Les hackeurs Anonymous déclarent la « guerre totale » à Daesh

Les hackeurs Anonymous déclarent la « guerre totale » à Daesh

---

Les Anonymous ont publié une nouvelle vidéo dans laquelle ils entendent renforcer leurs offensives contre l'Etat islamique suite aux attentats ayant touché Bruxelles cette semaine.

Daesh a revendiqué les deux attentats survenus en Belgique dans la ville de Bruxelles. Face à cette menace terroriste, le groupe de hackeurs Anonymous a diffusé une nouvelle vidéo sur YouTube dans laquelle ils affirment vouloir renforcer leurs offensives contre les sites et infrastructures de l'Etat islamique.

Anonymous rappelle les actions précédemment menées après les attaques survenues à Paris en novembre dernier. Le groupe a ainsi fait fermer des milliers de comptes Twitter liés à des sympathisants de l'El. Ils ont hacké plusieurs sites de propagande et récupéré l'argent obtenu des Bitcoin.

« *Cependant, tant qu'il y aura des attaques à travers le monde, nous ne nous arrêterons pas (…) nous défendrons le droit à la liberté (…)*

Sympathisants de Daesh, nous vous traquerons, nous vous trouverons, nous sommes partout et nous sommes bien plus nombreux que ce que vous pouvez imaginer », affirme Anonymous dans cette nouvelle vidéo. Chacun est invité à rejoindre les efforts de ce groupe de hackeurs.

En novembre, 22 000 comptes Twitter liés à Daesh avaient été listés par Anonymous et un site de l'Etat islamique avait subi les foudres des hackeurs.

Un peu plus tôt ce mois-ci, Anonymous avait déclaré une guerre totale au candidat à la présidence des Etats-UnisDonald Trump pour ses diverses déclarations choc au sujet des femmes, des étrangers ou des handicapés…. [Lire la suite]

Réagissez à cet article

Source : *Terrorisme : les Anonymous déclarent la « guerre totale » à Daesh*

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

Dans le cadre du projet de loi sur la réforme pénale, le rapporteur Michel Mercier veut instaurer en France un délit d'entrave au blocage des sites « terroristes ».

En préparation de l'examen en Commission des lois, le sénateur a déposé un amendement visant à condamner ceux qui viennent entraver les procédures de blocage des sites faisant l'apologie ou provocant au terrorisme. Celui qui viendrait extraire, reproduire et transmettre intentionnellement les données concernées par ces mesures, « en connaissance de cause », serait ainsi éligible à cinq ans de prison et 75 000 euros d'amende.
Cette mesure, puisée directement dans une proposition de loi sénatoriale contre le terrorisme (UDI/LR), viendra épauler les mesures de blocage administratif de ces sites, permises depuis la loi du 13 novembre 2014 sur le terrorisme, ou celles décidées par un juge en application de l'article 706-23 du code de procédure pénale.
« *Ces blocages, administratif ou judiciaire, ont pour but de lutter contre la diffusion de contenus faisant l'apologie d'actes de terrorisme,* explique l'auteur de l'amendement dans son exposé des motifs. *Néanmoins, ces blocages peuvent être entravés par certains comportements. Ces derniers, s'ils ne consistent pas en la diffusion publique de ces contenus, ne peuvent être appréhendés sous le délit d'apologie d'actes de terrorisme ou de provocation à de tels actes* ».
Cette mesure est rédigée en des termes suffisamment larges pour qu'on puisse imaginer la sanction de celui qui viendrait tweeter ou publier sur Facebook les données litigieuses, puisqu'il n'est pas possible de bloquer l'un ou l'autre de ces réseaux. Remarquons surtout que le texte n'exige pas nécessairement de diffusion publique. Il joue dès lors qu'on extrait, reproduit et transmet ces données d'une manière ou d'une autre, à destination par exemple d'un serveur distant. Du coup, l'amendement est également taillé pour frapper ceux qui multiplient des contre-mesures aux blocages par IP ou DNS… [Lire la suite]

Réagissez à cet article

Source : *Vers un délit d'entrave au blocage des sites faisant l'apologie du terrorisme ? – Next INpact*

Des millions de smartphones Android touchés par une faille critique

Des millions de smartphones Android touchés par une faille critique

Une faille figurant dans un nombre considérable de smartphones Android permet à des applications d'accéder au contrôle total du système d'exploitation.

