

Comment les salariés peuvent lutter contre la cybercriminalité | Denis JACOPINI



Comment les salariés peuvent lutter contre la cybercriminalité

Les entreprises -queles que soient leur taille économique et leur secteur d'activité- subissent des cyberattaques ciblées qui visent leurs actifs stratégiques. Ce qui entraîne des pertes de plusieurs millions de dollars. Au-delà des offres technologiques de sécurité et des discours méthodologiques qui fleurissent sur le marché, une véritable politique organisationnelle formée et informée face aux dangers doit être développée dans l'entreprise. Quel rôle pour les RH?

Le cybercrime est un phénomène complexe intégrant en son sein un spectre très large de méthodes, de cibles et de motivations. On assiste de moins en moins aux actions de l'hacker isolé uniquement motivé par la mise en lumière de ses exploits ou à celles de l'hacktiviste politique développant des attaques à des fins de sabotage. Le cybercrime est aujourd'hui de plus en plus organisé. Appâté par des gains financiers directs, il met en œuvre ses exactions via des mécaniques sophistiquées comme le spear fishing, l'ingénierie sociale ou encore les menaces furtives APT (Advanced Persistent Threats) au travers d'attaques ciblées, de grande envergure et de plus en plus dévastatrices. Et comme l'a dévoilé la retentissante affaire Edward Snowden aux Etats-Unis, les cyber armées misent en branle par les gouvernements à des fins de renseignement ou d'espionnage industriel sont également très actives.

Un contexte technologique propice aux failles mais pas uniquement -

Si les attaques cybercriminelles réussissent aujourd'hui, c'est que les évolutions technologiques majeures comme le Cloud, le BYOD (Bring Your Own Device) ou encore les objets connectés - en augmentant de manière exponentielle les données disponibles au niveau mondial - ont ouvert et donc fragilisé le réseau de l'entreprise. Ce contexte de démultiplication des périphériques, des utilisateurs et des usages génère des failles et des vulnérabilités, largement exploitées par les cyber assaillants. Mais même si leur impact est bel et bien réel, les transformations technologiques ne sont pas les seules au banc des accusés. En 2015, selon un rapport de sécurité Check Point, 81% des entreprises ont subi des fuites de données causées par des négligences humaines. L'humain, ce « maillon faible » est un élément clé de toute stratégie cyber défense même s'il n'est toujours pas appréhendé sérieusement par les entreprises. Et c'est là que les RH ont leur carte à jouer.

Le rôle déterminant des RH: transformer l'humain en atout pour la sécurité de l'entreprise

Redoublant d'ingéniosité pour arriver à leurs fins, les cyber assaillants mettent en œuvre des attaques d'ingénierie sociale et d'hameçonnage qui exploitent les faiblesses humaines (vanité, reconnaissance, ignorance, gentillesse...) avec pour finalité le vol de données sensibles, le gain direct ou encore l'espionnage industriel. Ces attaques sont très difficiles à détecter par les entreprises car elles ne sont pas identifiées par leurs barrières technologiques et peuvent même passer inaperçues aux yeux de leurs victimes! Pour déjouer les manœuvres des cybercriminels, une culture « sécurité » portée par les RH doit être mise en œuvre pour sensibiliser et responsabiliser les employés de l'entreprise, à chaque couche fonctionnelle et dans le cadre d'une véritable démarche collaborative. Comment?

1/ En assumant la responsabilité des risques de sécurité posé par les collaborateurs de l'entreprise. La grande majorité des employés ne se sent pas vraiment concernée par les problématiques de sécurité de leur entreprise. Elle les considère comme seule responsabilité du département informatique et cette attitude rend les entreprises bien trop vulnérables. Une politique de sécurité interne sera efficace que si elle est comprise et intégrée par les collaborateurs via un véritable état d'esprit associé à une somme de comportements quotidiens. Les RH doivent mener des politiques de sensibilisation actives, sur la durée, portant sur les dangers, les techniques employées par les cyber délinquants et l'impact comportemental des employés sur la sécurité de l'entreprise.

