Que risquent les enfants sur les réseaux sociaux ?

Que risquent les enfants sur les réseaux sociaux ?

Avoir des profils dans les réseaux sociaux peut représenter de nombreux dangers pour les enfants.
Denis JACOPINI, expert Informatique assermenté spécialisé en cybercriminalité a souhaité couvrir le sujet et a collecté quelques informations bien utiles pour comprendre le phhénomène.

Quels sont les risques d'une trop grande exposition sur les réseaux sociaux?

Attardons nous rapidement sur quelques analyses bien inquiétantes :
• 38% des 9-12 ans ont un profil sur un réseau social, alors que la plupart de ces réseaux ne sont autorisés qu'à partir de 13 ans !
• 77% des 13-16 ans sont présents !
• 1/4 ont un profil public ;
• 1/5 y communique son adresse, son numéro de téléphone…
• Seulement 55% des jeunes discutent avec leurs parents de ce qu'ils font sur Facebook ;
• 92% des jeunes de 8 – 17 ans utilisent leur vraie identité sur Facebook et livrent des informations personnelles ;
• 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook ;
• 36% ont déjà été choqués par certains contenus.

1°/ Les jeunes, trop peu sensibilisés, ont tendance à communiquer bien trop d'éléments (photos, éléments de leur vie). L'effet immédiat est que les cybercriminels auront tous les éléments dont ils auront besoin pour pouvoir usurper leur identité.

2°/ Sur Internet, tout peut être copié collé (et altéré dans le processus), il n'y a aucune garantie de confidentialité dans les échanges électroniques via les réseaux sociaux. Des photos prises lors de soirées ou dénudées peuvent facilement se retrouver à la vue de tout le monde, tout comme un message insultant, écrit dans un moment d'énervement. Les jeunes n'hésitent pas à « taguer » des amis sur les photos de groupe, sans se rendre compte que cette action impacte directement la vue privée des amis tagués.

3°/ Autre risque bien réel, s'exposer sur les réseaux sociaux augmente le risque de contact avec un pédophile cherchant avant tout à rencontrer des enfants ou des ados naïfs, crédules ou confiants.

4°/ Autre faits inquiétants, 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook. Les cyberviolences, souvent initiée à l'école est souvent poursuivies sur les réseaux sociaux sont très courantes. Une publication d'albums de photos de vacances ou d'une soirée entre amis peut vite déraper et se transformer en détournement obscène en ligne avec un impact sur la vie réelle. Intimidations, insultes, piratage de compte, commentaires humiliants, création de groupes de discussion pour moquer la victime – la violence des rapports entre jeunes peut pousser la victime jusqu'au suicide.
Le phénomène d'entraînement peut conduire les plus influençables à imiter des comportements violents et à se lancer dans des campagnes d'insultes contre le bouc émissaire désigné par le leader du groupe.

5°/ Enfin, risque souvent méconnu, les cybercriminels rivalisent d'ingéniosité pour concevoir des messages séduisants qui invitent à « Liker » un post viral avec un lien corrompu, des applications contenant des virus, des campagnes de phishing pour soutirer les informations de connexion, etc.

A la suite d'une exposition trop massive sur les réseaux sociaux, est-ce qu'un nouveau type de criminalité est né ?
Je répondrais à celà qu'un nouveau terrain de jeu est né !
Un espace rempli de prédateurs ou les jeunes sont des proies potentielles.

