Fic 2016 : Etude d’impacts sur la vie privée : suivez la méthode de la CNIL

Fic 2016 : Etude d’impacts sur la vie privée : Suivre la méthode de la CNIL

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.
Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :
• Étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
• Étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
• Étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
• Validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Denis JACOPINI EST FORMATEUR EN ETUDE D'IMPACT SUR LA VIE PRIVÉE

Réagissez à cet article

Source : *Etude d’impacts sur la vie privée : suivez la méthode de la CNIL – CNIL – Commission nationale de l’informatique et des libertés*

Fic 2016 : l’avenir du Safe Harbor fixé début février

Fic 2016 : l’avenir du Safe Harbor fixé début février

Lundi 25 Janvier, en fin de journée à Lille, lors d'une conférence plénière organisée au sein du FIC 2016, Isabelle Falque-Pierrotin a indiqué d'autre part que le G29 se réunirait début février pour savoir ce qu'il adviendra de l'annulation du Safe Harbor.

Si la présidente de la CNIL a été discrète sur le sujet, plusieurs pistes se dégagent selon nos sources. Les clauses types et les Binding Corporate Rules (ou BCR), à savoir les codes de conduite internes aux entreprises, pourraient ne pas perdurer, sans doute parce qu'elles ne rabotent en rien la curiosité des services américains. Au-delà des autorisations individuelles, la seule issue disponible pour les acteurs du Web resterait finalement les décisions d'adéquation. Avec elle, dans un État déterminé, une autorité de contrôle devrait ainsi mener une analyse approfondie des lois nationales du pays tiers pour autoriser ou interdire le transfert.
Bien entendu, une telle position pourrait être jugée inutile si les États-Unis et l'Europe parvenaient finalement à un accord sur un hypothétique #Safe Harbor 2. Sur le terrain politique, cependant, cette réalité n'est qu'un rêve encore trop lointain. Toujours au FIC, David Martinon, représentant spécial de la France pour les négociations internationales sur la société de l'information et l'économie numérique, a pointé aujourd'hui encore l'absence d'accord entre les différents pays européens sur ce dossier.

Réagissez à cet article

Source : *Données personnelles : l'avenir du Safe Harbor fixé début février*

Fic 2016 : Orange a de grands projets pour la France

#Fic 2016 : Orange a de grands projets pour la France

Une introduction calibrée sur mesure pour Stéphane Richard, PDG d'Orange, qui a succédé à Xavier Bertrand et au général Favier, directeur général de la Gendarmerie Nationale, sur la scène du FIC.