La sécurité du système d'exploitation Android est une source régulière d'inquiétude et mobilise constamment l'attention des spécialistes, qui scrutent sans relâche l'OS open source porté par Google afin d'y déceler des vulnérabilités.
Si celles-ci ne manquent pas – les récents correctifs publiés par la firme de Mountain View sont là pour le prouver –, elles sont néanmoins corrigées avec une relative célérité. Toutefois, une faille repérée depuis un certain temps est parvenue à passer entre les mailles du filet. Et pour ne rien arranger, celle-ci s'avère très sérieuse.

TOUTE LA GAMME NEXUS EST CONCERNÉE

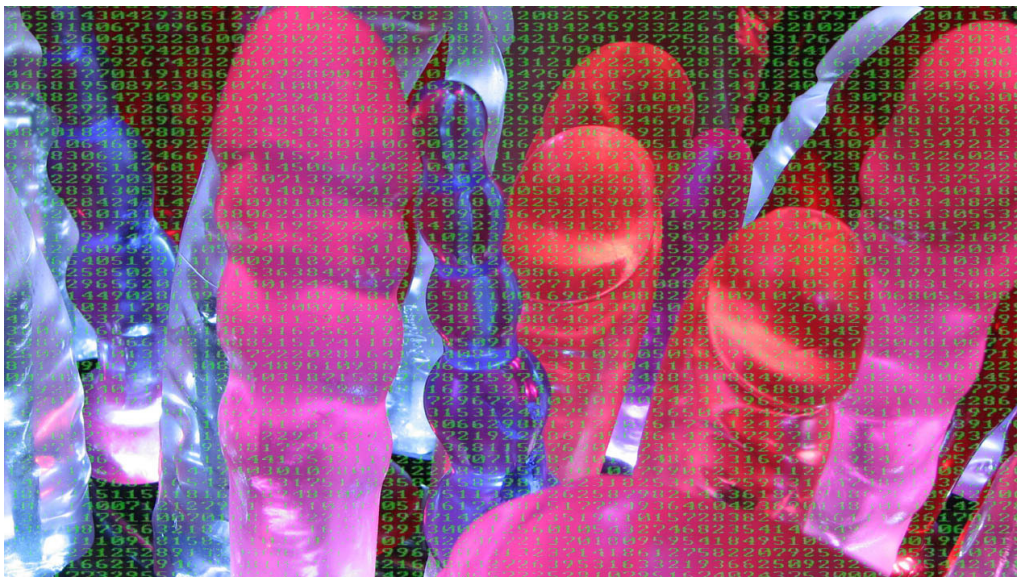
Depuis 2014, une vulnérabilité permettait à une application d'accéder aux privilèges root sur un grand nombre de téléphones Android, dont toute la gamme Nexus. Sur un téléphone rooté, il est possible d'accéder au contrôle total du système d'exploitation et ainsi effectuer des actions normalement bloquées par le constructeur pour des raisons de sécurité.
En l'occurrence, avec cette brèche, une application pouvait accéder à des fonctionnalités bloquées de l'OS et installer du code malveillant. « Une vulnérabilité du noyau qui permet l'élévation des privilèges pourrait permettre à une application nuisible d'exécuter du code arbitraire [sans l'accord du propriétaire, nlr] dans le noyau », explique Google.
Les noyaux Linux 3.4, 3.10 et 3.14 sont touchés, mais ceux plus récents (à partir de 3.18) sont hors de danger.
Cette faille a été identifiée depuis février 2015 sous la référence CVE-2015-180 et un patch est en préparation depuis le mois dernier, après la notification envoyée à Google par la CORE Team, un regroupement d'experts en sécurité informatique. En mars, Zimperium, une startup également spécialisée dans ce domaine, a notifié Google de la présence d'une application profitant de cette faille sur le Google Play.

