L’évolution De La Carte SIM

	L’évolution De La Carte SIM

Une carte SIM, ou Suscriber Identity Module en anglais (module d'identification de l'abonné), est un élément familier d'un téléphone portable. Elle peut facilement être échangée ou remplacée, mais elle n'est néanmoins pas née en même temps que le téléphone portable. Les premiers téléphones portables ne permettaient que des normes de communication « intégrées » : les paramètres de souscription étaient codés en dur dans la mémoire du terminal mobile.

Les normes analogues les plus anciennes comme NMT-450 n'utilisaient aucune sécurité : les données d'abonnement pouvaient être copiées sur un autre appareil et clonées, ce qui permettait d'appeler et d'accepter des appels au nom du propriétaire légitime sans payer.

Le premier dispositif de sécurité, inventé un peu plus tard, fut le code SIS, Suscriber Identity Security en anglais (sécurité de l'identité de l'abonné) : il s'agissait d'un nombre à 18 chiffres unique à chaque appareil et codé en dur dans un processeur d'application. Les codes SIS étaient répartis entre les fournisseurs de manière à ce que deux appareils ne puissent pas partager le même code SIS. Le processeur comportait également un code RID de 7 chiffres qui était transmis à une station de base lorsqu'un abonné s'inscrivait dans un réseau mobile.

La station de base générait un nombre aléatoire que le processeur SIS utilisait couplé avec une réponse SIS unique pour produire la clé d'autorisation.

Les clés et les nombres étaient relativement courts, mais appropriés pour l'année 1994 ; de façon assez prévisible, le système a été décrypté plus tard, tout juste trois ans avant l'apparition de la norme GSM, Global System for Mobile en anglais (Communications – Système global pour les communications mobiles). Il était conçu de manière plus sûre étant donné qu'il utilisait un système d'autorisation similaire, mais au chiffrement plus résistant. Ainsi, la norme est devenue « détachée » .

Cela signifie que l'autorisation dans sa totalité avait lieu sur un processeur externe intégré dans une carte intelligente. La solution a été appelée SIM. Avec l'introduction des cartes SIM, l'abonnement ne dépendait plus l'appareil et l'utilisateur pouvait changer d'appareil aussi fréquemment qu'il le désirait tout en gardant son identité mobile.

Fondamentalement, une carte SIM est une carte intelligente selon la norme ISO 7816, qui ne présente pas de différence significative par rapport à d'autres cartes intelligentes de contact comme les cartes de crédit ou les cartes téléphoniques. Les premières cartes SIM faisaient même la taille d'une carte de crédit, mais la tendance globale de réduction des dimensions a mené à une nouvelle forme plus compacte.

Les cartes SIM traditionnelles 1FF (1st Form Factor) de taille complète ne rentraient plus dans les téléphones, et l'industrie a donc trouvé une solution de compatibilité simple : une carte SIM plus petite (mini-SIM, 2FF ou 2nd Form Factor) qui est commune pour les utilisateurs modernes, a été placée dans un support en plastique de taille 1FF afin que la nouvelle forme de carte comporte la puce et les contacts, mais avec une empreinte plus petite, et puisse facilement être sortie.

Bien que cette tendance à la réduction continue avec la micro-SIM (3FF) puis la nano-SIM (4FF) , la forme et les contacts ainsi que les fonctionnalités de ces puces intégrées n'ont pas changé depuis presque 25 ans. De nos jours, de grands supports en plastique sont produits pour répondre aux besoins des utilisateurs qui préfèrent encore des combinés à l'ancienne.

Ceci dit, de nombreux appareils obsolètes ne supporteraient pas les cartes SIM actuelles, même dans leur version complète. Cela vient du fait que la tension de fonctionnement était de 5 V dans les anciennes cartes SIM alors que les actuelles exigent 3 V. De nombreux fabricants de SIM préfèrent sacrifier la compatibilité pour réduire les coûts, et la majorité des cartes SIM modernes ne supporteraient donc pas deux tensions. C'est pour cela que dans un ancien téléphone uniquement compatible avec 5 V, les cartes SIM de seulement 3V ne fonctionneraient même pas à cause de la protection de la tension de leur processeur.

Lors de la production, certaines informations sont écrites dans la mémoire d'une carte SIM : l'IMSI (International Mobile Suscriber Identity, Identité de l'abonné mobile international), en accord avec le porteur ayant commandé la carté, ainsi qu'une clé de 128 bits nommée Ki (Key Identification, identification de clé). Pour résumer simplement, on peut dire que l'IMSI et le Ki sont le l'identifiant et le mot de passe respectifs de l'abonné codés en dur dans la puce de la carte SIM.

La correspondance entre l'IMSI d'un abonné et son numéro de téléphone est stockée dans une base de données spéciale appelée HLR (Home Location Register). Ces données sont copiées sur une autre base de données, VLR (Visitor Location Register) dans chaque segment du réseau, sur la base de l'enregistrement temporaire de l'abonné en tant qu' « invité » sur une autre station de base.

Le processus d'autorisation est relativement simple. Lorsqu'un abonné est inscrit dans la base de données temporaire, VLR envoie un numéro de 128 bits aléatoire (RAND) au numéro de téléphone. Le processeur de la carte SIM utilise l'algorithme A3 pour créer une réponse de 32 bits (SRES) au VLR basé sur le numéro RAND et le Ki. Si VLR obtient une réponse qui correspond, l'abonné est inscrit dans le réseau.

La SIM crée également une autre clé temporaire appelée Kc. Sa valeur est calculée sur la base du RAND et du Ki mentionnés ci-dessus, à l'aide de l'algorithme A8. Cette clé est ensuite utilisée à son tour pour chiffrer des données transmises par l'algorithme A5.

Les noms de tous ces acronymes peuvent paraître un peu compliqués, mais l'idée de base est très simple : vous avez tout d'abord un identifiant et un mot de passe codés en dur dans la SIM, puis vous créez des clés de vérification et de chiffrement avec quelques trucs mathématiques et ça y est : vous êtes connecté !

Ce chiffrement est toujours activé par défaut, mais dans certaines circonstances (par exemple si un mandat est fourni), il peut être désactivé, ce qui permet qu'une agence de renseignement puisse intercepter les conversations par téléphone. Dans ce cas, les anciens dispositifs affichaient un cadenas ouvert, alors que les téléphones modernes (à part Blackberry) n'affichent aucune indication de ce type.

Il existe une attaque spécifiquement conçue pour intercepter les conversations téléphoniques ; pour la réaliser, l'adversaire a seulement besoin d'un appareil appelé IMSI Catcher qui imite une station de base et enregistre les téléphones qui se connectent avant d'envoyer tous les signaux vers une station de base réelle.

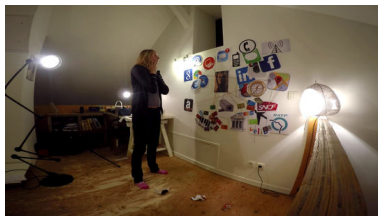
Dans ce cas, tout le processus d'autorisation se déroule de façon normale (il n'est pas nécessaire de décrypter les clés de chiffrement), mais la fausse station de base ordonne au dispositif de les transmettre sous forme de texte brut afin qu'un adversaire puisse intercepter les signaux sans que la compagnie ou l'abonné ne le sachent.

Cela peut paraître étrange, mais cette vulnérabilité n'en est pas vraiment une : en fait, cette fonctionnalité a été conçue pour faire partie du système depuis le début, afin que les services de renseignements puissent réaliser des attaques intermédiaires dans les cas appropriés… [Lire la suite]

Réagissez à cet article

Source : *L'évolution De La Carte SIM – Kaspersky Daily – | Nous Utilisons Les Mots Pour Sauver Le Monde | Le Blog Officiel De Kaspersky Lab En Français.*

Comment je suis devenu invisible (sur le Net) Replay du 28 mars 23h35



Comment je suis devenu invisible (sur le Net) Replay du 28 mars 23h35

Peut-on encore, en 2016, échapper à la surveillance de masse sans renoncer totalement aux outils bien pratiques que sont le téléphone et l'ordinateur ? C'est la question que s'est posée la journaliste Alexandra Ranz dans le très efficace documentaire Comment je suis devenue invisible.

Echapper à la surveillance, qu'elle soit « *étatique ou commerciale* », s'avère un véritable parcours du combattant, constate rapidement la journaliste. Si les mesures de base d'« *hygiène numérique* » que lui conseillent des activistes sont simples – utiliser la navigation privée, doter son téléphone d'un mot de passe –, l'ampleur de la surveillance dont elle fait l'objet, comme chacun, la pousse rapidement vers des méthodes plus élaborées.

Le replay sur pluzz.fr jusqu'au dimanche 3 avril 2016

Echapper aux cinquante caméras de vidéosurveillance qu'elle croise sur un trajet à vélo ? C'est possible, mais il faut porter un masque. Naviguer sur Internet de manière anonyme ? Oui, en utilisant le navigateur anonyme Tor. Empêcher la RATP, la SNCF et l'Etat de savoir où elle se rend ? Oui, là encore, à condition d'abandonner son passe Navigo et de payer son billet de transport en liquide. De toute façon, la carte bancaire est un outil de surveillance ultra-performant, qui donne des informations sur tous nos achats : poubelle, là aussi.

Outil de flicage

Reste l'outil de flicage par excellence, qui est aussi l'accessoire indispensable du XXIe siècle : le téléphone portable. Un nettoyage des applications et un réglage précis des paramètres de confidentialité n'y changent pas grand-chose. « *Le réseau des opérateurs mobiles n'est pas du tout sécurisé* », explique le spécialiste Karsten Nohl, lors d'une rencontre des « hacktivistes » du Chaos Computer Club. « *Avec simplement votre numéro de téléphone, on peut savoir où vous êtes* » – démonstration à l'appui. Pire, renchérit le spécialiste en sécurité informatique Bruce Schneier, « *votre téléphone sait avec qui vous couchez si votre partenaire en a un aussi* ». Pour devenir invisible, il faut l'abandonner.

Même en prenant les mesures les plus radicales, impossible de déjouer totalement les yeux qui nous espionnent, car surveillance d'Etat ou des entreprises, tout se mêle. « *Les entreprises qui gèrent les plates-formes collectent en permanence des données sur nous. Qui aurait imaginé que Facebook, destiné à nos loisirs, deviendrait la source principale des services de renseignement ?* », s'étonne David Lyon, professeur de sociologie.

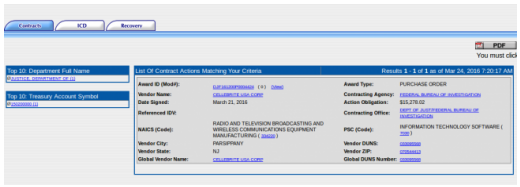
Alors, faute de pouvoir échapper à la surveillance, au moins peut-on lutter contre, et le documentaire nous emmène, dans un certain désordre, à la rencontre de militants. Au Musée de la Stasi, à Berlin, dirigé par un ancien opposant à la police secrète est-allemande, Jörg Drieselmann, la question est évidente : « *Est-ce qu'il y avait des moyens d'échapper à la surveillance ?* » Une longue pause. « *Non. Mes parents m'ont appris dès mon plus jeune âge qu'il fallait que je mente quand j'étais en public : ne dis surtout pas ce que tu penses, dis-leur ce qu'ils veulent entendre. Il n'était pas possible de vivre en RDA sans que cela laisse des séquelles psychiques.* » Restent, cependant, des outils et des attitudes qui fonctionnent, sans devenir asocial ou complotiste, montre le documentaire. Le chiffrement, d'abord, seule protection efficace contre les oreilles indiscrètes. Mais aussi l'action politique, le choix de « *se cacher en subvertissant le système* »… [Lire la suite]

Réagissez à cet article

Source : *Echapper à Big Brother, une gageure*

---

iPhone chiffré : une boîte israélienne à la rescousse du FBI ?



iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*

Google déclare la guerre à Daech

	**Google déclare la guerre à Daech**

Le moteur de recherche vient d'annoncer la mise en place de nouveaux moyens pour lutter contre la radicalisation en ligne. Facebook et Twitter collaborent.

Le moteur de recherche Google prend des mesures pour lutter contre la radicalisation sur Internet. Le moteur de recherche Google prend des mesures pour lutter contre la radicalisation sur Internet.

La cyberguerre est déclarée. Engagée après les attentats de Paris par les très mystérieux hackers d'Anonymous, elle est aujourd'hui rejointe par Google. Lors d'une réunion avec le comité des affaires intérieures britanniques, Anthony House, un cadre de l'entreprise de Moutnain View, a exposé les plans mis en place pour lutter contre la propagande djihadiste, rapporte The Telegraph . Le géant du Web prévoit de rediriger les recherches « pro-Daech » vers des sites luttant contre la radicalisation. En effet, parmi les recrues de l'État islamique, nombreuses sont celles qui ont été endoctrinées derrière leur écran.

Mais, si l'offensive semble nouvelle, les géants d'Internet n'en sont pas à leur coup d'essai. En 2014, Google avait déjà fait retirer 14 millions de vidéos, dont certaines pour propagande, de sa plateforme YouTube.

Selon Yahoo News, Facebook a pour sa part développé au moins cinq cellules dédiées à la lutte contre le terrorisme et suit au plus près les profils signalés. Enfin, le réseau social travaille en collaboration étroite avec des imams, pour aider à la déradicalisation.

De son côté, Twitter déclare avoir supprimé plus de 10 000 comptes ouvertement djihadistes. Nick Pickles, chargé de la politique publique du site de microblogging en Grande-Bretagne, a annoncé : « Twitter, qui a 320 millions d'utilisateurs, emploie plus de 100 personnes pour s'occuper du contenu inapproprié. » Dans cette cyberbataille, Anonymous vient de trouver des alliés de taille. … [Lire la suite]

Réagissez à cet article

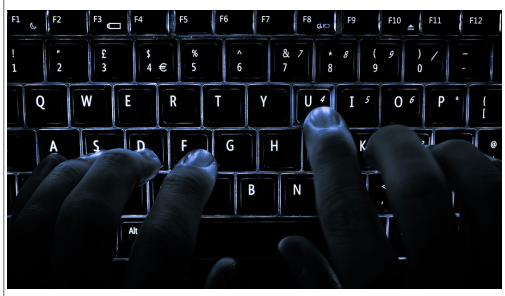
Source : *Google déclare la guerre à Daech*

Comment les hackers font-ils pour pirater toutes vos données informatiques ?

	Comment les hackers font-ils pour pirater toutes vos données informatiques ?

Aujourd'hui, les informations sont partout avec le développement d'Internet. Il est donc important de savoir se prémunir contre les techniques employées pour nous pirater ou nous nuire. Surtout que les hackers, ces pirates du web, se développent de plus en plus et emploient des techniques toujours plus redoutables. SooCurious vous présente les techniques développées par ces génies malveillants de l'informatique.

Vous le savez certainement, le monde d'Internet est dangereux et est le terrain de jeu de personnes malveillantes. Ces gens sont appelés des hackers : ce sont des pirates informatiques qui se servent de leur ordinateur pour récupérer des informations privées ou pour infiltrer des serveurs de grosses entreprises. D'où l'importance de bien choisir ses mots de passe. Avant de pirater, le hacker va enquêter sur sa cible. Il va chercher tout ce qu'il peut savoir sur la personne, à savoir l'adresse IP, le type de logiciels installés sur l'ordinateur de la « victime ». Ils trouvent facilement ces informations grâce aux réseaux sociaux, aux forums en ligne. Une fois qu'ils ont récupéré ces données, le travail de piratage peut commencer.



Hacker n'est pas à la portée de tout le monde : il faut une maîtrise totale de l'informatique pour y parvenir. Ces pirates 2.0 ont plusieurs techniques pour parvenir à leurs fins. La première d'entre elles est le clickjacking. L'idée est de pousser l'internaute à fournir des informations confidentielles ou encore de prendre le contrôle de l'ordinateur en poussant l'internaute à cliquer sur des pages. Sous la page web se trouve un cadre invisible, comme un calque, qui pousse la personne à cliquer sur des liens cachés.
Par exemple, il existe des jeux flash où l'internaute doit cliquer sur des boutons pour marquer des points. Certains clics permettent au hacker d'activer la webcam.

Autre technique, peut-être plus courante, celle du phishing.
Appelée aussi l'hameçonnage, cette action opérée par le pirate vise à soutirer une information confidentielle comme les codes bancaires, les mots de passe ou des données plus privées. Pour récupérer un mot de passe, un hacker peut aussi lancer ce qu'on appelle « une attaque par force brute ». Il va tester une à une toutes les combinaisons possibles (cf. faire un test avec Fireforce) avec un logiciel de craquage. Si le mot de passe est trop simple, le hacker va rapidement pénétrer votre ordinateur. D'autre part, les hackers cherchent parfois à craquer les clés WEP, afin d'accéder à un réseau wi-fi. Encore une fois, si la clé est trop courte, le craquage est facile. Le hacking se développant, des techniques de plus en plus pointues se développent.

Vol des données bancaires via Shutterstock
Il existe maintenant des armées de hackers ou des groupes collaborant dans le but de faire tomber des grosses entreprises ou des banques. Début 2016, la banque internationale HSBC a été piratée. A cause de cela, leur site était totalement inaccessible, ce qui a créé la panique chez les clients de cette banque. Cet épisode n'est pas isolé. Il est même le dernier d'une longue série. Pour parvenir à semer la panique dans de grandes firmes, ils utilisent des techniques plus ou moins similaires à celles présentées ci-dessus, mais de plus grande envergure.

La technique du social engineering n'est pas une attaque directe.
C'est plutôt une méthode de persuasion permettant d'obtenir des informations auprès de personnes exerçant des postes clés. Les pirates vont cibler les failles humaines, plutôt que les failles techniques. Un exemple de social engineering serait l'appel fait à un administrateur réseau en se faisant passer pour une entreprise de sécurité afin d'obtenir des informations précieuses.

Autre méthode, celle du défaçage.
Cette dernière vise à modifier un site web en insérant du contenu non désiré par le propriétaire. Cette méthode est employée par les hackers militants qui veulent dénoncer les pratiques de certains gouvernements ou entreprises. Pour ce faire, le hacker exploite une faille de sécurité du serveur web hébergeant le site. Ensuite, il suffit de donner un maximum d'audience au détournement pour décrédibiliser la cible. En avril 2015, le site de Marine Le Pen a été victime de défaçage : des militants ont publié une photo de femme voilée avec un message dénonçant la stigmatisation des musulmanes par le FN.

Enfin, les hackers se servent aussi du DDOS (déni de service distribué), qui sature un service pour le rendre inaccessible et du Buffer Overflow, qui provoque une défaillance dans le système pour le rendre vulnérable… [Lire la suite]

Réagissez à cet article

Source : *Comment les hackers font-ils pour pirater toutes vos données informatiques ? | SooCurious*

Critical Infrastructure Sectors of Nations facing cybercrime

Critical Infrastructure Sectors of Nations facing cybercrime

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.
PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector
The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century.

Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Réagissez à cet article

Source : *Critical Infrastructure Sectors | Homeland Security*

L’aviation civile n’est pas à l’abri du cyber-terrorisme

L’aviation civile n’est pas à l’abri du cyber-terrorisme

A la demande de l'Agence européenne de sécurité aérienne (Aesa), un hacker pourvu d'une licence de pilote d'avion commercial a démontré qu'il pouvait en quelques minutes entrer dans le système de messagerie des compagnies maritimes.

A l'instar des machines industrielles et des objets domestiques connectés, les véhicules et les avions n'échapperont pas aux attaques des cybercriminels. « L'aviation civile doit se préparer aux cyber-risques », prévient d'ailleurs Patrick Ky, le directeur exécutif de l'Agence européenne de sécurité aérienne (Aesa). En poste depuis 2013, ce dernier s'est exprimé lors d'un petit déjeuner organisé par l'association des journalistes de la presse aéronautique et spatiale (Aspae) en octobre dernier. Ses propos ont été rapportés dans de nombreux journaux tels que Les Echos, Le Parisien ou encore l'Usine Nouvelle. Patrick Ky est formel : le piratage informatique d'un avion est possible et la cybercriminalité représente bien une véritable menace pour le transport aérien.

Pour illustrer ses propos, le directeur exécutif de l'Aesa a confié qu'il avait fait appel à un Hacker. Cet expert en informatique – également titulaire d'une licence de pilote d'avion commercial – est parvenu en quelques minutes à entrer dans le système de messagerie Acars (Aircraft Communication Addressing and Reporting System) en se faisant passer pour un des administrateurs du réseau. Lequel sert aux compagnies aériennes à envoyer des messages automatiques et réguliers de l'avion vers le sol pour s'assurer du bon fonctionnement des systèmes critiques de l'avion.
Risque accru. Demain, le risque de cyberattaque va être accru avec la mise en place du système Sesar (Single European Sky ATM Research ; en français : Ciel unique européen) qui vise à harmoniser en Europe le trafic aérien en déployant un réseau et de nouveaux systèmes de gestion d'ici 2025. Ce nouveau réseau européen de contrôle du trafic aérien aura la possibilité de donner directement des instructions aux systèmes de contrôle de l'avion. Pour limiter les risques de piratage, l'agence européenne pourrait, à long terme, se charger de certifier les équipements contre les risques de cyberattaques sachant qu'elle a déjà la responsabilité de certifier les aéronefs en Europe. A court terme, Patrick Ky veut mettre en place une structure en charge d'alerter les compagnies aériennes sur les cyberattaques. Un risque sur lequel Air France, que nous avons contacté, ne s'est pas encore publiquement prononcé.

Réagissez à cet article

Source : *L'aviation civile n'est pas à l'abri du cyber-terrorisme*

Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

	Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

A ce jour, il existe certains exemples de moyens, usités par les terroristes, permettant de contourner une mesure de blocage d'un site, notamment, l'utilisation d'un « Virtual Private Network » (Réseau Privé Virtuel).

Ce dernier établi un réseau fictif, reliant un ordinateur (celui du client VPN) à un serveur (le serveur VPN), afin de permettre une connexion à Internet de manière anonyme.

De cette façon, les échanges de données sont cryptés et sont protégés par des clés de chiffrement. De plus, ce système permet d'utiliser une adresse IP différente de celle réellement utilisée par un ordinateur, ce qui complique considérablement la localisation de cette machine. De même, le logiciel « Tor » permet de se connecter à Internet par le biais de serveurs répartis dans le monde dans l'anonymat. Il convient de noter que ces procédés cryptologiques sont parfaitement légaux, effectivement, l'article 30 de la loi LCEN du 21 juin 2004 érige en principe que « l'utilisation des moyens de cryptologie est libre ». Dès lors, peut-on envisager l'introduction d'un contrôle par l'autorité administrative, sous forme d'autorisation préalable, lorsque l'utilisation de tels procédés est faite à des fins de provocation au terrorisme ?

Enfin, ces mesures de blocage de sites peuvent sembler illusoires étant donné que celles-ci ne s'appliquent qu'à des FAI et hébergeurs situés sur le territoire français. D'autant que de telles mesures drastiques ne sont pas exemptes de risques de « surblocage ». En 2013, l'Australie a pu en faire les frais en bloquant par accident 250 000 sites sur sa toile.

En conséquence, loin d'être la panacée, cette nouvelle disposition, faussement pragmatique, semble foncièrement superfétatoire.

Sur la conformité de la loi par rapport au bloc de constitutionnalité ?
A titre liminaire, il importe de se poser la question de savoir si la loi du 20 novembre 2015 est susceptible d'être déclarée non conforme à la constitution compte tenu de l'absence de consécration constitutionnelle du statut de l'état d'urgence. A cette fin, il conviendra d'appliquer mutatis mutandis le raisonnement adopté par le Conseil Constitutionnel dans deux décisions : celle du 10 juin 2009 concernant la loi HADOPI et celle relative à la loi sur la pédopornographie du 10 mars 2011.

Dans sa décision du 10 juin 2009, le Conseil en raison du caractère disproportionné du blocage et de sa contrariété avec l'article 11 de la DDHC censure la loi HADOPI soumise à son contrôle « considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ».

En substance, les Sages expliquent que l'octroie par la loi à une autorité administrative du pouvoir de suspendre l'accès à internet est une entorse à la « la libre communication des pensées et des opinions ». L'autorité administrative n'ayant pas le statut de juridiction, elle ne peut se voir octroyer ce pouvoir exorbitant de bloquer un site illicite.

A rebours, dans sa décision du 10 mars 2011, les Sages valident l'article 4 de la loi Loppsi 2 permettant de procéder au blocage administratif de sites pédopornographiques « considérant, en second lieu, que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

Dans cette décision, la mesure de blocage est déclarée conforme à l'article 11 de la DDHC de 1789 au motif qu'il existe un recours au fond ou en référé des décisions de blocage et qu'il est consacré un objectif à valeur constitutionnelle de sauvegarde de l'ordre public (ici l'exploitation sexuelle des mineurs).
En ce qui concerne la conformité du nouveau dispositif, il est à noter que ce nouvel article 11 de la loi de 1955 énonce que « le ministre de l'Intérieur peut prendre toute mesure » de blocage de sites faisant l'apologie du terrorisme. La large marge d'appréciation laissée à l'exécutif amène à s'interroger sur le caractère proportionné de cette disposition. Ainsi, un parallèle peut être opéré avec l'article L. 336-2 du CPI prévoyant des mesure de blocage en cas de violation d'un droit d'auteur ou d'un droit voisin. Celui-ci met en évidence l'éventuel caractère excessif du nouveau dispositif. Si ce dernier rend possible « toutes mesures », l'article L. 336-2 du CPI autorise seulement « toutes mesures propres » en vue de bloquer un site.

La référence au principe de proportionnalité, tangible dans cet article du CPI, ne l'est pas en ce qui concerne cette nouvelle mesure. Dans le cadre d'un raisonnement analogue à celui employé dans la décision du 10 juin 2009, on peut appréhender une potentielle censure par les Sages. En effet, la loi du 20 novembre 2015, compte tenu de sa rédaction large et générale, peut habiliter le ministre de l'Intérieur à « restreindre ou à empêcher l'accès à Internet ». De ce fait, un accroc à l'article 11 de la DDHC peut être redouté. D'ailleurs, le rapporteur au Sénat énonçait que « la disposition proposée [la loi lopssi 2] présente une portée beaucoup plus restreinte [que la loi HADOPI] puisqu'elle tend non à interdire l'accès à internet mais à empêcher l'accès à un site déterminé en raison de son caractère illicite ». Ainsi, le nouveau texte de 2015 risque de connaître le même sort que celui donné à la loi HADOPI, en ce que rien n'interdit au ministre de l'Intérieur de prendre des mesures bloquant l'accès à un site sans pour autant bloquer un site en particulier.
Par ailleurs, une autre incertitude juridique semble planer sur cette loi du 20 novembre 2015 au regard de la décision du 10 mars 2011. S'il est vrai que la suppression du délai de 24 heures ne semble pas impacter la conformité de ce texte, il en va autrement de l'éviction du rôle de contrôle de la CNIL. En effet, l'article 66 de la Constitution dispose que l'autorité judiciaire est « gardienne de la liberté individuelle ». Auparavant, la loi de 2014, chargeait la CNIL d'assurer ce rôle de gardien a posteriori, c'est-à-dire, en actionnant en aval les recours nécessaires devant la juridiction compétente. De même, la CNIL détenait la faculté de contrôler le bien fondé des demandes de retrait de l'autorité administrative. La nouvelle loi éludant cet encadrement exercé par la CNIL, peut laisser sceptique sur sa conformité au texte constitutionnel. D'autant que la loi ancienne (de 2014) n'a jamais fait l'objet d'un contrôle, que ce soit de manière a priori ou a posteriori, devant le Conseil Constitutionnel !

Sur le risque de contrariété de la loi avec la Convention Européenne des Droits de l'Homme ?
Dans un récent arrêt CEDH du 1er décembre 2015, la Cour censure des mesures de blocage de sites pratiquées par le gouvernement turc. En l'espèce, les autorités turques avaient ordonné le blocage de Youtube en raison de dix vidéos accusées de faire outrage à la mémoire d'Atatürk, fondateur de la République laïque turque. Des mesures de blocage ont été ordonnées entre 2008 et 2010.
La Cour reconnait une ingérence de l'autorité publique dans l'exercice des droits garantis par l'article 10 de la convention portant sur la liberté d'expression. De la même façon, la loi de novembre 2015 n'excluant pas la possible coupure d'un site Internet, elle encourt le risque d'être déclarée disproportionnée au regard de l'intérêt légitime poursuivi, à savoir, la lutte contre l'apologie du terrorisme.
Toutefois, l'article 15 de la CEDH autorise dérogation aux obligations de cette convention dans une situation d'état d'urgence, excepté pour les principes non dérogeables, dont ne fait pas partie l'article 10 de la CEDH. Mais un prolongement durable de l'état d'urgence posera nécessairement une difficulté relative à sa compatibilité avec l'article 15 de la CEDH. A moins, (ce que le gouvernement envisage) d'établir un socle juridique solide de l'état d'urgence, au sein de la constitution. En conséquence, de lege lata, la conformité de ce nouveau dispositif semble loin d'être évidente au regard d'un certain nombre de droits fondamentaux garantis.
Somme toute, est-ce qu'« à force de sacrifier l'essentiel pour l'urgence, on finit par oublier l'urgence de l'essentiel » ? (Edgar Morin)

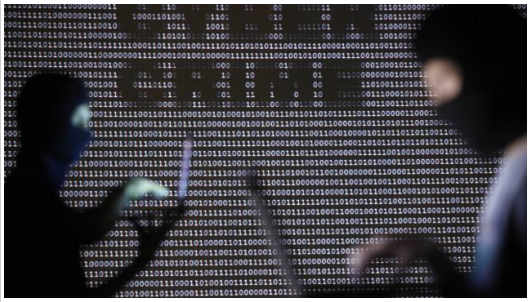
Réagissez à cet article

Source : *Utilité et conformité des mesures de blocage de sites Internet faisant l'apologie du terrorisme dans le cadre de l'état d'urgence. Par Dan Scemama.*

Crainte d'attentats pilotés à partir d'Internet en 2016

Crainte d'attentats pilotés à partir d'Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*

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*