JP Morgan piraté : les données de 83 millions de clients exposées

JP Morgan piraté : les données de 83 millions de clients exposées

Cet été, JP Morgan a été victime d'une attaque informatique de grande envergure. La banque américaine admet que les données de 83 millions de clients ont pu être exposées. Toutefois, il ne s'agirait pas d'informations sensibles pour la porte-parole de la société.

76 millions de foyers et 7 millions de PME seraient concernés par ce qui pourrait être l'une des plus grandes fuites de données de l'histoire. Cet été, les systèmes informatiques de la banque JP Morgan ont été compromis par une attaque ayant permis aux pirates d'accéder aux noms, adresses, numéros de téléphone, et adresses e-mail de 83 millions de clients, annonce JP Morgan dans un document transmis à la SEC, le gendarme américain de la bourse.

La banque ajoute qu'il n'y a « pas de preuve » que des données sensibles comme les numéros de comptes, mots de passe, identifiants, dates de naissance ou numéros de sécurité sociale aient été compromises. Les responsables de l'attaque n'auraient pas eu accès à ce type de données sensibles, pense Patricia Wexler, porte-parole de JP Morgan. Il ne serait donc pas nécessaire que les clients changent leurs mots de passe.

Pour le moment, la banque n'aurait pas constaté de fraude relative à cet incident.
Mais l'attaque, très sophistiquée, aurait tout de même permis aux pirates d'accéder « au plus haut niveau des droits administrateurs » selon le New York Times qui s'appuie sur des sources proches du dossier. Puis, les informations exposées restent potentiellement utiles aux cyber criminels : « ils pourraient littéralement utiliser l'identité de ces 83 millions de personnes et entreprises », affirme Tal Klein, de la société de sécurité informatique Adallom, à l'agence Reuters.
La banque avait annoncé en août qu'elle enquêtait avec les autorités sur une attaque informatique. Le FBI soupçonnait des pirates russes en raison de la crise ukrainienne et des sanctions économiques à l'encontre du régime de Moscou. Le New York Times affirmait que JP Morgan n'était pas la seule banque concernée mais qu'en tout, cinq banques auraient été visées le même mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-730905-clients-jp-morgan-pirates.html

Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites

	l’Assemblée nationale valide le blocage administratif des sites pour lutter contre le terrorisme

Après trois jours de débat, l'Assemblée nationale a adopté le 18 septembre dernier, en première lecture le projet de loi visant à lutter contre le terrorisme. Parmi les différents articles, le polémique blocage administratif des sites faisant l'apologie du terrorisme a été voté par les députés.

C'est un hémicycle bien vide qui s'est prononcé sur le projet de loi contre le terrorisme le 18 septembre dernier : au moment de l'adoption du texte dans son ensemble, une trentaine de députés seulement étaient présents pour voter. Ce texte, soutenu par le ministre de l'Intérieur Bernard Cazeneuve et par le rapporteur désigné, le député PS Sébastien Pietrasanta, a donc été adopté sans difficulté. Il doit encore obtenir l'approbation du Sénat avant de repasser au Palais Bourbon puis d'être ratifié par le président de la République.
Comme nous l'expliquions lundi, Bernard Cazeneuve appelait à un « consensus » autour de ce texte qui vise à lutter contre les nouvelles formes d'enrôlements et de propagandes terroristes, notamment via internet et dans les prisons françaises. Si l'objet du texte n'a en effet pas trop souffert de contradiction, on a pu voir une offensive de la droite qui juge le texte encore trop faible face à la menace qu'il entend combattre.