Dans son bulletin de sécurité, Google explique que l'application en question a été retirée du Google Play. « Les clients qui installent une application qui cherche à exploiter cette faille prennent des risques.
Les applications de root sont interdites sur le Google Play et nous allons bloquer l'installation de cette application en dehors du Google Play grâce à la vérification d'applications », tranche l'entreprise.
Cela étant dit, un utilisateur qui aurait désactivé la vérification d'application peut toujours installer manuellement une application profitant de l'exploit sur son appareil via le fichier APK ou sur un magasin d'application alternatif.
Pour corriger ce problème, Google va déployer un patch sur l'ensemble de la gamme Nexus dans les prochains jours. Celui-ci a été transmis aux différents constructeurs, mais à cause de la fragmentation d'Android, il pourrait se passer plusieurs semaines, voire mois, avant que les fabricants n'appliquent le correctif sur leurs appareils… [Lire la suite]

Réagissez à cet article

Source : *Une faille de sécurité critique touche des millions de smartphones Android – Tech – Numerama*

Piratage de sextoys ! Que faut il craindre ?



Piratage de sextoys ! Que faut il craindre ?

Un éditeur de logiciels de sécurité a mis en lumière le danger que représentent les objets connectés en piratant un vibromasseur. De quoi limiter le potentiel ludique de l'engin!

Les hackers pourront peut-être pourrir nos vies jusque dans notre plus stricte intimité… c'est en tous les cas ce qu'ont essayé de démontrer des ingénieurs de l'éditeur de logiciels de sécurité Trend Micro au salon informatique allemand CeBit qui vient de s'achever à Hanovre.

Les attaques récentes contre les données informatiques d'un… hôpital nous ont mis en garde sur l'impact que peut avoir le piratage sur les systèmes professionnels connectés, mais la menace concerne tous les objets connectés. Y compris les sextoys !

Face à un panel de journalistes, un ingénieur de Trend Micro a en effet piraté un vibromasseur en l'allumant à distance, une action qui a s'abord provoqué l'hilarité, selon l'agence Reuters qui rapporte les faits. Cité par l'agence, le responsable de la technologie de l'éditeur a affirmé que si un « hacker un vibromasseur est amusant […] mais si j'accède au back end (le logiciel de contrôle, ndr) je peux faire chanter le constructeur ».

Un individu mal intentionné et assez qualifié pourrait tout à fait contrôler la vitesse du moteur de l'appareil, accélération qui pourrait potentiellement mener à sa destruction… limitant ainsi son potentiel ludique !

Si nous commençons à nous habituer aux piratages d'infrastructures, le fait que de plus en plus d'objets soient connectés – à nos smartphones voire directement à internet – ne va faire qu'augmenter le périmètre des menaces potentielles.

Espérons que les constructeurs n'attendent pas d'incidents graves pour prendre les mesures de sécurité qui s'imposent…. [Lire la suite]

Réagissez à cet article

Source : *Tout ce qui est connecté peut être piraté, y compris… les sextoys!*

Téléphone, SMS et Internet coupés au Congo pendant les présidentielles…

Téléphone, SMS et Internet coupés au Congo pendant les présidentielles…

Ce n'est pas une rumeur. Les réseaux de téléphonie mobile et d'Internet sont coupés sur toute l'étendue du territoire de la République du Congo (Brazzaville).
Intervenue ce dimanche 20 mars, jour des élections présidentielles, cette mesure court jusqu'à ce lundi 21 mars.
Blackout. La coupure des télécommunications a plongé le pays dans un blackout sans précédent que les autorités justifient par la nécessité de sécuriser le Congo en cette période électorale. Ainsi, pour des « raisons de sécurité et de sureté nationales », le pays a été coupé du reste du monde pendant deux jours. Ce qui n'est pas fait pour rassurer la population, dans la mesure où ces élections se déroulent dans un climat tendu.
Les opposants et la communauté internationale pointent une mauvaise organisation de ce scrutin. Celui-ci met aux prises le Président sortant Dénis Sassou Nguesso (32 ans au pouvoir) face à huit challengers… [Lire la suite]

