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

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

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

Les bons réflexes contre les attaques informatiques | Denis JACOPINI

350 milliards d'euros par an : selon le McAfee Report on the Global Cost of Cybercrime publié en 2014, tel est le coût estimé des attaques informatiques à l'échelle mondiale.Depuis le début de l'année, les attaques se sont multipliées, notamment suite aux attentats de Charlie Hebdo, mettant plus que jamais en péril la sécurité des données des entreprises et des institutions. Un rapport publié le 16 février dernier par Kaspersky Lab a quant à lui révélé l'attaque d'une centaine de banques depuis 2013 par un gang organisé.

Afin d'appréhender au mieux ces offensives, il est important d'en comprendre les tenants et les aboutissants et d'avoir à l'esprit les réflexes qui permettent de s'en prémunir.

Des attaques aux motivations multiples

De plus en plus de sites internet sont victimes d'attaques dites de « défiguration » perpétrées par des hacktivistes revendiquant des convictions religieuses, politiques ou encore contestataires. On trouve également certains attaquants qui agissent uniquement pour l'amusement, mais ces scénarios se font de plus en plus rares. En général, seule la page d'accueil du site est modifiée pour signifier leur passage et évoquer leurs revendications.

On trouve également d'autres attaques qui, elles, sont plus furtives (ou en tout cas tentent de l'être) et consistent à voler des informations à des fins de rançonnage par exemple. Les vols de données bancaires (carte de crédit, numéros de comptes) permettent quant à eux du détournement d'argent, l'achat de services ou encore de matériels en ligne. Ces criminels, bien organisés, offrent des services de tout type à d'autres criminels : du kit d'infection, à l'envoi de spam massif, en passant par des serveurs de contrôle (c&c) pilotant des milliers de machines « zombies » permettant des attaques DDOS (Déni de service distribué). Tous n'ont pas le même niveau technique, certains ne sont d'ailleurs que des « presse-bouton », alors que d'autres ont la capacité de créer des virus, ou des programmes exploitant des failles de sécurité.

Mais comment s'y prennent-ils ? Ces malfaiteurs utilisent une faille de sécurité dans un programme qui peut provenir d'une erreur de conception (un protocole mal sécurisé par exemple), de programmation ou d'implémentation (failles connues comme shellshock, heartbleed ou ghost), de configuration (oubli du mot de passe par défaut après une installation) ou encore d'une erreur d'utilisation par une personne utilisant un mot de passe trop faible par exemple. L'humain est donc au centre de cette problématique.

Le plus souvent ces attaques débouchent sur du détournement d'argent ou la diffusion de données sur internet. Les conséquences financières pour les entreprises peuvent être considérables, sans compter l'impact que cela peut avoir sur l'image de l'entreprise victime d'un piratage. Dès lors, quels réflexes adopter face à ces diverses attaques et failles ?

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

Adopter les bonnes pratiques pour limiter les risques

Les attaques ne cessent de croitre dans la mesure où l'enjeu financier pour les criminels est très important. Lorsque l'on sait que l'attaque par déni de service est accessible pour seulement 30 à 70 dollars la journée et qu'un spam ne revient qu'à 10 dollars par tranche d'1 million d'e-mails*, ce type de pratique n'est pas prêt de cesser. A ce premier enjeu s'ajoute le manque de vigilance dont font preuve les internautes. Le risque de s'infecter est en effet omniprésent : il suffit de cliquer sur un lien drainant un logiciel malveillant ou encore de partager un contenu infecté.

Quand bien même le risque zéro n'existe pas, la grande majorité de ces attaques pourrait être bloquée, dès lors que l'on adopte les bonnes pratiques pour se protéger et protéger autrui. Le maître mot est l'anticipation et la capacité à réagir rapidement en cas d'intrusion, la mise en œuvre d'un pare-feu ou d'un anti-virus pour se protéger n'étant pas suffisante. Le processus organisationnel de sécurisation est en effet plus important que les outils de protection eux-mêmes (on a en général un rapport de 80-20).

Pour ce faire, l'un des points majeurs est la gestion des mises à jour. Lorsqu'une faille tombe, celle-ci peut-être déjà exploitée plus ou moins massivement. S'en suit la douloureuse phase consistant à tester si le programme régresse ou non dans son fonctionnement avant une mise en production. Durant toute cette période, le programme est encore exposé à une potentielle exploitation de la faille. Cela sous-entend qu'il faut d'une part valider aussi vite que possible, et d'autre part essayer de se protéger temporairement avec des outils de type Firewall ou IPS. Il est aussi bon de rappeler que ces outils de protection sont aussi faillibles que les autres et qu'ils peuvent être contournés.