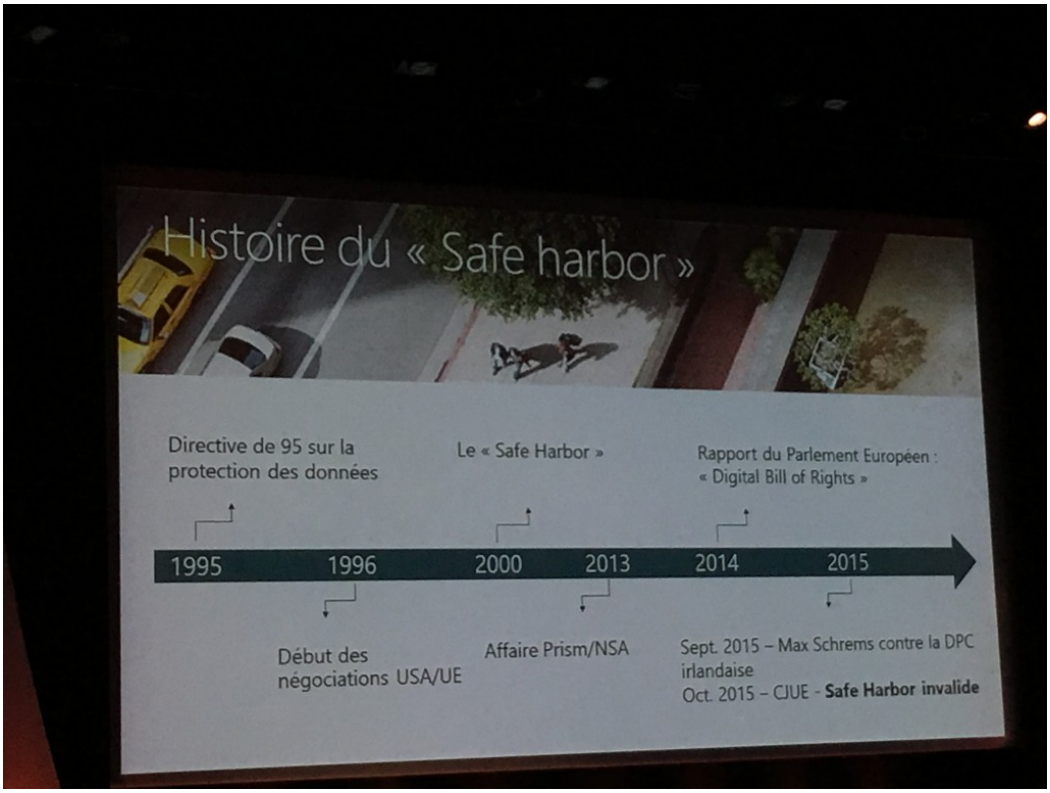
Lundi 25 janvier 2016, au FIC (Forum International de la Cybersecurité) à Lille Grand Palais
« La politique de cybersécurité d'Orange a été boostée par des attaques et nous peinons à recruter des talents.
2600 postes sont aujourd'hui ouverts à Paris pour la cyberdéfense et il est difficile de les pourvoir.
Notre cyber SOC (security operation center) est installé à Rennes mais nous allons également nous positionner à Lille pour déployer des ressources capables de se projeter à Lille, Bruxelles et Paris », a assuré le PDG.
« Notre croissance – près de 20% par an – est aujourd'hui freinée car nous manquons de ressources », a ajouté Michel van den Bergue, directeur d'Orange Cyberdéfense. « Il est rageant de voir ce domaine avec une perspective énorme manquer de ressources ». Pour Lille, Orange va s'appuyer sur Euratechnologies et travailler avec le personnel de la compagnie qui désire évoluer vers les métiers de la cybersécurité pour répondre à des projets sur Paris, Londres et Bruxelles.

Réagissez à cet article

Fic 2016 : Comment mériter la confiance à l’heure de la remise en question du Safe Harbor

	Fic 2016 : Comment mériter la confiance à l’heure de la remise en question du Safe Harbor

Le 6 octobre, la cours de justice de l'union européenne a invalidé le Safe Harbor. Cette session a pour but d'expliquer comment il est possible de mériter la confiance et de respecter la loi pour un fournisseur de service Cloud comme Microsoft.



Pour rassurer le groupe de travail de l'article 29, et pour venir compléter des mesures de sécurité se basant sur la norme iso 27001, plusieurs pistes ont été envisagées par Microsoft dont :
Faire appel à des contrôleurs de mises en conformité indépendants
S'engager à fournir la liste des sous-traitants…
Modifier ses conditions générales de ventes
S'engager à conserver confidentielles les données stockées hors cadre judiciaire

---

Réagissez à cet article

Source : *FIC 2016*

Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes

Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes

Deux entrepreneurs se retrouvent en garde en vue après avoir trouvé une vulnérabilité dans le site de Forum international de la cybercriminalité (FIC). Ce dernier, en effet, a porté plainte pour accès frauduleux dans un système informatique.

Attention, le métier de chercheur en sécurité n'est pas totalement sans risque, comme viennent de le constater deux jeunes entrepreneurs qui viennent tout juste de créer Cesar Security, une société spécialisée dans les audits de sécurité et la prévention contre la fraude bancaire.

La semaine dernière, ils trouvent une faille sur le site web du Forum International de Cybersécurité (FIC) qui se déroule ce jour à Lille.