Lutter contre le terrorisme et au passage, réguler Internet
Si le texte a de lourde implication pour les droits fondamentaux des citoyens, celui-ci n'est pas pour autant sans conséquence pour internet. En effet l'article 4 du texte punit donc de 5 ans d'emprisonnement et d'une forte amende le fait d'utiliser Internet pour faire la promotion du terrorisme. La particularité de cet article est de considérer la diffusion via Internet comme une circonstance aggravante : lorsque l'incitation est faite sur un site web public, au vu et au su de tous, la condamnation pourra monter jusqu'à 7 ans et l'amende à 100.000 euros.
Conséquence logique, l'Assemblée a également entériné le blocage administratif (sans décision de justice donc), véritable serpent de mer des lois relatives à Internet. L'article 9, a fait l'objet de nombreuses critiques de la part de parlementaires de tout bord, notamment Laure de la Raudière et Lionel Tardy du coté de l'UMP ou encore Patrick Bloch et Corinne Erhel chez les socialistes.
Cette mesure « est une erreur et je vous invite, je nous invite, à ne pas la commettre », a lancé Christian Paul (SRC). « Faut-il faire reculer encore la liberté, contre le terrorisme ? » s'interroge de son côté Lionel Tardy, « la France s'engage à petits pas dans la direction de la NSA ».

Pas une volte face ?
Face à ces critiques, le rapporteur Pietrasanta a fait valoir plusieurs gardes fous mis en place pour éviter les dérives : il faudra d'abord passer par l'éditeur et l'hébergeur afin de faire retirer les contenus problématiques, et le blocage ne sera mis en place que dans les cas ou les premiers recours n'auront rien donné. De plus, une personnalité qualifiée sera nommée pour jauger de la conformité de ces blocages. Reste le risque de surblocage, évoquée par la députée EELV Isabelle Attard qui cite en exemple le récent cas australien de blocage hasardeux de 250.000 sites.

Bernard Cazeneuve est donc revenu sur la méthode de blocage, expliquant que le blocage par DNS, jugé plus précis, serait privilégié mais que la méthode ne serait pas inscrite dans la loi, préférant attendre de fixer cet aspect là par décret.
La volte face du PS sur la question de blocage administratif, qu'il a largement combattu lorsque la droite était au pouvoir, est revenu à intervalle régulier dans les débats, mais la majorité a assuré que son texte disposait de suffisamment de garanties permettant d'assurer la protection des libertés fondamentales. Il faut donc la croire sur parole.

Prochaine étape : le Sénat
Autres articles adoptés qui pourraient bien changer la donne : les articles 10 et 11, qui simplifient les procédures de perquisition policières dans le Cloud et faciliter le déchiffrement de données récupérées au cours d'une perquisition. Le texte a donc été adopté sans changement majeurs, la droite n'ayant pas réellement réussi à durcir les mesures proposées par le PS et les mesures majeures prévues par le texte sont globalement restées intactes.
Le projet de loi doit maintenant obtenir l'approbation du sénat. Pour plus de détails, le site NextInpact a couvert de très près les débats et un compte rendu des échanges est en ligne sur leur site. Armez vous néanmoins de patience, l'article dépasse allégrement les 60 000 signes, soit un texte environ 15 fois plus long que celui que vous venez de lire. Mais cette loi n'aura plus aucun secrets pour vous.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/loi-sur-le-terrorisme-l-assemblee-nationale-valide-le-blocage-administratif-des-sites-39806557.htm
Par Louis Adam

Information importante pour

votre site Internet. Les grands changements de 2014

Traitements de données personnelles non déclarés à la CNIL, mentions légales absentes ou incomplètes, conditions générales non réglementaires… d'après le baromètre d'E-Mail Brokers, les mauvaises pratiques sont légion sur les sites professionnels français.

Faille d'iCloud : Apple avait-il été alerté depuis des mois ?

Faille d'iCloud : Apple avait-il été alerté depuis des mois ?

Au début du mois, Apple a été sévèrement mis en cause suite au vol et à la publication sur Internet de photos intimes de nombreuses célébrités américaines. La firme a assuré que ses serveurs n'avaient pas été piratés et promis une meilleure protection à l'avenir.

