Qui est responsable de la cybersécurité : le RSSI, le DSI, le PDG ou vous ? | Le Net Expert Informatique

La menace informatique est changeante et les décideurs IT peinent à s'adapter à un danger croissant. La cybermenace, certes significative, ne constitue qu'un élément de la sécurité de l'entreprise. Dès lors, qui devrait être responsable de la sécurité et comment les entreprises peuvent adopter une approche plus proactive face aux menaces ? Cinq experts IT donnent leur avis.

1. Faites de la sécurité la responsabilité de tous les salariés

« Le directeur général, et n'importe qui d'autre » répond David Allison à la question de savoir qui est responsable de la sécurité au sein de l'entreprise. Le responsable des systèmes métier pour Aggregate Industries estime que le PDG devrait être responsable de la sécurité, mais que chaque salarié a une responsabilité personnelle.

« La sécurité, ce n'est pas le confinement et la prévention » juge Allison, même si les pare-feu, les antivirus et les autres mesures IT doivent être considérés comme acquis. « Une grande sécurité, c'est affaire d'éducation, de sensibilisation et de responsabilité individuelle. »

Pour lui, le dirigeant de l'entreprise doit s'engager personnellement pour disposer d'une équipe en place formant le personnel dans un large éventail de domaines comme la gestion des courriels, la détection des liens suspects et l'adoption de bonnes pratiques pour les mots de passe.

« La sécurité a besoin d'être une culture diffusée au sein de l'organisation » souligne David Allison. « Le PDG met en place cette culture. Le responsable de la sécurité informatique (RSSI) définit et exécute la stratégie répondant à ce besoin – et chaque salarié est responsable de s'assurer d'adopter et de suivre les pratiques requises. »

2. Ne vous reposez pas sur des produits technologiques

Tim Holman, le président de l'ISSA, une association britannique de sécurité des SI, estime que la responsabilité au sein d'une entreprise se situe toujours au niveau des propriétaires ou des comités de direction. Certains Comex peuvent désigner un DSI, RSSI ou un directeur IT comme le responsable de la sécurité, mais ces individus ne peuvent jamais être tenus pour responsables.

« Les entreprises doivent avoir conscience de l'ampleur de la menace lorsqu'elles font du commerce sur Internet ou stockent leurs données sur le Cloud » déclare Holman. « Les entreprises peuvent charger un DSI d'implémenter une solution Cloud, mais elles resteront toujours responsables si quelque chose tourne mal. »

Face aux cybermenaces, les firmes doivent adopter une attitude proactive, et elles peuvent le faire au travers d'une simple analyse de risques, ou en suivant des standards comme IASME ou Cyber Essentials. D'après Tim Holman, la compréhension des enjeux liés à la sécurité progresse en consacrant du temps avec des dirigeants et en leur expliquant en termes simples les risques inhérents au business en ligne.

« La cybermenace ne peut pas être résolue en achetant des produits. Une approche de bon sens consistant à réduire le volume de données sensibles stockées, à éjecter les fournisseurs non-sécurisés, à restreindre l'accès aux données et à souscrire une cyber-couverture sera souvent dix fois plus efficace et dix fois moins chère que la dernière génération d'appliance de sécurité vendue par les experts de la vente. »

3- Gardez sous contrôle les périls des terminaux mobiles

David Reed, directeur des services d'information et de l'infrastructure à la Press Association (PA), juge complexe la discussion autour de la sécurité, mais est d'avis que la responsabilité commence au sommet de l'IT. « Si en tant que DSI, vous n'êtes pas en mesure de percevoir les dangers liés à la sécurité, vous ne faites pas un assez bon travail » tranche-t-il.

Un des domaines les plus importants pour Press Association est ainsi la gestion du mobile. Les journalistes de la société ont à traiter des informations extrêmement sensibles, et la menace de piratage d'un terminal, bien que sérieuse, n'est pas aussi répandue qu'une simple perte ou un vol. PA travaille avec EE pour implémenter une stratégie mobile COPE (un terminal de l'entreprise pour un usage personnel et professionnel) utilisant des Samsung S4 Mini et le système de sécurité Knox.

« Un conteneur peut être créé sur chacun des téléphones pour stocker séparément documents de travail, courriels et contacts et éléments personnels. Nos journalistes disposent principalement de deux zones sur leurs téléphones : une pour l'usage personnel et l'autre pour le travail » précise David Reed.

« Chez PA, nous aidons les journalistes en recommandant des apps. Nous avons appliqué ce principe pour les jeux du Commonwealth de 2014 en envoyant aux journalistes présents sur l'évènement un message pour télécharger l'app Team GB. L'appli était en liste blanche et installée simplement dans le conteneur. »

4- Obtenez le soutien du dirigeant pour les démarches de gouvernance

Pour Omid Shiraji, ex-DSI de Working Links, la responsabilité de la sécurité est totalement liée à l'entreprise et à la nature de ses activités. Il n'est pas persuadé de la nécessité de disposer d'un RSSI dans la majorité des organisations.

« La sécurité IT est une commodité. Vous pouvez acheter des produits et de l'expertise auprès d'un fournisseur » juge-t-il. « La même chose est vraie en ce qui concerne la sécurité des entreprises dans de nombreux cas – les processus et la gouvernance sont une marchandise que vous pouvez acheter comme un service géré. »

Omid Shiraji préférerait consacrer son budget IT limité aux opérations en première ligne, et ensuite s'appuyer sur une expertise spécifique pour l'aider à protéger ses données et guider son personnel. La société a récemment été certifiée ISO 27001 et le support du PDG s'est révélé essentiel.

« Les individus changent leur comportement car ils entendent le PDG parler des conséquences majeures des activités non protégées » déclare-t-il. « La sécurité IT est en fait le travail de chaque employé, mais le patron doit soutenir chaque initiative en matière de sécurité et de gouvernance dans l'entreprise. Et c'est ce qui s'est passé chez Working Links. »

5. Créez une culture du risque pragmatique

Julian Self, un DSI expérimenté qui a travaillé pour de nombreux acteurs de la finance, fait lui une analyse différente et estime que l'importance du RSSI dans l'entreprise continue de grandir. Selon lui, il est du ressort du DSI de promouvoir auprès des dirigeants les avantages d'un spécialiste de la sécurité.