2/ En identifiant le personnel vulnérable. Un des risques majeurs en matière de sécurité est l'accès des employés aux données sensibles de l'entreprise. Dans le cas du piratage de Sony Pictures, les experts ont évoqué l'implication d'un ou de plusieurs ex-employés du Groupe dont l'accès toujours actif au réseau a permis le vol d'informations critiques. En outre, les cybercriminels ont besoin du support de collaborateurs ou de partenaires de l'entreprise qui vont les aider volontairement ou non à arriver à leur fins. Ils utilisent ainsi les réseaux sociaux pour identifier leur cible/victime potentielle, celle qui aura une prédisposition à briser les systèmes de sécurité de l'entreprise, sera démotivée ou en désaccord avec sa hiérarchie. Au cœur de ces informations, les RH doivent ainsi redoubler de vigilance vis-à-vis de ressources à risques ou plus exposées comme les nouveaux arrivants, les employés sur le départ, des fonctions spécifiques (accueil/helpdesk, secrétariats, ...) ou stratégiques tels que les directeurs financiers -

3/ En sensibilisant la Direction Générale. La mise en place d'une culture de la sécurité au sein de l'entreprise doit bénéficier du support du top management. Or les Directions Générales ne sont pas encore forcément sensibles à la mise en place de ces programmes de formations, orientant leurs investissements sécuritaire plutôt vers des dispositifs technologiques. Messieurs les Directeurs, comme l'a si justement souligné Derek Bok, Président de la prestigieuse université d'Harvard « Si vous pensez que l'éducation est chère, alors tentez l'ignorance » ! Il est aujourd'hui impératif pour les entreprises de mettre en place une vraie stratégie de sécurité basée sur une mobilisation interne transverse associant les métiers, le comité de direction, les RH et le RSSI.

Le cybercrime est bien réel, organisé, déterminé et atteint son but même pour les plus grandes organisations internationales aux murailles technologiques dites « infranchissables ». C'est aux entreprises maintenant de penser et de développer une organisation de sécurité enfin, dotée d'un niveau de maturité technique et organisationnel tout aussi élevé que celui de leurs cybers assaillants. La sensibilisation de l'humain, clé de voûte d'une bonne stratégie de cyberdéfense ne doit pas être négligée et les RH devront vite s'emparer du sujet avant que l'ennemi ne soit dans la place !

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

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

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.challenges.fr/tribunes/20150624.CHA7247/comment-les-salaries-peuvent-lutter-contre-la-cybercriminalite.html>
par Emmanuel Stanislas, fondateur du cabinet de recrutement Clémentine.

Mettre son établissement en conformité avec la CNIL, mode d'emploi | Denis JACOPINI



Mettre son établissement en conformité avec la CNIL, mode d'emploi

Se mettre en conformité avec la CNIL est une obligation depuis 1978.

Cependant, les préoccupations des établissements et organismes étant principalement orientés vers des réglementations sociales, fiscales et celles liées à leur métier, la réglementation numérique est longtemps restée délaissée.

En rapport direct avec l'explosion de la cybercriminalité en France, le non respect de la Loi Informatique et Libertés est de plus en plus montré du doigt et les établissements piratés ont de plus en plus leur image salie et leurs comptes bancaires siphonnés.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés.

Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données.

UNE MISE EN CONFORMITÉ CNIL DOIT PASSER PAR UN AUDIT DE L'ENSEMBLE DE VOS SYSTÈMES DE TRAITEMENTS DE DONNÉES

Que se cache derrière cette loi ?

Quels sont les étapes indispensables et les pièges à éviter pour que cette mise en conformité ne se transforme pas en fausse déclaration ?

Plus d'information sur : www.cnil.lenetexpert.fr

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

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.aide.cnil.fr/selfcnil/site/template.do?id=572&back=true>

Comment se préparer aux incidents de sécurité ?



Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.

Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.

Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

- 1. Plan de cybersécurité**
- 2. Gestion du risque**
- 3. Gestion de l'identité**
- **Contrôle d'accès**
- **Authentification**
- **Autorisation**
- **Responsabilité**
- 4. Surveillance de réseau**
- 5. Architecture de sécurité**
- 6. Contrôle des actifs, des configurations et des changements**
- 7. Cartographie de la gestion des incidents**

...[lire la suite]

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

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

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



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

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

Source : *Se préparer aux incidents de sécurité*

Un baccalauréat en cybersécurité à Polytechnique Montréal



Un baccalauréat
en
cybersécurité
à
Polytechnique
Montréal

La Commission des études a approuvé la création d'un nouveau baccalauréat en cybersécurité qui sera offert à Polytechnique Montréal à l'automne 2017.