Comment optimiser la sécurité sur les réseaux sociaux?
Limitez la navigation et les échanges dans un périmètre adapté à l'âge et aux besoins du jeune. Si besoin, bloquez les réseaux sociaux jusqu'à ce qu'il soit en mesure de comprendre l'impact de ses interactions en ligne.
Discutez régulièrement avec votre enfant ou ado de ce qu'il fait sur Internet : quels sites il aime consulter, avec qui il tchatte, ce qu'il ou elle a découvert de nouveau. Expliquez-lui la différence entre de vrais amis et des connaissances numériques.
Apprenez aux enfants l'importance de la protection des informations personnelles, que ce soit les leurs ou celles de leurs amis. Informer le monde que l'on est seul ce week-end n'est peut être pas l'action la plus prudente, tout comme « taguer » ses amis sur une photo peu valorisante.
Vérifiez que les paramètres de protection de vie privée sont activés sur toutes les plates-formes utilisées par l'enfant. Expliquez que les traces numériques resteront dans le temps et qu'ils seront un jour ou l'autre confrontés à leurs actions en ligne. Soulignez l'importance de mesurer ses propos et de ne pas participer aux chasses à l'homme digitales.
Expliquez au jeune que si jamais il (ou elle) est victime d'harcèlement, ou bien s'il voit ses camarades s'acharner contre quelqu'un, il doit avertir le plus rapidement un adulte, parents ou professeur.
Souvent les enfants n'osent pas avouer, par honte ou bien parce qu'ils sont manipulés par les harceleurs.
Pour plus d'informations, consultez le site du Ministère de l'Éducation Nationale Agir Contre le Harcèlement à L'École (http://www.agircontreleharcelementalecole.gouv.fr).

Réagissez à cet article

Sources :

Denis JACOPINI

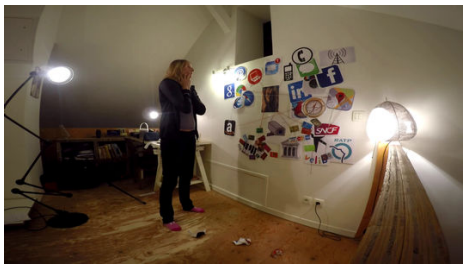
http://www.e-enfance.org/actualite/enfants-et-reseaux-sociaux-prudence-_151.html

http://www.e-enfance.org/enfants-danger-reseaux-sociaux.php

http://www.witigo.eu/controle-parental/dangers-reseaux-sociaux

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*

Comment limiter simplement les risques de piratage informatique en entreprise ?

Comment limiter simplement les risques de piratage informatique en entreprise ?

La plupart du temps, les entreprises redoutent les cyberattaques provenant de l'extérieur. Pourtant, le personnel opérant dans les murs disposent souvent de droits d'accès excessifs par rapport à leurs rôles, et constituent le vecteur le plus probable de défaillances de sécurité, que ce soit en s'impliquant activement dans des activités malveillantes ou, plus souvent, en devenant inconsciemment les fournisseurs de comptes piratés et des droits associés. Entre 50% et 70 % des attaques réussies sont attribués à des utilisateurs internes. D'où la nécessité d'adopter un système IAM pour gérer dans les règles de l'art les identités des utilisateurs, et surveiller en permanence leurs droits d'accès aux ressources informatiques.

En collectant l'ensemble des informations liées à la structure d'autorisations, les solutions d'Identity and Access Intelligence offrent une vue d'ensemble des droits d'accès et des risques associés. Ces solutions disposent d'une ergonomie moderne et intuitive pour explorer, manipuler et restituer les données. S'appuyer sur des analyses approfondies et exhaustives facilite très largement le contrôle et l'audit des risques, la prise de décision et la gouvernance.
Ce guide pratique revient sur les principes de base de l'Identity and Access Intelligence. Il fournit un cadre simple pour aider votre entreprise à identifier les risques associés aux utilisateurs et liés à leurs droits d'accès.

1. Analyser les données de droits d'accès et évaluer les risques associés
Les solutions d'Identity and Access Intelligence s'appuient sur les technologies de business intelligence pour collecter les données d'identités et d'accès existantes, et les convertir en informations qualitatives facilitant la prise de décision. Elles fournissent à leurs utilisateurs une vue à 360° de toutes les informations liées aux droits d'accès (utilisateurs, rôles, groupes, ressources…) qui permet de naviguer de manière active au sein de ces données. Ils pourront les analyser depuis de multiples angles et axes à l'aide d'une interface graphique optimisée. Les systèmes les plus avancés proposent des analyses prêtes à l'emploi ainsi que des analyses ad-hoc pour construire ses propres requêtes.
Les solutions d'Identity and Access Intelligence permettent également d'identifier les risques potentiels associés aux utilisateurs et liés à leurs droits d'accès : utilisateurs à haut risque, comptes orphelins, failles de sécurité… Grâce à des indicateurs de risque et de conformité, l'entreprise peut se concentrer sur l'essentiel et dispose d'une aide précieuse au pilotage. Elle est alors en mesure de corriger plus rapidement des incohérences et des erreurs d'attribution de droits, et de mieux protéger ses ressources informatiques contre des interventions non autorisées et potentiellement dangereuses. En s'appuyant sur des faits démontrés, l'entreprise dispose des moyens nécessaires pour prouver l'efficacité des procédures de contrôle mises en place.