Selon eux, la vulnérabilité – désormais corrigée – était assez banale, mais permettait quand même d'accéder à la base de données des participants. Pas terrible pour l'image de marque d'un tel évènement qui accueille chaque année le gratin français en matière de cybersécurité. Les deux hommes veulent faire les choses bien et contactent l'éditeur du site, à savoir la Compagnie Européenne d'Intelligence Stratégique (CEIS), co-organisateur de l'évènement. Parallèlement, ils envoient une alerte sur Twitter.

Ils sont aimablement reçus au téléphone par un consultant en sécurité du CEIS auprès de qui ils détaillent leur trouvaille. Ils lui envoient un rapport technique de la faille avec une proposition de correctif, un accord de confidentialité ainsi qu'un devis pour un audit de sécurité. « Au départ, nous lui avons proposé un audit gratuit, mais il a dit que ce n'était pas un problème, que l'on pouvait lui envoyer un devis chiffré », nous explique S. Oukas, l'un des deux entrepreneurs. Puis, c'est le silence radio, plus aucune nouvelle. Le 20 janvier, ils envoient donc un nouveau tweet, pour « prendre des nouvelles ».

© DR

Le jour suivant, c'est la surprise. A 9h du matin, les gendarmes sur Centre de lutte contre les cybercriminalités numériques (C3N) toquent à leur porte. Ils apprennent que l'éditeur du site a porté plainte pour « accès frauduleux à un système de traitement automatisé de données » (STAD), un délit passible de deux ans d'emprisonnement et d'une amende de 60 000 euros.

Tout le matériel informatique est saisi. « Nous avons tout perdu : les trois ordinateurs dans notre bureau, un téléphone, un ordinateur personnel et même une PlayStation. Nous sommes tombés de très haut. Nous qui pensions que le FIC aurait encouragé une jeune startup, ils nous mettent à genou. Nous avons perdu nos outils de travail, nous ne pouvons plus rien faire », souligne M. Oukas.

Vente forcée ou chevalier blanc ?

De son côté, le CEIS n'a pas la même interprétation des choses. « Cette société nous a bien contactés, mais ce n'était pas désintéressé car elle nous a proposé ses services. Nous ne l'avons jamais autorisé à effectuer cette recherche. C'est de l'audit sauvage », estime Guillaume Tissier, directeur général du CEIS, qui n'a pas apprécié non plus que Cesar Security publie son alerte de sécurité de manière publique sur Twitter, aux yeux de tous. « Au tribunal, le débat tournera certainement autour de cette question, car on peut le voir comme une forme de vente forcée », estime pour sa part Bernard Lamon, avocat.

L'ironie du sort, c'est que cette affaire tombe pile au moment où les députés votent un amendement visant à protéger les lanceurs d'alerte qui trouvent des failles informatiques. Selon le texte, une telle personne sera exempte de peine « si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système ». Ce texte, s'il est adopté au final, pourrait néanmoins jouer en faveur de Cesar Security. « Même si les faits sont antérieurs, le texte sera applicable car il est plus clément », souligne Bernard Lamon.

Réagissez à cet article

Source : *Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes*

D’où vient le danger des Objets connectés ?

D’où vient le danger des Objets connectés ?

Le développement des objets connectés s'accélère de plus en plus tandis que la mise en place de moyens de sécurité reste quant à elle beaucoup plus discrète… Tout le monde connaît le récit mythique du cheval de Troie, alors ne sommes-nous pas en train de danser sur ce qui va causer la perte de notre identité à chacun ? Qu'en est-il des normes de sécurité dans le domaine des objets connectés ? Comment pouvons-nous protéger nos données personnelles ?

Deux étudiants en médecine, ont pointé du doigt les failles que pourraient comporter certains objets connectés, dans des actions spectaculaires : prendre le contrôle d'un Pacemaker à distance ou encore désactiver les freins d'une voiture connectée. Ces actions coups de poing mettent à nu les faiblesses que comportent certains objets connectés face à des hackers malveillants. En effet, c'est précisément là que ce situe le paradoxe des nouvelles technologies qu'utilisent les objets connectés… Car s'ils sont conçus pour nous faciliter le quotidien, ils peuvent au contraire nous faire beaucoup de mal et en particulier à nos données personnelles ! Pour pouvoir se protéger, il faut avant tout comprendre cette technologie et adopter quelques habitudes très utiles.