Les demandes pour un programme de formation en ligne en cybercriminalité, incluant des stages en entreprise, se sont faites pressantes au cours des dernières années et Polytechnique Montréal a décidé de créer un baccalauréat par cumul avec appellation en cybersécurité. La Commission des études de l'Université de Montréal a donné son approbation à ce projet à sa réunion du 21 mars.

Le nouveau programme permettra de combiner deux certificats liés à la thématique (cyberenquête, cyberfraude ou cybersécurité) avec un autre programme de 30 crédits de l'UdeM ou de HEC Montréal en vue de l'obtention d'un diplôme de baccalauréat. L'école de génie, rappellent les responsables, offre une formation en cybersécurité au premier cycle depuis 2007. Le projet vise à répondre «le plus adéquatement possible aux nouveaux besoins du marché du travail, qui est confronté à une pénurie de main-d'œuvre amplifiée par un taux de cybercriminalité en hausse exponentielle. De plus, la multiplication des supports mobiles ainsi que l'émergence de l'infonuagique posent de nouveaux défis».

Considérant qu'une proportion importante des étudiants de ces programmes ne possèdent pas de diplôme universitaire de premier cycle, et considérant le manque de main-d'œuvre dans ces domaines, «il apparaît essentiel que le diplôme de baccalauréat qui pourrait être décerné par cumul de certificats présente une dénomination spécifique [du] domaine d'études et de pratique, dans une perspective de valeur ajoutée, tant pour la formation que pour l'employabilité et la reconnaissance des entreprises qui emploient ces diplômés», fait valoir Polytechnique Montréal.

Le nouveau programme devrait voir le jour l'automne prochain.

(MATHIEU-ROBERT SAUVÉ)

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

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

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Source : *Un baccalauréat en cybersécurité à Polytechnique Montréal | UdeMNouvelles*

Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée</p>
--	--

La Commission (Cnil) a publié, il y a peu, sa méthode pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits afin de mener des PIA (Privacy Impact Assessment).

Dans un communiqué du 2 juillet 2015, la Commission nationale de l'informatique et des libertés (Cnil) a publiée une méthode pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits afin de mener des PIA (Privacy Impact Assessment).

Cette méthode qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la Cnil.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

- les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés, et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :

- étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
- étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

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

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lemondedudroit.fr/droit-a-entreprises/technologies-de-linformation/208258-cnil-methode-pour-la-mise-en-conformite-et-la-prise-en-compte-de-la-vie-privee.html>

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



Votre responsabilité engagée en cas de piratage de vos données

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

Imaginez que vous disposez de différents appareils numériques 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 (Méchanticiel 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'intermédiaire de votre retenue.

Par contre, si vous êtes professionnel, en plus d'être victime du piratage (l'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 et notamment la sécurité des données selon les termes de son Article n°34 :

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'amende 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 Cochamboralds voit son système informatique piraté. Des investigations sont menées et le pirate information arrêté. Vis à vis de la loi Godfrain du 5 janvier 1988, le voqué risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochamboralds 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 voiteur.

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, boîtes e-mail.

Autre cas concret :

Monsieur Roudoulot-Mavilout 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, référer vous au cas contrôles 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 et de la Formation Professionnelle n°92 84 03042 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.teneteexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI



Denis JACOPINI est un expert informatique ayant bénéficié d'un accompagnement de sa part dans les domaines suivants :

- Expertise technique (virus, spyware, arachides, fraude, piratage, brevet, brevet des idées, contrefaçon, démontage, déprogrammation, dématriculation, etc.)
- Expertise de systèmes de vote électronique ;
- Formation et conférences en cybersécurité ;
- Formation de l'Etat (Conseiller Informatique et Cybersécurité)
- Accompagnement à la mise en conformité RGPD

Le Net Expert
INFORMATIQUE | CYBERSECURITE

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

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>

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

Vous souhaitez bénéficier un billet pour le RGPD (envisagez un peu plus de détails) et vous souhaitez nous faire part d'un projet. Nous vous remercions pour votre confiance.

