Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ?

I**l est très difficile de savoir si un ordinateur est piraté / piratable ou pas. Qu'il soit PC ou Mac, il possède ses failles qui peuvent sans limite être exploitées.**
Il n'y a plus beaucoup de protections qui résistes aux plus grands hackers.
La divulgation de documents dévoilant les techniques qu'utilise la NSA pour nous espionner (c.f. http://www.lenetexpert.fr/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner-le-net-expert-informatique) et les dessous de société d'espionnage informatique Hacking Team récemment piratée (c.f. http://www.lenetexpert.fr/les-dessous-de-la-societe-despionnage-hacking-team-le-net-expert-informatique) nous ont récemment démontré qu'il n'y a aucune limite au piratage.

Mais alors, comment se protéger ?
Comme pour votre maison ou votre appartement, il n'existe aucun moyen d'empêcher les voleurs de rentrer. Les moyens qu'ils utiliseront seront généralement à la hauteur de l'intérêt qu'ils y trouveront.
Cependant, les conseils que je peux donner, sont comme pour les moyens de protection de vos habitions. Au plus on met des barrières de sécurité, au plus on retarde l'intrusion et au plus on décourage l'auteur. Il sera en effet plus difficile de rentrer chez vous si vous avez la dernière serrure de protection avec les volets anti-effraction dernier cri, avec une alarme ultra perfectionnée etc. plutôt qu'un simple cadenas pour vous protéger.

Pour sécuriser un système informatique
1) J'analyse généralement ce qui, dans nos habitudes quotidiennes correspond à une attitude numérique dangereuse ou irresponsable. Pour cette phase, il est difficile de vous dire quoi faire exactement, puisque c'est généralement notre expérience, nos connaissances passées et notre intuition qui servent à produire une bonne analyse.

2) La phase suivante va consister à détecter la présence d'espions dans votre ordinateur. Compte tenu que la plupart des outils d'espionnage sont capables de détecter qu'on est en train de les détecter, vaut mieux déjà, faire des sauvegardes, puis couper d'internet votre appareil (du coup, il sera nécessaire de télécharger les logiciels de détection à partir d'un autre ordinateur, et les copier sur l'ordinateur à analyser à partir d'une clé USB par exemple).
Cette phase de détection est très difficile. En effet, les logiciels espions, programmés pour espionner ce que vous tapez au clavier, ce que voit votre webcam ou entend votre micro, sont aussi programmés pour ne pas être détectés.
Le dernier outil connu pour réaliser une détection de logiciels espions est le logiciel **Detekt**. Ce logiciel a pour but de détecter des logiciels espions (spywares) sur un système d'exploitation Windows.
Les spywares actuellement détectés sont :
• DarkComet RAT ;
• XtremeRAT ;
• BlackShades RAT ;
• njRAT ;
• FinFisher FinSpy ;
• HackingTeam RCS ;
• ShadowTech RAT ;
• Gh0st RAT.
Attention, car les développeurs de ce logiciels précisent cependant :
« Certains logiciels espions seront probablement mis à jour en réponse à la publication de Detekt afin d'éviter la détection. En outre, il peut y avoir des versions existantes de logiciels espions […] qui ne sont pas détectés par cet outil ».
Vous trouverez plus d'informations et le lien de téléchargement sur http://linuxfr.org/news/detekt-un-logiciel-de-detection-de-logiciels-espions
Sur Mac, il n'existe pas un tel outil. Vous pouvez cependant utiliser le logiciel MacScan pou des antispaywares du commerce.
Cependant, que ça soit sur PC ou sur Mac, ce n'est qu'une analyse approfondie (et souvent manuelle) des fichiers systèmes, des processus en mémoire et qui se lancent au démarrage qui permettra de détecter les applications malveillantes installées sur votre ordinateur.

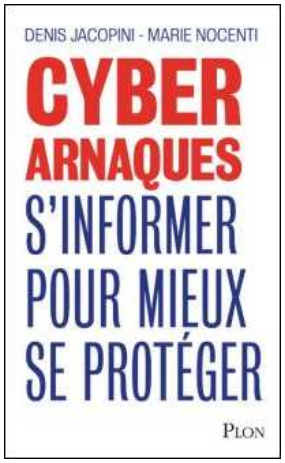
Et si on dispose d'un Mac plutôt que d'un PC ?
Il y a quelques années, avoir un Mac « garantissait » d'être un peu à l'abris des virus et des pirates informatiques. En effet, pouquoi un pirate informatique perdrait du temps à développer un logiciel malveillant et prendrait des risques pour seulement 5% de la population numérique mondiale. Désormais, avec l'explosion d'Apple, de ses téléphones, tablettes et aussi ordinateur, les systèmes IOS se sont répandu sur la planète numérique. De plus, c'est très souvent les plus fortunés qui disposent de ces types d'appareils… une aubaine pour les pirates qui trouvent tout de suite un intérêt à développer des dangereuxwares.