2. Adapter les informations à chaque type d'utilisateur
Le plus souvent, les solutions d'Identity and Access Intelligence intègrent des fonctionnalités d'exploration des données, comme l'analyse verticale et transversale, qui facilitent la recherche d'information et l'obtention de réponses pertinentes. La présentation graphique et intelligible des informations est adaptée à toutes les populations de l'entreprise : administrateurs informatiques, équipes métiers, auditeurs, direction générale…
Les RSSI et les auditeurs souhaitent visualiser les données de sécurité dans le moindre détail. Ils disposent d'un outil de surveillance dynamique à 360 degrés qui leur permet de déterminer le niveau de risque et le type de risque associés à un utilisateur. Ils peuvent aussi créer des rapports ad-hoc personnalisés pour croiser les informations comme bon leur semble et visualiser les données de sécurité qui les intéressent.
Les responsables métiers ont besoin de rapports standards prêts à l'emploi pour identifier rapidement les risques liés aux habilitations de leurs équipes et se concentrer sur les zones à haut risque. Pour aller à l'essentiel, la direction générale peut accéder à des tableaux de bord reprenant les principaux indicateurs de risque pondérés et hiérarchisés. Ils offrent un point de départ synthétique vers une analyse en profondeur si nécessaire. En pilotant l'évolution des indicateurs dans le temps, les décideurs déterminent les actions correctives à mener pour réduire le niveau de risque et améliorer la gouvernance à l'échelle de l'entreprise.

3. Réaliser un examen historique complet des droits d'accès
Les systèmes les plus avancés permettent de reconstituer tous les changements de droits ayant eu lieu au préalable, grâce à une historisation des modifications. Les changements de droits sont alors identifiés, tracés et consultables en toute simplicité.
Cette fonctionnalité est précieuse pour les auditeurs, car elle leur donne les moyens d'établir des pistes d'audit et de réaliser des investigations forensiques approfondies et exhaustives. En fonction de leurs besoins, ils passent en revue les droits d'accès d'un utilisateur à une date spécifique dans le passé, ou contrôlent ses changements successifs d'habilitations pendant une période donnée. Ainsi, l'historisation des droits d'accès est une fonctionnalité nécessaire pour détecter toute modification suspecte, identifier la source d'un problème, et réduire l'impact d'une fraude.

4. Identifier les utilisateurs à haut risque
Les solutions d'Identity and Access Intelligence offrent une visibilité à la demande sur les données de droits d'accès. Les informations relatives aux risques et aux habilitations sont mises à disposition dans un format compréhensible et intelligible, ce qui facilite très largement l'identification des groupes d'utilisateurs présentant le plus haut niveau de risque.
Une des recommandations de base de l'IAM est d'appliquer le principe du moindre privilège qui consiste à limiter les droits d'accès des utilisateurs au minimum requis pour leurs fonctions dans l'organisation. C'est pourquoi l'entreprise devra se concentrer sur la surveillance des utilisateurs à risque et évaluer régulièrement la pertinence de leurs droits d'accès spécifiques… [Lire la suite]

Réagissez à cet article

Source : *Bastien Meaux, Beta Systems : Le guide pratique de l'Identity and Access Intelligence – Global Security Mag Online*

L'eau d'une station

d’épuration manipulée par des hackers – Sciencesetavenir.fr

L’eau d’une station d’épuration manipulée par des hackers

L'opérateur de télécommunications américain Verizon révèle dans un rapport une cyberattaque ayant touché à la composition et à la distribution d'eau potable d'une station. Le système informatique était perclus de failles.