Or selon The Daily Dot, cet incident aurait pu être évité. Comment ? En corrigeant bien plus tôt une faille de sécurité d'iCloud. Car cette vulnérabilité serait celle finalement corrigée fin août. Pourtant, celle-ci aurait été signalée à deux reprises à Apple par un chercheur en sécurité, Ibrahim Balic.

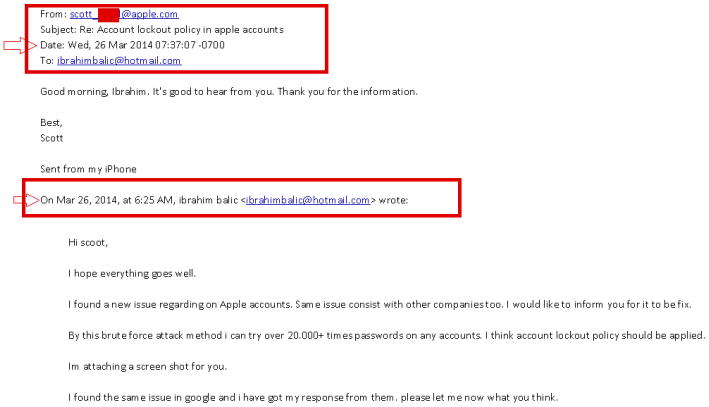
Apple réfute tout lien entre la faille et le vol des photos

Comme l'attestent des emails publiés par le Daily (ci-dessous), l'expert a informé Apple dès le 26 mars d'une méthode permettant d'exécuter une attaque en « brute force » afin de forcer l'accès à un compte iCloud.

Il était en effet possible de tester de très nombreuses combinaisons pour se connecter, Apple n'ayant pas introduit de limitations du nombre de tentatives autorisées. Balic expliquait ainsi avoir pu essayer plus de 20.000 mots de passe.

Début mai, la vulnérabilité ne semblait toujours pas corrigée, l'équipe sécurité d'Apple continuant d'interroger le chercheur sur sa découverte et jugeant par ailleurs la méthode de Balic trop longue pour accéder effectivement de manière illicite à un compte.

Cette faille au niveau de la fonction « Localiser mon iPhone » a-t-elle permis de dérober des photos sur iCloud ? Apple a réfuté tout lien et affirmé que ces divulgations résultaient uniquement d'attaques ciblées contre les victimes.



From : scott_[redacted]@apple.com
Subject: Re: Account lockout policy in apple accounts
Date: Wed, 26 Mar 2014 07:37:07 -0700
To: ibrahimbalic@hotmail.com

Good morning, Ibrahim. It's good to hear from you. Thank you for the information.

Best,
Scott

Sent from my iPhone

On Mar 26, 2014, at 6:25 AM, ibrahim balic <ibrahimbalic@hotmail.com> wrote:

Hi scoot,

I hope everything goes well.

I found a new issue regarding on Apple accounts. Same issue consist with other companies too. I would like to inform you for it to be fix.

By this brute force attack method i can try over 20.000+ times passwords on any accounts. I think account lockout policy should be applied.

Im attaching a screen shot for you.

I found the same issue in google and i have got my response from them. please let me now what you think.

Ibrahim Balic 26-Mar-2014 09:21 PM

Hi Again,

Same issue here:

GET https://p05-mailws.icloud.com:443/wm/ext/sendfrom HTTP/1.1
Host: p05-mailws.icloud.com:443
Connection: keep-alive
Proxy-Connection: keep-alive
Accept: */*
If-Modified-Since: Mon, 24 Mar 2014 00:18:15 Eastern European Standard Time
User-Agent: iPhone Mail (11D167)
Authorization: X-MobileMe-AuthToken base64(userid:password) // MTA[redacted]
Accept-Language: en-us
Accept-Encoding: gzip, deflate

Ibrahim Balic 26-Mar-2014 03:34 PM

Summary:
hi guys,

I found a method for brute-force attack. I found the same issue in google and I've tried 20.474 times password to any account. Account is not locked, malicious people can be exploit here.

