Comment se comporte notre cerveau surchargé par le numérique

Comment se comporte notre cerveau surchargé par le numérique

Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées : « HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être. Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression… : si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52′), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours !

si vous ne voyez pas la vidéo, le lien

Réagissez à cet article

Original de l’article mis en page : Hyperconnectés : le cerveau en surcharge

---

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…)| Denis JACOPINI

	Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…)	Denis JACOPINI

Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que *« ilfaitbeaudanstoutelafrancesaufdanslebassinparisien »* serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que *« p8)J#&=89pE »*, très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme *« Sur le pont d'Avignon, on y danse on y danse… »*.

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : *« jevaispromenermonchienTITIdansle93 ».*

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. **Dès lors, plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui vérouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien vérrouiller son ordinateur, etc…

Article original de Denis JACOPINI et Atlantico

Réagissez à cet article

Original de l'article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Atlantico.fr

L’entreprise victime ou coupable de Cyberattaques ? | Le Net Expert Informatique

L’entreprise victime ou coupable de Cyberattaques ?

LES FAITS En avril 2015, TV5 Monde a été la cible d'une cyberattaque massive entraînant la paralysie de la chaîne, du site Internet et des réseaux sociaux de la société. Si les attaques informatiques visant les grands groupes sont médiatisées, Symantec soulignait dans son rapport annuel 2014 que 77 % d'entre elles concernaient en France les PME.
Ces failles informatiques d'origines internes ou externes doivent être appréhendées car elles s'accompagnent de sévères répercussions en termes de sécurité, de pertes économiques et de dégradation de l'image de l'entreprise. Or, la majorité d'entre elles ignorent qu'elles sont tenues, en application de l'article 34 de la Loi Informatique et Libertés, d'une obligation de moyen de mettre en œuvre les mesures conformes aux règles de l'art pour protéger leur système d'information. Au-delà du risque civil, des sanctions administratives et même pénales peuvent être prononcées allant jusqu'à 5 ans de prison et 300 000 € d'amende. Ainsi, de victime, l'entreprise qui n'aurait pas pris toutes les « précautions utiles » pour préserver « la sécurité des données » peut, indépendamment de son dommage, se voir reconnaître responsable, comme Orange qui a été sanctionnée par la CNIL à la suite d'une faille de sécurité concernant les données de près de 1,3 million de ses clients en août 2014.

LA PRÉVENTION POUR LIMITER LES RISQUES
La mise en place d'une #politique de cybersécurité adaptée aux besoins de l'entreprise comportant des mesures techniques de sécurité informatique ainsi qu'une #politique de gestion des incidents, dont la mise en œuvre est préconisée par la #norme ISO 27035, est indispensable. Il convient également de concevoir la sécurité des données dans les relations avec les prestataires, en insérant des clauses spécifiques dans les contrats qui les lient précisant clairement le partage de responsabilité entre les deux parties. Dans ce cadre, un état des lieux du patrimoine informationnel détenu par l'entreprise s'impose afin d'assurer aux données sensibles la sécurité adéquate, ainsi que la réalisation d'#audits techniques et de #correctifs réguliers du système d'information (typologie et quantité de données, protections, vulnérabilités, etc.).
Par ailleurs, une communication en interne sensibilisant les salariés sur ces risques est essentielle. Le recours à une #charte informatique précise annexée au règlement intérieur de l'entreprise fixant les droits, devoirs et obligations des salariés est un outil efficace. À cet égard, l'ANSSI vient de publier, en coopération avec la CGPME, un #guide de recommandation de bonnes pratiques simples qu'il convient de mettre en œuvre. Au-delà de ces mesures de prévention, il est conseillé de bien soigner les contrats d'assurance afin d'anticiper sur ces causes de pertes d'exploitation. Enfin, rappelons que depuis l'ordonnance du 24 août 2011, les opérateurs de communications électroniques sont tenus à une obligation de notification de la faille de sécurité, sans délai, à la CNIL et aux personnes concernées, prévue par l'article 34 bis de la Loi Informatique et Libertés, dont le défaut est sanctionné pénalement. À noter que le projet de réforme de règlement européen prévoit d'étendre cette obligation à toutes les entreprises, comme c'est le cas aux États-Unis.

CE QU'IL FAUT RETENIR
Le cyber-risque constitue une menace réelle que les entreprises doivent appréhender et anticiper pour ne pas voir, à titre de double peine, leur responsabilité engagée.

Source : http://www.itforbusiness.fr/services/juridique/item/6693-cyberattaques-l-entreprise-victime-ou-coupable

Comment les salariés peuvent lutter contre la cybercriminalité | Denis JACOPINI

	Comment les salariés peuvent lutter contre la cybercriminalité

Les entreprises -quels 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 Devive) 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 un 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 barrages 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 posés 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 ne 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 sécuritaires 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 en miroir, 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 plait ? 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 établisement en conformité avec la CNIL, mode d'emploi | Denis JACOPINI

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

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

Cependant, les préoccupation 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 plait ? 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 ?

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 sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

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)

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

Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée

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 publée 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.

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 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

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