Le bilan dressé par l'opérateur américain Verizon publié en mars 2016 et consacré aux fuites de données a de quoi faire frémir. Il recense pas moins de cinq cents incidents de cybersécurité dans quarante pays en 2015 (le rapport en anglais ici**).** Parmi eux, l'un attire tout particulièrement l'attention : il concerne la Kemuri Water Company (KWC), une station d'épuration bien réelle mais dont le nom a été changé et le pays d'implantation non divulgué pour éviter de la compromettre. Et pour cause ! Verizon relate la façon dont des hackers ont réussi, très facilement, à manipuler la composition chimique de l'eau qui est redistribuée aux habitants après traitement ! Le tout, sans même en avoir eu l'intention au départ…
L'affaire a été révélée lorsque la société a décidé de faire appel aux équipes chargées du cyber-risque de Verizon pour renforcer son système d'information afin d'anticiper tout problème éventuel. Or, une fois sur place, les experts ont constaté avec stupeur que la station d'épuration était déjà la proie de pirates informatique depuis deux mois ! Et que ses responsables s'en doutaient… Des mouvements suspects de valves et de tuyauteries avaient été remarqués. Beaucoup plus grave ! Les gestionnaires avaient constaté des modifications inexpliquées de dosage dans les produits injectés dans l'eau pour la rendre portable. Sans conséquence désastreuse heureusement…

« Pour tout dire, KWC était un candidat tout trouvé pour une fuite de données. Son interface Internet présentait plusieurs failles à haut risque dont on sait qu'elles sont souvent exploitées» mentionne le rapport de Verizon. Et son système opérationnel, qui commande les applications industrielles (traitement des eaux, gestion du débit), reposait quant à lui sur une infrastructure informatique vieille de plusieurs dizaines d'années.
En outre, de nombreuses fonctions de ce système cohabitaient avec des applications « business » de l'entreprise sur un même et unique serveur, un AS/400 d'IBM, ordinateur commercialisé en… juin 1988. En clair, si des hackers pénétraient le système, ils pouvaient sans peine passer du contrôle du traitement des eaux aux informations financières et aux données de facturation de la compagnie. Et c'est exactement ce qui s'est passé.

L'opérateur liste une série de failles assez confondantes

Au cours de son enquête, Verizon s'est rendu compte que des adresses IP de hackers déjà rencontrées dans trois autres affaires s'étaient connectées au système de paiement en ligne de la KWC, cette interface permettant aux clients d'accéder à leur compte à distance (depuis un ordinateur, un mobile) ; c'est a priori par cette voie que les hackers sont passés, comme d'autres l'ont fait lors du piratage en octobre 2015 de l'hydrolienne Sabella.

2,5 MILLIONS. L'opérateur liste ensuite une série de failles confondantes : l'accès aux données clients n'était protégé que par un login/mot de passe, sans double authentification ; une « *connexion directe par câble* » existait entre l'application de paiement en ligne et l'AS/400, ce dernier ayant un accès ouvert à Internet, avec une adresse IP et des données d'identification administrative disponibles sur le serveur web de paiement, écrites en clair dans un fichier ! Au final, les pirates ont pu sortir du système 2,5 millions de dossiers clients avec leurs données de paiement. Pour l'heure, il semble qu'ils n'en aient pas fait usage.

ALERTE. Mais le plus grave restait à venir. Une fois à l'intérieur du réseau, les pirates se sont en effet rendus compte qu'ils pouvaient accéder aux fonctions opérationnelles.
En se servant des données d'identification administrative, ils ont ainsi pu intervenir sur des fonctions clés : le débit de l'eau potable, son traitement chimique et le temps de remplissage des réserves. A priori – et c'est une chance – les hackers ne semblent pas avoir eu l'intention de nuire et ne poursuivaient pas un but précis, mais les autorités frémissent à l'idée des conséquences dramatiques qu'une telle ingérence aurait pu occasionner. « *Si les attaquants avaient eu un peu plus de temps et avaient été un peu plus familiers du système de contrôle industriel, la KWC et les populations locales auraient pu subir de sérieux dommages* » conclut le rapport… [Lire la suite]

Réagissez à cet article

Source : *L'eau d'une station d'épuration manipulée par des hackers – Sciencesetavenir.fr*

La Cnil veille sur vos données de e-santé

La Cnil veille sur vos données de e-santé

Chercheurs et médecins ont de plus en plus recours à des objets connectés pour suivre les patients ou collecter des informations. La protection de ces données est devenu un enjeu de taille.

