# Hyperconnexion du corps humain : 3 règles pour ne pas faire n’importe quoi | Le Net Expert Informatique

| | |
|---|---|
| | Hyperconnexion du corps humain : 3 règles pour ne pas faire n’importe quoi |

**Face au déploiement des objets connectés au corps humain, qui permettent de recueillir des données de santé, utilisateurs et industriels doivent être particulièrement vigilants, nous explique Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI.**

Bracelets, montres, balances connectés… la m-santé envahit les magasins spécialisés. Au-delà de leur côté ludique, ces objets permettent aux entreprises de recueillir de très nombreuses données sur leurs utilisateurs : rythme cardiaque, nombre de pas effectués par jour, quantité et qualité du sommeil, taux de sucre dans les larmes, taux d'alcoolémie ou tension artérielle…
Ce mouvement de collecte massive de données – le big data – n'en est qu'à son début, selon la Cnil. En 2017, un utilisateur de smartphone sur deux aura installé au moins une application dédiée à son bien-être et à sa santé.

Les données recueillies sont traitées par de nombreuses entreprises qui les exploitent afin de mieux connaître leurs clients. Une pratique intrusive, qui doit susciter la vigilance des utilisateurs, mais aussi des industriels. En effet, leur responsabilité peut-être engagée. Les données recueillies, liées à la santé, ont un caractère sensible et font l'objet d'une protection renforcée. Ainsi, leur collecte et leur traitement, soumis à un contrôle accru, doivent être autorisés. Mais certaines data -celles se rapportant en général au bien-être-, échappent à une demande d'autorisation préalable grâce aux normes simplifiées. Attention cependant car la frontière entre bien-être et santé est particulièrement ténue.

Pour assurer leur sécurité juridique, les industriels du secteur mettre en place quelques règles.
**1. RESPECTER LE CADRE LÉGAL ET LE RAPPORT DE LA CNIL SUR LA PRATIQUE DU « QUANTIFIED SELF »**
Le rapport de la Cnil, déposé fin mai 2014, intitulé 'Le corps, nouvel objet connecté', traite des problèmes liés aux données personnelles de santé issues des applications et objets de mesure de soi (quantified self). Ces pratiques consistent généralement à mesurer et à comparer avec d'autres, des variables de notre mode de vie (nutrition, exercice physique, sommeil…). La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques.

Le « quantified self » constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La Cnil s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente – et face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles – les industriels développant des produits liés à la santé doivent veiller à rester dans les clous lors de la collecte.

**2. MISER SUR LE « CLIENT EMPOWERMENT » POUR GAGNER LA CONFIANCE DES CONSOMMATEURS**
Ce mouvement donne davantage de pouvoirs de contrôle au client. Il permet de rééquilibrer la relation entre l'entreprise collectrice de données et l'usager qui a souvent l'impression d'être négligé par les professionnels. Cette prise de pouvoir peut aussi permettre la patrimonialisation des données à condition d'obtenir le consentement direct du client. Cela ouvre aux industriels la possibilité de commercialiser les données collectées.

**3. SE CONFORMER AUX PRINCIPES DE « PRIVACY BY DESIGN »**
Le concept de « privacy by design » propose de faire de la protection de la vie privée de l'utilisateur une caractéristique majeure de l'objet afin « d'assurer la protection de la vie privée en l'intégrant dans les normes de conception des technologies, pratiques internes et infrastructures matérielles ». Les données recueillies ne sont alors pas extensivement partagées ou revendues. En intégrant ce concept au cahier des charges de l'objet connecté, l'industriel gagnera la confiance des clients et se démarquera aussi de ses concurrents.

**TOUT N'EST PAS PERMIS**
La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques. Elle constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont ainsi déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La CNIL s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente, face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles, les industriels développant des produits liés à la santé doivent tenir compte du fait que tout n'est pas permis.