Tout objet connecté peut être hacké

Pour comprendre comment une balance connectée peut devenir notre ennemi numéro 1, il faut d'abord comprendre comment cheminent des data (c'est-à-dire les données personnelles qui sont recueillies pendant l'utilisation de l'objet connecté) vous concernant, quels en sont les tenants et les aboutissants et où sont stocké ces données.
Il existe trois principaux canaux par lesquels voyagent nos data : les réseaux Wifi, le Bluetooth et les réseaux cellulaires pour objets connectés (Sigfox et Lora sont deux des principaux acteurs de ces réseaux).
Ces données sont ensuite acheminées jusqu'aux serveurs du fabricant ou du développeur de l'application pour ensuite revenir vers vous avant de repartir sur le Cloud… Au milieu de tous ces voyages, il devient très facile de voler ou de prendre le contrôle de vos objets, surtout si vous passez par un réseau public.

Le hackage est une menace très sérieuse à prendre en compte

En 2015, on a constaté une augmentation de 50 % de la cyber-criminalité en France ! Les concepteurs et développeurs d'objets connectés nous parlent sans cesse de nouveautés incroyables et parfaites pourtant comment celles-ci sont-elles sécurisés ? Est-ce que les différents fournisseurs appliquent ou suivent des normes ou une réglementation officielle pour sécuriser le matériel de fabrication ? Il semble qu'il n'y ai pas encore de législation officielle qui soit mise en place, même si la CNIL (Commission Nationale de l'Informatique et des libertés) s'est dernièrement attelé au sujet lors du Forum International de la cyber-sécurité.

Sécurité des objets connectés

C'est lors des voyages des data que celles-ci sont les plus vulnérables.
Mais le problème reste entier tant que les données qui voyagent ne seront pas cryptées… Ces données personnelles récoltés par les objets connectées peuvent avoir un intérêt économique pour certaines sociétés.
Ainsi, votre balance connectée peut en dire long sur vos habitudes alimentaires, votre traqueur de sommeil connecté peut donner, lui aussi, de précieuses informations sur vos habitudes de vie quotidienne. Ces données qui peuvent se monnayer très cher favorisent le profilage ciblé pour les publicités notamment et vous enlever petit à petit la liberté d'acheter ce qui vous plaît et non pas ce que l'on vous a suggéré. Le reste des data qui vous concerne, comme vos données bancaires ne sont, également, pas à l'abri d'un hackeur qui chercherait à vous voler de l'argent sans toucher à votre porte-monnaie !

Optimisez la sécurité de vos objets connectés

Face aux deux risques majeurs de la reprise malveillante de vos données personnelles : l'utilisation commerciale et le piratage des donnés personnelles, vous pouvez adopter quelques gestes simples pour augmenter la sécurité de vos data. Si les objets connectés s'avèrent être dans de nombreux cas, un formidable assistant dans la vie quotidienne pour surveiller votre alimentation, votre sommeil, … Au contraire, s'ils sont mal connus ou utilisés d'une mauvaise manière, ils peuvent devenir très dangereux pour le particulier. Vous ne devez pas oublier qu'il est essentiel de comprendre comment fonctionnent ces technologies pour en profiter au maximum sans crainte.
Dans un premier temps, vous devez lister tous les objets connectés en activité dans votre maison et déterminer pour chacun d'entre-eux à quoi ils sont connectés et par quel biais (Wifi ou Bluetooth ou réseau cellulaire). Par cet inventaire un peu minutieux mais très utile, vous pourrez contrôler le cheminement de vos données personnelles et savoir quel objet connecté communique par des biais peu sécurisés. Pour que votre sécurité soit optimale, vous devez également effectuer régulièrement des mises à jour en ce qui concerne la sécurité et surtout changer régulièrement les mots de passe et vos identifiants. Il ne faut pas oublier que même si vos objets connectés restent dans votre maison, les data qu'ils produisent voyagent eux sur le net et donc dans le monde !