Dans le cas où l'attaque a déjà eu lieu, sur un site web par exemple, la première chose à faire est de bloquer le site. Cette phase est primordiale dans la mesure où un site piraté peut renvoyer des logiciels malveillants aux internautes le consultant.

La deuxième étape est de sauvegarder tous les journaux, les données et programmes du site ainsi que la base de données, avant de procéder à une analyse du système pour connaître l'origine de l'attaque. Cette analyse est primordiale pour une remise en production du site. Elle permet de connaître par quel moyen les attaquants sont entrés dans le système et ce qu'il faut mettre à jour. Le mieux est de revenir sur une version de sauvegarde dont on est sûr qu'elle n'a pas été affectée par la compromission et de la mettre à jour. Parallèlement, il est également vivement conseillé de porter plainte afin que ces attaques soient référencées par les autorités et que des mesures soient prises.

S'il est crucial de prendre en compte la problématique de sécurité lors de la création d'un projet informatique, il est tout aussi indispensable d'en assurer la maintenance afin d'anticiper les attaques et de pouvoir les gérer efficacement, et ainsi minimiser leur impact sur l'activité de l'entreprise.

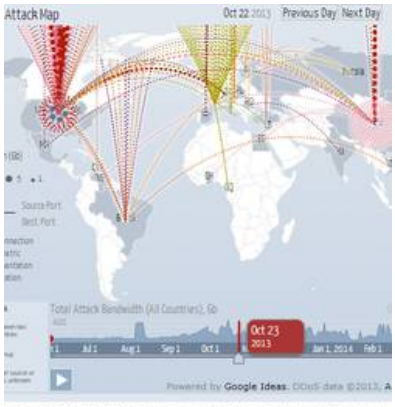
Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur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

Contactez-nous

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

Source : http://www.journaldunet.com/solutions/expert/60082/attaques-informatiques--decryptage-du-phenomene-et-reflexes-a-adopter.shtml
Par Sébastien Delcroix – NFrance

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



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).

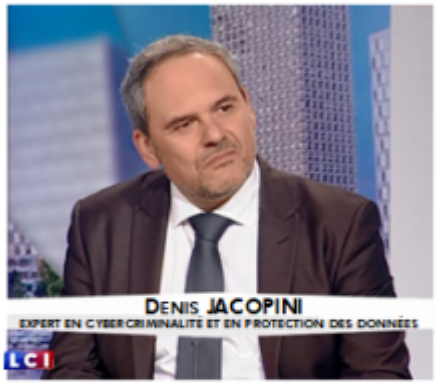
Les cyberdélinquants n'ont d'autre objectif que de gagner beaucoup d'argent. Virus, spams, et autres botnets drainent plusieurs centaines de millions de dollars chaque année à travers le monde.

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

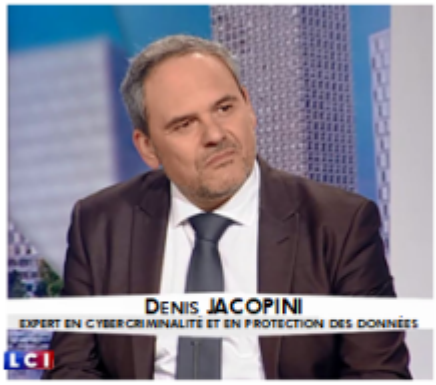
12/05/2015 : Kaspersky annonce être victime d’une Cyberattaque
Consulter

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.

Réagissez à cet article

---

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 Cybercriminalité 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

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

---

Comment retirer des

publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL				

Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus

Une donnée personnelle est « *toute information se rapportant à une personne physique identifiée ou identifiable*». Sur une publication, vous pouvez être identifié :
• **directement** (exemple : nom, prénom, etc.)
• ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :
• **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
• **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.
En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

1. Signaler la publication à effacer

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.
Twitter : Signaler la divulgation d'informations privées
Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram
Facebook : Utiliser le lien » Signaler «
situé à côté de la publication, de la photo ou du commentaire
Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image
LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité
Youtube : Réclamer une atteinte à la vie privée
Dailymotion : Sous chaque vidéo figure un bouton *» Signaler cette vidéo »*
en cliquant dessus, vous aurez à remplir un formulaire.

