Cinq questions importantes à se poser en matière de cybersécurité

	Cinq questions importantes à se poser en matière de cybersécurité

Pas un jour ou presque ne se passe sans que le sujet de la cybersécurité ne soit traité dans les médias. Entre les « cyberattaques », les « cybermenaces » et la nécessité de « connaître son adversaire », on pourrait croire que les entreprises sont en état de siège permanent.

Les cybermenaces revêtent plusieurs formes : États-nations qui se livrent à des activités d'espionnage, cybercriminels qui cherchent à dérober de précieuses informations en vue de les exploiter, ou encore groupes aux motivations diverses qui cherchent à perpétrer des vols ou à causer des perturbations.

Il peut même s'agir d'une personne interne de confiance qui vole des données de clients ou d'entreprise ou d'un employé bien intentionné qui, en effectuant son travail, perd sans le vouloir de précieuses données de clients ou d'entreprise. Nul doute que les cybercriminels peuvent être très adaptables et innovants, mais le contexte de menace est un fait établi. C'est la manière dont vous gérez le risque qui est importante.
Dans un environnement cacophonique, il est important que les dirigeants d'entreprise gardent les choses en perspective. L'environnement est inondé de toutes sortes de solutions techniques, promettant de vous donner un avantage en matière de détection et de prévention. Toutefois, il est essentiel que tous les dirigeants d'entreprise prennent du recul et se rappellent que le cyber risque n'est pas un risque informatique, mais un risque d'entreprise et, à l'instar de tout autre risque d'entreprise, il doit être géré.

La menace ne peut pas être éliminée, mais le risque peut être géré

Il est également important de comprendre que cette menace ne peut pas être éliminée, mais que le risque peut être géré. Il est facile de se laisser tenter par une « structure du risque », mais comme de nombreuses structures, elle peut nécessiter d'investir beaucoup de temps et d'efforts pour des résultats de sécurité négligeables.
Trop souvent, la cybersécurité est évoquée à l'aide de jargon technique ou militaire, mais cela ne fait que dissiper l'attention et la compréhension des dirigeants. Il est vital que les professionnels de la sécurité expliquent le contexte de menace et le défi de la cybersécurité dans un langage accessible. C'est pourquoi il est important de comprendre le cyber risque auquel votre entreprise est confrontée. Tous les dirigeants doivent pouvoir poser les questions simples et non techniques suivantes et obtenir des réponses.

1. **Connaissez la valeur de vos données :** savez-vous de quelles données de valeur dispose votre entreprise ? Sont à inclure les données qui ont de la valeur non seulement pour vous, mais aussi pour les cybercriminels qui peuvent vouloir les voler. Quelles sont les données qui vous causeraient le plus grand préjudice si vous deviez les perdre ? Vous devez avoir une liste de vos données de valeur.
2. **Sachez qui a accès à ces données de valeur :** qui possède les droits d'administration ou l'accès aux informations ? Toutes vos « personnes internes de confiance » ont-elles besoin d'avoir accès aux données de valeur pour effectuer leur travail ? Cette question est essentielle, car l'accès aux données de valeur doit être étroitement surveillé. Vous ne confieriez pas les clés de votre domicile à n'importe qui, alors surveillez de près les personnes qui ont accès à vos données de valeur.
3. **Sachez où se trouvent vos données de valeur :** vous devez savoir où elles sont stockées et comment vous y accédez. Vos données de valeur sont-elles délocalisées au loin, dans le pays, dans le cloud ou même stockées chez un tiers ? Allez plus loin et demandez-vous si vos fournisseurs ont partagé vos données de valeur avec des sous-traitants.
4. **Sachez qui protège vos données :** vous devez savoir qui protège vos données de valeur. Cet aspect est extrêmement important. Où se trouvent ces personnes ?
5. **Sachez dans quelle mesure vos données sont protégées :** vous devez savoir ce qui est fait par les professionnels de la sécurité pour protéger vos données 24 h/24 et 7 j/7. Les tiers qui ont accès à vos données les protègent-ils de manière adéquate ?