Réagissez à cet article

Source : *IOT et sécurité : ne laissez plus le cheval de Troie entrer chez vous*

Une Vauclusienne se fait escroquer de 23000 euros par téléphone

Une Vauclusienne se fait escroquer de 23000 euros par téléphone

Difficile de faire plus simple comme escroquerie : une fausse avocate a escroqué une habitante du Vaucluse de près de 23000 euros par de simples appels téléphoniques

En décembre dernier, la faussaire appelle cette habitante de Saint-Romain en Viennois, près de Vaison-la-Romaine, qui vient de perdre son père, pour lui annoncer qu'il avait contracté une assurance-vie à son bénéfice.
Pour toucher les 127 000 euros de capital, elle doit d'abord payer 9500 euros d'honoraires. Elle s'exécute, après avoir reçu des documents convaincants par mail, et fait un virement… en Lituanie. Quelques jours plus tard, rebelote, cette fois avec un virement de près de 13500 euros en Bulgarie. «Il lui faudra encore quelques jours pour se douter d'une entourloupe.
Elle s'adresse alors à sa banque, qui lui confirme qu'elle a été escroquée», raconte le journal. Un stratagème simple, qui rappelle «l'arnaque au PDG», dont sont victimes depuis plusieurs années de nombreuses entreprises françaises.

Réagissez à cet article

Source : *Une Vauclusienne se fait escroquer de 23000 euros par téléphone*

Après FREAK, une nouvelle

faille dans le chiffrement des connexions

Après FREAK, une nouvelle faille dans le chiffrement des connexions

Une nouvelle faille de sécurité vient de remonter à la surface : #Logjam. Né des cendres de FREAK, elle reprend le même principe de fonctionnement et permet d'établir une connexion chiffrée avec une clé trop petite pour être réellement efficace.

Au début du mois de mars, la #faille FREAK secouait Internet, pour plusieurs raisons. Tout d'abord, car elle permettait (et permet toujours) d'intercepter des échanges de données chiffrés entre un serveur et un navigateur. Ensuite car il s'agissait d'un reliquat des années 90 lorsque les États-Unis limitaient l'exportation des systèmes de chiffrements à 512 bits maximum (voir cette actualité pour plus de détail). Bien évidemment, bon nombre de serveurs et de navigateurs avaient été rapidement mis à jour suite à cette découverte.

Il convient néanmoins de relativiser puisqu'il faut procéder à une attaque de type « homme du milieu » pour l'exploiter, et donc être sur le même réseau (un « hot-spot » Wi-Fi par exemple), ce qui n'est pas toujours des plus pratiques. On est loin de la portée de Heartbleed par exemple, qui permettait à n'importe qui de lire des données directement dans la mémoire d'un serveur (identifiant, mot de passe, carte bancaire, etc.).

De FREAK à Logjam, toujours la même histoire de chiffrement « faible »

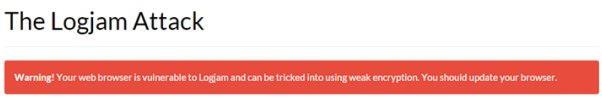
Mais une faille peut en cacher une autre et voilà désormais qu'il est question de Logjam. Elle est détaillée dans ce document, signé par des chercheurs de l'INRIA de Paris et de Nancy, de l'université de Pennsylvanie, de Johns Hopkins, du Michigan et de chez Microsoft Research. Selon les chercheurs, « *cette attaque rappelle FREAK, mais elle est due à une faille dans le protocole TLS plutôt qu'à une vulnérabilité dans son implémentation, et elle cible un échange de clés Diffie-Hellman plutôt que d'un échange de clés RSA* ».

Avec la faille FREAK et l'utilisation de la fonction « export RSA », un serveur répond avec une clé RSA de 512 bits, tandis qu'avec Logjam et « DHE_EXPORT », serveur et navigateur procèdent à un échange de clés via le protocole Diffie-Hellman, mais dans des groupes de 512 bits seulement… ce qui n'est pas suffisant pour résister à une attaque. On notera que ce problème avait déjà été évoqué par certains il y a plusieurs mois. La situation n'est donc pas nouvelle, mais elle prend une autre tournure.

Serveurs et navigateurs doivent se mettre à jour

Là encore, le problème concerne les navigateurs et les serveurs : il suffit que l'un des deux n'accepte pas un groupe de 512 bits pour que l'attaque échoue. De plus, et comme avec FREAK, il faut être sur le même réseau pour que cela fonctionne via une attaque de l'homme du milieu, ce qui limite évidemment la portée, mais n'enlève rien à sa dangerosité.

Du côté des navigateurs, Internet Explorer ne semble pas vulnérable si l'on en croit l'outil de test proposé par le site WeakDH.org, mais Chrome et Firefox le sont. Adam Langley, un cryptanalyste qui travaille chez Google, s'est exprimé sur le sujet sur l'un des forums du géant du web : « *En se basant sur leur travail, nous avons désactivé TLS False-Start avec Diffie-Hellman dans Chrome 42, qui est la version stable depuis plusieurs semaines maintenant* [NDLR : on est passé à Chrome 43 depuis ce matin, mais cela ne change rien sur le principe]*. Cette attaque sur les serveurs vulnérables sera un peu plus difficile* ».



Passer à 1 024 bits minimum, voire mieux à Diffie-Hellman sur des courbes elliptiques

Pour autant, cela n'est pas encore suffisant et Adam Langley ajoute que « *le tronc commun du code de Chrome changera afin d'imposer une nouvelle taille de 1024 bits pour Diffie-Hellman. Même si cela entraînera des problèmes pour certains sites, le travail d'aujourd'hui montre que nous ne devrions pas considérer de tels sites comme sécurisés de toute manière* ». Il précise que « *ce changement est en bonne voie d'être inclus dans Chrome 45* », mais que le calendrier pourrait être plus rapide.

Mais tout cela ne sera probablement qu'une solution temporaire. En effet, les chercheurs à l'origine de la publication de Logjam indiquent qu'un groupe de 1 024 bits peut être « cassé » par un pays ayant suffisamment de moyens (on pense notamment à la NSA qui décrypte à tout-va), et cela ne fera qu'empirer avec le temps. Le cryptographe de Google rejoint cette conclusion : « *Un minimum de 1024 bits ne suffit pas sur le long terme. Malheureusement, parce que certains clients ne prennent pas en charge les groupes de DH supérieurs à 1024 bits, et parce que TLS ne négocie pas spécifiquement certains groupes, il serait très problématique de pousser cette limite au-dessus de 1024. Alors que nous approchons de l'élimination du chiffrement RSA sur 1024 bits, nous nous interrogeons de manière plus générale sur la prise en charge des groupes non elliptiques DHE dans TLS* ». Cela laisse entendre que cette méthode pourrait disparaitre à terme, en tout cas chez Google.

Il existe en effet une version plus sécurisée de ce protocole : ECDHE pour Elliptic curve Diffie–Hellman (ou bien encore Diffie-Hellman sur des courbes elliptiques). Pour Google, « *les serveurs qui utilisent actuellement DHE devraient se mettre à jour et passer à ECDHE. Si cela est impossible, utilisez au moins DHE avec des groupes de 1024 bits et ne soyez pas trop surpris si Chrome commence à utiliser du chiffrement RSA avec votre site dans le futur* ».

Un guide des bonnes pratiques et un site pour tester navigateurs et serveurs

Cette recommandation est d'ailleurs également faite par l'équipe de chercheurs qui a mis en ligne un petit guide du déploiement de Diffie-Hellman, ainsi qu'un outil de test. Il recommande de désactiver les fonctions Export Cipher Suites, déployer un système de Diffie-Hellman sur des courbes elliptiques et utiliser un groupe fort et unique pour chaque serveur.