Réagissez à cet article

Source : *Présidentielles au Congo Brazzaville : téléphone, SMS et Internet coupés dans tout le pays | CIO-MAG*

La Côte d’Ivoire va exiger des passeports biométriques aux frontières

La Côte d’Ivoire va exiger des passeports biométriques aux frontières

---

Bientôt, la Côte d'Ivoire va exiger des passeports biométriques et des cartes d'identités sécurisées à ses frontières. « Sans ces documents, on ne pourra plus entrer en Côte d'Ivoire », a prévenu le ministre d'Etat, ministre de l'Intérieur et de la Sécurité, Hamed Bakayoko.

C'était au cours de la conférence de presse qu'il a co-animée mardi après-midi avec le Procureur général Adou Kouamé Richard, sur l'attentat terroriste de Grand-Bassam, survenu le dimanche 13 mars dernier.
Des propos du Procureur général Adou Kouamé Richard, il ressort que « *l'exploitation efficiente des documents électroniques* » trouvés sur la plage de Grand-Bassam a permis de remonter jusqu'au nommé Kounta Dallah. Cet individu, dont on ignore pour l'instant l'identité et la nationalité, a été présenté par les conférenciers comme le cerveau des attentats qui ont fait 19 victimes et 33 blessés.

A en croire le ministre d'Etat, Hamed Bakayoko, l'enquête se poursuit pour identifier certains individus. Déjà, il faut noter que les preuves numériques ont permis d'interpeller 15 personnes, qui sont à ce stade de l'enquête considérées comme des prévenus. Dans cette affaire, la Côte d'Ivoire bénéficie du soutien du Bureau régional du FBI basé au Sénégal, d'Interpol, de la France, du Mali et du Maroc… [Lire la suite]

Réagissez à cet article

Source : *Attentat de Grand-Bassam : la Côte d'Ivoire va exiger des passeports biométriques aux frontières | CIO-MAG*

Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

	Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

Le principe d'«Accountability » n'est pas nouveau dans le domaine de la protection des données et de la vie privée. Plusieurs textes y ont déjà fait référence et notamment les lignes directrices émises par l'OCDE en 1980, le Standard de la conférence Internationale de Madrid, la norme ISO 29100 ou les règles mises en place au sein de l'APEC. Au sein même de la directive 95/46, le possible recours aux règles internes de groupe pour encadrer les transferts de données en dehors de l'Union Européenne, reflètent cette notion qui vise à responsabiliser le responsable de traitement.

Comment définir le principe d'«Accountability » ?

Ce terme est difficile à traduire en français. Cela revient à montrer comment le principe de responsabilité est mis en œuvre et à le rendre vérifiable. Il est souvent traduit en français par l'« obligation de rendre compte ».
Pour le G29[1] , cela doit s'entendre comme des « mesures qui devraient être prises ou fournies pour assurer la conformité en matière de protection des données ».

Le principe d'«Accountability » dans le Règlement Général de Protection des Données

La traduction française du texte, à savoir « le principe de responsabilité », ne reflète pas toute la signification de ce terme. C'est en lisant le détail des dispositions du règlement, que l'on en saisit la portée.
– Le responsable du traitement est responsable du respect des principes (i.e.de la licéité, de la loyauté, de la transparence des traitements, du respect du principe de finalités, de minimisation des données, de l'exactitude des données, du respect de la durée de conservation et des mesures de sécurité) ;
– Et il est en mesure de démontrer que ces dispositions sont respectées. A cet effet, l'article 22 du Règlement précise que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Lorsque cela est proportionné aux activités de traitement de données, les mesures comprennent la mise en œuvre de politiques appropriées.
– Comme dans tout processus d'amélioration continue, ces mesures doivent être réexaminées et actualisées si nécessaire.

Qui est soumis au principe d'« Accountability » ?