"Authorization" parameter in header allowed userid and user password. (with base64 encode)

POST https://p05-keyvalueservice.icloud.com/sync HTTP/1.1
Host: p05-keyvalueservice.icloud.com
Accept: */*
X-Apple-Request-UUID: [redacted]
Authorization: X-MobileMe-AuthToken base64(userid:userpassword)
Content-Encoding: gzip
Proxy-Connection: keep-alive
X-MMe-Client-Info: <iPhone6,1> <iPhone OS;7.1;11D167> <com.apple.SyncedDefaults/166.7>
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
X-Apple-Scheduler-ID: com.apple.syncedpreferences
Accept-Encoding: gzip, deflate
User-Agent: SyncedDefaults/166.7 (iPhone OS;7.1 (11D167))
Content-Length: 395
Connection: keep-alive

Steps to Reproduce:

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/faille-d-icloud-apple-avait-il-ete-alerte-depuis-des-mois-39806921.htm
Apple warned of iCloud brute-force vulnerability 6 months before Celebgate

Google et Dropbox tentent eux aussi de simplifier la cybersecurité

Google et Dropbox tentent eux aussi de simplifier la cybersecurité

Les deux entreprises ont initié une alliance dédiée à la cybersecurité, nommée Simply Secure. Google et Dropbox entendent s'atteler au défi séculaire du monde de la cybersecurité : la simplicité d'accès et d'usage de ces outils.

Si l'on devait compter le nombre de start-ups et de projets qui promettent d'offrir un service garantissant à la fois la plus haute confidentialité des données et une simplicité d'utilisation inégalée, on pourrait probablement passer un moment à établir la liste.
En effet, les récentes révélations Snowden et autres fuites multiples de photos de stars dénudées n'ont fait que rappeler à la communauté des chercheurs en cybersecurité le douloureux problème qui frappe le secteur : les solutions existent, simplement personne ne sait vraiment les utiliser. Mais quand deux géants tels que Google et Dropbox s'allient autour du développement de solutions simples et faciles d'accès pour protéger la vie privée des utilisateurs, l'initiative mérite d'être notée. C'est l'objet de Simply Secure, le consortium dévoilé par les deux entreprises la semaine dernière.

Beaucoup de bruit pour rien ?
Si pour l'instant, Simply Secure n'a pas grand-chose à offrir, il promet beaucoup. Simply Secure l'explique ainsi sur son site « nous voulons aider la communauté de cybersecurité open source à faire mieux. Nous ne voulons pas racheter, nous ne voulons pas inventer » mais simplement apporter un soutien dans le domaine de la recherche. Leur cible : le taux d'adoption des outils déjà existant, qui reste particulièrement bas, comme le rapporte le Guardian.

Le programme de l'alliance Simply Secure est donc de s'ouvrir aux acteurs déjà existant et de mettre en place plusieurs partenariats. Pas vraiment de concret à l'horizon donc, et l'alliance s'attaque à un problème pour le moins épineux que beaucoup auparavant ont tenté d'aborder, sans réel succès.
Mais la question de la cybersecurité n'a jamais été aussi significative aux yeux du grand public, et cette initiative de la part de Google et Dropbox vient réaffirmer leur engagement en faveur d'un internet plus sécurisé. Pas sur que cela soit un réel souci pour la NSA, mais c'est l'intention qui compte.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/google-et-dropbox-tentent-eux-aussi-de-simplifier-la-cybersecurite-39806679.htm
Par Louis Adam | Lundi 22 Septembre 2014

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient de publier son rapport annuel pour l'année 2013, dans lequel, il souligne que le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité ont été les infractions sous-jacentes les plus fréquentes en 2013.