Intervenant sur des sujets RGPD depuis 2012, après avoir identifié différents types d'attentes, nous avons adapté nos offres pour se rapprocher au mieux à vos besoins.

2. **Recherchez l'assentiment ?**

Le RGPD (Règlement Général sur la Protection des Données à Caractère Personnel) et la nécessité pour comprendre et démontrer une mise en conformité. Une fois la formation achevée, vous êtes autorisés mais pourrez toujours compter sur notre soutien soit sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisé ;

L'issue de cette formation, nous vous remettons une attestation prouvant la protection des données à caractère personnel et la nécessité pour comprendre et démontrer une mise en conformité. Pour information, nous sommes référencés auprès de la CNIL.

Nous réalisons pour vous l'audit qui mettra en œuvre 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 modifications que vous aurez validées.

3. **Une formation pour la mise en conformité ?**

Une formation pour la mise en conformité, nous pouvons vous proposer une formation théorique et éventuellement avec votre service juridique, nous pouvons nous charger de la totalité de la 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 audit, vous pourrez compter sur notre expertise à la fois technique et pédagogique pour votre établissement qui accompagne de manière extraterritoriale.

4. **Un audit au sein de votre établissement ?**

Après une présentation pour comprendre les enjeux de votre établissement, conformité, votre stratégie et à vos priorités, nous souhaitons que nous devions à nos auditeurs :

Notre offre garantit une confidentialité extrême sur des informations communiquées; les personnes interrogées à les consulter sont soumises au secret professionnel.

Entre France / Non (obligatoire)

Secteur / Organisation

Votre adresse de messagerie (obligatoire)

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

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

Informations

Vous pouvez nous écrire directement un message dans la zone « INFORMATIONS COMPLÉMENTAIRES QUE VOUS AVEZ À VOUS » . Néanmoins, si vous souhaitez que nous établissons un chiffrement précis, nous aurons besoin dans un premier temps des informations ci-dessous.

POUR VOTRE MISE EN CONFORMITÉ RGPD

1. **Concernant l'audit :** Quelles sont les étapes pour réussir la mise en conformité pour comprendre et démontrer la mise en conformité ? (remplissez)

2. **Concernant l'audit :** Il convient à réaliser les éléments permettant de constituer un état des lieux précis puis à réaliser l'analyse réglementaire du contexte de départ.

3. **Concernant l'audit :** Notre conseil est de réaliser les éléments permettant de constituer un état des lieux précis puis à réaliser l'analyse réglementaire du contexte de départ.

4. **Concernant la mise en conformité :** Notre conseil est de réaliser la mise en conformité avec le temps par une mise à jour précise du registre des traitements...
5. **Concernant la mise en conformité :** Cette phase consiste à assurer la mise en conformité avec le temps par une mise à jour précise du registre des traitements...
6. **Notre conseil est de réaliser la mise en conformité avec le temps par une mise à jour précise du registre des traitements... (saisissez une réponse)**

INFORMATIONS COMPLÉMENTAIRES QUE VOUS AVEZ À VOUS

Un E-mail : envoyez un e-mail à rgpd@la-redevanceexpert.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 Information Assurante et **sécurité en RGPD - Protection des données à caractère Personnel et en cybersécurité**. Consultant depuis 1990 et formateur 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 (CL : Correspondant Informatique et Liberté) puis récemment dédié à la Protection des Données (RGPD n°1398/2016), en tant que praticien de la mise en conformité en Formation, 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



Denis JACOPINI
EXPERT INFORMATIQUE ALIMENTÉE SPÉCIALE EN CYBERSÉCURITÉ
LCI
vous informe

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 sécurité 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]

LE NET EXPERT

:

- FORMATIONS / SENSIBILISATION (utilisateurs / chefs d'entreprises / DSI) :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
 - MISE EN CONFORMITÉ RGPD / CNIL
 - ÉTAT DES LIEUX RGPD de vos traitements)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
 - EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est 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).

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** (sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Experts techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, décomptes de clientèle... ;
- **Expertises de systèmes de vote électronique** ;

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 installations 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 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.



DÉSIGNATION
N° DPO-15945



Data**dock**
Organisme **validé**
et référencé

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

Contactez-nous

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

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

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



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



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

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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