2. Si le réseau social ne fait pas partie de cette liste

• Rendez-vous vous en bas de la page d'accueil du réseau social ;
• Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
• Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
• Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

Quelle réponse attendre du réseau social ?
Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.
En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.
En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes

pratiques ?
Victime d’usurpation d’identité sur facebook, tweeter ? Portez plainte mais d’après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

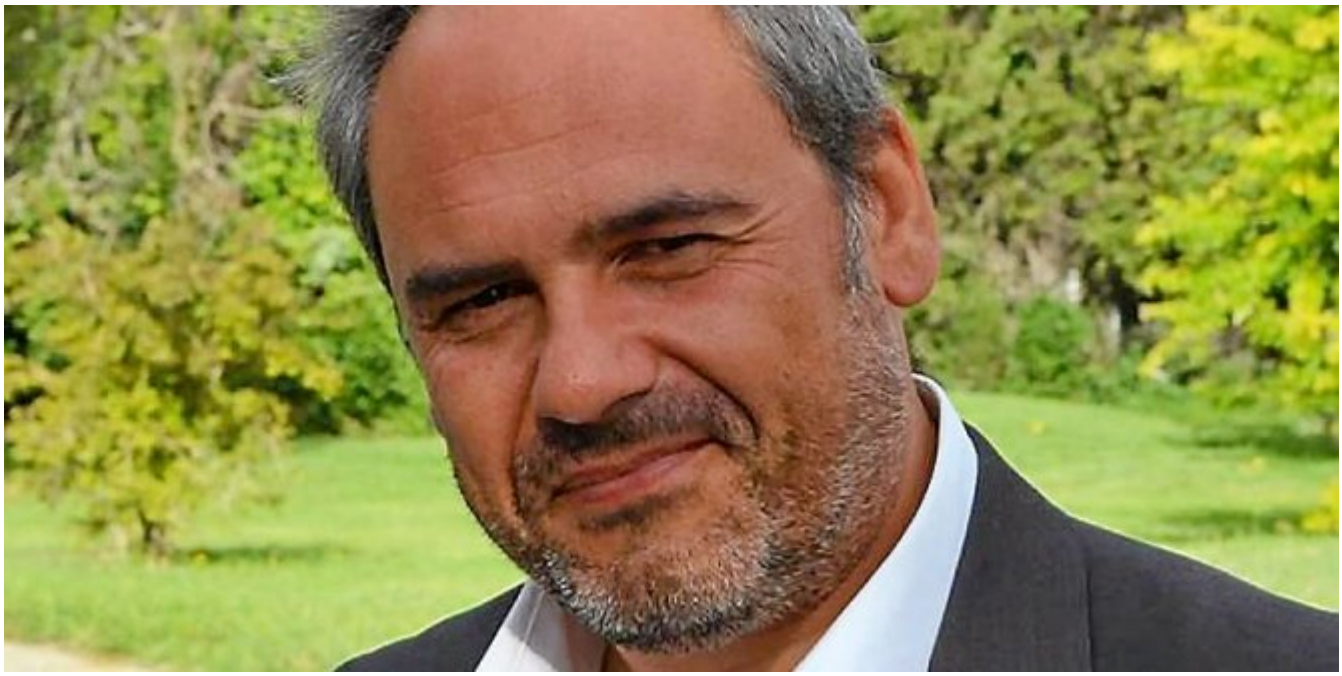
Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*

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

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

	Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore.Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

Réagissez à cet article

Source : *Nos ordinateurs ont-ils la mémoire courte ?*

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Mise en conformité RGPD : Accompagnement personnalisé par des Experts**				

Vous 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 Je veux apprendre à le faire
3. Concernant la mise en conformité : Elle consiste à mettre en place des améliorations :	Sélectionnez votre choix Je veux apprendre à le faire
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./td>	Sélectionnez votre choix Je veux apprendre à le faire
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