Comme toujours, on devrait voir arriver une série de correctifs dans les prochaines semaines, à la fois côté navigateur et serveur. Cela ne devrait pas tarder puisque les principaux concernés ont été mis au courant avant que la faille ne soit rendue publique.

Réagissez à cet article

Source : *Logjam : après FREAK, une nouvelle faille dans le chiffrement des connexions – Next INpact*

Le chaos à la suite d'une attaque informatique ?C'est théoriquement possible

Le chaos à la suite d'une attaque informatique ?C'est théoriquement possible

---

L’experte en cybersécurité Solange Ghernaouti évoque l’association des actes de terrorisme classique avec le cyberterrorisme. Elle explique comment des outils de communications peuvent déstabiliser la population.

Invitée du Journal du Matin à l’occasion de la « Journée stratégique 2016 » de l’Association suisse de la sécurité de l’information (Clusis), Solange Ghernaouti explique de quelle manière des systèmes informatiques complexes peuvent déstabiliser le monde réel. Surtout lorsqu’ils tombent dans de mauvaises mains, comme celles de terroristes.

« Le groupe Etat islamique est en train de monter en puissance dans ce domaine. Ils sont très forts dans l’usage de l’internet, notamment dans la communication. » La spécialiste en cybersécurité à l’Université de Lausanne cite l’exemple d’applications sur android pour téléphones portables, développés par l’EI pour communiquer de manière sécurisée.

« Cologne était délibéré »

Selon elle, les agressions sexuelles de Cologne étaient d’ailleurs organisées et aidées par des outils de communication sophistiqués. « Le viol est une arme de guerre », rappelle-t-elle. Or, ces événements étaient une volonté délibérée de déstabiliser la population.

« Nous n’avons pas encore pris la mesure de ce que pouvaient faire les outils de communication pour donner du pouvoir à des terroristes », souligne-t-elle.

Attaquer de gros ouvrages

Au-delà des outils de communication, Solange Ghernaouti évoque aussi les attaques informatiques sur des infrastructures critiques. « Le chaos est théoriquement possible », affirme-t-elle. Par exemple, la Suisse pourrait être privée d’électricité durant plusieurs jours.

Il est également possible, explique-t-elle, de prendre le contrôle des systèmes qui gèrent des barrages, pouvant engendrer des catastrophes naturelles. Pire: en manipulant des données informatiques servant à réguler la qualité de l’eau, il est possible d’infecter des réseaux de distribution.

« Le groupe Etat islamique n’a pas encore les moyens de pirater de grands ouvrages, mais c’est l’étape d’après », alerte Solange Ghernaouti.

Sous-effectifs en Suisse

Si la Confédération a déjà pris conscience des risques et des menaces informatiques possibles, le problème se situe ailleurs, estime-t-elle. « Il y a un décalage entre le conceptuel et les moyens à dégager pour mettre ces risques sous contrôle. »

L’effectif de la cyberdéfense en Suisse se compterait sur les doigts d’une main, selon l’experte, qui appelle le nouveau conseiller fédéral Guy Parmelin à « porter ce débat au niveau le plus haut du pays ».

Réagissez à cet article

Source : *« Avec une attaque informatique, le chaos est théoriquement possible » – rts.ch – Suisse*