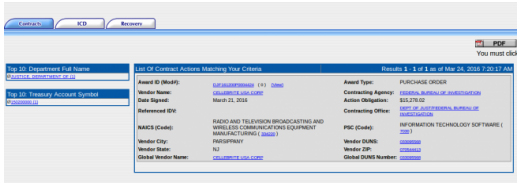
L'utilisation des technologies de l'information et de la communication dans le domaine de la santé pose un problème majeur : celui de la sécurisation des données. Portant sur la santé, elles sont dites « sensibles » au regard de la loi et donc soumises à une protection particulière.
En France, c'est la Commission nationale de l'informatique et des libertés (Cnil) qui y veille, en s'assurant de l'application de loi Informatique et Libertés de 1978.
Dans une étude de mai 2014, la Cnil a constaté que l'information sur l'utilisation des données personnelles par les éditeurs d'objets connectés et applications santé était insuffisante.

700 projets par an
Par ailleurs, la loi Informatique et Libertés impose que la sécurité porte « sur le fait que des tiers ne puissent pas accéder aux données, mais aussi sur l'intégrité des données », énonce Délia Rahal-Lofksög, responsable du service santé à la Cnil.
Il s'agit donc pour un éditeur de s'assurer qu'en cas de bug, piratage ou autre problème technique, les informations médicales délivrées ne seront pas erronées (diagnostic d'hyperglycémie au lieu d'hypoglycémie, par exemple).
Afin de renforcer et homogénéiser cette protection, un règlement européen en cours d'adoption, prévoit que des analyses d'impact sur la vie privée soient mises en place par les responsables de fichier afin d'évaluer, par exemple, les conséquences d'un piratage de données.
Enfin, tous les projets de recherches utilisant des données personnelles doivent préalablement faire l'objet d'une validation par la Cnil, qui en autorise en moyenne 700 par an, parmi lesquels figurent des projets impliquant des objets connectés… [Lire la suite]

Réagissez à cet article

Source : *E-santé : la Cnil veille sur vos données*

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*

L'Europe renforce la pression sur Apple pour ouvrir l'accès aux données personnelles des utilisateurs

L'Europe renforce la pression sur Apple pour ouvrir l'accès aux données personnelles des utilisateurs

---

Suite aux attaques terroristes de Bruxelles, les autorités européennes envisagent de forcer Apple et d'autres sociétés à ouvrir l'accès aux données personnelles des utilisateurs aux services spéciaux.

Les parlementaires français ont déjà commencé les débats sur le projet de loi à ce sujet. Ils sont convaincus qu'en choisissant entre l'élargissement des pouvoirs des services de sécurité en vue de prévenir des attentats terroristes et le respect de la vie privée, il est raisonnable d'opter pour le premier choix, lit-on dans le New York Times.
Les députés proposent de sanctionner les chefs des sociétés spécialisées dans les technologies de pointe, qui refusent de fournir des informations aux enquêteurs, d'une peine privative de liberté de cinq ans au maximum et d'une amende de 350.000 euros. Selon le New York Times, telle est également la position adoptée par le Royaume Uni.
Les sociétés en question quant à elles essayent de faire de leur mieux pour éviter un tel scénario. Ces derniers temps, le président d'Apple Tim Cook a personnellement rencontré plusieurs politiciens européens, y compris le premier ministre français Manuel Valls et la chef de la diplomatie britannique Theresa Mary May afin de s'assurer leur appui.Auparavant, le tribunal de Californie avait ordonné à Apple de fournir aux enquêteurs du FBI, dans l'affaire de l'attaque terroriste de San Bernardino, des données chiffrées sur l'iPhone du terroriste tué, après que l'entreprise ait refusé de coopérer volontairement avec les autorités.
Le directeur général d'Apple, Tim Cook, avait rétorqué que cette exigence présentait une menace pour la sécurité de ses clients, tandis que ses conséquences « étaient hors du cadre légal ». La société a refusé de se conformer à la décision du tribunal, déclarant avoir l'intention de faire appel… [Lire la suite]

Réagissez à cet article

Source : *Après Bruxelles, l'Europe renforce la pression sur Apple*

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

Les autorités américaines affirment avoir « accédé avec succès aux données contenues dans l'iPhone de Syed Farook » et ont demandé à la justice d'annuler l'injonction obligeant la firme à la pomme à assister les enquêteurs.