« Dans un monde déjà hyper-connecté, et avec l'avènement de l'Internet des Objets, le travail de sécurisation des données de l'entreprise devient infiniment plus complexe avec des flux de données qui entrent et sortent de nombreux terminaux » commente Julian Self, pour qui le panorama de la menace continue d'évoluer.

« Les RSSI ne réussiront pas à moins d'avoir l'adhésion et l'engagement des métiers. Sans cela, ils seront simplement perçus comme des freins à l'activité et leurs efforts seront contournés. »

« Fondamentalement, les RSSI ont besoin de créer une prise de conscience et une culture pragmatique du risque afin que la sécurité de l'information soit appliquée de façon inconsciente dans tous les domaines de l'entreprise. Cette approche doit aller de pair avec une réponse à incidents qui soit proportionnée et sans alarmisme, et la gestion et la réaction au risque, restaurant in fine la confiance de l'entreprise. »

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

Source : http://www.zdnet.fr/actualites/qui-est-responsable-de-la-cybersecurite-le-rssi-le-dsi-le-pdg-ou-vous-39826198.htm

---

Comment réagir face à une cyberattaque | Le Net Expert Informatique

Comment réagir face à une cyberattaque

Choc, sidération, déni… Une attaque informatique paralyse souvent les entreprises qui en sont victimes. L'idéal est donc de s'y préparer pour avoir les bons réflexes le moment venu. « Au début, une cyberattaque ne fait pas de bruit. L'entreprise continue apparemment à fonctionner normalement. Les cellules de crise classiques ont donc du mal à se mobiliser. Il faut s'adapter en prenant en compte la dimension cyber de l'attaque », remarque Gérôme Billois, expert en cybersécurité chez Solucom.

1 MONTER UNE CELLULE DE CRISE CYBER

La cellule de crise décisionnelle (direction générale, service juridique, RH, informatique, communication…) doit être secondée par une cellule de crise cyber. Idéalement, cette équipe est pilotée par le responsable sécurité des systèmes d'information (RSSI). Elle regroupe des membres de la direction informatique et les responsables des applications informatiques liées aux métiers de l'entreprise. Tous ces protagonistes doivent être sensibilisés à travers des exercices spécifiques, organisés annuellement.

« Suivant le scénario d'attaque, cela peut prendre la forme d'un exercice sur table de quelques heures à la simulation d'un début de crise », explique Gérôme Billois. Tout le monde doit être sur le pont. Les managers pour identifier les ressources à protéger, les RH pour répondre aux interrogations des collaborateurs, le service juridique pour évaluer les suites judiciaires, la communication si l'information de l'attaque a fuité…

2 DÉCONNECTER LES MACHINES INFECTÉES

Dès les premiers soupçons d'attaque, il faut réagir. Un grand industriel européen s'est mordu les doigts de ne pas avoir pris au sérieux les alertes remontées en 2012 par les autorités nationales. Résultat : le pirate a eu tout le loisir de sonder en profondeur son réseau informatique. « La crainte est qu'il ait eu accès au code source de nos outils informatiques qui permettent de gérer les infrastructures de nos clients », confie cet industriel. Il ne faut toutefois pas confondre vitesse et précipitation, prévient Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces au ministère de l'Intérieur. Les entreprises sont entre deux feux. D'une part, elles doivent isoler leur système de l'extérieur pour éviter la propagation de l'attaque. D'autre part, il faut éviter d'en effacer les traces. « Si on coupe et on efface les disques durs, les enquêteurs perdent les preuves et la possibilité de remonter aux auteurs de l'attaque », souligne le préfet.

La déconnexion peut être utile. Victime, en avril dernier, d'une attaque sévère qui a interrompu ses programmes, la chaîne de télévision TV5 Monde a agi ainsi pour limiter la casse. « Par chance, les équipes informatiques étaient présentes le soir de l'attaque. Elles ont pu déconnecter les machines infectées. Cela été salutaire. Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), l'objectif était de détruire notre société », précise Yves Bigot, le directeur général de la chaîne.

L'urgence passée, il faut rapidement faire appel à des professionnels expérimentés dans la neutralisation des attaques informatiques. L'Anssi dispose sur son site internet d'une liste de prestataires disposant du label CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques). Certains s'engagent à intervenir en moins de quatre heures.

3 PORTER PLAINTE ET ESTIMER LES PRÉJUDICES

« Les entreprises hésitent à porter plainte, car elles craignent que cela nuise à leur réputation. Or, sans cela, on ne peut traiter policièrement et judiciairement une affaire », déplore le « préfet cyber ». Il faut donc déposer plainte au commissariat ou à la brigade de gendarmerie locale. Certains disposent d'un investigateur en cybercriminalité qui fournira les conseils d'urgence. La seconde étape est de se rapprocher d'interlocuteurs techniques qui pourront apporter leur expertise.

Les entreprises en région parisienne doivent solliciter la Befti, la brigade d'enquête sur les fraudes aux technologies de l'information. Cette unité spécialisée conseille les entreprises victimes d'intrusion informatique ou de détournement de fonds… Les entreprises en province auront accès à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Il faut venir avec le maximum d'éléments qui vont aider les enquêteurs : le journal des connexions, la configuration des machines, les disques durs des machines infectées… « Il faut aussi estimer les préjudices subis sur la base d'éléments concrets. Cela permettra de présenter un dossier solide auprès du procureur de la République. C'est sur ce dossier qu'il décidera des suites à donner à l'enquête », explique le colonel Freyssinet, spécialisé dans la lutte contre les cybermenaces au ministère de l'Intérieur.