La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

	**La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité**

Installé au sein du pôle judiciaire de la gendarmerie nationale à Cergy-Pontoise, le centre de lutte contre les criminalités numériques (C3N) utilise une palette d'outils pour patrouiller sur le web et détecter toutes sortes d'infractions en ligne.
Depuis un an, l'unité lutte de manière active contre la propagande djihadiste et l'apologie du terrorisme. Elle s'est dotée pour cela de nouveaux outils et a renforcé ses équipes.
« Nous sommes un peu la Bac du net. Notre travail consiste à patrouiller sur Internet pour détecter des infractions », explique le colonel de gendarmerie **Nicolas Duvinage**, chef du centre de lutte contre les criminalités numériques. Cette entité, baptisée le **C3N**, rassemble 35 militaires. Elle est installée au Pôle judiciaire de la gendarmerie nationale (**PJGN**), dont les nouveaux locaux se situent à Cergy-Pontoise (Val d'Oise).
Le C3N mène trois principales missions : il anime et coordonne le réseau **CyberGend,** déployé sur tout le territoire, effectue du renseignement criminel (pour réaliser une cartographie et une typologie des auteurs et des victimes et détecter les modes opératoires émergents) et réalise des enquêtes judiciaires pour détecter les fameuses infractions commises en ligne. Dans le cadre de cette mission, les gendarmes interviennent dans plusieurs cas : pour les atteintes aux stades (attaques informatiques), les atteintes aux biens (contrefaçon), et les atteintes aux personnes (porno-pédographie). *« Depuis janvier 2015, nous participons également de manière active à la lutte contre la propagande djihadiste et l'apologie du terrorisme. Nous nous inscrivons dans une activité plus pérenne dans ce domaine»,* confie le colonel Nicolas Duvinage, avant de poursuivre : *« Le but n'est pas simplement de fermer un site ou de retirer des tweets, mais d'identifier les auteurs des tweets et de les interpeller pour les juger ».*

OsintLab pour patrouiller sur Twitter
35 personnes pour patrouiller sur la toile cela fait peu… Les équipes se sont donc équipées d'une palette d'outils de surveillance automatique ou semi-automatique. Un investissement logiciel qui représente plusieurs centaines de milliers d'euros par an. Parmi ces outils, le logiciel **OsintLab** développé par **Thales**et acheté en 2015. Celui-ci permet de sillonner **Twitter** en s'appuyant sur des mots clefs. *« Cet outil nous a permis de mener plusieurs dizaines d'enquêtes judiciaires au travers desquelles nous avons pu identifier des personnes radicalisées »,* assure le colonel. Après avoir « logé » ces personnes, les équipes du C3N transfèrent le dossier à l'échelon spécialisé ou l'échelon territorial compétent, qui se chargera de réaliser l'interpellation.

Advestisearch pour identifier les primo-diffuseurs
Le C3N utilise également le logiciel **Advestisearch** d'**Hologram Industries**, qui permet de rechercher et d'identifier des contenus illégaux et illicites sous forme de texte, d'image ou de vidéo. *« Grâce à une image fournie en entrée, nous pouvons trouver en sortie des images similaires. Par exemple, lorsqu'une équipe de gendarmes récupère une vidéo de 10 secondes, l'outil nous permet de retrouver la vidéo complète. Cela nous permet aussi de détecter les primo-diffuseurs »,* détaille le colonel.

Et bientôt un *Scraper Deep Web* maison
Le C3N n'utilise pas uniquement des logiciels « sur étagère », mais développe également ses propres outils. L'unité s'attèle, par exemple, à mettre au point son propre *Scraper Deep Web*, un outil qui permet de collecter automatiquement des petits morceaux d'information sur des réseaux comme **TOR.** Une démarche qui rappelle le projet **Memex** mené par la **Darpa.** L'agence pour les projets de recherche avancés de défense américaine a, en effet, récemment créé un « *Google du Deep Web* » afin d'aider la police dans ses enquêtes en tout genre.

Le C3N s'emploie également à scruter les jeux en ligne. *« Les auteurs détournent de plus en plus les jeux en ligne comme **Clash of Clan**, **Call of Duty** ou encore **Oh My Dollz** »*, assure le spécialiste. *« Sur Clash of Clan, par exemple, nous avons identifié en 2015 plusieurs dizaines de cas d'apologie du terrorisme et de menaces d'attentats ».*
Outre les logiciels, le C3N mise également sur les compétences humaines. L'unité a récemment recruté plusieurs officiers commissaires, dont un docteur en informatique, un ingénieur en électronique et un universitaire spécialiste des systèmes d'information.

Réagissez à cet article

Source : *Cybercriminalité : la boîte à outils des gendarmes du Net*