---



---



---



Source : http://www.usine-digitale.fr/article/hyperconnexion-du-corps-humain-3-regles-pour-ne-pas-faire-n-importe-quoi.N335953
Par Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI

# Cookies et tracking : la Cnil a mis en demeure une vingtaine de sites | Le Net Expert Informatique

**La Cnil publie un premier bilan de ses contrôles sur l'application de la loi relative aux cookies et au tracking publicitaire sur les sites web. La Commission a mis en demeure une vingtaine de sites qui se contentent d'informer l'utilisateur mais ne prennent pas en compte son consentement.**

Manifestation la plus visible des évolutions autour des données personnelles : aujourd'hui, les sites qui vous traquent et ont recours à des cookies prennent la peine de vous le dire. Depuis un peu plus d'un an, l'entrée en vigueur des lois européennes a poussé de nombreux sites web à signaler aux utilisateurs qu'ils avaient recours à des cookies et autres outils de traçage des utilisateurs dans un but commercial, le plus souvent grâce à un bandeau s'affichant sur le site lors de la première visite.
Mais pour la Cnil, cela ne suffit pas. En effet la commission Nationale Informatique et Liberté explique dans son bilan avoir mis en demeure une vingtaine d'éditeurs de se mettre en conformité avec la loi dans un délai déterminé. En effet, la Cnil rappelle qu'il ne s'agit pas uniquement d'informer l'utilisateur mais bien de recueillir le consentement avant de déposer les cookies, et donc d'offrir à l'internaute la possibilité d'opt-out lors de sa visite du site.

**Bientôt plus de contrôles**
« En effet, si certains sites ont apposé un bandeau informant les internautes que des cookies sont déposés sur leur ordinateur, aucun des sites contrôlés n'attend d'avoir recueilli le consentement des internautes avant de déposer lesdits cookies. » La Cnil précise également que renvoyer l'internaute aux paramétrages de son navigateur n'est pas une attitude valable à l'égard de la loi.
Au cours de l'année 2014, la Cnil a effectué au total 24 contrôles sur place, 27 contrôles en ligne et deux auditions afin de s'assurer du respect des règles en vigueur. Et la Commission entend bien poursuivre sur sa lancée : elle a récemment annoncé vouloir augmenter le nombre de ses contrôles sur les domaines relevant de sa juridiction. La Cnil tiendra notamment une session de question/réponse sur ce sujet aujourd'hui à 13h via son compte Twitter, @Cnil.

---



---



---



Source : http://www.zdnet.fr/actualites/cookies-et-tracking-la-cnil-a-mis-en-demeure-une-vingtaine-de-sites-39821796.htm

# La Marine Française infectée par Thales ? | Le Net Expert Informatique

La Marine Française infectée par Thales ?

**L’affaire du piratage dont a été victime Thales en début d’année rebondit. Selon le Canard Enchaîné, son programme classé-défense SIC21 livré à la Direction Générale de l’Armement et équipant des navires et des installations terrestres, pourrait avoir été infecté.**

L’attaque informatique dont a été victime Thales en avril dernier continue de faire couler beaucoup d’encre. Dans un document confidentiel daté du 18 mai évoqué par le Canard Enchaîné, l’entreprise de défense confirme en effet que l’ensemble des postes, serveurs et équipements du groupe aux Etats-Unis ont été infectés en décembre par un virus à partir des serveurs des sites de Thales Avionics à Piscataway, dans le New Jersey, et à Irvine, en Californie, avant de se répandre au Canada et de toucher la messagerie France de Thales en mars dernier. Mais l’histoire ne s’arrête pas là : dans un mail envoyéle 13 mai à Olivier Daloy (directeur du système informatique de Thales), Ivan Maximoff (le spécialiste sécurité informatique maison) aurait fait aussi état de ses inquiétudes concernant la découverte du virus Courch Yeti spécialisé dans l’espionnage industriel, dans le programme classé-défense SIC21 datant de 2004.
Problème : le programme SIC21 équipe aussi des navires et des installations terrestres. « Six livraisons de Thales au centre d’expertise de la Direction Générale de l’Armement dans le domaine de la guerre électronique installé près de Rennes, et à la DGA Techniques navales à Toulon, pourraient avoir été infectées », indique le Canard Enchaîné. Dans un extrait du mail du 13 mai d’Ivan Maximoff repris par le journal satirique, ce dernier fait également mention que des programmes potentiellement indésirables ont été livrés dans le cadre du programme SIC21. Afin de faire le point sur la situation, une réunion aurait eu lieu le 18 mai entre Thales, la DGA mais aussi l’Agence nationale de la Sécurité des Systèmes d’Information pour évoquer la sécurisation du groupe.