Ce déblocage a été rendu possible par *« l'assistance récente d'un tiers »* (ndlr Cellebrite), selon un communiqué de la procureure fédérale du centre de la Californie, Eileen Decker. Elle indique en conséquence avoir demandé à la justice d'annuler l'injonction obligeant Apple à aider les enquêteurs. La firme refusait de se plier aux demandes judiciaires, soutenant qu'aider à décrypter le téléphone de Syed Farook créerait un précédent, sur lequel les autorités risquaient de s'appuyer à l'avenir pour réclamer l'accès aux données personnelles de nombreux citoyens pour diverses raisons.

« Viabilité »

Lundi 21 mars, les autorités fédérales avaient annoncé être sur la piste d'une méthode qui pourrait leur permettre d'accéder aux données du téléphone. Une audience clé, qui devait avoir lieu mardi au tribunal de Riverside en Californie, avait été annulée, après le dépôt d'une motion demandant un délai pour tester *« la viabilité »* de cette solution alternative.

Le gouvernement expliquait avoir *« poursuivi ses efforts pour accéder à l'iPhone »* pendant la procédure judiciaire et annonçait que des *« tierces parties »* lui avaient présenté une manière de décrypter son contenu sans la coopération d'Apple. La police fédérale demandait un peu de temps pour s'assurer que la méthode ne *« détruit pas les données du téléphone ».*

Une semaine plus tard, il semble donc que la méthode fonctionne. Washington affirme à la cour fédérale avoir *« accédé avec succès aux données contenues dans l'iPhone de Syed Farook »* et *« ne plus avoir besoin de l'assistance d'Apple »*… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : Washington a débloqué l'iPhone du*

tueur et renonce à poursuivre Apple

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*

Mise à jour urgente Java. Patch d'une vulnérabilité critique de 2013

Mise à jour urgente Java. Patch d'une vulnérabilité critique de 2013

Oracle vient de livrer un correctif de sécurité pour combler une faille critique dans Java remontant à 2013. Cette dernière avait été découverte seulement en début d'année.

Oracle a publié une mise à jour de sécurité **urgente** pour corriger une vulnérabilité critique dans Java permettant à des attaquants de compromettre les ordinateurs d'internautes se rendant sur des sites web spécialement conçus pour les piéger. L'identifiant de cette vulnérabilité est CVE-2016-0636, suggérant qu'il s'agit d'une nouvelle mais cela n'est pas vraiment le cas. Dans un mail, la société de sécurité polonaise Security Explorations a confirmé que cette mise à jour patche une faille originellement rapportée à Oracle en 2013.
En début de mois, cette même société avait indiqué qu'un correctif publié par Oracle en octobre 2013 pour une vulnérabilité critique, portant l'identifiant CVE-2013-5838, s'était révélé inefficace et pouvait être contourné en changeant seulement 4 caractères de l'exploit original. Cela signifie que la vulnérabilité était toujours exploitable dans les dernières versions de Java. Or, dans son dernier bulletin, Oracle n'a fait aucune mention à l'ancienne faille trouvée par Security Explorations. Etrange renvoi d'ascenseur, non ?

L'update 77 pour Java SE 8 indispensable

Oracle recommande d'installer dès que possible cette nouvelle mise à jour Java, compte-tenu du degré de sévérité de la vulnérabilité et des détails techniques de contournement désormais rendus publics. Les utilisateurs de Java SE 8 sont prévenus d'installer l'update 77 (8u77), sachant que pour les possesseurs de Java 6 et 7, la mise à jour n'est proposée qu'en cas de support long terme, ces versions n'étant plus supportées … [Lire la suite]

Réagissez à cet article

Source : *Une vulnérabilité critique de 2013 patchée dans Java – Le Monde Informatique*