

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)

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>



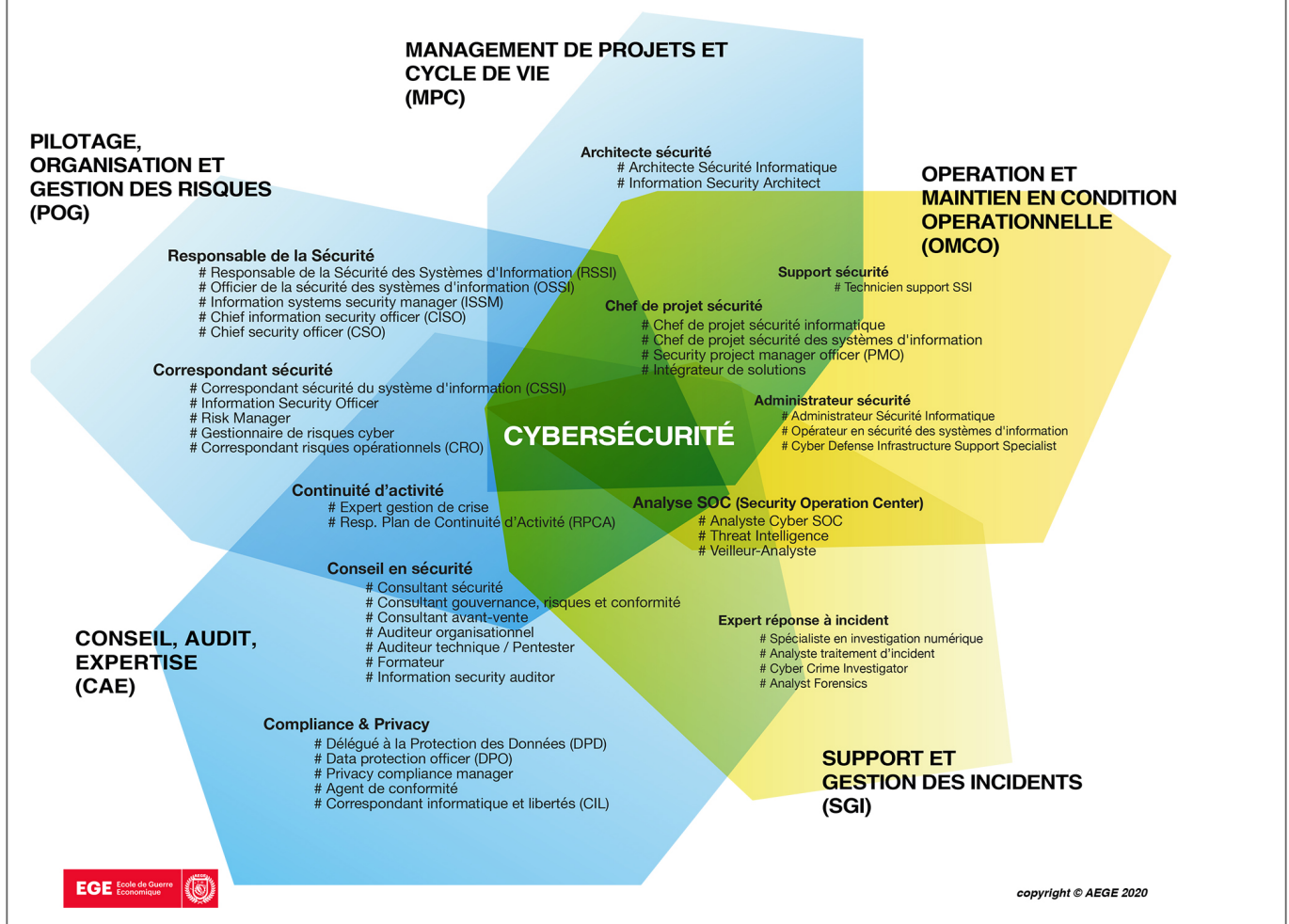
Réagissez à cet article

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

Les métiers de la cybersécurité en 2020

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
x	x	x	x	x	x
x	Les métiers de la cybersécurité en 2020				

L'Ecole de Guerre Economique et le Club Cyber de l'AEGE publient la « Cartographie des métiers de la Cybersécurité » dans le cadre des formations dispensées à l'Ecole depuis 2016. Les zones bleues se rapportent à des familles de métiers Cyber typés management, alors que celles en jaune sont plus orientés ingénierie et technique.