Le rapport annuel 2013 du Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient d'être publié. En ce qui concerne notre pays, le Giaba a signalé que «le rapport national du Sénégal répertorie le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité comme infraction sous-jacentes les plus fréquentes en 2013». Il a aussi rappelé que «le rapport de l'Organe international de contrôle des stupéfiants (Incsr) 2013 du développement d'Etat américain étend la liste pour y inclure les fraudes bancaires et de dépôt, la falsification de documents, la revente de voitures volées et les combines de la Ponzi. Un taux de corruption élevé a également été signalé dans le pays, un phénomène qui frappe tous les niveaux de gouvernance et le commerce, selon le rapport ».
Le Giaba a souligné que «le Sénégal a de plus en plus démontré son engagement à lutter contre les crimes financiers, y compris le Bc/Ft» surtout en prenant des mesures pour renforcer son dispositif de lutte contre le blanchiment des capitaux et de lutte contre le financement du terrorisme (Lbc/Ft). Cependant, «Un projet de stratégie national de Lbc/Ft est actuellement en attente d'approbation par les autorités, conformément à la loi de Lbc/Ft».
Le rapport annuel renseigne aussi que, chez nous, «plusieurs décisions de justice ont été rendues, y compris des peines d'emprisonnement, des amendes et confiscations, suite à des accusations de blanchiment de capitaux». Et en 2013, la Cellule de renseignement financier a reçu 109 déclarations d'opérations suspectes liées au blanchiment, 14 des cas analysés ont été envoyés aux autorités d'exécution, aux fins d'enquête et de poursuite et 3 condamnations ont été prononcées. Il faut dire que dans les premières lignes de la partie du rapport consacré à notre pays, la traduction en justice, pour enrichissement illicite de Karim Wade, a été rappelée : «En 2013, la répression de la corruption a conduit à la mise en accusation devant les tribunaux de plusieurs ministres dans le gouvernement du Président Wade, dont son fils, Karim Wade, pour corruption» y lit-on.
Même si le Sénégal a fait des progrès d'envergure dans le renforcement de son système de Lbc/Ft, les lacunes suivantes demeurent, selon le Giaba «l'adoption d'un cadre approprié de l'approche fondée sur les risques, la mise en oeuvre de mesures de vigilance pour la surveillance continue des relations et transaction avec les clients, la conduite de l'application de mesures renforcées de vigilance pour les clients à risques élevés».
Egalement, «le renforcement de l'obligation de déclarer les tentatives d'opération et un mécanismes pour la mise en oeuvre des résolutions 1267 et 1373 du conseil de sécurité de l'Onu et les résolutions qui les ont suivies».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.dakaractu.com/Rapport-2013-DU-GIABA-trafic-de-drogue-fraude-fiscale-cybercriminalite-constituent-les-infractions-les-plus-frequentes_a73269.html

Chine : première hausse des infections aux virus informatiques en cinq ans

Chine : première hausse des infections aux virus informatiques en cinq ans

Plus de la moitié des ordinateurs en Chine sont infectés par des virus, indique une récente enquête, précisant que ce nombre est en hausse pour la première fois en cinq ans.

Ce taux a augmenté de 9,8% en glissement annuel en 2013, mettant fin à une baisse successive de cinq ans, a annoncé mardi le Centre national des mesures d'urgence face aux virus informatiques.
D'après une enquête menée par le centre, 54,9% des ordinateurs examinés étaient touchés par des virus.
Les sites bancaires et les méthodes de paiement en ligne restent les principales cibles des virus, et les pirates tentent de dérober à la fois des fonds et des informations privées. Les utilisateurs de Weibo sont aussi vulnérables aux attaques de virus, selon le centre.
Chen Jiamin, directeur adjoint du centre, a affirmé que les failles de sécurité mettaient en lumière les manques en matière d'administration des sites Internet et de technologies de sécurité des réseaux dans plusieurs organisations.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://french.people.com.cn/n/2014/0917/c31357-8783700.html

Home Depot : finalement 56 millions de cartes bancaires piratées

Home Depot : finalement 56 millions de cartes bancaires piratées

Début septembre, l'enseignement américaine Home Depot révélait avoir observé une activité inhabituelle concernant les données de paiement de ses clients avant de reconnaître une intrusion informatique.

Home Depot expliquait ainsi que tout client ayant utilisé, depuis le mois d'avril, une carte bancaire pour régler un achat dans l'un de ses magasins aux Etats-Unis et au Canada est potentiellement concerné par le vol de ces données de paiement.
Le groupe ne chiffrait pas le nombre de clients affectés ni le détail exact des données personnelles compromises. Le New York Times évoquait le nombre de 60 millions de cartes de paiement compromises.

EMV
Bingo, Home Depot indique aujourd'hui que ce sont 56 millions de cartes bancaires ont été « mises en péril ». De quoi constituer un nouveau triste record en la matière, jusqu'ici détenu par Target (40 millions de cartes de paiement compromises).
D'ailleurs, comme pour Target, il semble que les pirates aient exploité une variante du programme malveillant BlackPOS installé dans le système de paiement de l'entreprise.
Seule bonne nouvelle, Home Depot estime qu'à ce stade de l'enquête aucune preuve ne permet d'établir que les codes PIN des cartes bancaires compromises figurent également parmi les données dérobées. Mais cette protection est assez peu utilisée aux Etats-Unis…
A la suite de cette intrusion informatique, dont l'ampleur doit encore être précisée, Home Depot a fait savoir qu'il déploierait sur l'ensemble de ses magasins, d'ici à octobre 2015, la technologie EMV de paiement pour cartes à puce. Ce standard international, en vigueur notamment en France, apporte en principe une sécurité accrue des transactions et contribue donc à réduire la fraude.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/home-depot-finalement-56-millions-de-cartes-bancaires-piratees-39806615.htm

Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites

	Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites

Après trois jours de débat, l'Assemblée nationale a adopté en première lecture le projet de loi visant à lutter contre le terrorisme. Parmi les différents articles, le polémique blocage administratif des sites faisant l'apologie du terrorisme a été voté par les députés.

C'est un hémicycle bien vide qui s'est prononcé sur le projet de loi contre le terrorisme aujourd'hui : au moment de l'adoption du texte dans son ensemble, une trentaine de députés seulement étaient présents pour voter. Ce texte, soutenu par le ministre de l'Intérieur Bernard Cazeneuve et par le rapporteur désigné, le député PS Sébastien Pietrasanta, a donc été adopté sans difficulté. Il doit encore obtenir l'approbation du Sénat avant de repasser au Palais Bourbon puis d'être ratifié par le président de la République.
Comme nous l'expliquions lundi, Bernard Cazeneuve appelait à un « consensus » autour de ce texte qui vise à lutter contre les nouvelles formes d'enrôlements et de propagandes terroristes, notamment via internet et dans les prisons françaises. Si l'objet du texte n'a en effet pas trop souffert de contradiction, on a pu voir une offensive de la droite qui juge le texte encore trop faible face à la menace qu'il entend combattre.

Lutter contre le terrorisme et au passage, réguler Internet
Si le texte a de lourde implication pour les droits fondamentaux des citoyens, celui-ci n'est pas pour autant sans conséquence pour internet. En effet l'article 4 du texte punit donc de 5 ans d'emprisonnement et d'une forte amende le fait d'utiliser Internet pour faire la promotion du terrorisme. La particularité de cet article est de considérer la diffusion via Internet comme une circonstance aggravante : lorsque l'incitation est faite sur un site web public, au vu et au su de tous, la condamnation pourra monter jusqu'à 7 ans et l'amende à 100.000 euros.