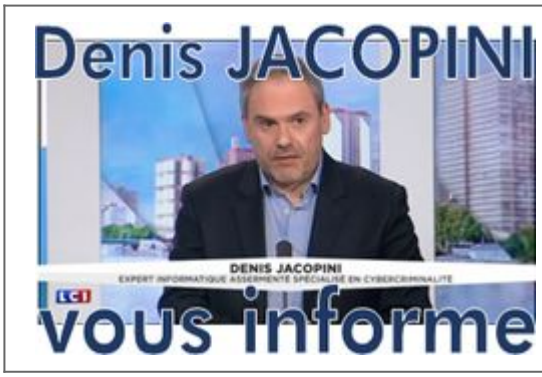
Les informations recueillies sont enregistrées dans la messagerie électronique et le système informatique de LeNetExpert pour les traitements correspondant à la gestion de vos demandes et la proposition de services correspondant à votre demande. Le lieu de traitement de stockage et de sauvegarde se situe en France et auprès d'établissements respectant le bouclier de protection des données UE-Etats-Unis (en anglais : EU-US Privacy Shield). Elles sont conservées 3 ans après notre dernier échange et sont destinées aux services internes. Une démarche de mise en conformité a été entamée en interne depuis 2010 et jusqu'à ce jour par des formations régulières, l'identification des traitements, la réalisation d'un registre des traitements, une analyse de risques sur nos traitements manipulant des données sensibles ou des « données à caractère hautement personnel » pour lesquels leur violation pourrait avoir de graves conséquences dans la vie quotidienne des personnes concernées et un suivi semestriel. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit RGPD (Règlement Général sur la Protection des Données), à la loi n°78-17 dite «Informatique et Libertés» du 6 janvier 1978 et à la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant Le Net Expert, Monsieur le Délégué à la Protection des Données – 1 les Magnolias – 84300 CAVAILLON par Recommandé avec accusé de réception. Enfin, sur le fondement des articles 131-13, 222-17, 222-18, 222-18-1, 322-12, 322-13, R.621-1, R-621-2, R-623-1, R-624-3, R-624-4, R 631-1 et R634-1 du code Pénal et l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse, votre adresse IP horodatée est également collectée.
Sauf indication contraire ou information publique, nous nous engageons à la plus totale discrétion et la plus grande confidentialité concernant les informations que vous nous communiquez.

a
ou bien, envoyez un e-mail à rgpd[a-ro-ba-se]lenetexpert.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 1998, 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. »

Cybersécurité : Aller plus loin dans la formation des salariés



Cybersécurité : Aller plus loin dans la formation des salariés

Alors que les entreprises sont de plus en plus sensibilisées aux risques de failles, de mise hors service de leurs systèmes (attaques DDOS) et de destruction de leurs données (via des ransomwares), elles ne pensent pas forcément que leurs outils de communication unifiée sont également concernés par les règles de protection.

• **Le chiffrement** : toutes les données, qu'elles soient stockées ou en transmission, doivent être protégées, les premières avec au minimum un chiffrement AES 128 bits et les secondes en ajoutant au moins le protocole TLS. Point important : il faut bien évidemment que les messages de tous les interlocuteurs, externes compris, soient cryptés.

• **Le pare-feu** : attention à ne pas tomber dans le piège d'une solution qui exposent des applications, des serveurs ou des équipements hors du pare-feu. De plus, il faut s'assurer que les solutions gèrent correctement le parcours des données au travers des serveurs d'authentification déjà en place.

• **Les mises à jour** : puisque les mises à jour de firmwares et autres logicielles corrigent essentiellement des vulnérabilités ou apportent des dispositifs de sécurité plus robustes, il est primordial qu'elles se fassent de manière automatique pour s'assurer que le SI est protégé le plus tôt possible. Une des approches consiste à passer par une solution en Cloud, automatiquement mise à jour par le fournisseur lui-même **mais à manier avec précaution car si vous avez déjà opté pour le Cloud, avez-vous la certitude que seuls les utilisateurs autorisés accèdent à cet espace de stockage externalisé ? Qui peut bien se connecter pendant que vous dormez ?**

• **La sécurité physique** : où se situent les données que stocke la solution de communication ? Il est essentiel d'avoir la garantie que le datacenter du fournisseur soit protégé 24/7 et qu'il soit régulièrement audité et protégé contre les intrusions physiques.

• **Changer les paramètres par défaut** : Changer tous les identifiants et mots de passe de ceux proposés par défaut pour quelque chose de plus complexe est une règle d'or en matière de cybersécurité.
« Parmi les nombreuses cyberattaques survenues en 2016, la plus célèbre fut celle lancée par le botnet Mirai qui ciblait les webcams. Or, si cette attaque a autant réussi, c'est parce que les mots de passe administrateurs par défaut de ces équipements étaient toujours actifs », dit-il.

• **Sécuriser le réseau, jusqu'aux utilisateurs** : Un segment non sécurisé du réseau est une porte d'entrée par laquelle peuvent passer les cyber-attaques pour atteindre tout le SI d'une entreprise. Les méthodes pour sécuriser le réseau comprennent l'application de restrictions d'accès, le blocage au niveau du pare-feu de certaines pièces attachées et le test régulier des failles de sécurités connues. Mais Gustavo Villardi prévient qu'il ne s'agit là que de résoudre une partie du problème. « Selon une étude récente menée par Verizon sur les failles de sécurité, l'erreur humaine continue d'être la cause principale des cyber-attaques. Les collaborateurs sont le maillon faible et les entreprises se doivent de former leur personnel pour qu'ils restent protégés en ligne et depuis quelque appareil que ce soit », témoigne-t-il.

• **L'usage à domicile** : les collaborateurs en télétravail ne bénéficient pas de l'encadrement de la DSI pour sécuriser leur accès domestique. Il est donc nécessaire de leur indiquer comment sécuriser une box pour activer le chiffrement du Wifi et passer par un VPN.

• **Les mots de passe** : des bonnes pratiques doivent être appliquées pour que les mots de passe de chaque salarié soient impossibles à deviner ; cela comprend aussi bien de la complexité dans l'enchaînement des caractères que la fréquence de remplacement des mots de passe.

• **L'accès** : les collaborateurs devraient toujours éteindre un équipement lorsqu'ils ne s'en servent pas, afin d'éviter que quelqu'un ne se connecte sur les services restés ouverts

• **Le mode privé** : l'utilisation d'un système de visioconférence uniquement avec les paramètres du mode privé évite que quelque des personnes extérieures puissent se greffer sur une conférence.

[lire l'intégralité de l'article source]

Réagissez à cet article

Source : *Cybersécurité : les trois mesures à prendre pour protéger la communication unifiée – Global Security Mag Online*

Formations RGPD Protection des données personnelles et en Cybercriminalité

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment.

NOS SERVICES :

- Formations **RGPD** (Règlement Général sur la Protection des Données) ;
- Formations en **Cybercriminalité** ;
- **Sensibilisations** à la cybercriminalité ;
- **État des lieux** RGPD ;
- **Mise en conformité** RGPD ;
    - **Analyses de risques** (PIA / DPIA) ;
- **Audits sécurité ;**

VOTRE PROFIL :

- **CLUB D'ENTREPRISES, ORDRES, FÉDÉRATIONS, CORPORATION :** Quelles sont vos responsabilités, quels sont vos risques, quelles devraient être vos priorités ? Que ça soit en matière de Protection des Données Personnelles (RGPD) ou de cybercriminalité, faisons ensemble un état des lieux. Agir sur vos équipements ? Sensibiliser votre personnel ? Libre à vous ensuite d'agir en fonctions de nos recommandations sur les points qui vous sembleront prioritaires.
- **ÉTABLISSEMENTS / CENTRES DE FORMATION / ORGANISATEURS D'ÉVÉNEMENTS :** Que ça soit en protection des données personnelles ou en Cybercriminalité, permettez à vos stagiaires de découvrir les notions essentielles ;
- **CHEFS D'ENTREPRISE / ÉQUIPE INFORMATIQUE :** Nous vous formons dans vos locaux et réalisons en collaboration avec votre équipe informatique une analyse détaillée de vos installation à la recherche de failles et d'axes d'amélioration conformément aux règles de l'art ou de la réglementation en vigueur (RGPD).

LES SUJETS DE FORMATION :

Consultez notre catalogue

COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

Durée : 2 jours ou 4 jours (2 jours tout public + 2 jours approfondissement pour techniciens/informaticiens)

VIRUS, DEMANDES DE RANÇONS, VOL DE DONNÉES… PROTÉGEZ-VOUS !

Durée : 1 jour

LES ARNAQUES INTERNET À CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Durée : 1 jour

COMMENT BIEN UTILISER LE CLOUD

Durée : 1 jour

COMMENT PROTÉGER VOTRE IDENTITÉ ET VOTRE VIE PRIVÉE SUR INTERNET

Durée : 1 jour

DÉCOUVREZ 50 LOGICIELS GRATUITS À CONNAÎTRE ABSOLUMENT

Durée : 1 jour

RGPD CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Durée : 1 jour

RGPD : ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Durée : 1 jour (il est recommandé d'avoir déjà mis en pratique une mise en conformité au moins 15 jours avant)

COMMENT BIEN UTILISER LES DONNÉES DANS LE CLOUD

Durée : 1 jour

À LA DÉCOUVERTE DU DARKNET (LE WEB CLANDESTIN)

Durée : 1 jour

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Durée : 2 jours

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

Remarque :
Un sujet peut être traité en quelques heures mais aussi en quelques jours.
Malgré un minimum de théorie à connaître, nous pouvons réaliser un mélange de ces thèmes afin de vous proposer un contenu personnalisé en fonction des thèmes et durées globales souhaités.