---



---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemondeinformatique.fr/actualites/lire-piratage-de-thales-la-dga-pourrait-avoir-ete-infectee-par-le-virus-courch-yeti-61453.html
Par Dominique Filippone

---

# Les voitures promises aussi à des bugs logiciels et des mises à jour ? | Le Net Expert Informatique

# Les voitures promises aussi à des bugs logiciels et des mises à jour ?

**Ford doit rappeler 433.000 voitures en Amérique du Nord en raison d'un bug logiciel, à savoir l'impossibilité de couper le moteur. Les propriétaires doivent retourner chez leur garagiste pour effectuer une mise à jour. On n'arrête plus le progrès ?**

Fin mai, Frédéric Charles du blog Green SI de ZDNet.fr expliquait pourquoi il avait été obligé rebooter sa voiture en raison d'un problème logiciel. Car en effet, le logiciel est de plus en plus présent dans nos véhicules. Pour les automobilistes, les pannes mécaniques ne sont plus le seul tracas qui les guette.
Et notre bloggeur n'est pas un cas isolé. Le constructeur Ford a ainsi été contraint d'émettre un rappel portant sur 433.000 voitures en Amérique du Nord (modèles Focus, C-MAX et Escape). C'est précisément le logiciel du système de commande qui est en cause.

**Le logiciel apporte des fonctions, et des bugs potentiels**
Sur son site Internet, Ford mentionne un dysfonctionnement du module de contrôle ayant pour conséquence l'impossibilité de couper le moteur de la voiture, y compris lorsque le conducteur tourne et retire la clé.
Les propriétaires concernés sont invités à se rendre chez leurs concessionnaires… afin d'appliquer une mise à jour logicielle sur leur véhicule, un peu comme cela se fait déjà, et depuis de nombreuses années, sur un ordinateur.
Confronté à l'impossibilité de reprendre la route, Frédéric Charles avait procédé à ce qui s'apparente à une forme de « reboot » ou redémarrage de sa voiture. Comment ?
« Clef dans la poche en dehors du véhicule, je débranche [la batterie], j'attends 30s, je rebranche, la voiture se réinitialise, je redémarre, et voilà que tout rentre dans l'ordre. Mon garagiste étant le premier surpris. J'ai depuis avalé des centaines de kilomètres sans aucun problème » racontait-il.
« L'enjeu des véhicules connectés est aussi le support numérique, de véhicules de plus en plus sophistiqués. Sinon, il ne nous restera plus qu'à apprendre à rebooter notre voiture régulièrement et croiser les doigts à chaque fois, comme avec les bon vieux PCs. Nostalgie, nostalgie… » commentait-il encore.

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/les-voitures-promises-comme-les-pc-a-des-bugs-logiciels-et-des-mises-a-jour-39822008.htm

# Une nouvelle loi en matière de protection des données obligera les entreprises à de l’autocontrôle | Le Net Expert Informatique

© Thinkstock

Une nouvelle loi en matière de protection des données obligera les entreprises à de l’autocontrôle

**L'Europe va moderniser la loi portant sur la conservation des données personnelles. Cela devrait simplifier la vie des entreprises européennes, mais celles-ci devront aussi veiller à ne pas enfreindre cette loi par mégarde.**

Il s'agit en l'occurrence de la 'general data protection regulation', un ensemble de règles qui s'appliquent actuellement dans chaque état membre et qui spécifient quelles données peuvent être tenues à jour, pendant combien de temps et ce que l'on peut en faire. L'objectif de l'Europe est de la moderniser au niveau européen, pour qu'une série de règles unique entre en vigueur dans toute l'Union européenne, en ce compris aussi une seule autorité susceptible de prendre des décisions à propos des litiges et infliger des amendes pour l'ensemble de l'UE.
L'un des éléments sur la table est d'y voir figurer ce qu'on appelle le droit à l'oubli, permettant aux citoyens de demander aux moteurs de recherche de ne plus afficher certains résultats, mais aussi à des entreprises de supprimer des données personnelles, si elles n'ont aucune raison légale de les conserver.
L'Union européenne estime que les entreprises économiseront annuellement 2,3 milliards d'euros avec une loi uniformisée. Il y a pourtant un revers à la médaille: quiconque est aujourd'hui en règle avec la législation belge, ne le sera peut-être pas avec la loi européenne, selon James Luby de BalaBit, spécialisé dans le 'log management': « La proposition de loi se caractérise par la 'privacy by design'. Mais nombre d'entreprises possèdent aujourd'hui automatiquement des données générées par les utilisateurs, tout en ne sachant pas qu'il s'agit de données personnelles. Elles devront également en faire plus pour conserver et gérer ces données. »
Luby évoque notamment des données de connexion, comme par exemple en e-commerce. « Beaucoup d'entreprises ne savent pas ce qu'elles collectent via leurs plates-formes. Or elles devront en être conscientes bientôt. »
Les entreprises devraient donc faire des économies à long terme, mais d'ici à l'entrée en vigueur de la loi modernisée, elles devront également veiller à se mettre en règle avec celle-ci. Mais ce n'est pas encore urgent, puisque les entretiens entre la Commission européenne, le Parlement européen et les ministres nationaux concernés débutent à peine. Il est probable que cela se traduira en texte de loi au début de l'année prochaine.

---



---



---



Source : http://datanews.levif.be/ict/actualite/une-nouvelle-loi-en-matiere-de-protection-des-donnees-obligera-les-entreprises-a-de-l-autocontrole/article-normal-402231.html
Par Pieterjan Van Leemputten

---

# Les dessous de la société d'espionnage Hacking Team… | Le Net Expert Informatique


## Les dessous de la société d'espionnage Hacking Team…

**La firme, qui s'est fait voler plus de 400 gigaoctets de données confidentielles, avait présenté ses technologies aux services de renseignements français. La société Hacking Team, soupçonnée d'avoir livré des logiciels d'espionnage à des régimes autoritaires, assure n'avoir rien commis d'illégal.**

On soupçonnait Hacking Team de rouler sa bosse pour des dictatures. Et voilà que le journal Le Monde nous apprend que la sulfureuse entreprise d'espionnage a également eu des contacts avec les services d'espionnage français… Lundi 6 juillet, la société italienne a été victime d'un piratage de grande ampleur de ses données confidentielles et des comptes Twitter de plusieurs de ses responsables. Des centaines de gigaoctets de données se sont déversées sur le Web et ont été immédiatement téléchargées et consultées par ceux qui l'accusaient de faire bénéficier de ses technologies des régimes autoritaires.
L'entreprise est en effet spécialisée dans le développement et la commercialisation de logiciels de surveillance ou de piratage très performants, principalement destinés à des États. Logiciels de blocage de pages internet, systèmes de mise sous surveillance de boîtes mails jugées suspectes… Hacking Team a développé une impressionnante gamme de services. Leur produit phare, dénommé RCS (pour Remote Control Systems), est un packaging incluant des logiciels tels que DaVinci et Galileo, qui permettent de visualiser les frappes effectuées sur le clavier de l'ordinateur visé, d'en collecter les informations sensibles telles que les adresses mails, les documents enregistrés ou les mots de passe, ou encore de récupérer les historiques de navigation.

**Ennemie d'Internet**
La facilité avec laquelle ces outils peuvent être utilisés à des fins d'espionnage de masse avait conduit certaines ONG à dénoncer les pratiques de cette société. Cette dernière avait même fini par être classée parmi les ennemis d'Internet par Reporters sans frontières en 2013, en raison des rapports commerciaux qu'elle entretenait alors avec le Maroc et les Émirats arabes unis. Des traces de ses logiciels avaient ainsi été retrouvées sur les ordinateurs du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 remis par Global Voices et Google.
Autre soupçon : « Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un e-mail envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team », écrit également RSF.
L'entreprise jouit dans le milieu d'une réputation douteuse, et est soupçonnée de collaborer avec des pays peu recommandables. Jusqu'à présent, la société clamait son innocence et aucune preuve de son implication dans la mise en place des systèmes de surveillance électronique de ces pays n'avait été découverte. « Nous faisons extrêmement attention à qui nous vendons nos produits. Nos investisseurs ont mis en place un comité légal qui nous conseille continuellement sur le statut de chaque pays avec lequel nous entrons en contact », assurait le PDG de Hacking Team, David Vincenzetti, dans une interview accordée en 2011 au journaliste Ryan Gallagher.

**Des régimes autoritaires en clients**
Kazakhstan, Arabie saoudite, Azerbaïdjan… De nombreux États – dont les dirigeants ne font pas toujours des libertés individuelles une priorité de leur règne… – font partie de la liste des clients. Parmi ces pays, certains sont connus pour une répression dure de leur population et leurs violations répétées des droits de l'homme. On peut ainsi noter l'exemple du Soudan, avec lequel Hacking Team a toujours nié avoir collaboré. Cependant, les documents publiés révèlent l'existence d'un contrat de 480 000 euros avec le gouvernement actuellement en place. La Russie fait également partie des heureux bénéficiaires des services de Hacking Team. La firme prend même la peine d'indiquer sur ses documents internes que ces deux pays ne sont « officiellement pas clients » (« oficially not supported ») de l'entreprise.
Interrogé au sujet de la série de contrats signés avec le Soudan, le porte-parole de l'entreprise, Éric Rabe, a quant à lui maintenu que le document cité remontait à avant les sanctions décidées par les Nations unies contre le pays.

**La France, elle aussi intéressée par les services de l'entreprise**
D'après certains documents, la France et Hacking Team seraient entrés en contact plusieurs fois ces dernières années. La prise de contact entre le ministère de la Défense et l'entreprise a eu lieu en 2013, alors qu'une réunion de présentation s'est tenue fin 2014 dans un hôtel près de l'aéroport Charles-de-Gaulle à Paris. Étaient représentés à cette réunion la DGSI et le Groupement interministériel de contrôle (GIC) chargé quant à lui des écoutes administratives (c'est-à-dire menées sans mandat judiciaire), et dirigé par le Premier ministre.
Si la DGSI affirme n'avoir donné aucune suite à cette réunion, ce n'est pas le cas du GIC qui a poursuivi ses échanges avec Hacking Team. Comme le révèle un échange de courriels entre le GIC et Hacking Team, Philippe Vinci, l'un des responsables de l'entreprise, s'est rendu au siège du GIC le vendredi 3 avril 2015. Cette information est confirmée par un échange de courriels entre la société et le groupement interministériel datant du mardi 7 avril. On y apprend également que le GIC serait intéressé par une démonstration de la part d'Hacking Team. L'entreprise aurait alors proposé aux représentants du GIC de venir assister à une telle démonstration en Italie courant mai. Aucune information concernant la suite à donner à ces rendez-vous n'a pour le moment fuité.

**« Nous n'avons rien à cacher »**
Après deux jours sans réaction, l'entreprise a finalement commenté ce vol de données dans une interview accordée au site IBTimes : « Nous n'avons rien à cacher sur nos activités et nous pensons qu'il n'y a aucune preuve dans ces 400 gigabits de données que nous avons violé une quelconque loi », a ainsi affirmé le porte-parole de l'entreprise, Éric Rabe.
Pour le moment, et en attendant de connaître exactement le contenu des données qui ont été piratées, la société italienne a demandé à ses clients de cesser d'utiliser ses logiciels. Les auteurs du piratage ne se sont pas encore manifestés.

---



---



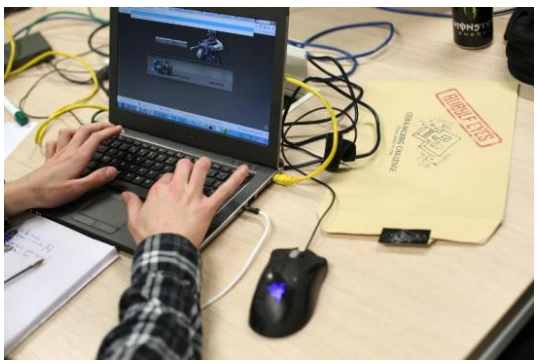
---



Source : http://www.lepoint.fr/high-tech-internet/les-curieux-clients-de-la-societe-d-espionnage-hacking-team-08-07-2015-1943190_47.php
Par Ian BEAURAIN

---

# Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team | Le Net Expert Informatique



## Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team

**Les cybercriminels s'en frottent déjà les mains entre deux piratages. Deux jours après la mise en ligne de données piratées de l'éditeur de logiciels espions Hacking Team, les experts, qui ont épluché les 400 Go de documents, ont fait la découverte d'une faille de sécurité importante de Flash Player, un lecteur multimédia autonome utilisé par des sites commes Youtube, Dailymotion ou encore Facebook.**

C'est l'éditeur d'antivirus Micro Trend qui a révélé sur son blog cette faille «zero-day», c'est à dire inconnue jusqu'à présent et sans correctif pour l'instant. Elle permet à un attaquant de prendre le contrôle à distance d'un ordinateur en exécutant un code arbitraire à distance ou dans le cas plus précis d'une entreprise de surveillance comme Hacking Team d'installer ses logiciels espions sans se faire remarquer.
Symantec a confirmé cette porte d'entrée dans votre ordinateur et conseille sur son blog (en anglais) de désactiver temporairement Flash Player sur les sites Internet douteux surtout sur Internet Explorer, le navigateur le plus exposé.
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a lui aussi confirmé la faille et ses potentielles conséquences. Le CERT-FR précise que des «plusieurs kits d'exploitation (de pirates informatiques, NDLR) ont intégré cette vulnérabilité qui est activement exploitée».
Prise à défaut, l'entreprise américaine Adobe, à l'origine de Flash Player, a promis d'apporter un patch correcteur dans la journée de mercredi. D'autres failles de sécurité pourraient être révélées sur la masse de documents qui ont fuité. Mais les plus dangereuses restent celles dont seul un groupe d'initiés est au courant.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.leparisien.fr/high-tech/flash-player-une-faille-de-vulnerabilite-revelee-par-le-piratage-de-hacking-team-08-07-2015-4928849.php
Par Damien Licata Caruso

---

# Des communications ultra-sécurisées avec TEOREM | Le Net Expert Informatique

## Des communications ultra-sécurisées avec TEOREM

**TEOREM est un système de téléphonie mobile et fixe à usage gouvernemental et de Défense. Il permet de protéger les communications vocales ainsi que les SMS sur tous les réseaux opérateurs. TEOREM assure également le rôle de modem chiffrant permettant ainsi l'échange de données entre deux ordinateurs personnels en toute sécurité.**

Grâce à sa parfaite interopérabilité avec les différents réseaux de télécommunication fixes (analogiques et numériques) et mobiles (2G / 3G), TEOREM offre une grande polyvalence aux utilisateurs. Enfin, son autonomie, sa miniaturisation et sa grande flexibilité en font une solution unique pour répondre aux besoins des utilisateurs nomades.

Une solution hautement sécurisée et simple d'utilisation :
• Configuration fixe ou mobile (2G / 3G).
• Certifiée jusqu'au niveau Secret Défense pour la France.
• Communications sécurisées de bout en bout.
• Signal lumineux permettant de différencier les appels sécurisés et non sécurisés.

Un système flexible et performant :
• Compatible avec les réseaux d'opérateurs et gouvernementaux.
• Système de gestion centralisé à distance.
• Gestion sans intervention de l'utilisateur final.
• Grande qualité audio : + 15%* comparé aux téléphones standards.

* Selon norme PESQ.