Réagissez à cet article

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

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

Quel sont nos principales activités ?

▪ **RGPD**

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

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

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



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

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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



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



[Contactez-nous](#)



Source : L'Ecole de Guerre Economique publie la cartographie des métiers de la cybersécurité 2020 | Ecole de Guerre Economique

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

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

x

x

x

x

x

x

x

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

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

Une webcam cachée pour s'éviter bien des ennuis

A l'heure où les hackers multiplient les attaques contre les machines des entreprises et des particuliers, beaucoup se sont moqués de Mark Zuckerberg et de son bout de scotch sur la webcam et sur la prise jack, certains allant même jusqu'à le traiter de « parano ».

Pourtant, il semblerait qu'il s'agisse d'un réflexe à prendre et ce pour tout le monde. En effet, un pirate talentueux peut assez simplement prendre le contrôle d'une webcam à distance et pousser ainsi l'utilisateur à télécharger un malware sur sa machine.

Aussi, lors d'une interview, James Comey, le directeur du FBI, a défendu l'idée de masquer la webcam. Il a même précisé que ce devait être un réflexe de base en matière de sécurité. En prenant le contrôle de votre caméra, un pirate peut effectivement visionner vos saisies sur clavier et récupérer ainsi identifiants, mots de passe et coordonnées bancaires pour ne citer qu'eux...[lire la suite]

Conseils de Denis JACOPINI :

Les personnes averties croient utiliser la méthode miracle pour protéger leur vie privée en masquant leur Webcam.

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

Mais avez-vous pensé à protéger votre microphone ?

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

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Pion) ISBN : 2259264220

Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime. Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées. Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ? Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques. Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAIM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAIM et ses invités.
Commandez sur Fnac.fr

https://youtu.be/usgl2zkr09I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet
Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).
Commandez sur Fnac.fr

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

Nos ordinateurs ont-ils la

mémoire courte ? Vidéo



Nos ordinateurs ont-ils la mémoire courte ? Vidéo

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

<https://www.youtube.com/watch?v=KCD1h8o7QTg>

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

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **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).



Réagissez à cet article

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

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

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

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

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.

Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant... Les accès gratuits pullulent et se généralisent.

Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit » assure-t-il. « Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants... »

Des sniffeurs de données

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

Les données sur le Wi-Fi ne sont pas chiffrées

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

Conseils

Alors quels conseils ? « Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites. » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.

Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Android.

Article original de Samuel NOHRA.

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



Réagissez à cet article

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Mise en conformité RGPD : Accompagnement personnalisé

par des Experts

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



Mise en conformité RGPD
: Accompagnement
personnalisé par
des Experts



Formation RGPD
pour devenir DPO
de votre
organisme -
Prochaine
formation les 17
18 et 19
septembre 2018
à Paris

Depuis le 25 mai 2018, le RGPD (Règlement européen sur La Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

**Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours
(Mettez en place une démarche de mise en conformité RGPD)**

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.

Consultez les prochaines dates d'animation autour de chez vous ?



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique **spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel)**, consultant depuis 1996 et formateur depuis 1998. J'ai 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

- la formation « Comprendre le RGPD » : 1 jour
- la formation « Je veux devenir Délégué à la Protection des Données » 2 jours
- la formation « Je mets en conformité mon établissement » 3et 4 jours
- la formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) à la formation :

Formation pour TPE/PME : « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



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

Contactez-nous

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

« Mon objectif, vous assurer une démarche de mise en

conformité validée par la CNIL. ».