3) La troisième et dernière phase de ces recommandations est la protection. Une fois votre système considéré comme sain (il est complètement inutile de protéger un système qui est infecté car ça ne soignera pas l'équipement et les conséquences pourraient être pires), il est temps d'adopter l'attitude d'un vrai utilisateur responsable et paranoïaque.
• Mettez à jour votre système d'exploitation (Windows, MasOs, IOS, Androis, Linux…) avec la version la plus récente. En effet, l'enchaînement des mises à jour des systèmes d'exploitation est peu souvent fait pour améliorer le fonctionnement ou ajouter des fonctions à votre appareil. Le ballet incessant des « updates » sert prioritairement à corriger les « boulettes » qu'ont fait volontairement ou involontairement les informaticiens « développeurs » détectées par d'autres informaticiens plus « contrôleurs ».
• Mettez à jour vos logiciels avec leurs versions les plus récentes (et particulièrement pour vos navigateurs Internet et les logiciels Adobe). En effet, la plupart des intrusions informatiques se font pas des sites Internet malveillants qui font exécuter sur votre ordinateur un code informatique malveillant chargé d'ouvrir un canal entre le pirate et vous. Ces codes informatiques malveillants utilisent les failles de vos logiciels pour s'exécuter. Lorsque l'utilisation d'une faille inconnue (sauf par les pirates) d'un logiciel est détectée par les « Gardiens de la paix numérique », un correctif (ou patch) est généralement développée par l'éditeur dans les jours qui suivent leur découverte. Ceci ne vous garantira pas une protection absolue de votre ordinateur, mais renforcera son blindage.Les pirates utilisent parfois d'anciens serveurs ou d'anciens postes de travail connecté sur le réseau, qui ont de vieux systèmes d'exploitation qui ne se mettent plus à jour et qui ont des failles ultra-connues pour pénétrer votre réseau et des postes pourtant ultra-sécurisés. Pensez donc à les déconnecter du réseau ou à copier le contenu ou les virtualiser sur des systèmes plus récents et tenus à jour.
• Mettez à jour les firmwares des matériels et objets connectés. Pour les mêmes raisons qu'il est important de mettre à jour vos logiciels avec leurs versions les plus récentes, il est aussi important de mettre à jour les logiciels de vos matériels et objets connectés (routeurs, modems, webcams etc.).
• Adoptez une politique sécurisée dans l'utilisation des mots de passe. Vos mots de passe doivent êtres longs, complexes et doivent changer souvent. Conseil primordial dans l'utilisation des mots de passe au bureau : Il doit être aussi précieux et aussi secret que le code de votre carte bancaire. Personne ne doit le connaître, sinon… quelqu'un pourra facilement se faire passer pour vous et vous faire porter le chapeau pour ses actes malveillants.
• Méfiez-vous des sites Internet proposant des vidéos gratuites, du streaming gratuit ou autres services inespérément gratuit. Les sites sont souvent piégés et ont destinés soit à collecter des données personnelles, soit contaminer votre ordinateur par des petits codes malveillants.
• Méfiez-vous également des e-mails douteux de demande d'aide (même d'un ami) ou autre participation humanitaire utilisant le paiement par Manda Cash, Western Union ou monnaie virtuelle telle le Bitcoin. Ce sont des moyen de paiement qui sont généralement utilisés par les pirates pour se faire payer et disparaître dans la nature. Les emails destinés à vous hameçonner auront aussi quelques détails qui devraient vous mettre la puce à l'oreille (Faute d'orthographe, huissier ou directeur ayant une adresse e-mail yahoo ou gmail).
• Vous avez un doute, vous pensez que votre ordinateur ou votre boite e-mail est victime d'intrusion, changez immédiatement de mot de passe. Certains systèmes de messagerie permettent d'avoir un historique des accès et des connexions. L'analyse de cet historique pourrait bien vous donner une indication pour savoir si quelqu'un d'autre à accès à votre messagerie (alias, double diffusion, collecte d'un compte mail sur un autre compte etc).

Conclusion
Voila, vous avez maintenant toute une liste de recommandations qui peut vous rassurer (ou non) et vous permettre de prendre conscience de la complexité qu'est à ce jour la lutte de la #cybercriminalité.
Si maintenant tout ceci vous semble complexe, rassurez-vous, c'est notre métier. Nous seront donc en mesure de vous accompagner dans la sensibilisation des utilisateurs, la détection ou la protection contre ces « ennuiwares ».
Contactez-moi

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : Denis JACOPINI

Un Employeur peut-il examiner

les messages échangés par ses employés sur leur téléphone professionnel ?

Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Dès lors que le téléphone du salarié est professionnel, l'employeur a ce droit, à moins d'avoir mentionné avant le message «personnel». Dans ce cas, l'employeur n'a plus le droit. Mais souvent, on n'oublie de l'écrire… »

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 d'expertises, d'audits, de formations et de sensibilisation 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.

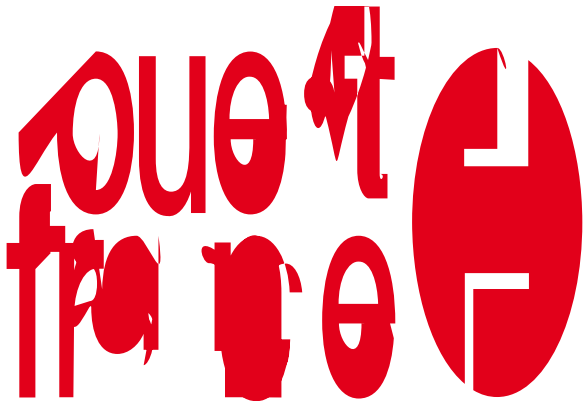
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

Est-il risqué de se connecter au wifi public ? | Denis JACOPINI

	Est-il risqué de se connecter au wifi public ?

Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français).
Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.

Denis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?
Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

Quel est le danger ? Se faire espionner ?
Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.

Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » – par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. – ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?
Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates !

Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

Peut-on se faire abuser par une fausse borne wifi ?
Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

Comment se protéger ?
En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.

Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

Source : http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/7
Par Corinne Bourbeillon

Peut-on être licencié pour ce

qu’on y a écrit dans les réseaux sociaux ? | Denis JACOPINI

Peut-on être licencié pour ce qu’on y a écrit dans les réseaux sociaux ?

Peut-on être licencié pour ce qu’on y a écrit dans les réseaux sociaux ?

Oui.
Dans une affaire concernant trois salariés licenciés pour avoir dénigré leur hiérarchie sur Facebook, un Conseil des prud’hommes a considéré que les propos publiés sur le mur d’un des salariés étaient publics car accessibles aux « amis d’amis ».
Ces propos ont perdu leur caractère privé du fait qu’ils étaient accessibles à des personnes non concernées par la discussion.
Soyez donc vigilant lorsque vous publiez des commentaires sur un réseau social !