---



---



Source : https://www.thalesgroup.com/fr/cybersecurite/teorem

# Comment prémunir les visiteurs de votre site internet de cyberattaques ? | Le Net Expert Informatique

## Comment prémunir les visiteurs de votre site internet de cyberattaques?

**Switch propose un site web visant à aider les propriétaires de noms de domaines internet en Suisse à protéger leur site web contre des cyber-attaques.**

Afin d'aider les propriétaires de sites internet à lutter contre les malwares qui pourraient y être installés, Switch met en ligne Safer Internet, un site internet d'information sur  les menaces que représentent les criminels sur internet et les mesures préventives à adopter. Michael Hausding, expert en sécurité de Switch, explique les raisons de la mise en place d'un tel site: «Par la plateforme de sécurité Safer Internet, nous nous adressons à tous les détenteurs d'un site web .ch. Nous y donnons des conseils sur la prévention de l'abus de noms de domaine et informons sur les dangers relatifs à des contenus online.»
Les propriétaires de noms de domaines y trouveront notamment cinq conseils pour prévenir des attaques par Drive-by (qui infectent les usagers d'un site contenant un malware) et par Phishing (qui consistent à obtenir des informations personnelles via notamment des sites contrefaits). Parmi ses conseils se trouvent par exemple le fait d'utiliser une système de gestion du contenu (CMS) toujours à jour.
Ce site est disponible en quatre langues: allemand, français, italien et anglais. Il s'adresse en premier lieu aux gestionnaires de sites web qui sont tenus de nettoyer leur site s'il est infecté au risque de les voir bloqué.
La fondation Switch a pour objectif de rendre internet sûr en Suisse.

Le lien vers le site Internet « Safer Internet » de la société « Switch » : http://www.switch.ch/saferinternet

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.ictjournal.ch/fr-CH/News/2015/07/07/Comment-premunir-les-visiteurs-de-votre-site-internet-de-cyberattaques.aspx

# Le responsable des attaques DDoS du Playstation Network et du Xbox Live échappe à 15 ans de prison ! | Le Net Expert Informatique

Le responsable des attaques DDoS du Playstation Network et du Xbox Live échappe à 15 ans de prison !

**Vous souvenez-vous de Julius « zeekill » Kivimak ? Le jeune homme de 17 ans est le responsable des attaques DDoS du Playstation Network et du Xbox Live survenues en fin d'année dernière. Il avait témoigné à visage découvert quelques temps après avoir oeuvré puis avait été interpellé par les autorités. Son jugement a eu lieu, et figurez-vous que le bougre a réussi à échapper à 15 ans de prison !**

Le jeune Julius « zeekill » Kivimak est le hacker à l'ego surdimensionné qui a pris le risque de se faire repérer par les autorités en accordant une interview plutôt qu'en restant discret. Se revendiquant comme étant membre de Lizard Squad, il avait affirmé être l'auteur des attaques DDoS du Playstation Network et du Xbox Live l'année dernière.
Appréhendé par les autorités finlandaises, il a dû répondre (enfin son avocat) à 50 700 charges qui pesaient contre lui parmi lesquelles on compte la fraude bancaire, l'intrusion dans un système informatique, le harcèlement, la fraude etc.
Mais visiblement la quantité de charges retenues contre lui n'ont pas suffi à le faire condamner. Le jeune homme risquait 15 à 16 ans de prison et s'en est finalement sorti quasiment indemne puisqu'il n'a écopé que de 2 ans de prison avec sursis. En outre le tribunal lui a demander de combattre le cybercrime.
Ce jugement, Blair Strater l'a en travers de la gorge. Car, outre les attaques DDoS, le jeune Julius « zeekill » Kivimaki avait également harcelé pendant trois ans cet américain. Il est allé extrêmement loin puisqu'il a fait intervenir le SWAT (forces d'intervention américaines) chez lui, a usurpé son identité et a plus ou moins détruit sa vie ainsi que celle de sa famille. Le jeune américain de vingt ans a déclaré qu'il était « absolument dégoutté par le jugement ».

L'interview du pirate en question : https://youtu.be/fPX8yCBdIZ8

---



---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.phonandroid.com/responsable-attaques-ddos-playstation-network-xbox-live-echappe-15-ans-prison.html