Selon les dispositions de l'article 5 du règlement européen, ce principe concerne le responsable de traitement.
Les sous-traitants auront eux aussi des responsabilités portant sur la mise en œuvre de mesures ou sur la documentation des traitements ; mais si le vocabulaire utilisé dans le texte du règlement est souvent similaire, il ne semble pas que l'on puisse en déduire que les sous-traitants seront soumis au respect du principe d'« Accountability ».
Il en va probablement différemment du représentant qui agit pour le compte et au nom du responsable de traitement établi en dehors de l'Union Européenne et qui de ce fait, doit remplir les obligations qui lui incombent.

De quelles mesures technique et organisationnelles s'agit-il ?

Ces mesures doivent être prise en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes.
Le G29 précise que la mise en pratique du principe d' « Accountability » suppose une analyse au « cas par cas ».
L'article 23 du Règlement relatif à la protection des données dès la conception et par défaut, précise que le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à donner effet aux principes de protection des données et notamment à la minimisation.
Il est par ailleurs indiqué à l'article 28 du Règlement, que chaque responsable du traitement tient un registre décrivant les traitements et dans la mesure du possible, les mesures de sécurité techniques et organisationnelles mise en place.
Selon l'article 30 du Règlement européen, le responsable de traitement est tenu de prendre des mesures de sécurité et notamment selon les besoins :
– la pseudonymisation et le cryptage des données à caractère personnel ;
– des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données ;
– des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci (…) en cas d'incident ;
– une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures de sécurité.

Les mesures indiquées dans le Règlement Européen font écho à celles citées en exemple par le G29 à l'occasion de son avis[2] émis sur l'« Accountability »:
– Des politiques et procédures internes permettant de garantir le respect des principes de protection des données (notamment lors de la création ou la modification d'un traitement),
– L'inventaire des traitements,
– La répartition des rôles et responsabilités,
– La sensibilisation et formation du personnel,
– La désignation d'un délégué à la protection des données,
– La vérification de l'efficacité des mesures (contrôles, audits).

Lors de la 31ème Conférence des Commissaires à la Protection des Données et à la Vie Privée de Madrid, le principe d'«Accountability » avait été illustré de la manière suivante:
– Implémentation de procédures destinées à prévenir et détecter les failles,
– La désignation d'un ou de plusieurs délégués à la protection des données,
– Des sessions de sensibilisation et de formation régulières,
– La conduite régulière d'audits indépendants,
– La prise en compte de la réglementation au travers de spécificités techniques,
– La mise en place d'études d'impacts sur la vie privée,
– L'adoption de codes de conduite.
Le G29 a également indiqué que la transparence sur les politiques de confidentialité et sur la gestion interne des plaintes contribuait à un meilleur niveau d'« Accountability ».

Le rôle de la certification

Le Règlement européen précise que l'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à attester du respect des obligations incombant au responsable du traitement au titre de l' « Accountability ».
De manière générale, les actes délégués de la Commission devraient fournir de plus amples informations sur le sujet.

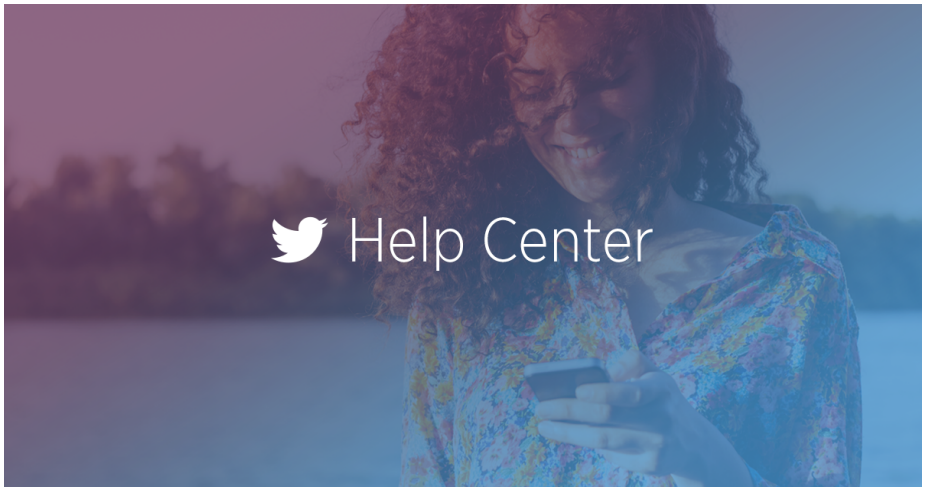
Le principe d'« Accountability » : une évolution plus qu'une révolution