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 : https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=D48813C492DFE134132210B5E195173E?id=199&back=true

Detekt un logiciel pour supprimer des programmes espions | Denis JACOPINI

	#Detekt, un logiciel pour supprimer des programmes espions

Voila un logiciel qui va vous aider à supprimer les RAT que vous pouvez trouver éventuellement sur vos PC.
Les RAT sont des programmes espions (Remote Administration Tool, ou Outil d'Administration Distante), ce sont des programmes qui peuvent effectuer une prise de contrôle à distance de votre ordinateur, sans que vous sachiez même que ce programme est sur votre machine.
Le logiciel proposé est le logiciel Detekt, il est également disponible avec son code source et vous aidera grandement à scanner votre PC et à éradiquer les RAT facilement de votre machine.
Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.
« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

Quelques articles sélectionnés par nos Experts :
Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications | Denis JACOPINI

	Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications

Maintenant que la Loi Renseignement est votée, et en attendant la suite du processus législatif, apprenons à résister à la surveillance de masse avec quelques outils cryptographiques plus ou moins simples, mais efficaces et légaux.

Nous sommes le soir du mardi 5 mai, et c'est un jour funeste pour la démocratie. La France s'était autoproclamée « pays des Lumières » parce qu'il y a 250 ans notre pays éclairait l'Europe et le monde grâce aux travaux philosophiques et politiques de Montesquieu, qui prônait la séparation des pouvoirs, et de Voltaire et Rousseau.
À dater d'aujourd'hui, jour du vote en première lecture du projet de loi sur le renseignement, à cause d'une classe politicienne d'une grande médiocrité, s'enclenche un processus au terme duquel le peuple français va probablement devoir subir une loi dangereuse, qui pourrait s'avérer extrêmement liberticide si elle tombait entre de mauvaises mains, par exemple celles de l'extrême droite.
Même si la loi doit encore passer devant le Sénat puis peut-être revenir en seconde lecture à l'Assemblée Nationale, même si une saisine du Conseil Constitutionnel va être déposée par une soixantaine de courageux députés en complément de celle déjà annoncée par François Hollande, mieux vaut se préparer au pire, en imaginant que cette loi sera un jour promulguée. En faisant un peu de mauvais esprit, j'ai imaginé un nom pour le dispositif qui sera chargé de collecter nos données personnelles afin de détecter les comportements suspects : « Surveillance Totalement Automatisée via des Systèmes Informatiques » et bizarrement l'acronyme est STASI !
Dès lors, à titre préventif et sans préjuger de l'avenir, il me semble important d'apprendre à protéger sa vie privée. Ceci passe par le chiffrement de ses communications, qu'il s'agisse d'échanges sur Internet ou via SMS, et cela peut se faire au moyen de différents outils à la fois efficaces et légaux.
Bien évidemment, les « vrais méchants » que sont les terroristes, djihadistes, gangsters et autres trafiquants connaissent et utilisent déjà ces outils : vous vous doutez bien qu'ils n'ont pas attendu ce billet de blog pour les découvrir….

Une boîte à outils pour protéger votre vie privée

Anonymat sur Internet

Pour protéger votre identité sur Internet et notamment sur le web, vous pouvez combiner l'utilisation d'un réseau privé virtuel, ou VPN, et de TOR, un système d'anonymisation qui nécessite l'installation d'un logiciel spécifique, TOR Browser. Je ne vous donne pas de référence particulière en matière de VPN, car l'offre est pléthorique.

MAJ : un lecteur m'a indiqué l'existence de La brique Internet, un simple boîtier VPN couplé à un serveur. Pour que la Brique fonctionne, il faut lui configurer un accès VPN, qui lui permettra de créer un tunnel jusqu'à un autre ordinateur sur Internet. Une extension fournira bientôt aussi en plus un accès clé-en-main via TOR en utilisant la clé wifi du boîtier pour diffuser deux réseaux wifi : l'un pour un accès transparent via VPN et l'autre pour un accès transparent via Tor.

Chiffrement des données

Pour chiffrer le contenu de vos données, stockées sur les disques durs de vos ordinateurs ou dans les mémoires permanentes de vos smartphones, vous pouvez mettre en œuvre des outils tels que LUKS pour les systèmes Linux ou TrueCrypt pour les OS les plus répandus : même si TrueCrypt a connu une histoire compliquée, son efficacité ne semble pas remise en cause par le dernier audit de code effectué par des experts.

Je vous signale aussi que l'ANSSI – Agence nationale de la sécurité des systèmes d'information – signale d'autres outils alternatifs comme Cryhod, Zed !, ZoneCentral, Security Box et StormShield. Même si l'ANSSI est un service gouvernemental il n'y a pas de raison de ne pas leur faire confiance sur ce point

Chiffrement des e-mails et authentification des correspondants

GPG, acronyme de GNU Privacy Guard, est l'implémentation GNU du standard OpenPGP. Cet outil permet de transmettre des messages signés et/ou chiffrés ce qui vous garantit à la fois l'authenticité et la confidentialité de vos échanges. Des modules complémentaires en facilitent l'utilisation sous Linux, Windows, MacOS X et Android.

MAJ : un lecteur m'a signalé PEPS, une solution de sécurisation française et Open Source, issue d'un projet mené par la DGA – Direction générale de l'armement – à partir duquel a été créée la société MLState.

Messagerie instantanée sécurisée

OTR, Off The Record, est un plugin à greffer à un client de messagerie instantanée. Le logiciel de messagerie instantanée Jitsi, qui repose sur le protocole SIP de la voix sur IP, intègre l'outil de chiffrement ZRTP.

Protection des communications mobiles

A défaut de protéger les métadonnées de vos communications mobiles, qu'il s'agisse de voix ou de SMS, vous pouvez au moins chiffrer les données en elles-mêmes, à savoir le contenu de vos échanges :

RedPhon est une application de chiffrement des communications vocales sous Android capable de communiquer avec Signal qui est une application du même fournisseur destinée aux iPhone sous iOS.

TextSecure est une application dédiée pour l'échange sécurisé de SMS, disponible pour Android et compatible avec la dernière version de l'application Signal. Plus d'information à ce sujet sur le blog de Stéphane Bortzmeyer.

MAJ : un lecteur m'a indiqué l'application APG pour Android qui permet d'utiliser ses clés GPG pour chiffrer ses SMS.

Allez vous former dans les « cafés Vie Privée »

Si vous n'êtes pas geek et ne vous sentez pas capable de maîtriser ces outils sans un minimum d'accompagnement, alors le concept des « cafés Vie Privée » est pour vous : il s'agit tout simplement de se réunir pour apprendre, de la bouche ceux qui savent le faire, comment mettre en œuvre les outils dont je vous ai parlé plus haut afin de protéger sa vie privée de toute intrusion, gouvernementale ou non.

Tout simplement, il s'agit de passer un après-midi à échanger et à pratiquer la cryptographie. Pour cela sont proposés des ateliers d'une durée minimum de 1 heure, axés autour de la sécurité informatique et de la protection de la vie privée.

Et comme le disent avec humour les organisateurs, « les ateliers sont accessibles à tout type de public, geek et non-geek, chatons, poneys, loutres ou licornes. ». Bref, le « café Vie Privée » est à la protection de la vie privée ce que la réunion Tupperware était à la cuisine

Voilà, vous avez je l'espère suffisamment d'éléments pratiques pour commencer à protéger votre vie privée… en espérant vraiment que le Conseil Constitutionnel abrogera les points les plus contestables de cette loi et nous évitera d'avoir à déployer un tel arsenal sécuritaire.

PS : l'image « 1984 was not a manual » a été créée par Arnaud Velten aka @Bizcom.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/loi-renseignement-la-bo-te-a-outils-pour-apprendre-a-proteger-votre-vie-privee-en-chiffrant-vos-donnees-et-communications-39818894.htm
Par Pierre Col

Vidéosurveillance en entreprise : règles et limites | Denis JACOPINI

#Vidéosurveillance en entreprise : règles et limites

Un système de vidéosurveillance en entreprise se doit d'observer certaines limites pour rester dans un cadre de protection des biens et personnes.

Le cadre législatif de la vidéosurveillance
C'est la loi dite « informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004, qui fixe le cadre de mise en place d'une vidéosurveillance sur un lieu à usage professionnel.
Ainsi dans des lieux non accessibles au public (bureaux, entrepôts, réserves, locaux d'administration) l'installation d'une vidéosurveillance doit faire l'objet d'une déclaration à la CNIL (Commission Nationale Informatique et Libertés).
C'est également une obligation pour les guichets de réception de clients et les commerces, lorsque le système enregistre les images dans un fichier et permettant de conserver d'identité des personnes filmées.
Si toutefois les fichiers ne sont pas conservés à des fins d'identification, un assouplissement de la loi permet de solliciter une simple autorisation préfectorale (pour les lieux accueillant du public).

Information des salariés et du public
Une information préalable est requise auprès des représentants des salariés avant tout installation d'un dispositif de vidéosurveillance, en mettant l'accent sur les objectifs de sécurité et en spécifiant que les enregistrements ne sont pas conservés plus d'un mois.
De la même manière, l'entreprise doit mettre en place une signalisation informant les visiteurs de la présence d'un système de vidéosurveillance.
Cet affichage doit se faire dès l'entrée dans l'établissement, en précisant les raisons ainsi que les coordonnées de l'autorité ou de la personne chargée de l'exploitation du système et en rappelant les modalités d'exercice du droit d'accès des personnes filmées aux enregistrements qui les concernent (loi du 6 août 2004).

Le principe de proportionnalité
On pourrait dire aussi principe de bon sens. L'employeur doit en premier lieu démontrer l'intérêt légitime à la mise en place d'un système de surveillance. Il peut s'agir de la nécessité de protéger des personnes ou des biens, ou de se prémunir contre des risques tels que le vol.
Partant de là, le dispositif installé doit être proportionnel au regard des intérêts à protéger.
Il y a une différence notoire entre installer une caméra dans un entrepôt à des fins de sécurité et le fait d'en installer une permettant d'observer en permanence des postes de travail.
Bien évidemment des caméras installées dans des lieux de repos des salariés ou dans des toilettes constituent une surveillance excessive. La CNIL a récemment mis à l'amende des entreprises pour des situations de surveillance jugées excessives et non proportionnées par rapport aux risques à prévenir.
La CNIL a fait valoir que des caméras peuvent être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation, ou encore filmer les zones où de la marchandise ou des biens de valeur sont entreposés. Pas question en revanche de filmer en permanence un employé sur son poste de travail, sauf si celui-ci manipule par exemple de l'argent, en vertu du principe de proportionnalité.
En synthèse, bien que frappée du sceau du bon sens, la mise en place d'un système de vidéosurveillance doit s'accompagner de certaines précautions. Eventuellement prenez avis auprès de votre conseiller en assurances, qui saura vous orienter vers un prestataire de vidéosurveillance homologué et bien au fait des contraintes législatives.

Source :
http://www.comptanoo.com/assurance-prevention/actualite-tpe-pme/23794/videosurveillance-entreprise-regles-et-limites

Windows 8 : Identifier les applications malveillantes à partir des services par défaut | Denis JACOPINI

	Windows 8 : Identifier les applications malveillantes à partir des services par défaut

Afin de vérifier si votre ordinateur dispose d'applications malveillantes ou non, nous vous mettons en ligne la liste des services lancés par défaut de Windows 8.

Exécutez Services.msc

Nom du service	Fichier	Démarrage par défaut	Démarrage conseillé	Remarques
Acquisition d'image Windows (WIA)	stisvc	Manuel	Manuel	Fournit des services d'acquisition d'images pour les scanners et les appareils photos. Si votre scanner ou webcam ne fonctionne pas correctement, utilisez le démarrage automatique.
Agent de protection d'accès réseau	napagent	Manuel	Désactivé	Le service Agent de protection d'accès réseau (NAP) recueille et gère les informations d'intégrité pour les ordinateurs clients d'un réseau. Les informations recueillies par l'agent NAP sont utilisées pour s'assurer que l'ordinateur client pos[illegible]
Agent de stratégie IPsec	PolicyAgent	Manuel	Manuel	La sécurité du protocole Internet (IPSec) prend en charge l'authentification de l'homologue réseau, l'authentification de l'origine des données, l'intégrité des données, la confidentialité des données (chiffrement) et la pr[illegible]
Alimentation	Power	Automatique	Automatique	Gère la stratégie d'alimentation et la remise de notification de stratégie d'alimentation.
AMD External Events Utility	atiesrxx	Automatique	Désactivé	Fait partie des pilotes graphiques AMD. Permet de modifier les réglages de votre carte graphique à partir d'évènements externes comme des raccourcis clavier par exemple.
Appel de procédure distante (RPC)	RpcSs	Automatique	Automatique	Ce service est le Gestionnaire de contrôle des services pour les serveurs COM et DCOM. Il traite les demandes d'activation d'objets, les résolutions d'exportateur d'objets et le nettoyage de la mémoire distribuée pour les serveurs COM et DCOM. Ce service est indispensable, [illegible]
Application système COM+	COMSysApp	Manuel	Manuel	Gère la configuration et le suivi des composants de base COM+ (Component Object Model).
Assistance IP	iphlpsvc	Automatique	Désactivé	Fournit une connectivité de tunnel à l'aide des technologies de transition IPv6.
Assistant NetBIOS sur TCP/IP	lmhosts	Automatique	Désactivé	Utilisé pour partager et imprimer des fichiers à travers le réseau local. Activez le service si vous avez plusieurs ordinateur dans votre réseau local et que vous échangez des fichiers entre eux.
Assistant Connectivité réseau	NcaSvc	Manuel	Manuel	Fournit la notification du statut DirectAccess aux composants de l'interface utilisateur.
Assistant Connexion avec un compte Microsoft	wlidsvc	Manuel	Désactivé	Utilisé pour autoriser les utilisateurs à ouvrir une session avec un compte utilisateur Microsoft en ligne. Si vous utilisez uniquement des comptes locaux, désactivez ce service.
Audio Windows	AudioSrv	Automatique	Automatique	[illegible]
BranchCache	PeerDistSvc	Manuel	Désactivé	[illegible]
Cache de police de Windows Presentation Foundation	FontCache	Manuel	Manuel	[illegible]
Carte à puce	SCardSvr	Manuel	Désactivé	[illegible]
Carte de performances WMI	wmiApSrv	Manuel	Manuel	[illegible]
Centre de sécurité	wscsvc	Automatique	Automatique	[illegible]
Cliché instantané des volumes	VSS	Automatique	Automatique	[illegible]
Client de stratégie de groupe	gpsvc	Automatique	Automatique	[illegible]
Client de suivi de lien distribué	TrkWks	Automatique	Désactivé	[illegible]
Client DHCP	Dhcp	Automatique	Automatique	[illegible]
Client DNS	dnscache	Automatique	Automatique	[illegible]
Collecteur d'événement Windows	Wecsvc	Automatique	Automatique	[illegible]
Configuration automatique de réseau câblé	dot3svc	Manuel	Manuel	[illegible]
Configuration automatique des périphériques connectés au réseau	NcdAutoSetup	Manuel	Manuel	[illegible]
Configuration des services Bureau à distance	SessionEnv	Manuel	Manuel	[illegible]
Connaissance des emplacements réseau	NlaSvc	Automatique	Automatique	[illegible]
Connexions réseau	Netman	Manuel	Manuel	[illegible]
Contrôle parental	WPCSvc	Manuel	Désactivé	[illegible]
Coordinateur de transactions distribuées	MSDTC	Manuel	Manuel	[illegible]
Découverte SSDP	SSDPSRV	Manuel	Manuel	[illegible]
Détection de services interactifs	UI0Detect	Manuel	Manuel	[illegible]
Détection matériel noyau	ShellHWDetection	Automatique	Automatique	[illegible]
Disque virtuel	vds	Manuel	Manuel	[illegible]
Dossiers de travail	workfolderssvc	Manuel	Manuel	[illegible]
Ecouteur du groupement résidentiel	HomeGroupListener	Manuel	Manuel	[illegible]
Evènements d'acquisition d'images fixes	WiaRpc	Manuel	Manuel	[illegible]
Expérience audio-vidéo haute qualité Windows	QWAVE	Manuel	Manuel	[illegible]
Expérience d'application	AeLookupSvc	Manuel	Manuel	[illegible]
Explorateur d'ordinateurs	Browser	Manuel	Manuel	[illegible]
Extensions et notifications des imprimantes	PrintNotify	Manuel	Manuel	[illegible]
Fichiers hors connexion	CscService	Manuel	Manuel	[illegible]
Fournisseur de cliché instantané de logiciel Microsoft	swprv	Manuel	Manuel	[illegible]
Fournisseur du Groupement résidentiel	HomeGroupProvider	Manuel	Manuel	[illegible]
Générateur de points de terminaison du service Audio Windows	AudioEndpointBuilder	Automatique	Automatique	[illegible]
Gestion à distance de Windows (WSM)	WinRM	Manuel	Désactivé	[illegible]
Gestion d'applications	AppMgmt	Manuel	Désactivé	[illegible]
Gestion des clés et des certificats d'intégrité	hkmsvc	Manuel	Désactivé	[illegible]
Gestionnaire d'identité réseau homologue	p2pimsvc	Manuel	Désactivé	[illegible]
Gestionnaire d'informations d'identification	VaultSvc	Manuel	Désactivé	[illegible]
Gestionnaire d'installation de périphérique	DsmSvc	Manuel	Manuel	[illegible]
Gestionnaire de comptes de sécurité	SamSs	Automatique	Automatique	[illegible]
Gestionnaire de session locale	LSM	Automatique	Automatique	[illegible]
Gestionnaire des connexions automatiques d'accès à distance	RasAuto	Manuel	Manuel	[illegible]
Gestionnaire des connexions Windows	RasMan	Manuel	Manuel	[illegible]
Groupement de mise en réseau de pairs	p2psvc	Manuel	Manuel	[illegible]
Hôte de DLL de compteur de performance	PerfHost	Manuel	Manuel	[illegible]
Hôte de périphérique UPnP	upnphost	Manuel	Manuel	[illegible]
Hôte du fournisseur de découverte de fonctionsfdPHost		Manuel	Désactivé	[illegible]
Hôte système de diagnostics	WdiSystemHost	Manuel	Désactivé	[illegible]
Identité de l'application	AppIDSvc	Manuel	Manuel	[illegible]
Information d'application	Appinfo	Manuel	Manuel	[illegible]
Infrastructure de gestion Windows	Winmgmt	Automatique	Automatique	[illegible]
Interface de services d'invité Hyper-V	vmicguestinterface	Manuel	Désactivé	[illegible]
Interruption SNMP	SNMPTRAP	Manuel	Désactivé	[illegible]
Isolation de clé CNG	KeyIso	Manuel	Manuel	[illegible]
Journal d'événement Windows	EventLog	Automatique	Automatique	[illegible]
Journaux & alerte de performance	pla	Manuel	Manuel	[illegible]
Lanceur de processus serveur DCOM	DcomLaunch	Automatique	Automatique	[illegible]
Localisateur d'appels de procédure distante (RPC)	RpcLocator	Manuel	Désactivé	[illegible]
Mappage de découverte de topologie de la couche de liaison	lltdsvc	Manuel	Désactivé	[illegible]
Mappeur de point de terminaison RPC	RpcEptMapper	Automatique	Automatique	[illegible]
Microsoft Keyboard Filter	MsKeyboardFilter	Désactivé	Désactivé	[illegible]
Modules de génération de clés IKE et AuthIP	IKEEXT	Manuel	Manuel	[illegible]
Moteur de filtrage de base	BFE	Automatique	Automatique	[illegible]
Netlogon	Netlogon	Manuel	Désactivé	[illegible]
Optimiser les lecteurs	defragsvc	Manuel	Manuel	[illegible]
Ouverture de session secondaire	seclogon	Manuel	Désactivé	[illegible]
Pare-feu Windows	MpsSvc	Automatique	Automatique	[illegible]
Partage de connexion Internet (ICS)	SharedAccess	Manuel	Désactivé	[illegible]
Planificateur de classes multimédias	MMCSS	Automatique	Automatique	[illegible]
Planificateur de tâches	Schedule	Automatique	Automatique	[illegible]
Plug and Play	PlugPlay	Manuel	Manuel	[illegible]
Préparation des applications	AppReadiness	Manuel	Manuel	[illegible]
Prise en charge de l'application Rapports et solutions aux problèmes du Panneau de configuration	wercplsupport	Manuel	Désactivé	[illegible]
Programme d'installation ActiveX	AxInstSV	Manuel	Désactivé	[illegible]
Programme d'installation pour les modules Windows	TrustedInstaller	Manuel	Manuel	[illegible]
Propagation du certificat	CertPropSvc	Manuel	Désactivé	[illegible]
Protection logicielle	sppsvc	Manuel	Manuel	[illegible]
Protocole EAP (Extensible Authentification Protocol)	Eaphost	Manuel	Manuel	[illegible]
Protocole PNRP	PNRPsvc	Manuel	Désactivé	[illegible]
Publication des ressources de découverte de fonctions	FDResPub	Automatique	Désactivé	[illegible]
Redirecteur de port du mode utilisateur des services Bureau à distance	UmRdpService	Manuel	Désactivé	[illegible]
Registre à distance	RemoteRegistry	Manuel	Désactivé	[illegible]
Requête du service VSS Microsoft Hyper-V	vmicvss	Manuel	Désactivé	[illegible]
Routage et accès distant	RemoteAccess	Désactivé	Désactivé	[illegible]
Serveur	LanmanServer	Automatique	Automatique	[illegible]
Serveur de priorité des threads	THREADORDER	Manuel	Manuel	[illegible]
Service Arrêt de l'invité Microsoft Hyper-V	vmicshutdown	Manuel	Désactivé	[illegible]
Service Broker des évènements système	SystemEventsBroker	Manuel	Désactivé	[illegible]
Service Broker pour les connexions réseau	NcbService	Manuel	Désactivé	[illegible]
Service Broker pour les évènements horaires	TimeBroker	Manuel	Désactivé	[illegible]
Service Collecteur ETW d'Internet Explorer	IEEtwCollectorService	Manuel	Désactivé	[illegible]
Service d'administration IIS	IISADMIN	Automatique	Automatique	[illegible]
Service d'association de périphérique	DeviceAssociationService	Automatique	Automatique	[illegible]
Service d'énumération de périphériques de carte à puce	ScDeviceEnum	Manuel	Désactivé	[illegible]
Service d'historique des fichiers	fhsvc	Manuel	Manuel	[illegible]
Service d'infrastructure de localisation Windows	lfsvc	Manuel	Désactivé	[illegible]
Service d'infrastructure des tâches en arrière-plan	BrokerInfrastructure	Automatique	Automatique	[illegible]
Service d'installation de périphérique	DeviceInstall	Manuel	Manuel	[illegible]
Service de biométrie Windows	WbioSrvc	Manuel	Désactivé	[illegible]
Service de cache de police Windows	FontCache	Manuel	Manuel	[illegible]
Service de chiffrement de lecteur BitLocker	BDESVC	Manuel	Désactivé	[illegible]
Service de configuration automatique WLAN	WlanSvc	Manuel	Manuel	[illegible]
Service de configuration automatique WWAN	WwanSvc	Manuel	Désactivé	[illegible]
Service de découverte automatique de Proxy Web pour les services http Windows	WinHttpAutoProxySvc	Manuel	Manuel	[illegible]
Service de déploiement AppX	AppXSvc	Manuel	Manuel	[illegible]
Service de l'assistant Compatibilité des programmes	PcaSvc	Automatique	Désactivé	[illegible]
Service de la passerelle de la couche Application	ALG	Automatique	Désactivé	[illegible]
Service de moteur de sauvegarde en mode bloc	wbengine	Manuel	Manuel	[illegible]
Service de notification d'événement système	SENS	Automatique	Automatique	[illegible]
Service de partage de ports Net.Tcp	NetTcpPortSharing	Désactivé	Désactivé	[illegible]
Service de prise en charge Bluetooth	bthserv	Manuel	Désactivé	[illegible]
Service de profil utilisateur	ProfSvc	Automatique	Automatique	[illegible]
Service de publication des noms d'ordinateurs PNRP	PNRPAutoReg	Manuel	Désactivé	[illegible]
Service de rapport d'erreurs Windows	WerSvc	Manuel	Désactivé	[illegible]
Service de stockage	StorSvc	Manuel	Désactivé	[illegible]
Service de stratégie de diagnostic	DPS	Automatique	Désactivé	[illegible]
Service de surveillance des capteurs	SensrSvc	Manuel	Désactivé	[illegible]
Service de transfert intelligent en arrière-plan	BITS	Automatique	Automatique	[illegible]
Service de virtualisation Bureau à distance Hyper-V	vmicrdv	Manuel	Désactivé	[illegible]
Service du clavier tactile et du volet d'écriture manuscrite	TabletInputService	Manuel	Manuel	[illegible]
Service du périphérique d'interface utilisateur	hidserv	Manuel	Manuel	[illegible]
Service Echange de données Microsoft Hyper-V	vmickvpexchange	Manuel	Désactivé	[illegible]
Service énumérateur d'appareil mobile	WPDBusEnum	Manuel	Désactivé	[illegible]
Service hôte du fournisseur de chiffrement Windows	WEPHOSTSVC	Manuel	Manuel	[illegible]
Service hôte WDIServiceHost	WdiServiceHost	Manuel	Désactivé	[illegible]
Service Initiateur iSCI de Microsoft	MSiSCSI	Manuel	Désactivé	[illegible]
Service inspection du réseau Windows Defender	WdNisSvc	Manuel	Manuel	[illegible]
Service interface du magasin réseau	nsi	Automatique	Automatique	[illegible]
Service KtmRm pour Distributed Transaction Coordinator	KtmRm	Manuel	Manuel	[illegible]
Service Liste des réseaux	netprofm	Manuel	Manuel	[illegible]
Service mains libres Bluetooth	BthHFSrv	Manuel	Désactivé	[illegible]
Service Partage réseau du Lecteur Windows Media	WMPNetworkSvc	Automatique	Désactivé	[illegible]
Service Pulsation Microsoft Hyper-V	vmicheartbeat	Manuel	Désactivé	[illegible]
Service Synchronisation date/heure Microsoft Hyper-V	vmictimesync	Manuel	Désactivé	[illegible]
Service Windows Defender	WinDefend	Automatique	Automatique	[illegible]
Service Windows Store (WSService)	WSService	Manuel	Manuel	[illegible]
Service SSTP (Secure Socket Tunneling Protocol)	SstpSvc	Manuel	Manuel	[illegible]
Services Bureau à distance	TermService	Manuel	Désactivé	[illegible]
Services de chiffrement	CryptSvc	Automatique	Automatique	[illegible]
SMP de l'espace de stockages Microsoft	smphost	Manuel	Désactivé	[illegible]
Spouleur d'impression	Spooler	Automatique	Automatique	[illegible]
Station de travail	LanmanWorkstation	Automatique	Automatique	[illegible]
Stratégie de retraite de la carte à puce	SCPolicySvc	Manuel	Désactivé	[illegible]
Superfetch	SysMain	Automatique	Automatique	[illegible]
Système d'événement COM+	EventSystem	Automatique	Automatique	Prend en charge le service de notification d'événements système.
Système de couleurs Windows	WcsPlugInService	Manuel	Désactivé	Le service WcsPlugInService héberge des modules de plug-in tiers du modèle de périphérique couleurs et du modèle de gamme de couleurs du système de couleurs Windows.
Système de fichiers EFS (Encrypting File System)	EFS	Manuel	Manuel	Fournit la technologie de chiffrement des fichiers de base utilisée pour stocker les fichiers chiffrés sur les volumes NTFS.
Télécopie	Fax	Manuel	Désactivé	Vous permet d'envoyer et de recevoir des télécopies, d'utiliser les ressources de télécopie disponibles sur cet ordinateur ou le réseau.
Téléphonie	TapiSrv	Manuel	Manuel	Prend en charge l'interface TAPI (Telephony API) pour les programmes qui contrôlent les périphériques de téléphonie sur l'ordinateur local et, via le réseau local (LAN), sur les serveurs qui exécutent également le service.
Temps Windows	W32Time	Manuel	Manuel	Conserve la synchronisation de la date et de l'heure sur tous les clients et serveurs sur le réseau.
Thèmes	Themes	Automatique	Automatique	Fournit un système de gestion de thème de l'expérience utilisateur.
Vérificateur de points	svsvc	Manuel	Manuel	Vérifie les endommagements éventuels du système de fichiers
WebClient	WebClient	Manuel	Désactivé	Permet à un programme fonctionnant sous Windows de créer, modifier et accéder à des fichiers Internet.
Windows Connect Now – Registre de configuration	wcncsvc	Manuel	Désactivé	Héberge la configuration de connexion immédiate Windows pour le protocole WFP. Utilisé pour configurer rapidement une connexion sans fil.
Windows Driver Foundation – Infrastructure de pilote mode-utilisateur	wudfsvc	Manuel	Manuel	Gère les processus hôtes de pilote mode-utilisateur.
Windows Installer	msiserver	Manuel	Manuel	Ajoute, modifie et supprime des applications fournies en tant que package Windows Installer (*.msi).
Windows Search	Wsearch	Automatique	Désactivé	Fournit des fonctionnalités d'indexation de contenu, de mise en cache des propriétés, de résultats de recherche pour les fichiers, les messages électroniques et autres contenus. Si vous utilisez beaucoup la fonction Recherche de Windows, laissez le service activé. Sinon, désactivez-le. La recherche sera toujours [illegible]
Windows Update	wuauserv	Automatique	Automatique	Active la détection, le téléchargement et l'installation des mises à jour de Windows et d'autres programmes.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.winhelponline.com/blog/windows-8-services-default-startup-type/

Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 | Denis JACOPINI

	Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 2h24

Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?

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 !

Déplacements professionnels. Attention au Wi-Fi de l’hôtel…

	Déplacements professionnels. Attention au Wi-Fi de l’hôtel…

De nos jours, qui réussirait à se passer d'Internet plus d'une journée, en vacances, en déplacement, lors d'une conférence ou au travail ? Nos vies aujourd'hui digitalisées nous poussent à nous connecter quasi automatiquement au premier réseau Wi-Fi disponible, quitte à mettre la confidentialité de nos données en danger.

Cela devient d'autant plus problématique lorsque nous voyageons : une étude Kaspersky Lab révélait récemment que 82% des personnes interrogées se connectent à des réseaux Wi-Fi gratuits non sécurisés dans des terminaux d'aéroports, des hôtels, des cafés ou des restaurants.
Dans la tribune ci-dessous, Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord analyse les vulnérabilités des réseaux Wi-Fi dans les hôtels, une mine d'or pour des cybercriminels en quête de données personnelles ou d'informations confidentielles.
Depuis 10 ans, le cyber crime s'est largement professionnalisé pour devenir une véritablement industrie, portée sur la rentabilité. Les cybercriminels sont en quête permanente de victimes qui leur assureront un maximum de gains pour un minimum d'investissements techniques.
De son côté, l'industrie hôtelière a passé la dernière décennie à se transformer pour répondre aux nouvelles attentes digitales de ses clients. Alors que plus d'un quart d'entre eux annoncent qu'ils refuseraient de séjourner dans un hôtel ne proposant pas de Wi-Fi, la technologie n'est plus un luxe mais bien une question de survie pour les établissements hôteliers. Face aux ruptures liées à la numérisation, il a donc fallu repenser les modèles existants et s'équiper, parfois en hâte, de nouvelles technologies mal maîtrisées. Il n'était donc pas surprenant de voir émerger rapidement des problèmes de sécurité, dans les hôtels bon marché comme dans les 5 étoiles.
Par Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord

Le paradoxe du Wi-Fi à l'hôtel : privé mais public
Ils ont beau être déployés dans des établissements privés, les Wi-Fi d'hôtels restent des points d'accès publics. Ils sont même parfois complètement ouverts. Le processus de connexion, qui nécessite le plus souvent de confirmer son identité et son numéro de chambre, limite l'accès au réseau mais ne chiffre pas les communications. Il ne garantit pas non plus leur confidentialité. Est-ce que cela signifie que nos informations sont à la portée de tous ? La réalité n'est pas aussi sombre, mais elles sont à la portée de n'importe quel criminel équipé d'un logiciel de piratage, dont certains sont disponibles gratuitement en ligne, et disposant de connaissances techniques de base.
Concrètement, il suffit à un criminel de se positionner virtuellement entre l'utilisateur et le point de connexion pour récupérer toutes les données qui transitent par le réseau, qu'il s'agisse d'emails, de données bancaires ou encore de mots de passe qui lui donneront accès à tous les comptes de l'internaute.
Une approche plus sophistiquée consiste à utiliser une connexion Wi-Fi non sécurisée pour propager un malware, en créant par exemple des fenêtres pop-up malveillantes qui invitent faussement l'utilisateur à mettre à jour un logiciel légitime comme Windows.

Le mythe de la victime idéale
En 2014, le groupe de cybercriminels Darkhotel avait utilisé une connexion Wi-Fi pour infiltrer un réseau d'hôtels de luxe et espionner quelques-uns de leurs clients les plus prestigieux. Un an plus tard, les activités de ce groupe étaient toujours en cours, continuant d'exfiltrer les données des dirigeants d'entreprises et dignitaires. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisateurs continuent de penser qu'ils ne courent aucun risque car les informations qu'ils partagent sur Internet ne méritent pas d'être piratées. C'est oublier que la rentabilité d'une attaque repose aussi sur le nombre de victimes. Parmi les 30 millions de clients pris en charge par l'hôtellerie française chaque année, seuls 20% sont des clients d'affaires. Les 80% de voyageurs de loisirs représentent donc une manne financière tout aussi importante pour des cybercriminels en quête de profit.
Dans certains cas, une faille Wi-Fi peut même exposer l'hôtel lui-même, en servant de porte d'entrée vers son réseau. Si l'on prend le cas d'une chaîne d'hôtellerie internationale qui disposerait d'un système de gestion centralisé et automatisé, une intrusion sur le réseau pourrait entrainer le vol à grande échelle d'informations confidentielles et bancaires sur les employées, le fonctionnement de l'hôtel et ses clients.

Hôtels indépendants vs. chaînes hôtelières : des contraintes différentes pour un même défi
Pour une industrie aussi fragmentée que celle de l'hôtellerie, la sécurité est sans aucun doute un défi. Les hôtels indépendants ont une capacité d'accueil réduite et traitent donc moins de données. Le revers de la médaille est qu'ils disposent souvent d'une expertise informatique limitée et leur taille ne permet pas de réaliser les économies d'échelle qui rentabiliseraient un investissement important dans la sécurité informatique. Quant aux grands groupes, qui comptent des ressources humaines et financières plus importantes, ils sont mis à mal par l'étendue de leur écosystème, qui rend difficile l'harmonisation d'une politique de sécurité sur des centaines, voire des milliers de sites.
Il est important que tous les hôtels, quelle que soit leur taille ou leur catégorie, respectent quelques règles simples à commencer par l'isolation de chaque client sur le réseau, l'utilisation de technologies de chiffrement et l'installation de solutions de sécurité professionnelles. Enfin, le réseau Wi-Fi offert aux clients ne doit jamais être connecté au reste du système informatique de l'hôtel, afin d'éviter qu'une petite infection ne se transforme en épidémie généralisée. En respectant ces règles, la sécurité pourrait devenir un argument commercial au moins aussi efficace que le Wi-Fi.
Article original de Robert Kassous

Denis JACOPINI est Expert Informatique et aussi **formateur en Cybercriminalité** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous pouvons vous animer des **actions de sensibilisation ou de formation** à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles
Denis JACOPINI

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 : Etude Kaspersky sur le Wi-Fi à l'hôtel… | InfoTravel.fr