C'est seulement une fois que vous aurez la réponse à ces questions que votre entreprise sera préparée à comprendre le niveau de cyber risque et l'efficacité avec laquelle il est géré… [Lire la suite]

Réagissez à cet article

Source : *Cinq questions importantes à se poser en matière de cybersécurité – ZDNet*

Cyberprotect | Nouvelles vagues de rançongiciels : comportement, conseil, solution

Nouvelles vagues de rançongiciels : comportement, conseil, solution

Les actes de cybercriminalités se comptent en nombre et de façon récurrente. Beaucoup d'entreprises, d'administrations ou de commerces sont victimes de cyberattaques. Parmi ces attaques nous trouvons des logiciels malveillants comme les rançongiciels. Pour citer l'ANSSI, « c'est une technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de p

Ces rançongiciel sont de plus en plus présents en ce moment et se renouvellent. Actuellement les alertes portent sur le rançongiciel Locky qui se propage via un e-mail de relance qui contient une facture sous le format Word. Ce serait ce même logiciel qui aurait attaqué il y a quelques jours un centre hospitalier américain, perturbant et endommageant considérablement ses activités.
http://www.lefigaro.fr/secteur/high-tech/2016/02/16/32001-20160216ARTFIG00205-un-hopital-americain-paralyse-par-des-pirates-informatiques.php
http://www.lemonde.fr/pixels/article/2016/02/18/un-hopital-americain-paye-une-rancon-a-des-pirates-informatiques_4867296_4408996.html

Malheureusement ce type de logiciel malveillant n'est pas nouveau et s'inspire même de maliciels déjà connus comme le trojan bancaire Dridex. Plusieurs campagnes de prévention avaient été déployées suite à l'identification de ce maliciel par l'ANSSI notamment, mais également par Cyberprotect, service de contrôle et de prévention en continu de la cybersécurité en entreprise :
https://www.cyberprotect.fr/bulletin-dalerte-Cyberprotect-campagne-courriel-malveillant-trojan-bancaire-dridex/

La principale raison d'être et/ou motivation de ces cyberattaques est d'extorquer de l'argent à leur victime, comme ce fut le cas pour cet hôpital américain cité plus haut qui a dû s'acquitter de 17 000 dollars de rançon pour pouvoir rétablir son activité. Et ce n'est qu'une victime parmi d'autres. La propriété intellectuelle de l'entreprise est également visée par ce type d'attaque.

Se pose maintenant la question : comment se prémunir contre ces cyberattaques ?
Une première chose est de ne pas cliquer sur un lien ou d'ouvrir une pièce jointe dont on ne connait pas la provenance. Maintenir le système d'exploitation ainsi que les antivirus à jour est également une bonne pratique. Toutefois, avec le volume de données échangées, il est devenu plus difficile d'éviter ces attaques dont les techniques d'infection se font toujours plus subtiles et discrètes… [Lire la suite]

Réagissez à cet article

Source : *Cyberprotect | Nouvelles vagues de rançongiciels : comportement, conseil, solution*

Les entreprises françaises touchées par une explosion de

la cybercriminalité

Les entreprises françaises touchées par une explosion de la cybercriminalité

Plus des deux tiers (68%) des entreprises françaises ont été victimes de fraude au cours des deux dernières années, un phénomène dû en particulier à l'explosion de la cybercriminalité, selon une étude de PwC publiée début mars 2016.

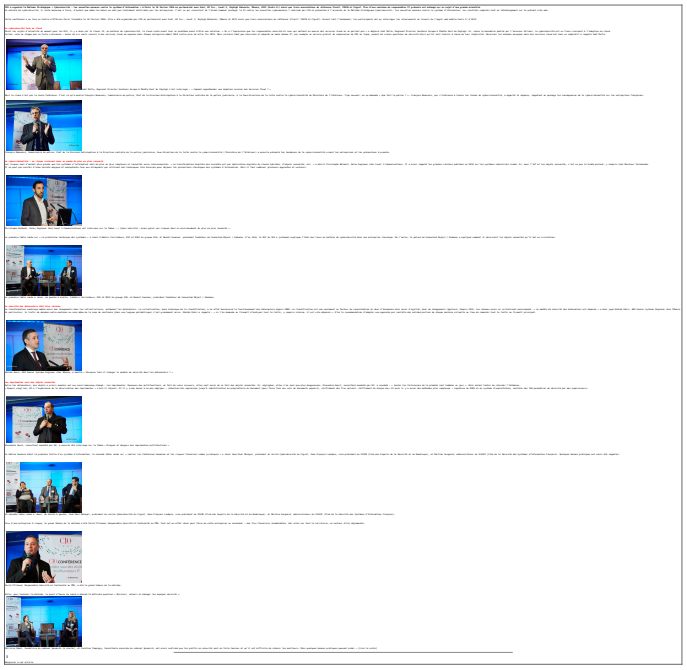
Ce chiffre est en progression de 13 points par rapport à la dernière étude de PwC publiée en 2014 sur le sujet, et est nettement supérieur au taux constaté au niveau mondial, qui s'établit à 36%, selon cette enquête réalisée auprès de 6.337 entreprises dans le monde dont 120 françaises.
Les entreprises de moins de 100 salariés sont de plus en plus touchées, 43% d'entre elles déclarant être victimes de fraudes (+14 points par rapport à 2014).
Au premier rang des fraudes figure toujours le détournement d'actifs au sens large, même si ce risque diminue, avec 56% d'entreprises s'étant déclarées victimes de ce phénomène en 2016 contre 61% en 2014.
La cybercriminalité explose pour sa part: 53% des entreprises ont déclaré avoir été victimes de ce type de fraudes contre 28% en 2014. Et 73% des dirigeants français redoutent de subir une cyber-attaque au cours des deux prochaines années, contre 34% au niveau mondial.
Pour autant, « plus de la moitié (des entreprises françaises) n'ont pas encore de plan d'action opérationnel pour répondre à une cyber-attaque », souligne Jean-Louis Di Giovanni, associé de PwC, cité dans le communiqué.
Parmi les autres risques figurent la fraude aux achats (25%), qui se traduit par des surfacturations de biens ou de prestations, et la « délinquance astucieuse », protéiforme, qui recouvre la fraude au président (une personne se fait passer pour le dirigeant de la société et ordonne de procéder en urgence à un virement) ou encore celle aux changements de RIB de fournisseurs.
Celle-ci a presque doublé en deux ans, passant de 10% en 2014 à 18% en 2016, selon PwC… [Lire la suite]

Réagissez à cet article

Source : *Fraude: les entreprises françaises touchées par une explosion de la cybercriminalité*

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?



Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*

IT Forum Sénégal 2016 : Interview de Mohamadou Diallo : Directeur de publication de CIO-MAG

	**IT Forum Sénégal 2016 : Interview de Mohamadou Diallo : Directeur de publication de CIO-MAG**

18 et 19 février 2016, IT Forum Sénégal 2016 : Mohamadou Diallo : Directeur de publication de CIO-MAG interviewé

Réagissez à cet article

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

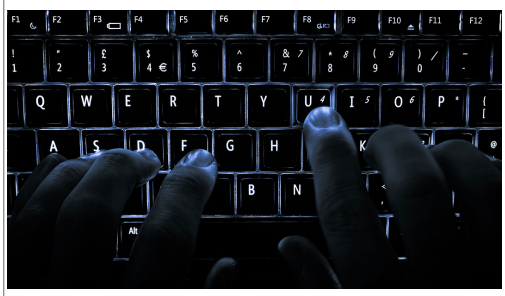
Source : *Google déclare la guerre à Daech*

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*

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.

« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés (…) *toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage »*, a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.
« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones », a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs *« aveugles »* dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.
L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « *cassé* » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.
Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les *« téléphones cryptés ».« Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner »*, expliquait au *Monde* le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : *« Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. »* C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, *« huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé »*, a détaillé M. Molins.

Concernant le cryptage, *« il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données »*, assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par *Le Monde*.

UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, *« cette possibilité semble ignorée par de nombreux services »*. Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, *« dans le cadre d'une urgence vitale »*, de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.
Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. *« Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal… Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger »*, conclut le SCITT.

Réagissez à cet article

Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon