Une faille de sécurité dans le système de messagerie Whatsapp ?

	Une faille de sécurité dans le système de messagerie Whatsapp ?

Le quotidien britannique The Guardian affirme que le « backdoor » (porte dérobée) de l'application de messagerie détenue par Facebook permettrait d'avoir accès aux conversations des utilisateurs.

Pourrait-on pirater les données partagées sur WhatsApp? L'application de messagerie, détenue par Facebook, possède une porte dérobée (« backdoor ») la rendant vulnérable à l'espionnage, a affirmé vendredi le quotidien britannique *The Guardian*.

Tobias Boelter, un chercheur en cryptographie et sécurité de l'université de Californie à Berkley, a expliqué au journal avoir découvert la présence d'une « porte dérobée » permettant d'avoir accès aux conversations cryptées du plus d'un milliard d'usagers que compte WhatsApp, alors que ces conversations sont censées être protégées par le chiffrement de bout en bout.

Des messages décryptés à l'insu de destinataire

Cette porte dérobée, affirme le *Guardian*, permet à WhatsApp de récupérer, lorsque les téléphones sont éteints, des messages cryptés envoyés mais pas encore lus. WhatsApp peut alors les déchiffrer et les envoyer à nouveau au destinataire qui n'est pas informé du changement de chiffrement. L'expéditeur est quant à lui prévenu seulement s'il a activé une option de sécurité.

Cette nouvelle opération de cryptage permet en pratique à WhatsApp d'intercepter et de lire les messages de ses utilisateurs, explique le journal britannique. Tobias Boelter estime donc que « si WhatsApp se voit demander par une agence gouvernementale de révéler ses messages archivés, il peut tout à fait donner accès (à ces archives) grâce aux changements dans les clés » de cryptage.

Un porte-parole de WhatsApp s'est défendu d'offrir « toute porte dérobée vers ses systèmes » et ajouté dans un communiqué que WhatsApp « se battra contre toute demande de gouvernement réclamant la création d'une porte dérobée »,

« WhatsApp peut continuer de changer les clés de sécurité »

WhatsApp a justifié la possibilité de forcer la génération de nouvelles clés de cryptage comme une facilité offerte à ses clients qui dans de nombreux pays changent fréquemment de carte Sim et d'appareil téléphonique, afin que leur messages ne soient pas perdus. Steffen Tor Jensen, responsable de la sécurité et de la contre-surveillance digitale de l'Organisation européenne-bahreïnite pour les droits de l'Homme a vérifié les découvertes du chercheur américain, selon le *Guardian*.

« WhatsApp peut effectivement continuer de changer les clés de sécurité quand les téléphones sont hors ligne et renvoyer le message sans que les utilisateurs aient connaissance du changement » avant que celui-ci ait lieu, a-t-il dit, qualifiant le service de « plateforme extrêmement peu sûre »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Une faille de sécurité détectée dans le système de messagerie Whatsapp? – L’Express L’Expansion

---

Le réseau électrique américain pénétré par des pirates Russes

Le réseau électrique américain pénétré par des pirates Russes

---

Washington – Des pirates informatiques russes sont parvenus à pénétrer le réseau électrique américain via un fournisseur du Vermont, une cyberattaque sans conséquence sur les opérations de cette entreprise mais qui a pu révéler une « vulnérabilité », rapporte vendredi le Washington Post.

« Un code associé à l'opération de piratage informatique baptisée Grizzly Steppe par l'administration Obama a été détecté à l'intérieur du système d'un fournisseur d'électricité du Vermont », écrit le quotidien sur son site Internet, sans indiquer de date.
Se référant à des responsables américains non identifiés, il souligne que ce si code *« n'a pas été activement utilisé pour perturber les opérations du fournisseur* […] *la pénétration du réseau électrique national est importante parce qu'elle représente une vulnérabilité potentiellement grave ».*
Les autorités américaines ignorent à ce stade quelles étaient les intentions des Russes, poursuit le *Washington Post*, supputant qu'ils pourraient avoir tenté de porter atteinte aux activités du fournisseur –non identifié par les sources du journal– ou qu'il pourrait simplement s'agir d'un test de faisabilité.
Selon le journal, le Vermont compte deux importants fournisseurs d'électricité : Green Mountain Power et Burlington Electric.
Les pirates russes auraient envoyé des emails pour piéger les destinataires, leur faisant révéler leurs mots de passe.
En décembre 2015, 80 000 habitants de l'ouest de l'Ukraine avaient été plongés plusieurs heures dans le noir à la suite d'une cyberattaque d'une ampleur inédite. Les Russes avaient été désignés comme en étant les auteurs, ce qu'ils avaient nié…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Des pirates russes ont pénétré le réseau électrique américain | Le Devoir

---

Le boîtier connecté d'Amazon, témoin-clé d'une affaire de meurtre aux États-Unis ?

	Le boîtier connecté d'Amazon, témoin-clé d'une affaire de meurtre aux États-Unis ?

CLUEDO. Qui a tué le docteur Lenoir ? À l'heure de la maison connectée, il suffira peut-être de le demander aux objets domotiques qui enregistrent silencieusement nos faits et gestes, et pourraient ainsi contribuer à blanchir ou accabler un suspect aux yeux de la justice.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..

(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Quelles tendances en 2017 pour la sécurité du Cloud ?

Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ». Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? – Globb Security FR

Tendances actuelles et émergentes pour la cybersécurité en 2017

Tendances actuelles et émergentes pour la cybersécurité en 2017

Original de l’article mis en page : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 – Global Security Mag Online

---

Les mails de Clinton piratés par des «hackeurs russes», stratégie de diversion ?

Les mails de Clinton piratés par des «hackeurs russes», stratégie de diversion ?

Les Etats-Unis utilisent la Russie comme un «ennemi commode», dont l'existence est indispensable pour entretenir leur complexe militaro-industriel, explique Jean-Robert Raviot, professeur des études russes.

RT France : Barack Obama a donné vendredi passé sa dernière conférence de presse en tant que président, où il a évoqué la Russie et les hackers russes qui auraient piraté les comptes du Parti démocrate américain alors que, selon la déclaration du procureur général des Etats-Unis, il n'y a pas de preuve de l'origine de ces attaques. Pourquoi alors accuser la Russie ?

Jean-Robert Raviot (J.-R. R.) : Il faut chercher la réponse dans une logique qui n'est pas proprement en Russie, mais plutôt à Washington. C'est à dire qu'on assiste aujourd'hui à un tir de barrage contre Donald Trump de la part du Parti démocrate et d'un certain nombre de gens qui soutenaient la candidature de Hillary Clinton. Dans cette affaire il y a trois points qui soulèvent question pour moi. Premièrement, sur un plan technique – pourquoi est-ce que ce hacking, s'il est avéré qu'il a été repéré par la CIA, n'est-il pas rendu public ? Et surtout, pourquoi la NSA, qui en principe devrait avoir une vision assez claire des opérations de hacking sur le territoire américain, ne s'est-elle pas prononcée ?

Le fait d'accuser le Kremlin et les hackers russes d'avoir monté cette opération, permet de détourner l'attention du fond des mails

Je crois qu'il faut remarquer que personne de la NSA n'a donné son avis sur la question. Pour moi, ça met déjà un gros doute sur la réalité de ce hacking, sur la preuve qu'on peut avoir que des hackers russes ont agi pour prendre possession de ces mails de Podesta et ceux de Clinton. C'est un point technique, mais qui me semble important quand-même. Parce que cette question n'est pas résolue, et personne ne la pose vraiment.

On a cherché à discréditer Bernie Sanders. C'est ça le problème

Le deuxième point, comme je l'analyse, c'est la volonté de brouiller un peu l'information. Le fond de l'affaire c'est ce qu'il y a dans ces mails, et la preuve, que du côté de Hillary Clinton, on a cherché à discréditer Bernie Sanders. C'est ça le problème. On voit très clairement dans ces mails une opération interne du Parti démocrate visant tout simplement à mettre de côté Bernie Sanders, à lui mettre des bâtons dans les roues dans cette campagne électorale et dans cette primaire. C'est très clairement avéré. Le fait d'accuser la Russie ou le Kremlin ou les hackers russes d'avoir monté cette opération, permet de détourner l'attention du fond des mails.

Barack Obama exige un rapport sur le piratage, dont les résultats ne seraient pas rendus publics

Du coup, plus personne ne parle de la réalité de ce qui est dit dans ces mails, et du fait qu'ils ne sont pas rédigés par les hackers, mais par les gens qui ont tenu ces correspondances. Je dirais, c'est un moyen de détourner l'attention du grand public sur un problème qui n'est pas le même. C'est comme le vieux proverbe chinois : «Le sage montre la lune, et l'idiot regarde le doigt qui montre la lune». C'est absolument une stratégie de diversion.

La volonté c'est de se servir d'un ennemi assez commode, parce que c'est l'ennemi historique de la guerre froide – ça permet de mobiliser des récits qui sont déjà écrits et qui résonnent dans les têtes des gens

Le troisième point c'est la véritable volonté de la part d'un groupe dirigeant actuellement aux Etats-Unis, qui est autour d'Obama, autour du Parti démocrate, de Hillary Clinton et leurs soutiens, d'essayer de ramasser un maximum d'arguments. Pour l'instant, je pense qu'il y a des gens qui préparent l'impeachment de Trump. Je pense que c'est un peu rapide de dire ça – pour le moment, il n'est pas encore investi, on ne peut pas faire la destitution de quelqu'un qui n'est pas encore investi. Mais je pense que l'objectif c'est de faire une campagne, de tenter d'orienter le vote des grands électeurs et de faire en sorte qu'ils ne votent pas pour Trump.

RT France : Pourquoi ont-ils choisi Vladimir Poutine et la Russie, et non pas la Chine, par exemple, en guise de bouc émissaire ?

***J.-R. R. :** Parce que la Russie, je dirais, a été désignée comme l'ennemi principal non seulement des Etats-Unis, mais aussi de l'Alliance atlantique. Rappelez-vous, quand en juillet 2016, au sommet de Varsovie de l'OTAN, **on a désigné la Russie comme menace principale**, alors que le djihadisme apparaît à peine dans le texte. C'est quand-même incroyable. La volonté c'est de se servir d'un ennemi qui existe, un ennemi qui est assez commode, parce que c'est l'ennemi historique de la guerre froide – ça permet de mobiliser des récits qui sont déjà écrits et qui résonnent dans les têtes des gens. C'est un ennemi familier, en quelque sorte. En même temps, l'image de Poutine permet d'associer cette image à un homme fort, anti-Obama, par sa personnalité, on peut facilement l'opposer aux dirigeants occidentaux. Et puis, ça résonne aussi assez bien dans le contexte de la guerre en Syrie et surtout de la guerre qu'on veut mener. C'est la narration de cette guerre qu'on veut imposer, c'est-à-dire, un soutien certainement des forces anti-Assad et anti-régime, de continuer ces opérations de «regime change», qui ont commencé en 2003, tout en s'appuyant sur le pays qui s'y oppose pour l'instant militairement, d'une manière directe…**[lire la suite]**

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.*

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

*Plus d'informations sur : **https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles***

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les «hackeurs russes», une stratégie de diversion pour oublier le contenu des mails de Clinton – RT en français

---

La chasse aux pirates informatiques est bien lancée

La chasse aux pirates informatiques est bien lancée

Les forces de l'ordre enquêtent aussi devant des ordinateurs. Rencontre et décryptage avec le lieutenant-colonel Cyril Piat, du Centre de lutte contre les criminels numériques (C3N), qui dépend de la gendarmerie nationale.
A la télévision, il y a Les experts, capables de retrouver des criminels à l'autre bout du pays, via une connexion internet, ou de dévoiler une identité en « crackant » le mot de passe d'un site. Dans le réel, la gendarmerie française fait la même chose, et bien d'autres investigations encore.
La cybercriminalité est en effet un phénomène regardé avec beaucoup d'attention. Et s'il est difficile de donner des chiffres précis pour le quantifier, une minorité d'affaires étant au final connue, son importance et son évolution sont réelles, indique avec le lieutenant-colonel Cyril Piat, numéro 2 du Centre de lutte contre les criminels numériques, le C3N (la police a un équivalent).

Le darkweb, c'est quoi ?
Beaucoup d'utilisateurs ne connaissent d'internet que sa face lumineuse d'échanges d'informations et de connexions humaines à travers le monde entier. Pourtant, existe aussi le darkweb, l'autre face, parfois très sombre d'internet. Celle qui se cache derrière des mots de passe, dans laquelle il faut déjà connaître l'adresse du site que l'on souhaite rejoindre pour pouvoir y accéder, et que l'on découvre à travers Tor, I2P ou Freenet, des navigateurs et réseaux très spécifiques qui pratiquent l'anonymat.

Que peut-on y trouver ?
Imaginés pour contourner la surveillance et la censure, ces derniers sont devenus un lieu parfait pour les criminels. Ils utilisent des nœuds de serveurs dans le monde entier et pratiquent le chiffrement des données en cascade et sont souvent intraçables. Que peut-on y trouver ? De nombreux services tels que la vente de drogues, d'armes, de faux papiers, ou le piratage informatique. Sur Alphabay Market, par exemple, 31 000 annonces pour fraudes sont proposées. On trouve aussi un service de mise en relation de personnes pour des bijoux ou des armes.

Des dizaines d'enquêteurs
« Cela peut représenter de 2 à 5 millions d'euros par mois. Et la cybercriminalité est en permanente évolution, tous les trois ou six mois, en fonction des évolutions technologiques. » Avec une difficulté supplémentaire : intervenir à l'échelle mondiale et devoir demander la coopération d'opérateurs pas toujours conciliants…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité en région : la chasse numérique est bien lancée

---

L’essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg

La surveillance au travail pourrait être modifiée

Les députés se sont penchés lundi sur le nouveau cadre concernant la protection des données au Grand-Duché.

Un patron pourrait bientôt ne plus avoir besoin de demander une autorisation préalable à la Commission nationale pour la protection des données (CNPD) avant de placer ses employés sous vidéosurveillance au travail. Cette mesure fait partie d'un projet de loi concernant la protection des données privées que les députés ont commencé à étudier lundi et qui s'inscrit dans le nouveau règlement européen qui entrera en vigueur le 25 mai 2018.

Le texte supprime la liste de traitement des données qui est aujourd'hui soumis à autorisation préalable de la CNPD, dont les traitements effectués à fin de surveillance. La CNPD fera, selon le projet de loi, des contrôles a posteriori, dans un but de simplification administrative. Un changement qui a suscité l'inquiétude de plusieurs députés, soucieux de protéger les citoyens d'une surveillance illégale par leurs employeurs.

La Chambre des salariés avait émis un avis défavorable en novembre, «dénonçant d'emblée la suppression de l'autorisation préalable (…). Elle s'oppose plus particulièrement, et de manière formelle, à cette exemption en faveur des traitements à des fins de surveillance sur le lieu de travail», expliquant que la loi actuelle, de 2002, «traduisait justement la volonté expresse du législateur luxembourgeois de protéger les personnes physiques de certains traitements « susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »». À noter que le projet de loi introduit également des sanctions financières.
(JW/JV/*L'essentiel*)

Réagissez à cet article

Original de l’article mis en page : L’essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg

---

Le FBI a désormais le droit de pirater n’importe quel ordinateur dans le monde !

Le FBI a désormais le droit de pirater n’importe quel ordinateur dans le monde !

Le FBI est désormais doté de nouveaux pouvoirs, à savoir l'extension de ses capacités actuelles en matière de piratage informatique. Sur la base d'un mandat spécial, les agents du bureau pourront s'introduire sur n'importe quel ordinateur, situé aux États Unis mais également dans le monde.

Applicable dès aujourd'hui, la réforme est à nuancer. En effet, l'application de la **règle 41** du *Federal Rules of Criminal Procedure* (équivalent de notre code de procédure pénale) est strictement encadrée par un **juge fédéral**, qui instruit au préalable le dossier. Il s'agira d'une procédure **exceptionnelle**, la spécificité de l'affaire devant justifier de l'**opportunité** d'une telle mesure.
L'intervention reste, en effet, une **intrusion dans la vie privée des gens** *–qui ne sont pas forcément coupables de ce qui pourrait leur être reproché*. Cela n'empêche pas les politiques américains de s'inquiéter sur des atteintes aux libertés personnelles, des abus possibles ou d'éventuelles finalités politiques.
Précisons que ce pouvoir n'est pas unique en son genre, il existe déjà en France où il est actuellement renforcé du fait du plan *vigipirate* au même titre que certains pouvoirs de surveillance.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les nouveaux pouvoirs de piratage informatique du FBI

Au Royaume-Uni, une loi de surveillance aussi extrême qu’effrayante vient d’être votée

Au Royaume-Uni, une loi de surveillance aussi extrême qu’effrayante vient d’être votée

Le Royaume-Uni pourrait bien voir appliquer l’une des lois les plus extrêmes en matière de surveillance de ses concitoyens. Celle-ci, déjà baptisée la Charte des fouineurs, autoriserait l’État à fouiller quand il le souhaite, dans chaque élément de votre vie numérique.…[Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article