en 5 étapes – REPUTATION PROTECT*

Hyatt : encore une chaine d'hôtels prise pour cible par un logiciel malveillant

Hyatt : encore une chaine d'hôtels prise pour cible par un logiciel malveillant

La chaine d'hôtels Hyatt vient d'annoncer avoir découvert un logiciel malveillant dans son système de paiement. Il est désormais éradiqué, mais l'étendue des dégâts n'est pas connue. Hyatt n'est que le dernier d'une longue liste d'hôtels dont la sécurité a été mise à mal.

Alors que l'histoire de la porte dérobée dans les pare-feu de Juniper n'est pas encore terminée, une nouvelle affaire de sécurité informatique remonte à la surface. La chaine d'hôtels Hyatt vient en effet d'annoncer officiellement qu'elle a « identifié un logiciel malveillant sur les ordinateurs qui gèrent les systèmes de paiements ».

Le groupe ne donne pas d'informations supplémentaires sur les tenants et aboutissants de cette histoire, pas plus que sur le nombre de clients potentiellement touchés ou sur les données dérobées. Il est simplement demandé aux clients de scruter attentivement leurs relevés bancaires afin de vérifier qu'aucune transaction suspecte n'a été effectuée.

Bien évidemment, Hyatt ajoute avoir pris des mesures pour renforcer sa sécurité informatique (notamment avec l'aide d'une société spécialisée dans ce domaine) et indique que, désormais, ses « clients peuvent utiliser en toute confiance des cartes de paiement dans les hôtels Hyatt dans le monde entier ».
Mais il faut également rappeler que cette brèche dans la sécurité d'un hôtel n'est que la dernière d'une longue série pour 2015. En effet, il y a tout juste un mois, c'était la chaine Hilton qui annonçait avoir découvert un logiciel malveillant dans certains terminaux de paiements. Sur son blog, Krebs dresse une triste liste d'hôtels ayant fait face à une importante brèche dans leur sécurité informatique en 2015 : Starwood, Mandarin Oriental, White Lodgging et Trump Collection.

Réagissez à cet article

Source : *Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant*