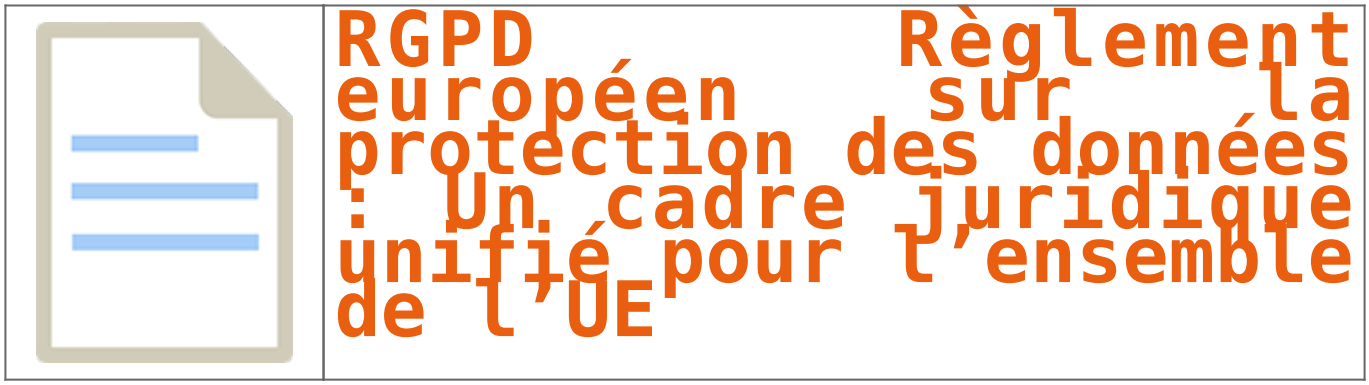
RGPD Règlement européen sur la protection des données : Un cadre juridique unifié pour l’ensemble de l’UE



Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu

Le critère du ciblage

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

La responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational – donc qu'il concernera les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernées seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État.

Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
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
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
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)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

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

Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI

Votre responsabilité engagée en cas de piratage de vos données

---

Si vous vous faites pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-avis des données que ce support numérique renferme.

Imaginez que vous disposiez de différents appareils numériques informatiques renfermant une multitude de données, dont des données d'amis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un Malware (Méchangiciel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l'intention de nuire retenue.
Par contre, en tant que professionnel, en plus d'être victime du piratage (intrusion causée par une faille, un virus, un crypto virus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi godfrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous prendre une seconde claque vis à vis de la loi Informatique et Libertés du 6 janvier 1978.

En effet, Les entreprises, les sociétés, tous ceux exerçant une activité professionnelle réglementée ou non, les associations, les institutions, administrations et les collectivités, sont tenues de respecter la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amendes vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.

Partons d'un cas concret.
La société Cochamboptnalds voit son système informatique piraté. Des investigations sont menées et le pirate informatique arrêté.
Vis à vis de la loi Godfrain du 5 janvier 1988, le voyou risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochamboptnalds n'était pas en règle avec la CNIL la dénonce auprès de cette dernière.
Le responsable de traitement, généralement le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.
Est-ce bien normal ?
Non, mais pourtant c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boites e-mail…

Autre cas concret
Monsieur Roudoudou-Maxitout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ?
La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, référez vous au cas contrés précédent. Si par contre le téléphone portable est personnel, vis à vis de la loi Informatique et Libertés, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.
Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.

Denis JACOPINI est Expert Informatique et aussi ***formateur en Protection des données personnelles*** *(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
Cabinet de Consultants et Formateurs en Sécurité Informatique et Protection des Données Personnelles

Contactez-nous

Réagissez à cet article
Original de l'article mis en page : ***Informatique et Libertés : suis-je concerné ? | CNIL***

Cybercriminalité – Retour sur les principales attaques informatiques en France et dans le monde | Denis JACOPINI

rte ne répertorie qu'un seule type de piratage : les attaques DDOS (Attaque

Cybercriminalité – Retour sur les attaques informatiques en France et dans le monde qui ont fait la une

Selon a commission européenne, la cybercriminalité englobe 3 catégories d'activité criminelles :

1) Les atteintes directes à des systèmes informatiques (ou Système de traitement automatisé de données, ou encore S.T.A.D.) en perturbant leur fonctionnement, tels que les attaques par déni de services (appelé aussi denial of service attack ou aussi DOS) destinées à faire tomber un serveur (comprenez rendre inaccessible ou mettre en panne un serveur) à distance.

2) Réaliser des actes illicites en utilisant les outils numériques (escroqueries, vols de données bancaires ou personnelles, espionnage industriel, atteinte à la propriété intellectuelle, sabotage, accès frauduleux, fraudes, usurpation d'identité, phishing, création de PC zombies, contamination d'autres postes informatiques ou d'autres serveurs…)

3) Modifier le contenu d'un espace numérique pour y déposer ou diffuser des contenus illicites (pédopornographie, racisme, xénophobie).

Les cyberdélinquants n'ont d'autre objectif que de gagner beaucoup d'argent. Virus, spams, et autres botnets drainent plusieurs centaines de millions de dollars chaque année à travers le monde.

Sans nous étaler sur les 144 milliards de courriers électroniques qui transitent dans le monde chaque jour dont 70% ne sont que du spam, les 10 millions de français victimes d'actes cybercriminels et 75% de ces actes de cybercriminalité qui sont de grande envergure (Norton 2013) qui concernent les 3,2 milliards d'internautes dans le monde en 2014 (dont la moitié pour l'Asie), vous trouverez ci-dessous, par ordre anté-chronologique, quelques principaux actes cybercriminels recensés par notre Expert, Denis JACOPINI.

Vous pouvez directement contacter Denis JACOPINI ici

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

30/09/2015 : Les sites Web du gouvernement thaïlandais attaqués
Consulter

12/09/2015 : Cyberattaque contre le site officiel de la Commission électorale centrale (CEC) de Russie
Consulter

05/08/2015 : La SNCB victime d'un piratage
Consulter

25/07/2015 : Le Pentagone visé par une cyber-attaque russe

Consulter

28/07/2015 : Les e-mails de hauts gradés de l’armée américaine piratés
Consulter

18/07/2015 : Piratage du site de rencontres adultères Ashley Madison
Consulter

06/07/2015 : Hacking Team, société d’espionnage informatoque hacké
Consulter

19/05/2015 : Un hacker a modifié en vol la puissance d’un réacteur
Consulter

14/05/2015 : Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag
Consulter

14/05/2015 : Des hôtels suisses victimes d’un piratage informatique
Consulter

12/05/2015 : Kaspersky annonce être victime d’une Cyberattaque
Consulter

05/05/2015 : Arnaque aux faux virement : Vol de 15 millions d’euros à Intermarché
Consulter

29/04/2015 : Des pirates informatiques volent 5 millions de dollars à Ryanair
Consulter

10/04/2015 : Lufthansa victime d’une cyberattaque
Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

05/05/2015 : Les états -Unis (Office of Personnal Management) victime de piratage. Plus de 4 millions de données personnelles de personnels fédéraux piratées;
Consulter

09/04/2015 : Arte victime d'une attaque informatique
Consulter

08/04/2015 : La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique | Le Net Expert Informatique
Consulter

02/2015 : Thales aurait été la cible d'une cyberattaque

Consulter

02/01/2015 : Les données de deux millions d’abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.
Consulter

26/12/2014 : PlayStation et Xbox victimes d’une panne après une cyber-attaLes joueurs de Xbox (ci-dessus) et de Playstation ne peuvent actuellement plus connecter leur console aux services en ligne en raison d’un piratage.
Consulter

21/12/2014 : Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30

ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.
Consulter

19/12/2014 : Le régulateur mondial d'internet, l'Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.
Consulter

18/12/2014 : Une usine métallurgique allemande a subi une cyberattaque qui a provoqué des dégâts matériels conséquents, a révélé jeudi la publication d'un rapport gouvernemental allemand, cité par le site ITworld.
Consuler

18/12/2014 : L'ICANN (Le régulateur mondial d'Internet)

victime d’un piratage informatique
Consulter

21/10/2014 : Staples a annoncé mener une enquête concernant un possible piratage de cartes de paiement, le numéro deux mondial des articles de bureau allongeant ainsi potentiellement la liste des entreprises américaines visées par une cyber-attaque.
Consulter

14/10/2014 : Le service de stockage de documents a pris les devants et réinitialisé les comptes utilisant les informations volées. Il affirme ne pas avoir subi d’intrusion sur ses serveurs.
Consulter

02/10/2014 : JP Morgan Chase a indiqué que 76 millions de foyers et 7 millions de PME parmi ses clients avaient été piratés lors d'une attaque informatique dans le courant du mois d'août.
Consulter

08/09/2014 : Home Depot : finalement 56 millions de cartes bancaires piratées
Consulter

16/06/2014 : Payer une rançon ou voir les données de centaines de milliers de ses clients publiées sur Internet. C'est le choix auquel devait faire face jusqu'à lundi 16 juin au soir l'entreprise de livraisons de pizzas Domino's Pizza.

Consulter

21/05/2014 : Victime d'une attaque, eBay demande à ses utilisateurs de changer de mot de passe
Les vols de données se suivent et se ressemblent (Target, Orange…). Le spécialiste de l'e-commerce, eBay, vient de communiquer sur une attaque informatique qui aurait visé ses bases de données.

Consulter

20/05/2014 : Malware BlackShades : 100 arrestations dont 29 en France
A l'origine de l'infection de plus de 500.000 ordinateurs, le logiciel espion BlackShades a donné lieu à une opération de police internationale. En France, 29 personnes ont été placées en garde à vue, en majorité des adolescents ayant avoué avoir exploité le malware.

Consulter

15/04/2014 : Les deux premiers sites internet reconnaissant avoir subi une attaque liée à la Faille Heartbleed
Au Royaume Uni, le site parental Mumsnet a été attaqué via la vulnérabilité Heartbleed.
Au Canada, l'administration fiscale CRA a admit publiquement avoir été victimes de la faille de sécurité découverte dans l'outil de chiffrement OpenSSL. (900 numéros d'assurance sociale volés) .

Consulter

12/02/2014 : Une attaque par déni de service (DDoS) a frappé de multiples serveurs aux Etats-Unis et en Europe en début de semaine. Il s'agit de l'**attaque informatique de ce type la**

plus grande recensée à ce jour.

Consulter

31/01/2014 : **La messagerie de Yahoo! victime d'une attaque informatique** massive
Des cybercriminels se sont introduits dans des comptes email, à la recherche de données personnelles. Les utilisateurs impactés sont invités à modifier leur mot de passe.

Consulter

27/11/2013 : La chaîne américaine de grande distribution Target a été victime de pirates informatiques qui se sont procuré les coordonnées bancaires de plus de 40 millions de ses clients entre le 27 novembre et le 15 décembre. Ce piratage tombe mal en pleine période des fêtes et ses conséquences sont potentiellement désastreuses pour les

clients ainsi que pour la marque.

Consulter

28/04/2013 : L'auteur présumé de la cyberattaque contre Spamhaus arrêté

Un Néerlandais de 35 ans a été interpellé en Espagne. Il est soupçonné d'être à l'origine d'une cyberattaque fin mars contre une entreprise basée en Suisse, Spamhaus, qui fournit aux messageries des listes permettant de bloquer les mails indésirables – les fameux spams.

Consulter

15/02/2013 : Facebook a subi une attaque informatique « sophistiquée »

Le réseau social Facebook a annoncé avoir subi, le mois dernier, une attaque informatique « sophistiquée », qui n'aurait toutefois pas compromis les données de ses utilisateurs.

« Nous avons remédié au problème dans tous les appareils infectés, nous avons informé la police et commencé une vaste enquête qui se poursuit à ce jour », a ajouté le réseau.

Consulter

02/02/2013 : Twitter touché par des attaques informatiques
Le réseau social Twitter a annoncé, vendredi 2 février, que certains de ses utilisateurs avaient été victimes d'attaques informatiques similaires à celles portées contre des sociétés et des médias américains.

Consulter

28/12/2012 : Le groupe pétrolier d'Arabie Saoudite Aramco a révélé avoir fait l'objet d'une attaque informatique de grande ampleur au milieu du mois d'août. Ce sont ainsi 30.000 postes de travail de l'entreprise qui ont été infectés par un virus informatique, provenant de l'extérieur.
Consulter

21/08/2012 : Le nouveau virus Shamoon illustre une fois de plus la progression des attaques visant de 'nouvelles'

cibles. Le virus Shamoon (ou Disttrack) semble écraser des fichiers dans les PC Windows, puis les ‘master boot records’. Il en résulte que ces fichiers ne peuvent être récupérés. Or le PC ne peut être redémarré sans qu’ils soient réinstallés.

Consulter

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

29/05/2012 : Flame, le virus le plus puissant de l’histoire du cyber-espionnage ?
Découvert au Proche-Orient, ce malware circulerait depuis plus de cinq ans et viserait, comme Stuxnet, des entreprises sensibles et des sites académiques. Une nouvelle arme pour la cyber-guerre ?

Consulter

27/04/2011 : Sony s’est fait pirater en mai 2011 12700 numéros de cartes de crédit non américaines issues d’une vieille base de données.

Consulter

07/03/2011 : Bercy et plus précisément **la direction du Trésor victime d'une vaste opération de piratage** informatique
Au total, plus de cent cinquante ordinateurs du ministère ont été infiltrés et de nombreux documents piratés. La méthode des espions est classique : à partir d'une adresse e-mail piratée, le « hacker » prend le contrôle de l'ordinateur de sa cible grâce à un cheval de Troie, en l'occurrence une pièce jointe. Chacun de ses correspondants au sein de l'administration peut à son tour être infiltré.
Ingénierie sociale a encore frappé. Crédulité ou excès de confiance ?

Consulter

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

21/11/2010 : Quand le piratage informatique s'en prend au Nucléaire
Les experts sont maintenant convaincus que le virus Stuxnet a été conçu pour s'attaquer aux centrifugeuses de Natanz utilisées par Téhéran pour enrichir l'uranium.

Consulter

Pour combattre cela, les états organisent 3 branches : Cyberdéfense (atteinte à la sécurité nationale), Cybersécurité (anticipation des risques numériques) et Cybercriminalité qui est la délinquance transposée dans le monde numérique.

Des organismes sont créés ou réorganisés et des hommes embauchés :

O.C.L.C.T.I.C. : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

D.C.R.I. : Direction centrale du Renseignement intérieur qui depuis début Mai 2014 d'appelle :
D.G.S.I. : Direction Générale de la Sécurité Intérieure

Gendarmerie Nationale

A.N.S.S.I : Agence Nationale de la Sécurité des Systèmes d'Information (créé en juillet 2009)

Cyberdouanes

B.E.F.T.I. : Brigade d'enquête surles Fraudes aux Technologies de l'Information

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

La webcam, Est-ce une une vraie menace pour les utilisateurs d’ordinateurs

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

La webcam, est-ce une vraie menace pour les utilisateurs d’ordinateurs

Après Mark Zuckerberg et sa webcam masquée par du scotch, voilà que c'est le directeur du FBI, James Comey, qui admet avoir adopté le même réflexe.

Une webcam cachée pour s'éviter bien des ennuis

A l'heure où les hackers multiplient les attaques contre les machines des entreprises et des particuliers, beaucoup se sont moqués de Mark Zuckerberg et de son bout de scotch sur la webcam et sur la prise jack, certains allant même jusqu'à le traiter de « parano ».
Pourtant, il semblerait qu'il s'agisse d'un réflexe à prendre et ce pour tout le monde. En effet, un pirate talentueux peut assez simplement prendre le contrôle d'une webcam à distance et pousser ainsi l'utilisateur à télécharger un malware sur sa machine.
Aussi, lors d'une interview, James Comey, le directeur du FBI, a défendu l'idée de masquer la webcam. Il a même précisé que ce devait être un réflexe de base en matière de sécurité. En prenant le contrôle de votre caméra, un pirate peut effectivement visionner vos saisies sur clavier et récupérer ainsi identifiants, mots de passe et coordonnées bancaires pour ne citer qu'eux…[lire la suite]

Conseils de Denis JACOPINI :

Les personnes averties croient utiliser la méthode miracle pour protéger leur vie privée en masquant leur Webcam.
Certes, je recommande toutefois de masquer votre Webcam car, même si, en l'absence de logiciel de sécurité adapté, le pirate peut la mettre en fonction sans que vous vous rendez compte de rien. Le pirate peut en effet voir votre tête en train de taper au clavier ou de jouer (ce qui en soit n'aura rien d'intéressant) mais selon l'orientation, voir le reste de la pièce lorsque vous vous éloignez de l'ordinateur.

Mais avez-vous pensé à protéger votre microphone ?

A l'instar des baby phones piratés, mettre en route à distance le microphone de votre ordinateur est tout aussi facile que de mettre en route votre Webcam et même mieux d'ailleurs, car à ma connaissance, il n'existe pas de logiciel de sécurité qui empêche l'accès au microphone. Certes tout le monde n'est pas Mark Zuckerberg, mais tout professionnel devrait en plus de couper son téléphone pendant les réunions, penser aussi à boucher le microphone de son appareil ou mieux, enficher une fiche Jack vide.
[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/usgl2zkRD9I?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

Original de l'article mis en page : La webcam, une vraie menace pour les utilisateurs d'ordinateurs

---

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité

La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

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
formateur n°93 84 03041 84

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

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

Source : Denis JACOPINI et http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html

Les objets connectés représentent-ils un risque ? | Denis JACOPINI

Les #objets connectés représentent-ils un risque ?

Contrôler sa maison ou son appartement du bout des doigts, voici la promesse des fameux objets connectés. Des réfrigérateurs aux téléviseurs, en passant par les thermostats, les caméras de surveillance, les serrures, ou encore les éclairages… de plus en plus d'équipements du foyer peuvent être pilotés à distance à l'aide d'un smartphone via un réseau local et Internet. Mais derrière ce rêve de la maison intelligente et connectée, encore inimaginable il y a quelques années, se cachent d'inquiétants problèmes de sécurité. État des lieux.

Un marché en ébullition

Longtemps réservée aux technophiles fortunés, la domotique commence vraiment à se démocratiser grâce à l'émergence des appareils et objets connectés. Après les équipements multimédias (Smart TV, systèmes Hi-Fi, imprimantes…), les appareils électroménagers connectés – réfrigérateurs, lave-linge, cafetières, réveils, etc.– commencent à débarquer sur le marché. Mais ce sont surtout les systèmes prêts à l'emploi ou les modules adaptables permettant de connecter l'éclairage, les serrures de portes, les stores, les systèmes de surveillance (caméras, détecteurs de mouvements/fumée, alarmes…), ou encore le chauffage qui rencontrent un succès grandissant.
L'embellie du marché de la domotique s'explique notamment par la simplicité d'installation et d'usage de ces nouveaux produits, mais également par leur prix de plus en plus abordable. Toutefois, comme n'importe quel appareil qui se connecte à un réseau Wi-Fi et à Internet, ils s'exposent de fait à toutes sortes de risques. D'autant que pour la plupart, ils ne possèdent aucun système de protection de type antivirus, antimalware, etc. Des failles de sécurité, plus ou moins importantes en fonction de la nature des objets, ont été soit démontrées par des experts de sécurité, soit exploitées par des hackers. Nous verrons les cas les plus effrayants qui donnent matière à réflexion.

Des appareils sous haute surveillance

Outre les incidents révélés ici et là, la sécurité des objets connectés est devenue un sujet particulièrement sensible depuis la médiatisation d'un moteur de recherche public étonnant baptisé Shodan. Créé par un Américain du nom de John Matherly, ce dernier explore le Web en continu pour référencer et regrouper tous les appareils qui y sont connectés. Quelques clics suffisent pour trouver aussi bien des systèmes domotiques, que des imprimantes, des caméras, des alarmes, voire des installations industrielles sensibles telles que des centrales électriques, des raffineries, ou encore, des réacteurs.

Pas de quoi rassurer les utilisateurs, même si à l'origine Shodan n'aurait pas été créé pour nuire, mais au contraire pour aider les experts en sécurité à identifier les vulnérabilités des logiciels et infrastructures réseau des entreprises. Le service se targue de garder une trace de tous les faits et gestes de ses utilisateurs, qui doivent obligatoirement s'identifier et souscrire à un abonnement au-delà d'un certain nombre de recherches. Il n'en reste pas moins que désormais, tout objet connecté ayant une adresse IP peut être localisé, identifié, voire détourné.

Les promesses de la maison intelligente et connectée

Contrôler et gérer divers équipements de la maison à l'aide d'un smartphone, d'une tablette ou d'un ordinateur n'est plus une utopie. Inutile d'avoir à tirer des câbles partout et d'entreprendre de lourds et coûteux travaux avec des spécialistes. Tout le monde peut en principe concevoir une installation domotique soi-même grâce à la nouvelle génération de produits disponibles sur le marché. Au-delà du confort qu'offrent ces nouvelles technologies au quotidien, elles permettent de réaliser de substantielles économies d'énergie, de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation…).

Confort, sécurité, prévention, économie d'énergie…

Domotique

Les produits ont évolué, mais la promesse de la domotique est toujours la même : centraliser et automatiser grâce à diverses technologies l'ensemble ou une partie des équipements électriques du foyer. Des serrures qui se ferment à distance, des caméras et des détecteurs de mouvements capables de s'animer en votre absence et de vous envoyer des SMS en cas d'intrusion, des thermostats intelligents permettant de gérer la température au degré près dans chaque pièce, des stores électriques qui s'ouvrent et se ferment automatiquement en fonction de la lumière, des détecteurs de fumée (obligatoires dans toute l'Union européenne à partir de mars 2015) qui lancent des alertes en cas de départ d'incendie, des éclairages qui créent différentes ambiances lumineuses selon les heures de la journée… Les possibilités sont quasi-infinies.

Réaliser une installation domotique est maintenant à la portée du plus grand nombre grâce, notamment, à ce qu'on appelle les box domotiques. Ces systèmes prêts à l'emploi que l'on trouve dans tous les magasins de bricolage et d'électronique (Castorama, Leroy Merlin, Electro Dépôt…) et même dans certains hypermarchés permettent de connecter et de contrôler à distance des équipements de la maison via une seule et même interface. Ces packs se composent d'un serveur domotique / multimédia (relié au réseau Wi-Fi du foyer), et d'un éventail plus ou moins important d'équipements de surveillance, d'automatisation, de loisirs, etc.

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur (CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour planifier des actions immédiates ou différées.

Créer des scénarios

Dans le jargon de la domotique, un scénario désigne un ensemble d'actions programmées pour différents moments de la journée, de la semaine, du mois, voire de l'année. Les fabricants ont réalisé d'énormes progrès pour faciliter la gestion des produits domotiques et la création de scénarios en développant des applications très intuitives. Exit les lignes de code informatique, ou les menus interminables au vocabulaire incompréhensible, place aux icônes visuelles, aux photomontages représentant les différentes parties du foyer, et à des menus dynamiques inspirés de ceux des smartphones. Quelques clics suffisent pour créer plusieurs scénarios pour la journée, la nuit, le week-end, et les combiner entre eux.

Point d'orgue des maisons intelligentes, les applications mobiles facilitent la compréhension et l'utilisation des équipements domotiques

On peut imaginer, par exemple du lundi au vendredi, un scénario qui consisterait à déclencher une série d'actions à partir de 7 heures : ouvrir les stores, allumer le ballon d'eau chaude, faire chauffer la cafetière, lancer la radio, déverrouiller les portes, démarrer les caméras de surveillance, etc. Bien entendu, toutes les solutions domotiques n'offrent pas les mêmes possibilités. Les fabricants distillent généralement des packs spécialisés dans un domaine précis (surveillance, automatisation, éclairage, chauffage…) à compléter au fur et à mesure. En parallèle, il existe d'innombrables objets connectés autonomes (stations météo, balances Wi-Fi, réveils intelligents, ampoules connectées…) qui se connectent directement au réseau du foyer, sans passer par un serveur propriétaire.

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur

Le problème, c'est que tout ce petit monde ne parle pas le même langage. Les standards universels, que rêvent de concevoir Apple et Google pour que tous les appareils connectés puissent communiquer entre eux via leurs plateformes mobiles respectives, ne sont pas encore d'actualité. À moins de choisir du matériel très haut de gamme comme la box universelle Lifedomus Vision (2 988 euros) compatible avec la plupart des protocoles de communication des solutions domotiques (KNX, EnOcean, MyHome, Zwave, Modbus, Zigbee…), mieux vaut s'équiper chez le même fabricant pour pallier les éventuels problèmes de compatibilité.

Quels risques pour la sécurité ?

Depuis quelques mois, la sécurité de l'Internet des objets fait couler beaucoup d'encre. Aux quatre coins de la planète, des experts en sécurité prennent le sujet à bras le corps : ils multiplient les démonstrations pour montrer les vulnérabilités de certains produits et la façon dont les cybercriminels pourraient les exploiter pour réaliser des attaques. Les spécialistes n'ont pas tort d'alerter les fabricants, car les risques ne sont plus seulement virtuels. Depuis quelques mois, quelques cas concrets d'attaques basées sur des objets connectés prouvent le bien-fondé de leurs craintes.

Failles et vulnérabilité des objets connectés

La division de sécurité Fortify on Demand du constructeur HP a récemment publié un rapport alarmant sur la sécurité des objets connectés. Elle a ainsi annoncé avoir découvert plus de 25 vulnérabilités sur 10 objets connectés parmi les plus populaires (Smart TV, thermostats intelligents, webcams, boxs domotiques…). Sans donner plus de précisions sur les marques concernées, elle déclare que la plupart ne crypte pas les données échangées sur le réseau et n'exige pas de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance. Ces dispositifs autorisent des mots de passe comme « 123456 » particulièrement vulnérables (un fait que nous avons effectivement pu vérifier après quelques recherches sur Shodan). Par ailleurs, la protection de leurs logiciels serait insuffisante, car non chiffrée, et certaines interfaces Web ne sont pas du tout sécurisées.

Toujours selon ce rapport, 90 % des produits évalués collectent des informations personnelles sensibles (adresse email/postale, date de naissance…) susceptibles de circuler en clair sur Internet à cause du manque de protection. Difficile néanmoins de contester un rapport ne précisant pas les modèles et les marques des appareils incriminés. À travers cette étude, la division déclare vouloir sensibiliser les acteurs du marché, mais elle souhaite aussi promouvoir sa solution de sécurité Fortify on Demand auprès des fabricants.

Ce n'est pas la seule étude de ce type. Le groupe de chercheurs indépendant d'AV-Test avait mis en lumière d'importantes failles de sécurité, notamment sur les systèmes domotiques iComfort de REVRitter, et XAVAX MAX ! d'Hama, permettant de contrôler le chauffage, l'électricité, les prises de courant avec interrupteur, ou encore l'éclairage. Aussi incroyable que cela puisse paraître, leur communication n'était pas sécurisée sur le réseau lors des mises à jour logicielle ou firmware, mais en plus, la solution iComfort ne nécessitait aucune authentification que cela soit pour l'accès local ou via Internet.

Avec un moteur de recherche comme Shodan, n'importe qui aurait pu repérer les dispositifs de la marque sur Internet et en prendre le contrôle à distance… Effrayant. Gageons que les deux fabricants ont pris les mesures qui s'imposent pour sécuriser un tant soit peu leurs systèmes.

Le lapin Karotz sécurisé ? Pas tout à fait.

Dans la sécurité informatique, les experts réalisent des « exploits », c'est-à-dire des tests (appelés Proof-of-concept, preuve de concept) visant à démontrer la présence de vulnérabilités sur des systèmes ou des logiciels pour proposer des patchs. Certains exemples sont particulièrement croustillants. La spécialiste Jennifer Savage avait ainsi montré comment elle avait réussi à exploiter une faille de sécurité du fameux lapin multifonctions Karotz qu'elle avait offert à sa fille. Cela lui avait permis de prendre le contrôle à distance de l'appareil à son insu, à l'aide d'un ordinateur, et d'utiliser sa caméra et son micro pour l'espionner.

Des ampoules qui éclairent et déverrouillent les réseaux Wi-Fi

Plus récemment, des chercheurs sont parvenus à prendre le contrôle d'ampoules connectées Lifx en exploitant une faille de leur protocole de communication. Ils ont pu démontrer qu'ils pouvaient théoriquement s'introduire dans un rayon de 30 mètres dans le réseau Wi-Fi domestique auquel elles sont connectées et accéder à des données privées stockées sur d'autres appareils du foyer, par exemple. Depuis cette découverte, le fabricant s'est empressé de publier un correctif.

Des Smart TV qui espionnent les téléspectateurs

Les démonstrations les plus impressionnantes ont souvent lieu lors des conférences Black Hat organisées chaque année à Las Vegas, mais aussi à Amsterdam ou à Tokyo. Elles réunissent aussi bien des chercheurs, des experts en sécurité, que des hackers de haut vol. En 2013, plusieurs conférenciers ont exposé les vulnérabilités des TV connectées. L'un d'entre eux a prouvé notamment qu'il était possible de prendre le contrôle de la caméra et du micro d'une Smart TV et d'espionner leur propriétaire à leur insu. Et cela, même quand l'appareil était éteint.

Le thermostat Nest lui qui joue les « Big Brother »

À l'occasion de la dernière édition qui s'est déroulée au mois d'août 2014 à Las Vegas, des chercheurs d'une université de Floride ont montré comment pirater le thermostat intelligent de Nest (la start-up rachetée par Google). Avec un accès physique à l'appareil (uniquement), ils ont pu prouver qu'il est possible d'insérer un code pour détourner et récupérer les informations récoltées par l'appareil, sans que son propriétaire s'en aperçoive.

Nouvelle génération de cyberattaques

La sécurité et la protection des données privées ne sont clairement pas la priorité de certains acteurs du marché des objets connectés. Sans vouloir dresser un tableau catastrophique de la situation, les cyberattaques sur les objets connectés présentant des failles de sécurité ont tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, babyphones, Smart TV, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses et variées.

Des caméras au service des voyeurs

Impossible de ne pas citer la faille de sécurité qui avait permis à des hackers de diffuser sur Internet le flux vidéo de milliers de webcams et caméras de vidéosurveillance Trendnet, installées chez des particuliers. Malgré la publication rapide d'un correctif par le fabricant après sa découverte, de nombreux utilisateurs continuaient un an plus tard à être espionnés à leur insu, car ils n'avaient toujours pas fait la mise à jour.

Un hack jusque dans… le berceau d'un nourrisson !

Début 2014, la société spécialisée en sécurité FoolPoint a révélé pour la première fois une cyberattaque réalisée à partir de toutes sortes de dispositifs connectés dont des Smart TV, des NAS, des consoles de jeux vidéo, un réfrigérateur, etc. Les pirates auraient exploité leur vulnérabilité pour installer un serveur de spams (botnet) et envoyer plus de 750 000 emails frauduleux. Dans l'État de l'Ohio aux États-Unis au mois d'avril dernier, un hacker n'a rien trouvé de mieux que de pirater un babyphone pour terroriser un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, il s'est mis à hurler des insanités sur le nourrisson.

Analyse et collecte de données en règle

En Grande-Bretagne, le blogueur spécialisé en développement informatique connu sous le nom de DoctorBeet's a fait une étonnante découverte. Suite à l'acquisition d'une Smart TV de la marque LG, il a remarqué l'apparition de publicités ciblées comme on peut en voir sur des services Web tels que Gmail. Il en a donc déduit que la TV devait forcément analyser ses habitudes, les programmes qu'il regarde, les sites qu'il visite, etc. En cherchant à en savoir plus, il constate en effet que son téléviseur dispose d'une fonction activée par défaut de collecte d'informations de visionnage.

Même après avoir désactivé cette fonction, le téléviseur continuait de transmettre des informations à son insu à LG. Le constructeur ne se contentait pas de scruter ses habitudes de consommation, mais il récupérait également des données personnelles telles que des vidéos de famille qu'il avait projetées sur son écran depuis son ordinateur. Un scandale dont se serait bien passé LG qui aurait, depuis, décidé de permettre à ses clients de « vraiment » désactiver l'option de collecte de données. Outre le manque de sécurité constaté sur de nombreux objets connectés, il faudra donc aussi dorénavant se méfier des pratiques intrusives de certains fabricants !

Source DoctorBeet's Blog

Sous l'œil de Shodan

En faisant un tour d'horizon des objets connectés pour la maison, susceptibles de présenter des risques, on se rend compte qu'ils sont tous potentiellement vulnérables. Certains ne sont pas sécurisés ou pas suffisamment, tandis que d'autres présentent des failles de sécurité plus ou moins importantes pouvant être exploitées pour mener des attaques externes ou à courte distance. Mais la principale faille qu'exploitent les hackers est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Un vrai problème, d'autant qu'avec un moteur de recherche comme Shodan, tous les appareils connectés ayant une adresse IP visible sont désormais répertoriés sur le Web.

D'une efficacité redoutable, ce service permet d'effectuer des recherches globales, ou par pays, en saisissant une simple requête pour identifier, localiser, voire prendre le contrôle des appareils connectés non protégés par un mot de passe. Il suffit de saisir le nom d'une marque de produits connectés connue (DLink, Netgear, Samsung…) ou de cliquer sur les mots recherchés les plus populaires (Webcam, Camera, Netcam…) pour voir apparaître leurs adresses IP et s'y connecter. Le service indique de surcroît de nombreux détails sur les dispositifs, comme leur système d'exploitation, s'ils sont connectés, protégés ou non par des identifiants, etc.

Comme cela avait été démontré dans une enquête baptisée Null CTRL, réalisée par deux journalistes norvégiens pour le site Dagbladet en 2013, d'innombrables équipements connectés référencés par Shodan ne possèdent aucune protection. Quelques clics suffisent pour les repérer et visionner, par exemple, le flux vidéo de caméras de surveillance chez des particuliers, jouer avec le tableau électrique ou le thermostat d'un immeuble, s'introduire dans des bases de données, etc. Gageons qu'à terme, cette surexposition des objets connectés permette de sensibiliser les utilisateurs sur l'importance de sécuriser leur accès.

Qu'en pensent les experts ?

Au-delà des rapports alarmants, des exploits des chercheurs et des affaires relatées dans les médias, nous avons souhaité donner la parole à un expert en sécurité ainsi qu'à un fabricant de solutions domotiques. Tous deux apportent une vision concrète sur les risques que représentent les objets connectés à l'heure actuelle, et donnent quelques conseils aux utilisateurs pour mieux se protéger.

Cybermesures sur les maisons intelligentes

Pour en savoir un peu plus sur les menaces qui planent sur les maisons intelligentes et leurs installations domotiques, nous avons rencontré un expert en sécurité qui travaille depuis plus de dix ans pour Kaspersky Lab Angleterre. Il dresse un portrait plus nuancé que celui des cabinets d'experts en sécurité que nous avons évoqué précédemment.

David Emm

Clubic : Que pouvez-vous nous dire sur la sécurité des objets connectés pour la maison ?

David Emm : Les gens utilisent Internet pour faire des achats, gérer leurs comptes en banque, aller sur les réseaux sociaux mais aussi pour chercher des informations liées à tous les aspects de leur vie quotidienne. Et cela va encore plus loin maintenant que nous utilisons les technologies informatiques pour réaliser des actions qui étaient, par le passé, purement mécaniques, voire manuelles. Malheureusement, lorsque de nouvelles technologies voient le jour, ou lorsque la technologie génère de nouveaux usages, la sécurité n'est souvent pas l'une des priorités. Ce n'est pas un phénomène nouveau et si l'on regarde en arrière, on remarque que les évolutions sont portées par une volonté de simplicité, de réduction des coûts ou d'autres bénéfices, alors que la sécurité n'est envisagée qu'après l'émergence d'un problème. Les risques sont multiples, allant du vol à la manipulation des données. Il est facile d'imaginer par exemple qu'un compteur intelligent soit manipulé pour falsifier la consommation électrique. Pour l'instant, cela reste de l'ordre du possible plus que de celui du réel car à ma connaissance il n'y a eu aucune attaque réelle visant des compteurs électriques.

Clubic : Selon vous, quels sont les types d'appareils domotiques les plus vulnérables ?

David Emm : Lorsqu'ils entendent parler de l'Internet des objets ou de maisons intelligentes, la plupart des gens imaginent leurs appareils traditionnels disposant de nouvelles fonctionnalités (réfrigérateur, contrôle des portes, chauffage central, etc.). Pourtant, ces appareils ne sont pas encore massivement connectés et pour l'instant, leur vulnérabilité a été démontrée le plus souvent au travers d'exploits d'experts dans le cadre de tests. Bien sûr, lorsque ces appareils seront plus courants dans nos vies, je pense qu'ils deviendront régulièrement la cible d'attaques. Mais il faut surtout s'inquiéter de la vulnérabilité d'appareils qui sont aujourd'hui des incontournables, comme par exemples les modems Internet, les tablettes, les smart TV, etc.

Clubic : À quel type d'attaques les maisons intelligentes (Smart Home) sont-elles exposées ?

David Emm : Je dirais qu'il y a trois principales catégories :
1 – Obtenir l'accès à un appareil et l'utiliser pour prendre le contrôle d'autres systèmes connectés dans la maison
2 – Avoir accès à des informations privées ou sensibles, y compris des mots de passe
3 – Falsifier des informations reçues / envoyées par un appareil à l'insu des personnes du foyer

Clubic : Quelles sont les vulnérabilités que vous avez pu constater ?

David Emm : L'un de mes collègues David Jacoby a publié un rapport pour alerter sur les dangers de l'exécution de code à distance et des mots de passe faibles sur les appareils de stockage NAS, mais aussi la possibilité d'orchestrer une attaque de type « man-in-the-middle » (NDRL : l'attaque de « l'homme du milieu » consiste à s'infiltrer sans être vu dans un réseau et y intercepter des informations) via une Smart TV. Il a également découvert des fonctionnalités d'analyses non référencées intégrées dans les routeurs par les constructeurs (sans doute pour des raisons légitimes), mais qui pourraient être exploitées par un attaquant. Un appareil sans fil est repérable et potentiellement vulnérable aux attaques lorsque ses communications ne sont pas cryptées, et que le mot de passe d'accès utilisé est celui par défaut ou faible.

Clubic : Est-ce que Kaspersky envisage de proposer des solutions de sécurité pour les objets connectés ?

David Emm : Ce n'est pas parce qu'il est possible d'installer une solution de sécurité sur les terminaux traditionnels (PC, tablettes, smartphones…), que cela sera possible sur tous les appareils du quotidien qui sont connectés à Internet. Ces appareils pourraient recevoir et envoyer des données sans pour autant autoriser l'installation de code ou disposer de suffisamment d'espace pour le faire. Ils pourraient être vulnérables (par exemple si une Smart TV tourne sous un OS standard, il est possible que le code ne puisse être modifié que par le constructeur). En plus, le vendeur n'est pas toujours le constructeur des composants informatiques intégrés. Cela signifie qu'il pourrait être impossible de patcher ces appareils, même en cas de mise à jour de sécurité disponible via le constructeur des composants. On comprend mieux pourquoi il est primordial que les constructeurs d'appareils et les entreprises qui les exploitent prennent en compte la sécurité dès le début de la fabrication d'un produit. Il est essentiel de pouvoir établir un dialogue entre experts en sécurité et développeurs d'appareils informatiques pour maisons connectées.

Clubic : Que peuvent faire les utilisateurs pour protéger au mieux leurs systèmes domotiques ?

David Emm : La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à Internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route du hacker. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple…).

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

David Emm : C'est une question difficile, car LE scénario catastrophe impliquant un seul individu n'aura pas forcément le même impact au niveau d'une communauté. Pour les individus, le risque qui importe c'est le #vol de données personnelles – par exemple, les noms d'utilisateurs, les mots de passe, etc. Ou encore, le fait que l'on puisse vous espionner vous ou votre famille (comme le hack du babyphone survenu dans l'Etat de Ohio). Il y aussi le risque qu'une application contrôlant la sécurité de votre porte d'entrée puisse être hackée, vous laissant enfermé dehors. Du point de vue de la communauté, l'impact peut être plus important. Si un hacker arrive par exemple à intercepter des données d'un compteur intelligent (Smart Meter), cela peut affecter les relevés : il peut remettre les compteurs à zéro, voire créer une panne générale d'électricité.

Le point de vue d'un spécialiste de la domotique

Pour compléter ce dossier, nous avons voulu donner également la parole à un fabricant de solutions domotiques. Somfy, l'un des leaders du marché de la domotique, a bien voulu répondre à nos questions sur la sécurité des maisons intelligentes.

Clubic : Comment la box Somfy et les appareils qu'elle permet de piloter à distance sont-ils protégés ?

Somfy : En tant que spécialiste de solutions domotiques, notre box prend en compte les problématiques de sécurité. L'ensemble des actions effectuées avec nos solutions Tahoma et Somfy Box transite sur un serveur sécurisé et est chiffré sur 128 bits. Le protocole RTS propriétaire de Somfy (10 millions de systèmes installés dans le monde) qui est utilisé pour la commande radio est sécurisé grâce à un code tournant de 16 millions de combinaisons.

Clubic : En tant que fabricant, que pensez-vous du remous médiatique autour de la vulnérabilité supposée ou avérée de certains objets connectés pour la maison ?

Somfy : Nous sommes aujourd'hui en plein boom des objets connectés, avec de nombreux nouveaux acteurs qui lancent parfois des solutions un peu trop vite et pas suffisamment abouties. Il faut veiller à bien se renseigner sur le fabricant et sa légitimité sur le secteur. Somfy possède une expertise en matière de radio et d'IP qui nous rend légitimes sur ce secteur. Depuis que nous avons lancé notre box il y a quatre ans, aucun piratage ne nous a été signalé.

Clubic : Quels sont selon vous les points faibles d'une installation, ou quels pourraient-ils être ?

Somfy : Les points faibles de l'installation seraient de ne pas avoir de système de protection, d'avoir positionné les détecteurs de mouvements aux mauvais endroits ou de ne pas couvrir tous les accès de la maison.

Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?

Somfy : Le scénario catastrophe, s'il y en a un, serait de se faire voler son téléphone sans code pour le déverrouiller en laissant ainsi libre accès à l'application qui commande la maison intelligente. Il faut donc prendre les précautions nécessaires.

Conclusion

En moins de deux ans, la domotique est passée d'un marché de niche à un nouvel eldorado convoité par la plupart des géants de l'industrie high-tech. Apple, Google, Microsoft ou encore Samsung, pour ne citer qu'eux, se sont lancés tour à tour sur ce marché promis à une très forte croissance en multipliant les partenariats et les rachats de start-up spécialisées. Début 2014, Google n'a pas hésité par exemple à faire la troisième acquisition la plus importante de son histoire, en rachetant Nest Labs pour la bagatelle de 3,2 milliards de dollars et, plus récemment, le spécialiste de caméras IP Dropcam pour 555 millions de dollars.

Courant 2014, Samsung s'est offert la start-up spécialisée SmartThings (montant de l'achat non divulgué), Microsoft a noué un partenariat avec Insteon, un des leaders de la domotique aux USA, et Apple a dévoilé à l'occasion de la WWDC la plateforme HomeKit pour iOS8 qui permettra de contrôler les objets connectés de nombreux fabricants via Siri (l'assistant vocal d'Apple). En attendant les solutions des poids lourds des nouvelles technologies, le marché est déjà bien occupé par les acteurs historiques – Somfy, Philips, Haier, Legrand, etc. –, une foule de nouveaux fabricants de tous horizons, des fournisseurs d'électricité ou encore des opérateurs comme Orange et SFR, qui commercialisent en France des kits de domotique pour accompagner leurs box. Si tout ce monde frappe à la porte de nos foyers, c'est que le potentiel est énorme.

Il ne fait aucun doute que les produits du quotidien vont être de plus en plus connectés (comme nous avons pu le voir au CES cette année), mais pas toujours bien sécurisés. Les acteurs comme Google, Apple et Microsoft, qui ambitionnent qu'un maximum d'objets connectés puissent fonctionner à l'avenir avec leurs plateformes mobiles respectives, vont sans doute imposer aux fabricants un cahier des charges drastique en matière de sécurité s'ils veulent obtenir une certification. Cela pourrait peut-être permettre d'augmenter le niveau de protection des objets connectés, même si comme nous l'avons vu, il n'est pas toujours possible de patcher des produits comprenant des composants provenant de différents fabricants.

Le nombre croissant d'objets connectés risque d'intéresser de plus en plus les cybercriminels pour entreprendre des diffusions de spams ou de logiciels malveillants à grande échelle, par exemple. Mais le plus effrayant serait qu'ils puissent prendre le contrôle total des maisons intelligentes, espionner leurs habitants à l'aide des caméras de surveillance, s'introduire ni vu ni connu dans le foyer en déverrouillant la porte à l'aide d'un smartphone, couper l'électricité ou le chauffage en plein hiver, ou encore, déclencher l'alarme au beau milieu de la nuit…

Pour que les maisons intelligentes tiennent vraiment toutes leurs promesses, il est indispensable qu'à l'avenir leur sécurité soit garantie. En attendant, côté utilisateur, il faudra être de plus en plus vigilant, se renseigner sur le système de protection des produits, faire systématiquement les mises à jour, ou encore instaurer un mot de passe fort pour l'accès à distance de tous les appareils connectés. Le prix à payer pour que le rêve de posséder une maison intelligente ne tourne pas au cauchemar.

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

Source : #http://www.clubic.com/antivirus-securite-informatique/article-723729-1-objets-connectes-representent-risque.html
Par Jérôme Cartegini

Piratage de ses comptes sociaux : prévenir, repérer et réagir | Denis JACOPINI

Sur les réseaux sociaux, la plus grande vigilance est requise si l'on veut protéger ses données personnelles.

Les réseaux sociaux se multipliant de façon considérable, il convient de se montrer attentif à la protection des données personnelles, car ces dernières peuvent d'autant plus facilement être piratées.
A ce titre, la Commission nationale de l'informatique et des libertés (CNIL) publie une fiche pratique, agrémentée de liens directs vers les principaux réseaux sociaux, afin de mettre en oeuvre le contrôle des données personnelles.

Parmi les conseils donnés par la Commission, citons :
– le choix de mots de passe complexes, mais aussi différents les uns des autres, et avec un sens n'ayant aucun rapport avec une donnée personnelle relative à la vie privée du titulaire du compte (comme une date de naissance, etc…) ;
– l'absence totale de communication du mot de passe à une tierce personne ;
– l'activation d'un dispositif d'alerte en cas d'intrusion (dans ce cas, la personne titulaire du compte et qui se connecte depuis un poste informatique inconnu doit confirmer l'accès en entrant un code, reçu préalablement par sms ou par mail) ;
– la déconnexion à distance des terminaux encore liés au compte ;
– la désactivation des applications tierces encore connectées au compte ;
– le réglage précis des paramètres de confidentialité.
En outre, la CNIL donne des astuces pour repérer le piratage d'un compte. Des signes doivent en effet alerter l'utilisateur, par exemple un mot de passe invalide, ou des comportements inhabituels ayant lieu sur le compte, sans consentement préalable (comme suivre, se désabonner, ou encore bloquer…).

En cas de piratage, il convient donc :
– en premier lieu, de signaler le compte piraté auprès du réseau social ;
– cette première étape franchie, il convient alors de demander une réinitialisation du mot de passe. Si la réponse apportées par les modérateurs du réseau n'est pas satisfaisante, la CNIL peut être saisie.

Consultez la fiche pratique de la CNIL

Source : http://www.net-iris.fr/veille-juridique/actualite/34642/comment-prevenir-le-piratage-de-son-compte-en-ligne.php

10 conseils pour garder vos appareils protégés pendant les vacances | Denis JACOPINI

10 conseils pour garder vos appareils protégés pendant les vacances

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, voici un mini-guide conçu par les experts ESET pour voyager et surfer en toute tranquillité.
Brosse à dents ? ok.
Serviette de bain ? ok.
Ordinateur, téléphone, tablette ? ok.
Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails. Pas de panique ! Stephen Cobb et d'autres professionnels ESET ont créé un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

Conseils

1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.
2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.
3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.
4. Mettez un mot de passe fort et activez la fonction « délai d'inactivité » sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous nos conseils pour un mot de passe efficace en cliquant ici.
5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.
6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.
7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.
8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).
9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.
10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants
Article original de ESET
Cliquez ici

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 Liberté) ;
- 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 : ESET — Actualités

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.
Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant… Les accès gratuits pullulent et se généralisent.
Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « **Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit** » assure-t-il. « **Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants…** »

Des sniffeurs de données

Il exagère ? Non. « **L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés !** » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« **Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter.** » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « **Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi** ».

Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.
Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd.
Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]

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 : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

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

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.fr | RGPD CYBER . LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Nous semblez manifester un intérêt pour le RGPD (peut-être un peu par obligation) et vous souhaitez nous faire part d'un projet. Nous vous remercions pour votre confiance.
Intervenant sur des missions RGPD depuis 2012, après avoir identifié différents types d'attentes, nous avons adapté nos offres pour qu'elles correspondent au mieux à vos besoins.
Ainsi, nous pouvons vous accompagner dans la mise en conformité de votre structure de plusieurs manières :
1. **Vous recherchez l'autonomie ?**
Nous pouvons vous accompagner pour apprendre l'essentiel de la réglementation Européenne relative à la Protection des Données à Caractère Personnel et le nécessaire pour comprendre et démarrer une mise en conformité. Une fois la formation achevée, vous êtes autonome mais pourrez toujours compter sur notre soutien soit sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisés ;
A l'issue de cette formation, nous vous remettons une attestation prouvant la mise en place d'une démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données). Pour information, nous sommes référencés auprès de la CNIL.
2. **Vous souhaitez être accompagné pour la mise en place de la mise en conformité ?**
Nous réalisons pour vous l'audit qui mettra en exergue les points à améliorer. Au terme de cette étape vous pourrez, si vous le souhaitez, réaliser la mise en conformité ou nous laisser procéder aux améliorations que vous aurez validées ;
A l'issue de cet audit, nous vous remettons un compte rendu prouvant la mise en place de corrections dans le cadre de votre démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données).
3. **Vous souhaitez confier la totalité de votre mise en conformité ?**
De manière parfaitement complémentaire avec votre prestataire informatique et éventuellement avec votre service juridique, nous pouvons nous charger de la totalité de la démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données) et les différentes réglementations relatives à la protection des Données à Caractère Personnel.
De l'audit au suivi, vous pourrez compter sur notre expertise à la fois technique et pédagogique pour que votre établissement soit accompagné de manière externalisée.

Afin de vous envoyer une proposition personnalisée adaptée à la fois aux besoins de votre structure, conforme à votre stratégie et à vos priorités, nous souhaiterions que vous répondiez à ces quelques questions :

Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à les consulter sont soumises au secret professionnel.

Votre Prénom / NOM (obligatoire)

Société / Organisme

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (ne sera pas utilisé pour le démarchage)

Pouvez-vous nous décrire brièvement votre activité ? (obligatoire)

Remarque :
Vous pouvez nous écrire directement un message dans la zone « INFORMATIONS COMPLÉMENTAIRES QUE VOUS JUGEZ UTILES ». Néanmoins, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin dans un premier temps des informations ci-dessous.

POUR VOTRE MISE EN CONFORMITÉ RGPD :

1. **La découverte de vos obligations** : Souhaitez-vous découvrir le RGPD et l'essentiel pour comprendre et démarrer la démarche ? (recommandé)	●Oui/○Non
2. **Concernant l'Audit** : Il consiste à relever les éléments permettant de constituer un état des lieux précis puis à réaliser l'analyse réglementaire du contexte de départ. Nous considérons qu'au moins une journée dans vos locaux est indispensable. La suite de la démarche peut être faite à distance.	Sélectionnez votre choix (vous apprendrez la suite)
3. **Concernant la mise en conformité** : Elle consiste à mettre en place des améliorations :	Sélectionnez votre choix (vous apprendrez la suite)
4. **Concernant le suivi de la mise en conformité** : Cette phase consiste à maintenir la mise en conformité avec le temps par une mise à jour précise du registre des traitements./!\	Sélectionnez votre choix (vous apprendrez la suite)
5. **Votre demande concerne-t-elle un groupement de professionnels** ? (corporation, fédération, à nous préciser dans les commentaires...) ou est-elle formulée à titre individuel ?	○Groupement/●Individuel

INFORMATIONS COMPLÉMENTAIRES QUE VOUS JUGEZ UTILES :

Envoyer
block id="24886" title="Mentions légales formulaires"]

ou bien, envoyer un e-mail à rgpd[a-ro-ba-se]lanetexpert.fr

Denis JACOPINI est notre Expert qui vous accompagnera dans votre mise en conformité avec le RGPD

Je me présente : Denis JACOPINI. Je suis Expert en informatique assermenté et **spécialisé en RGPD (protection des Données à Caractère Personnel) et en cybercriminalité**. Consultant depuis 1996 et formateur depuis 1988, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15845), en tant que praticien de la mise en conformité et formateur, je vous accompagne dans toutes vos démarches de mise en conformité avec le RGPD.

« Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD. »