4 RECONSTRUIRE LA SÉCURITÉ INFORMATIQUE

Il faut agir sur les conséquences de l'attaque. Le grand industriel européen qui craignait qu'un pirate ait eu accès au code source de son outil de gestion à distance des infrastructures de ses clients n'a pas tergiversé. « Le code du produit a été totalement revu afin d'éviter la création d'un backdoor [une porte dérobée, ndlr] exploitable par les pirates. Nous avons également informé nos clients de l'attaque subie », confie-t-il. Après son attaque, TV5 Monde a remis à plat sa sécurité informatique. Elle a remplacé le matériel technique compromis et déployé des nouveaux équipements de sécurité.

Les 400 salariés suivent une formation pour apprendre les gestes de base dans ce domaine. La chaîne a imposé des mesures drastiques : suppression du Wi-Fi, interdiction de connecter des équipements électroniques personnels (tablette, smartphone…) aux ordinateurs de bureau, passage des clés USB au sas de décontamination… Soit, au total, une facture de 5 millions d'euros.

Pour soigner les machines infectées, l'Anssi préconise de réinstaller entièrement le système d'exploitation et d'appliquer tous les correctifs de sécurité avant de la reconnecter. Elle recommande de modifier les mots de passe de tous les comptes de l'entreprise sous peine de revoir débarquer le pirate informatique. L'agence incite également les entreprises victimes à communiquer avec leurs pairs. « Généralement, les pirates s'attaquent à plusieurs entreprises d'un même secteur, en réutilisant les mêmes techniques. En partageant son expérience, on renforce la sécurité collective », explique Guillaume Poupard, le directeur général de l'Anssi.

La messagerie sous écoute

Dans la panique, les membres de la cellule de crise communiquent par e-mails et s'échangent des fichiers via le réseau de l'entreprise. Grave erreur. Il y a de grandes chances pour que ces systèmes soient compromis et sous écoute. Le conseil pour communiquer en toute discrétion : ouvrir temporairement des comptes de messagerie à partir de services web. Les échanges informatiques doivent également se faire par l'intermédiaire d'un réseau de secours indépendant de celui de l'entreprise afin de garantir leur confidentialité.

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

Source : http://www.usine-digitale.fr/article/comment-reagir-a-une-cyberattaque.N354821
Par HASSAN MEDDAH

La progression impressionnante de la cybercriminalité | Le Net Expert Informatique

La progression impressionnante de la cybercriminalité

En 10 ans, le nombre d'attaques a explosé. De la simple intrusion au sabotage, les criminels exploitent toutes les failles des systèmes d'information.

Le chiffre impressionne. En effet si l'on en croit Eugène Kasperky – fondateur et PDG de la société éponyme spécialisée dans la sécurité des systèmes d'information – il y aurait eu en 2014, 237 millions d'attaques informatiques, contre 500 000 en 2004.
Cette vertigineuse croissance d'actes de malveillances tient bien sur à l'extension d'Internet dans le monde, qui compte désormais plus de 3 milliards d'utilisateurs. Cette progression provient également de la professionnalisation des pirates. De simples hackers, il y a encore une dizaine d'années, certains sont aujourd'hui des ingénieurs pointus recrutés par des Etats ou par des mafias qui ont fait du cyber-espace leur nouveau terrain d'action.

Windows et Android parmi les systèmes les plus piratés

Eugène Kaspersky met enfin en avant la faiblesse de la sécurisation des systèmes technologiques: « un ordinateur sur 20 doté d'un système Microsoft est infecté et les attaques sur les mobiles équipés du système Android se sont multipliées depuis 2011, notamment lorsqu'ont été lancés des services bancaires sur smartphone ». Le système d'Apple limite lui les dégâts: « il y a moins d'ingénieurs dans le monde pour concevoir des logiciels pour les machines Apple. Les pirates doivent avoir les mêmes problèmes de recrutement que nous » souligne, amer, le PDG russe qui distingue trois grands types de menaces informatiques: « la cybercriminalité qui veut récupérer de l'argent ; le cyber-espionnage qui s'intéresse aux données et enfin le cyber-sabotage qui cherche à tuer ».

Poursuivre les efforts de sensibilisation et de formation du public et des salariés

Des dangers qui ne vont que s'accroitre avec la multiplication des objets connectés et le développement des « smart » (Cities, building, voitures…). « Ce qui est particulièrement à redouter c'est le cyber-espionnage qui va s'attaquer aux infrastructures publiques comme les transports, les réseaux d'eau, d'électricité ».
Face à ce tableau noir, pas de miracle. Les entreprises, les Etats, les individus doivent être vigilants: « il faut être prêt pour la prochaine génération d'attaques. Il faut poursuivre les efforts de sensibilisation et de formation ». Dont acte…

Source :
http://bfmbusiness.bfmtv.com/entreprise/la-progression-impressionnante-de-la-cybercriminalite-919455.html
Par Florence Puybareau

Invalidation du « Safe Harbor » : quels sont les changements auxquels on doit s’attendre ? | Le Net Expert Informatique

La justice européenne a invalidé, mardi 6 octobre, l'accord « Safe Harbor » qui encadrait le transfert de données personnelles de l'Union européenne vers les Etats-Unis.

En quoi consiste Safe Harbor et que dit la Cour de justice de l'Union européenne (CJUE) ?
En Français « sphère de sécurité », le « Safe Harbor » est une décision de la Commission européenne, datant de 2000, qui affirme que le transfert de données personnelles d'Europe vers les Etats-Unis est possible car ce pays présente des garanties suffisantes pour la protection de la vie privée.
Très controversé, cet accord a notamment été mis à mal par les révélations d'Edward Snowden, en 2013, sur les programmes de surveillance de masse de la NSA. Les adversaires du Safe Harbor, dont Max Schrems, un Autrichien qui a déposé plusieurs plaintes contre Facebook, estimaient que ces révélations montraient que les données personnelles des Européens n'étaient en fait pas protégées lorsqu'elles étaient stockées aux Etats-Unis.
Dans son arrêt rendu mardi, la CJUE estime que le Safe Harbor n'est pas conforme au droit européen, pour plusieurs raisons détaillées sur une trentaine de pages. La Cour a notamment estimé que les recours possibles pour les citoyens européens estimant leurs droits malmenés étaient beaucoup trop faibles. Elle juge également que les programmes de surveillance de masse des Etats-Unis sont incompatibles avec une protection adéquate des droits des citoyens européens.

Cela veut-il dire que Facebook ne peut plus fonctionner en Europe, ou va devoir stocker les données des citoyens européens en Europe ?
Non : l'arrêt invalide un accord très générique. Facebook peut continuer à fonctionner comme il le faisait jusqu'à aujourd'hui, mais l'entreprise – tout comme Google ou tout autre entreprise qui stocke des données de citoyens européens aux Etats-Unis – ne peut plus s'abriter, en cas de procédure, derrière le fait qu'elle fait partie du Safe Harbor et que ses flux de données entre l'Europe et l'Amérique sont présumés légaux.
Facebook affirme en fait ne pas s'appuyer uniquement sur le Safe Harbor, mais « sur d'autres méthodes recommandées par l'Union européenne pour transférer légalement des données de l'Europe vers les Etats-Unis ».
Il existe en effet d'autres normes de transfert de données, comme par exemple les « clauses contractuelles type » ou les « règles internes d'entreprise » (dans le cas de transfert de données entre filiales), le Safe Harbor étant le cadre juridique simplifié et « par défaut ». Certaines entreprises du numérique utilisent déjà ces cadres juridiques alternatifs.
La Commission craint d'ailleurs que la décision de la CJUE ne favorise la multiplication de contrats spécifiques établis entre des entreprises et des pays européens, au détriment d'un cadre générique européen. Frans Timmermans, le vice-président de la Commission, a d'ailleurs annoncé que des « lignes directrices » à destination des autorités de protection des données seraient publiées afin d'éviter un « patchwork avec des décisions nationales ».
Par ailleurs, sans aller jusqu'à ces procédures juridiques, la loi européenne – plus spécifiquement l'article 26 de la directive de 1995 sur la protection des données personnelles – prévoit qu'un transfert vers un pays tiers peut être autorisé dans plusieurs cas. Par exemple, pour assurer la bonne exécution du contrat commercial (dans le cas d'une réservation d'hôtel par exemple, où les coordonnées du client sont nécessaires) ou lorsque intervient le consentement explicite de l'internaute à ce que ses données soient transférées.

Le Safe Harbor va-t-il être renégocié ?
La renégociation de cet accord était déjà en cours avant l'arrêt de la Cour. Malgré l'expiration de plusieurs dates butoirs, les négociateurs ont récemment affirmé qu'ils faisaient des progrès dans les discussions. Mais il sera difficile d'obtenir rapidement un accord qui puisse satisfaire les exigences de la CJUE : cette dernière rappelle dans son arrêt que, pour obtenir un régime de ce type, un pays doit faire la preuve qu'il offre des garanties de protection de la vie privée comparables à celles en vigueur au sein de l'UE.
Cela signifie qu'il faudrait des changements majeurs dans le droit américain pour qu'un nouvel accord ne soit pas, à son tour, invalidé par la Cour.

Que se passe-t-il dans l'immédiat ?
Plus de 4 000 entreprises étaient soumises à l'accord Safe Harbor. Nombre d'entre elles, particulièrement les plus petites, se retrouvent brusquement, au moins jusqu'à l'adoption d'un nouvel accord Safe Harbor, dans un vide juridique.
Les grands acteurs du Web, eux, sont dans l'attente. L'annulation du Safe Harbor semble les avoir pris de court. Dans un communiqué, l'association professionnelle Digital Europe, qui regroupe tous les grands acteurs du secteur (d'Apple à Toshiba en passant par Google, à l'exception de Facebook), « demande de toute urgence à la Commission européenne et au gouvernement américain de conclure leurs négociations pour parvenir à un nouvel accord "Safe Harbor" aussi vite que possible ».
« Nous demandons également à la Commission européenne d'expliquer immédiatement aux entreprises qui fonctionnaient sous le régime du Safe Harbor comment elles doivent opérer pour maintenir leurs activités essentielles durant ce vide juridique », poursuit l'association.
Facebook a, de son côté, estimé également qu'il « fallait impérativement que les gouvernements européens et américain donnent des méthodes légales pour le transfert des données et règlent toutes les questions de sécurité nationale ».

Quelles seront les conséquences plus larges de cette décision ?
Si l'arrêt de la CJUE ne porte que sur le Safe Harbor, il dénonce avec des mots très durs les programmes de surveillance de masse de la NSA américaine, présentés comme incompatibles avec les droits fondamentaux garantis par le droit européen.
Le jugement pourrait aussi influencer deux dossiers européens brûlants dont les négociations arrivent dans leur dernière ligne droite : l'accord « parapluie » sur l'échange de données personnelles pour la coopération policière, entre Europe et Etats-Unis, et le projet de règlement sur les données personnelles.
La commissaire européenne à la justice, Vera Jourova, a indiqué que l'arrêt de la Cour confortait la position de la Commission, notamment sur la nécessité d'avoir « des garde-fous solides » en matière de protection des données.
Washington s'est dit « déçu » par la décision de la justice européenne, estimant qu'elle créait une « incertitude pour les entreprises et les consommateurs à la fois américains et européens et met en péril l'économie numérique transatlantique qui est en plein essor ».

Source : http://www.lemonde.fr/pixels/article/2015/10/06/safe-harbor-que-change-l-arret-de-la-justice-europeenne-sur-les-donnees-personnelles_4783686_4408996.html

Réponse sur incidents et bonnes pratiques | Le Net Expert Informatique

	Réponse sur incidents et bonnes pratiques

Les 2/3 des cyberattaques mettent plusieurs mois à être détectées et près de 70% le seraient par des tiers ! Aujourd'hui c'est un fait, plus personne n'est à l'abri d'une cyberattaque, il est donc indispensable de se mettre en ordre de marche pour être prêt à réagir en cas d'attaque. La mise en place d'une politique de réponse sur incident de sécurité permet, en effet, de détecter la cyberattaque le plus tôt possible, de réagir très rapidement pour la contrer et de réduire ainsi au maximum les impacts d'image et business. Econocom nous livre son expertise en la matière, aux côtés de Maître Garance Mathias, à l'occasion de la 15ème édition des Assises de la Sécurité.

En 2014, 81% des entreprises ont déjà fait l'objet d'une cyberattaque, constate Marc Cierpisz, Directeur de l'offre Cybersécurité chez Econocom. 66% de ces attaques ont été découvertes après plusieurs mois, et 69% d'entre elles ont été découvertes par des tiers. Il observe, de plus, une difficulté à arrêter ce type d'attaque ; une incertitude plane quant aux délais de détection et de traitement de ce type d'incident.
La réponse sur incident est à la fois un défi technique, organisationnel et juridique pour les entreprises. L'enjeu est aussi de savoir s'adapter aux circonstances particulières.
Concernant les mesures techniques, il s'avère que la sécurité périmétrique reste inadaptée ou inefficace, car le SI est aujourd'hui de plus en plus diffus. La mise en place de firewalls n'a, par exemple, pas empêché TV5 Monde de se faire pirater. Il existe une grande diversité à l'heure actuelle des moyens de réaction : audits (test d'intrusion, tableaux de bord…), détection (SIEM, SOC, CERT, veille…). Toutefois, on constate beaucoup de manquements à ce niveau-là, à la fois en termes de budgets et de ressources adéquates, même si les enjeux de sécurité sont de mieux en mieux compris.
Au niveau juridique, le droit n'a pas encore clairement défini de manière intrinsèque la notion d'incident de sécurité, contrairement aux fuites de données, explique Me Garance Mathias. L'approche devra donc passer par une définition précise des incidents de sécurité et des responsabilités avec les différents prestataires.
Un cadre réglementaire existe néanmoins, avec la Loi Informatique et Libertés notamment mais pas seulement. Le projet de règlement européen relatif à la protection des données personnelles, le règlement eIdas, ou encore les différentes réglementations sectorielles, viennent compléter et complexifier les obligations relatives à la protection de l'information et au traitement des incidents. Le projet européen concernant la protection des données à caractère personnel va venir imposer l'obligation de déclaration pour le CIL des incidents de sécurité, ce qui changera la donne surtout dans un pays où la fuite de données se fait soi-disant plus « rare » qu'ailleurs. Le bénéfice d'être assuré sera certainement demain de plus en plus prégnant.

Les réponses juridiques diffèrent sur le plan civil et pénal, et les sanctions aussi. Le risque est bien réel pour les entreprises, en termes de dommages et intérêts bien sûr, d'atteinte à l'image et à la réputation également. Les illustrations jurisprudentielles varient, quant à elles, selon le fait que l'entreprise ait effectué ou non préalablement des audits de sécurité par exemple… La question est de savoir comment démontrer s'il y a eu un défaut de sécurisation ou non. Les incidents de sécurité ont mis globalement en avant un manque de sécurisation des systèmes d'information, qu'il faudra donc renforcer si les entreprises ne veulent pas être sanctionnées.

Parmi les mesures à mettre en place en entreprise pouvant réduire ces incidents de sécurité, elle cite entre autres :
– La politique interne à l'entreprise : la charte informatique est essentielle, mais combien la font signer aux employés… pourtant celle-ci permettrait de responsabiliser les utilisateurs ; la politique de sécurité en elle-même ; la politique contractuelle avec les prestataires, les sous-traitants… ; ou encore la sensibilisation des différentes acteurs ;
– Ensuite, des mesures de sécurité spécifiques doivent venir renforcer cette politique interne selon l'activité de l'entreprise : OIV, secteur médical, assurance, banque…

La cadre juridique est donc là, mais il est aussi à venir. On connaît déjà les textes, donc on n'est pas dans l'incertitude, que ce soit dans le secteur de la santé, ou dans le domaine de la protection des données à caractère personnel, conclut-elle.

La réponse n'est pas que technique ou juridique. Plusieurs défis se posent au niveau de l'organisation en matière de réponse à incident, reprend Marc Cierpisz :
– Identifier un incident de sécurité ;
– Etablir les objectifs de toute opération d'enquête et de nettoyage ;
– Analyser les informations relatives aux incidents ;
– Déterminer ce qui s'est réellement passé ;
– Identifier les réseaux et systèmes compromis ;
– Déterminer les informations divulguées à des tiers ;
– Etc.

Quelles démarches convient-il de mettre en place ? « Le bon stratège se prépare à tout, même au pire… »
– Concernant la partie renseignement sécuritaire, il convient en premier lieu d'évaluer la criticité de l'entreprise, d'analyser la menace sécuritaire du SI, les risques IT et métiers, d'examiner les implications des personnes, des processus, de créer un cadre de contrôle approprié, d'examiner l'état de préparation dans la réponse aux incidents de sécurité…
– Au niveau de la réponse sur incident, il faut déjà identifier les incidents de sécurité, définir les objectifs que l'on veut couvrir et les mesures à prendre quand on a qualifié les incidents de sécurité, récupérer les systèmes, les données et la connectivité…
– Le suivi post-intervention est également fondamental pour remettre en état l'entreprise : il s'agit ici d'enquêter sur l'incident de manière plus approfondie, de le signaler aux parties prenantes, d'effectuer un examen a posteriori, de réagir et de prendre les bonnes décisions, de communiquer et de s'appuyer sur les leçons apprises, de mettre à jour les informations clés, les contrôles et les processus, d'effectuer une analyse de tendance… L'objectif est que ça ne se reproduise pas.

Parmi les erreurs les plus fréquentes, les entreprises sous-estiment encore trop souvent les conséquences d'une attaque et les risques : « on traitera quand ça arrivera… » Pourtant 117 339 attaques seraient recensées chaque jour. On constate globalement une mauvaise estimation des risques, la destruction des preuves, une absence de plan de réponse à incident, de gestion de crise et de prise en compte de la réponse à incident dans les PCA, ou encore une mauvaise gestion de la e-réputation et de la communication. Pourtant, quand on subit un crash c'est violent, parfois même comme un accident de voiture.

Un certain nombre de bonnes pratiques doivent être mises en place au sein des organisations, comme la définition d'un plan de réponse à incident, la constitution d'une équipe dédiée, la définition d'un corpus documentaire, la préservation des preuves… Un plan de communication doit également être mis en œuvre. Il est essentiel d'identifier une autorité centrale en charge de cette communication, avec les médias par exemple. L'entreprise doit être impliquée en la matière, car « mieux elle va maitriser sa communication, mieux elle va gérer sa sortie de crise ». Enfin, en cas de gestion de crise, elle devra mettre en place une cellule de « war room », mais aussi gérer les relations avec les différents organismes et autorités concernés (CNIL, ANSSI…).

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

Source : http://www.globalsecuritymag.fr/Reponse-sur-incident-des-enjeux,20151001,56316.html

---

TOP 10 des méthodes de hacking les plus utilisées | Le Net Expert Informatique

TOP 10 des méthodes de hacking les plus utilisées

BalaBit présente en exclusivité lors de la 15è édition des Assises de la Sécurité, les résultats d'une étude menée auprès des participants de la Black Hat en août dernier, conférence de référence mondiale en matière de sécurité de l'information.

BalaBit a interrogé 349 professionnels de la sécurité afin de définir le top 10 des méthodes de hacking actuellement les plus populaires. Cette étude offre aux entreprises l'opportunité de mieux connaître leurs ennemis en identifiant les méthodes et les vulnérabilités les plus utilisées par les hackers lorsqu'il s'agit de s'attaquer à leurs données sensibles. Cette base de connaissance est la première étape fondamentale pour toute entreprise souhaitant mettre en place une stratégie de sécurité IT efficace, et cela quelque soit son secteur d'activité.

Attaquant interne ou externe ? Pas si évident…

Les menaces sont différentes et plus sophistiquées aujourd'hui et la frontière entre les menaces internes et externes est devenue très étroite. La majorité des attaquants externes tentent de pénétrer le réseau, d'acquérir des niveaux d'accès basiques et d'utiliser leurs droits pour petit à petit remonter jusqu'à des niveaux d'accès privilégiés. Dans la plupart des cas, ils restent invisibles dans le réseau pendant plusieurs mois, puisqu'ils parviennent à s'identifier comme des utilisateurs internes.

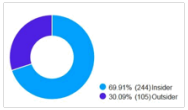
Qu'en est-il des utilisateurs internes malveillants ? : Sont-ils conscients des conséquences de leurs actes lorsqu'ils partagent leurs identifiants ou lorsqu'ils cliquent sur des liens de phishing – dans ce cas, la fuite de données est-elle le résultat d'actions intentionnelles ou accidentelles ? Doivent-ils être considérés comme malveillants seulement si leur action était intentionnelle ? Cela a t-il vraiment beaucoup d'importance si la fuite de données est très grave ?

70% des personnes interrogées considèrent les menaces internes comme les plus risquées

54% des personnes interrogées déclarent avoir très peur des hackers qui pénètrent au sein du réseau de l'entreprise via leur pare-feu, alors même que 40% d'entre elles déclarent qu'un pare-feu n'est pas assez efficace pour empêcher les hackers d'entrer.

Les participants ont également été interrogés sur les attaquants – internes ou externes – qu'ils considèrent les plus à risques :

> Les résultats soulignent un point important en vue de la définition d'une stratégie de défense efficace : 70% des personnes interrogées considèrent que les utilisateurs internes présentent le plus de risques (et seulement 30% estiment que les attaquants externes posent plus de risques).



Une chose est sûre : les attaquants externes cherchent à devenir des utilisateurs internes, et les utilisateurs internes les aident pour y parvenir – accidentellement ou intentionnellement.

Quelque soit la source de l'attaque, la liste des 10 méthodes de hacking les plus populaires -présentées ci-dessous – démontre qu'il est crucial pour les entreprises de savoir ce qu'il se passe sur leur réseau en temps réel. Qui accède à quoi ; est-ce le bon utilisateur derrière l'identifiant et le mot de passe ou est-ce un attaquant externe utilisant un compte compromis ?

Le top 10 des méthodes de hacking les plus utilisées :

1. Ingénierie sociale (ex : phishing).
2. Compromission de comptes (sur la base de mots de passe faibles par exemple).
3. Attaques web (ex : injection SQL/de commandes).
4. Attaques de clients de l'entreprise ciblée (ex: contre des destinataires de documents, navigateurs web).
5. Exploits avec des mises à jour de serveurs connus (ex: OpenSSL, Heartbleed).
6. Terminaux personnels non sécurisés (manque de politique de sécurité BYOD).
7. Intrusion physique.
8. Shadow IT (utilisation personnelle de services Cloud à des fins professionnelles).
9. Attaque d'une infrastructure outsourcée en ciblant un fournisseur de services externe.
10. Attaque de données hébergées sur le Cloud (via l'IaaS, le PaaS).

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

Source : http://www.programmez.com/actualites/balabit-presente-un-top-10-des-methodes-de-hacking-les-plus-utilisees-23280

La CNIL entend imposer un

droit à l’oubli bien au delà des frontières européennes | Le Net Expert Informatique

	La CNIL entend imposer un droit à l’oubli bien au delà des frontières européennes

La CNIL entend imposer un droit à l'oubli très large, bien au delà des frontières européennes. Va-t-elle avoir gain de cause?

La CNIL contre Google. David contre Goliath. A elle seule, l'affiche du duel suscite l'admiration. Il en faut du courage, une noble cause et des convictions bien trempées, pour croiser le fer avec un acteur mondial si puissant.
Le 21 septembre, Madame Isabelle Falque-Pierrotin, Présidente de la CNIL, a confirmé sa décision d'imposer à Google d'effacer, dans le monde entier, les résultats de recherche portant sur le nom d'une personne, lorsque ces résultats ne sont pas jugés nécessaires à l'information du public en France.
D'après le communiqué de la CNIL, cette décision serait la simple conséquence d'un arrêt rendu le 13 mai 2014 par la Cour de Justice de l'Union Européenne (CJUE). La CNIL se bornerait à « demander le plein respect du droit européen par des acteurs non européens offrant leurs services en Europe ». En outre, cette décision ne porterait pas atteinte au droit à l'information du public situé hors d'Europe, puisque les contenus déréférencés sur les moteurs de recherche resteraient toujours accessibles, à condition de les trouver autrement qu'en recherchant le nom d'une personne. Enfin, cette décision serait très strictement encadrée, puisque « placée sous le double contrôle de la CNIL et du juge »… français.

Google entend se conformer strictement à la législation locale
Google, pour sa part, estime devoir se conformer à la législation locale -française et européenne- en respectant les frontières juridiques et territoriales de la loi locale. Le géant américain admettrait de supprimer les résultats de recherche accessibles sur ses services destinés aux internautes européens (« .fr », « .de », « .co.uk », etc), mais pas pour ceux du monde entier.
Tous les arguments de la CNIL sont simples : quand elle demande la désindexation d'une information rapportée par un moteur de recherche et dont se plaint un ressortissant européen, c'est pour le monde entier. Peu importe l'organe de presse ou la liberté d'expression garantie dans le pays diffusant l'information en cause. Peu importe l'endroit du monde depuis lequel un internaute consulterait un moteur de recherche.
On voudrait y croire. Oublier les frontières, exporter nos valeurs, comme au Siècle des Lumières… Mais le faire en 2015, sur Internet, sans un instrument juridique international négocié entre Etats, c'est soit prétentieux, soit voué à l'inefficacité. Ou probablement les deux.

La simplicité ne suffit pas à faire la loi
Le droit européen et français s'impose principalement aux entreprises européennes, ainsi qu'aux entreprises non-européennes qui traitent ou font traiter des données personnelles sur le sol européen. Mais le fait d'offrir des services en Europe n'est pas, à l'heure actuelle, un critère suffisant pour appliquer à un acteur extra-européen nos règles européennes de protection de la vie privée.

On peut en être frustré, mais c'est l'état du droit en vigueur. Cette situation changera probablement dans deux ans, après que l'Union européenne aura adopté un projet de Règlement sur la protection des données personnelles. Ce projet est encore en cours de rédaction et on espère le voir finalisé dans quelques semaines -la fin de l'année 2015.

La CNIL anticipe donc des critères d'application du droit français et européen qui n'existent pas encore. En droit, il s'agit de déterminer si notre loi française « Informatique & Libertés » est une loi dite « de police ». Il s'agit de justifier qu'elle ait des effets contraignants hors de notre territoire national à l'encontre d'un acteur qui ne fabrique pas son moteur de recherches sur le sol européen.

Divergences de jurisprudence
La jurisprudence judiciaire française est divergente sur ce point. Déjà en juin 2011, l'Assemblée nationale, dans son rapport sur les « Droits de l'individu dans la révolution numérique », constatait que « la protection des données personnelles […] n'obéit aujourd'hui à aucun caractère juridique universel et contraignant », soulignant alors la nécessité de réformer le cadre européen adopté en 1995 . Et l'Assemblée de conclure qu' « il appartient aux pouvoirs publics des États concernés et non aux autorités de contrôle de réfléchir à la nécessité de mettre en œuvre l'adoption d'une convention internationale ».

Le Conseil d'État, pour sa part, dans son rapport d'études pour l'année 2014 , a listé les conditions à réunir : si le futur règlement européen sur la protection des données s'étend aux entreprises établies hors de l'Union européenne au motif qu'elles offrent leurs services en Europe et si les droits en cause sont garantis par la Charte des Droits Fondamentaux de l'Union européenne , on pourra alors qualifier de « lois de police » les règles de protection des données personnelles adoptées par l'Union européenne. Or, ces deux conditions ne sont pas réunies aujourd'hui.

Les autorités européennes elles-mêmes -la CNIL et ses homologues-, ont appelé en novembre 2014, dans une déclaration solennelle , à ce que ces futures règles européennes soient dites « d'ordre public international » – ou « de police » -, car elles devraient avoir des effets partout dans le monde. Mais ces déclarations, qui n'ont aucun caractère normatif, montrent précisément que ce qui « devrait être », n'est pas encore.

Sanctionner avant d'avoir régulé ?
Si Google résiste aux injonctions de la Présidente de la CNIL, cette dernière réunira dans les prochains jours la formation restreinte de la CNIL, qui est seule habilitée à prononcer un avertissement, une amende administrative plafonnée à 150 000 -ou 300 000 euros en cas de récidive-, voire une injonction de cesser le traitement illicite de données. Si la CNIL condamne et si son raisonnement est contesté par Google, ce débat pourra faire l'objet d'un recours devant le Conseil d'Etat, puis rebondir devant la CJUE, conduisant celle-ci à statuer dans quelques années.

Toutefois, la pression juridique exercée sur un acteur privé, fut-il un Léviathan, ne peut pas se substituer à l'absence de règles de droit international ou de traités bilatéraux. Ce débat ne peut donc se limiter longtemps à un rapport de forces entre un régulateur national ou européen et un acteur économique mondial. Car ce rapport de forces serait perdu d'avance par un régulateur impatient. Tout le paradoxe est là : la CNIL pourra prononcer des sanctions, même fortes, cela ne haussera pas le niveau de protection des données personnelles hors de l'Union européenne, tant qu'un accord international entre Etats ne sera pas trouvé.

En initiant un combat homérique deux ans avant d'être confortée par un texte ou contredite par un juge, la Présidente de la CNIL se garantit un feuilleton médiatique à rebondissements. Pour quelle efficacité réglementaire ? A chacun ses objectifs et son agenda.

Source : http://www.latribune.fr/opinions/tribunes/droit-a-l-oubli-la-cnil-a-la-conquete-du-monde-509984.html
Par Etienne Drouard, avocat au Barreau de Paris

La gestion des comptes personnels de formationencadrés par la CNIL (Commission nationale de l’informatique et des libertés) | Le Net Expert Informatique

La gestion des comptes personnels de formationencadrés par la CNIL (Commission nationale de l’informatique et des libertés)

Découvrez les règles relatives à la gestion des comptes personnels de formation avec la CNIL (Commission nationale de l'informatique et des libertés).
Autorisation Unique n° AU-044 – Délibération n° 2015-227 du 9 juillet 2015 portant autorisation unique de traitements de données à caractère personnel mis en œuvre aux fins de gestion des comptes personnels de formation (AU-44)

Consultez la délibération

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. 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.cnil.fr/documentation/deliberations/deliberation/delib/336/

Big Data et IoT bousculent le droit des individus | Le Net Expert Informatique

	Big Data et IoT bousculent le droit des individus

Gaspard Koenig, philosophe, apporte un éclairage original sur les relations entre Big Data, objets connectés et individus. Les paradigmes sont bousculés et l'intellectuel milite pour la création d'un droit de propriété sur les données personnelles.

Les Assises de la Sécurité ont pris comme habitude « d'aérer » les esprits des RSSI et des partenaires avec des contributions de personnes non issues du sérail. Luc Ferry, Jean-Christophe Ruffin, Laurent Alexandre se sont pliés à l'exercice sur des sujets aussi variés que les propos sécuritaires, les mouvements de rébellion ou le hacking du cerveau. C'était au tour de Gaspard Koenig de se plier à l'exercice pour la 15ème édition des Assises. Normalien, philosophe et ancienne plume de Christine Lagarde, il avait choisi un thème elliptique : « l'utopie numérique est-elle dangereuse pour l'individu ? ».

Basculer de la déduction à la corrélation

Pour sa démonstration, l'utopie numérique se focalise sur le Big Data et l'Internet des objets, la partie individu se concentre sur la transparence ou la fin de la confidentialité. Pour lui, il s'agit tout d'abord d'une question épistémologique. « Le Big Data est la revanche de la sensibilité sur la généralité », explique-t-il en se basant sur la seconde méditation de Descartes et l'épisode du morceau de cire, qui pose comme postulat que l'appréhension d'un objet dans sa globalité est dictée par la raison. Or le Big Data remet en cause cette façon de penser en appliquant des singularités au morceau de cire. Cela signifie que les objets ne sont plus classés dans des catégories, mais selon plusieurs subtilités, finalités. « Le Big Data fait évoluer la science de la déduction à la corrélation. On est dans le quantitatif, dans la convergence de données », constate le philosophe. Et ce changement de paradigme a déjà des applications concrètes. Dans les assurances, les objets connectés vont « redéfinir l'individu » (façon de conduire, habitude de vie et de consommation) alors qu'il était catégorisé selon certaines données (âges, sexes, etc).

Bonheur collectif ou individuel ?

Pendant de cette course à « la connaissance universelle », il y a les problématiques de vie privée et de transparence des données individuelles. « Le Big Data a une finalité qui est de gagner du bien-être, des gains de productivité, de confort, etc. Il s'agit d'une vision utilitariste pensée par Jeremy Bentham pour qui le but de toute politique est d'aboutir au bonheur des gens », remarque Gaspard Koenig. Une analyse qui ne lui convient pas et qui a été critiqué par « John Stuart Mill qui substituait le bonheur général au bonheur individuel, c'est-à-dire le droit à la diversité à la faillibilité ». Mais dans ce cas-là, « pourra-t-on refuser le trajet dicté par une voiture autonome ou ne pas vouloir partager les informations d'un compteur intelligent sans impacter le bonheur général ? ». Des exemples triviaux, mais qui pose la question des missions de l'Etat, « apporter le bonheur collectif ou protéger les droits individuels ».

Un droit de propriété des données personnelles

La réponse apportée par le philosophe est de « donner un droit de propriété sur les données personnelles ». Aujourd'hui, on part du principe que dans le Big Data, nos données sont gratuites. « Elles sont en réalité pillées par les GAFA avec l'aval des utilisateurs via les 'terms and conditions' qui comme dans le cas de Paypal sont plus longs que Hamlet », accuse Gaspard Koenig. Pour lui, il faut rentrer dans une logique patrimoniale des données personnelles. « Nous avons inventé le droit de propriété intellectuelle lors de la révolution industrielle. A l'heure du numérique, il faut créer une droit de propriété des données individuelles ». Une approche qui implique de reconfigurer le business model de l'Internet, « Google devrait rémunérer les gens pour obtenir leur données », conclut le philosophe un brin utopiste, mais qui sait….

Source : http://www.silicon.fr/assises-de-securite-2015-big-data-iot-bousculent-droit-individus-127948.html
Par Jacques Cheminat

La Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales | Le Net Expert Informatique

La Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales

2% de la surface de la terre sont occupés par les villes. Or, d'ici 2050, elles accueilleront 70% de la population mondiale et seront à l'origine de 80% des émissions de CO2.

Au-delà de ces questions démographiques, entrent également en ligne de compte des contraintes énergétiques, budgétaires, écologiques et technologiques.
La métropole intelligente, pour répondre aux défis de demain, a commencé à développer le numérique dans ses services. La ville réseau mettant en œuvre des infrastructures communicantes et durables pour le confort des citoyens devient ainsi une réalité.
Dans ce cadre, quid de la prévention des risques ? des données personnelles ou des aspects juridiques des smart cities ?

La chaire Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales a le plaisir de vous convier au :
Colloque Cybersécurité et villes intelligentes
Jeudi 15 octobre 2015
9h30-17h00
Musée de l'Armée
Hôtel National des Invalides, amphithéâtre Austerlitz.
L'inscription est obligatoire auprès de
invitations@chaire-cyber.fr

Consultez le programme

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. 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 plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.chaire-cyber.fr/