EN FORMAT CONFÉRENCE :

QUE NOUS RÉSERVE LA CYBERCRIMINALITÉ DANS LES 12 PROCHAINS MOIS ?

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

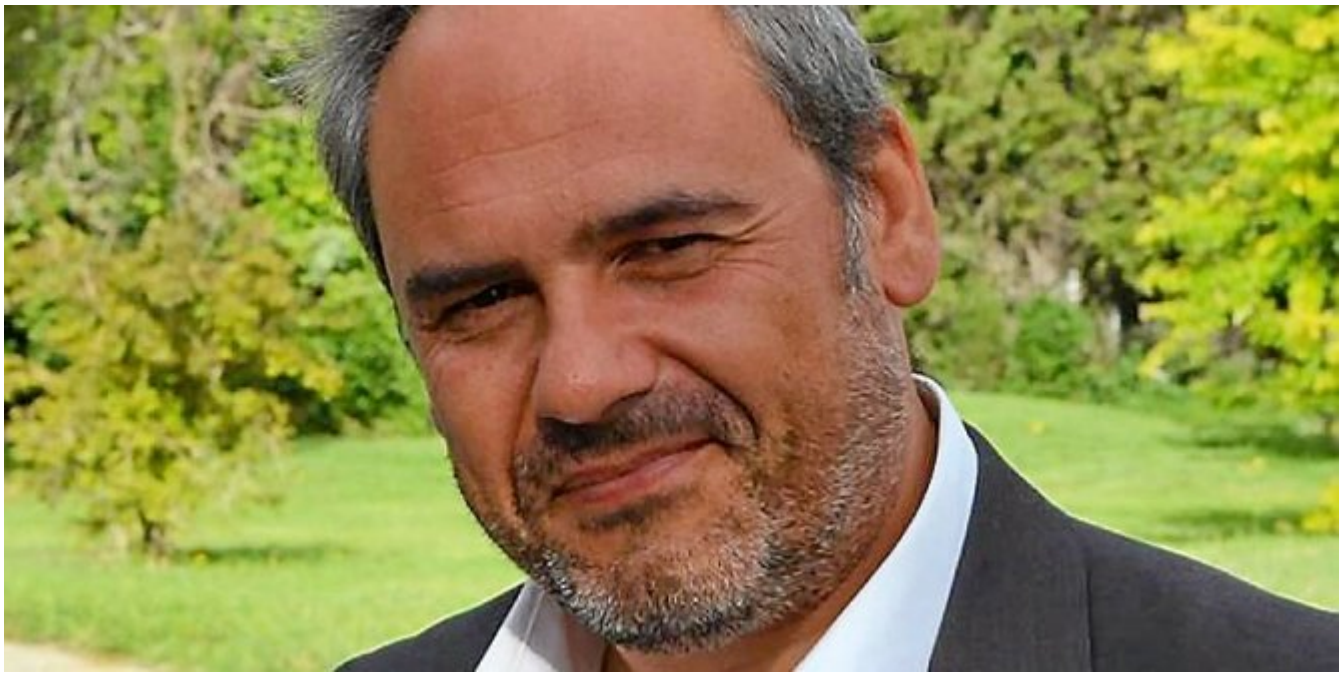
RGPD – CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

FONCTIONNEMENT :

- Vous organisez des formations dans votre établissement ou dans des locaux adaptés : Nous pouvons animer de 1 à 6 jours de formation sur les sujets ci-dessus ;
- Vous organisez un forum ou un salon, nous pouvons préparer une conférence de 20 minutes à 1h30 ou participer à des tables rondes ;
- En faculté ou établissement scolaire, nos interventions seront de 3 à 35 heures.
- Pour une journée de formation, nos interventions sont prévues sont prévues généralement prévues du mardi au jeudi (Lundi, Vendredi et Samedi sous conditions).
- Nos formations d'une journée sont prévues pour une durée de 7 heures par jour maximum.

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.



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 :

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)

Réagissez à cet article