Conséquence logique, l'Assemblée a également entériné le blocage administratif (sans décision de justice donc), véritable serpent de mer des lois relatives à Internet. L'article 9, voté jeudi 18 septembre, a fait l'objet de nombreuses critiques de la part de parlementaires de tout bord, notamment Laure de la Raudière et Lionel Tardy du coté de l'UMP ou encore Patrick Bloch et Corinne Erhel chez les socialistes.
Cette mesure « est une erreur et je vous invite, je nous invite, à ne pas la commettre », a lancé Christian Paul (SRC). « Faut-il faire reculer encore la liberté, contre le terrorisme ? » s'interroge de son côté Lionel Tardy, « la France s'engage à petits pas dans la direction de la NSA ».

Pas une volte face ?
Face à ces critiques, le rapporteur Pietrasanta a fait valoir plusieurs gardes fous mis en place pour éviter les dérives : il faudra d'abord passer par l'éditeur et l'hébergeur afin de faire retirer les contenus problématiques, et le blocage ne sera mis en place que dans les cas ou les premiers recours n'auront rien donné. De plus, une personnalité qualifiée sera nommée pour jauger de la conformité de ces blocages. Reste le risque de surblocage, évoquée par la députée EELV Isabelle Attard qui cite en exemple le récent cas australien de blocage hasardeux de 250.000 sites.
Bernard Cazeneuve est donc revenu sur la méthode de blocage, expliquant que le blocage par DNS, jugé plus précis, serait privilégié mais que la méthode ne serait pas inscrite dans la loi, préférant attendre de fixer cet aspect là par décret.
La volte face du PS sur la question de blocage administratif, qu'il a largement combattu lorsque la droite était au pouvoir, est revenu à intervalle régulier dans les débats, mais la majorité a assuré que son texte disposait de suffisamment de garanties permettant d'assurer la protection des libertés fondamentales. Il faut donc la croire sur parole.

Prochaine étape : le Sénat
Autres articles adoptés qui pourraient bien changer la donne : les articles 10 et 11, qui simplifient les procédures de perquisition policières dans le Cloud et faciliter le déchiffrement de données récupérées au cours d'une perquisition. Le texte a donc été adopté sans changement majeurs, la droite n'ayant pas réellement réussi à durcir les mesures proposées par le PS et les mesures majeures prévues par le texte sont globalement restées intactes.
Le projet de loi doit maintenant obtenir l'approbation du sénat. Pour plus de détails, le site NextInpact a couvert de très près les débats et un compte rendu des échanges est en ligne sur leur site. Armez vous néanmoins de patience, l'article dépasse allégrement les 60 000 signes, soit un texte environ 15 fois plus long que celui que vous venez de lire. Mais cette loi n'aura plus aucun secrets pour vous.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/loi-sur-le-terrorisme-l-assemblee-nationale-valide-le-blocage-administratif-des-sites-39806557.htm
Par Louis Adam | Jeudi 18 Septembre 2014

Le site internet de la région

PACA victime d’un piratage

Le site internet de la région PACA victime d’un piratage

Le site internet de la Région Provence-Alpes-Côte d’Azur (http://www.regionpaca.fr) a été victime d’un piratage informatique le mercredi 10 septembre. Après avoir été mis hors-ligne, le site est à nouveau accessible.

Les internautes ont vu s’afficher sur leur écran une page sans aucun lien avec l’Institution régionale. Le site a été rapidement mis hors ligne afin de stopper la diffusion de cette page. Les services de la Région procèdent actuellement aux analyses techniques afin de déterminer les conditions de cette attaque et travaillent au rétablissement de l’accès au site institutionnel.
La Région a également saisi la division cybercriminalité de la Police judiciaire et informé l’Agence Nationale pour la Sécurité des Systèmes d’Information. L’Institution entend porter plainte afin qu’une enquête soit menée et que des poursuites soient engagées à l’encontre des auteurs de ce piratage.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.nicematin.com/derniere-minute/le-site-internet-de-la-region-paca-victime-dun-piratage.1899236.html