L'« Accountability » n'est pas une révolution dans la mesure où les organisations ont déjà l'obligation de se conformer aux principes de protection des données et notamment à la loi Informatique et Libertés en France. Ce principe est d'ailleurs déjà connu des acteurs du secteur financier.
L'obligation de documentation à des fins de démonstration est en revanche plus novatrice et ce d'autant plus que les entreprises connaissent mal l'étendue de cette réglementation.
Ainsi en cas de violation des principes de protection des données, les autorités de protection des données devraient prendre en considération l'implémentation (ou pas) de mesures et l'existence de procédures de contrôle.
De plus, si les informations relatives aux procédures et politiques ne peuvent être fournies, les autorités de protection des données pourront sanctionner une organisation sur la base de ce seul manquement, indépendamment du fait qu'il y ait eu une violation des données.
Comme l'a indiqué le groupe de travail des autorités européennes de protection des données (G29), les personnes ayant des connaissances techniques et juridiques pointues en matière de protection des données, capables de communiquer, de former le personnel, de mettre en place des politiques et de les auditer seront indispensables à la protection des données.
[1] Opinion 3/2010 on the principle of accountability
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
… [Lire la suite]

Réagissez à cet article

Source : *Règlement Européen de Protection des Données Personnelles : Le principe d'« Accountability » ou comment passer de la théorie à la pratique – CIL Consulting*

Retrouvez l'historique de vos tweets depuis le tout premier envoyé



Retrouvez l'historique de vos tweets depuis le tout premier envoyé

Télécharger votre archive Twitter vous permet de parcourir les éléments publiés sur Twitter depuis votre tout premier Tweet.

Pour télécharger et visualiser votre archive Twitter :
Accédez à vos paramètres de compte en cliquant sur l’icône Profil en haut à droite de la page et en sélectionnant Paramètres dans le menu déroulant.
Cliquez sur Demander votre archive.
Une fois votre téléchargement prêt, nous enverrons un email contenant un lien de téléchargement à l’adresse confirmée associée à votre compte Twitter.
Quand vous recevez cet email, cliquez sur le bouton Télécharger maintenant pour vous connecter à votre compte Twitter et télécharger le fichier .zip de votre archive Twitter.
Dézippez le fichier et cliquez sur index.html pour voir l’archive dans le navigateur de votre choix.
Remarque : Il nous faudra peut-être plusieurs jours pour préparer le téléchargement de votre archive Twitter.
… [Lire la suite]

Réagissez à cet article

Source : *Télécharger votre archive Twitter | Centre d’assistance Twitter*

Le FBI pense pouvoir déchiffrer l’iPhone d’un terroriste sans l’aide d’Apple

Le FBI pense pouvoir déchiffrer l’iPhone d’un terroriste sans l’aide d’Apple

Alors qu'Apple refuse depuis des semaines d'aider le FBI à décrypter l'iPhone de l'un des auteurs de la tuerie de San Bernardino, le FBI vient d'annoncer qu'il tenait peut-être la solution.

La fin d'un bras de fer?

Le gouvernement américain pourrait ne plus avoir besoin des services d'Apple pour récupérer les données de l'iPhone de l'un des terroristes de l'attaque de San Bernardino survenue le 2 décembre 2015. Il a annoncé ce lundi être sur la piste d'une solution alternative. Si elle s'avère efficace, cela mettrait fin à la bataille juridique engagée depuis des semaines avec la marque à la pomme.
Une audience clé qui devait avoir lieu mardi a finalement été levée sur la demande des autorités fédérales. Les enquêteurs vont ainsi pouvoir tester « la viabilité » de leur « méthode ». Ils se sont engagés à remettre à la juge Sheri Pym d'ici le 5 avril, un rapport d'évaluation.

Les autorités optimistes

Dans un communiqué, le ministre de la justice a indiqué qu'il avait poursuivi ses efforts pour accéder à l'iPhone sans l'aide d'Apple depuis de le début de la procédure engagée contre la firme de Cupertino. Les recherches ont abouti dimanche avec la « présentation de la part de tierces parties d'une méthode possible pour débloquer le téléphone », indique le communiqué. Le gouvernement veut s'assurer que sa solution « ne détruit pas les données du téléphone », mais reste « raisonnablement optimiste ».
Les enquêteurs et les familles des victimes réclament de pouvoir accéder aux données du téléphone, potentiellement cruciales pour déterminer comment a été organisé l'attentat et si les deux terroristes ont bénéficié d'aide extérieure.

Apple de son côté campe sur ses positions

Permettre d'accéder aux données du téléphone de Syed Farook créerait un dangereux précédent qui pourrait justifier que les autorités demandent à l'avenir l'accès aux données personnelles de nombreux citoyens pour diverses raisons.
A l'occasion de la keynote d'Apple qui s'est tenue lundi, Tim Cook a justifié la position de la marque. « Nous devons décider en tant que nation quel pouvoir devrait avoir le gouvernement sur nos données et notre vie privée », a-t-il déclaré. « Nous pensons fermement que nous avons l'obligation d'aider à la protection de vos données et votre vie privée », a-t-il ajouté.
Pour rappel, le 2 décembre 2015, Syed Farook et sa femme Tashfeen Malik ont ouvert le feu dans un centre social à San Bernardino, dans l'Etat de Californie. 14 personnes ont été tuées dans la fusillade … [Lire la suite]

Réagissez à cet article

Source : *Le FBI pense pouvoir déchiffrer l'iPhone d'un terroriste sans l'aide d'Apple – L'Express*

Attaque informatique auprès de plusieurs grands sites de presse suédois

Attaque informatique auprès de plusieurs grands sites de presse suédois

---

Au moins 7 sites de grands journaux suédois ont été paralysés simultanément samedi 19 mars en raison d'une attaque par déni de service.

« *Il s'agit sans doute de la plus grande attaque jamais commise contre des sites de médias suédois* », estime le *Dagens Nyheter*, l'un des journaux ciblés, pour qui il était « *encore difficile de publier des articles* » quelques heures après le pic de l'attaque.

La police a ouvert une enquête pour tenter d'identifier le ou les auteurs de cette attaque, qualifiée « *de grande ampleur* » par Anders Ahlqvist, spécialiste de la criminalité en ligne au sein du département des opérations nationales suédois, l'organisme consacré au crime organisé.
« *Nous coopérons avec plusieurs partenaires, à la fois en Suède et à l'étranger* », a-t-il précisé dans les colonnes d'*Aftonbladet*, un des titres visés. Anders Ahlqvist laisse entendre que cette attaque aurait transité par la Russie, tout en soulignant que cela ne signifie pas automatiquement qu'elle est issue de ce pays.

Tweets menaçants

Une piste est notamment suivie, celle de l'auteur de deux tweets menaçants relatifs à cette attaque, dont le premier a été publié quelques minutes avant le début de l'offensive. « *C'est ce qui arrive quand on diffuse de la propagande mensongère* », indiquait ce message en anglais, accompagné du mot-clé #offline et de l'adresse du site d'*Aftonbladet*.

Moins d'une heure plus tard, un autre tweet, issu du même compte, renouvelait la menace pour les jours à venir : « *dans les prochains jours, le gouvernement suédois et les médias diffusant de la propagande mensongère seront visés par des attaques* ».

L'auteur de ces tweets, qui utilise un pseudonyme, est inconnu. « *Nous ne savons pas encore qui est derrière les attaques, mais ce qui est arrivé est une menace pour la démocratie* », a déclaré la responsable de l'Association suédoise des éditeurs de presse, Jeanette Gustafsdotter, au *Dagens Nyheter*… [Lire la suite]

Réagissez à cet article

Source : *Plusieurs grands sites de presse suédois victimes d'une attaque informatique*