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



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

Réagissez à cet article

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

RGPD : Vous voulez vous mettre en conformité ? Voici comment faire

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<p>RGPD : Vous voulez vous mettre en conformité ? Voici comment faire</p>			

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

La mise en conformité est une démarche avant tout réglementaire. Elle doit d'abord commencer par un audit avec de nombreux référentiels relatifs à la protection des données à caractère personnel parfois précédée par une sensibilisation du Responsable de Traitement et de certains de ses salariés (à la partie pédagogique de la démarche).
Enfin, doit suivre la mise en conformité destinée à améliorer l'existant en vue de l'approcher le plus possible des règles. Enfin, doivent suivre des contrôles réguliers compte tenu que les éléments tels que le contexte, les règles et les risques évoluent sans cesse.

Vous souhaitez faire appel à un expert informatique qui vous accompagne dans la mise en conformité avec le RGPD de votre établissement ?



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

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

Pour cela, j'ai créé des services sur mesure :

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclut dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

- « Faire » (nous vous apprenons et vous poursuivons le maintien de la mise en conformité tout en ayant la sécurité de nous avoir à vos côtés si vous en exprimez le besoin) ;
- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Nous laisser faire » (nous réalisons les démarches de mise en conformité de votre établissement en totale autonomie et vous établissons régulièrement un rapport des actions réalisées opposable à un contrôle de la CNIL).

Demandez un devis avec le formulaire ci-dessous

Pour ceux qui veulent apprendre à faire, nous proposons 3 niveaux de formation

1. Une formation d'une journée pour vous sensibiliser au RGPD : « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer » ;
2. Une formation de deux jours pour les futurs ou actuels DPD : « Je veux devenir le Délégué à la Protection des Données de mon établissement » ;
3. Une formation sur 4 jours pour les structures qui veulent apprendre à mettre en conformité leurs clients : « J'accompagne mes clients dans leur mise en conformité avec le RGPD ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

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

N'hésitez pas à nous communiquer le plus de détails possibles, ceci nous permettra de mieux connaître vos attentes.

Votre Prénom / NOM (obligatoire)

Votre Organisation / Société (obligatoire)

Votre adresse de messagerie (obligatoire)

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

Vous pouvez nous écrire directement un message dans la zone de texte libre. Néanmoins, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin des informations ci-dessous.

Afin de mieux comprendre votre demande et vous établir un devis, merci de nous communiquer les informations demandées ci-dessous et cliquer sur le bouton «Envoyer les informations saisies» en bas de cette page pour que nous les recevions. Une réponse vous parviendra rapidement.

MERCI DE DÉTAILLER VOTRE DEMANDE, VOS ATTENTES...

Votre demande, vos attentes... :
 Détails sur votre activité :
 Êtes-vous soumis au secret professionnel ?
 Votre activité dépend-elle d'une réglementation ?
 Si "Oui", laquelle ou lesquelles ?

VOTRE SYSTÈME INFORMATIQUE

Pouvez-vous nous décrire la composition de votre système informatique. Nous souhaiterions, sous forme d'énumération, connaître les équipements qui ont un quelconque accès à des données à caractère personnel avec pour chacun des appareils TOUS le(s) logiciel(s) utilisé(s) et leur(s) fonction(s).
 Exemples :
 - 1 serveur WEB avec site Internet pour faire connaître notre activité ;
 - 1 ordinateur fixe avec logiciel de facturation pour facturer mes clients ;
 - 2 ordinateurs portables dont :
 > 1 avec logiciel de messagerie électronique pour correspondre avec des clients et des prospects « traitement de textes pour la correspondance » logiciel de facturation pour facturer mes clients...
 > 1 avec logiciel de messagerie électronique pour correspondre avec des clients et des prospects « logiciel de comptabilité pour faire la comptabilité de la structure ;
 - 1 smartphone avec logiciel de messagerie électronique pour correspondre avec des clients et des prospects.
 Avez-vous un ou plusieurs sites Internet ?
 Quel(s) est(ont) ce(s) site(s) Internet ?
 Avez-vous des données dans le Cloud ?
 Quel(s) fournisseur(s) de Cloud(s) utilisez-vous ?

VOS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Si vous avez déjà établi la liste des traitements de données à caractères personnels, pourriez-vous nous en communiquer la liste (même incomplète) ?

DIMENSIONNEMENT DE VOTRE STRUCTURE

Nombre de salariés de votre structure :
 Parmi ces salariés, combien utilisent un équipement informatique ?
 Nombre de services** dans votre structure (exemple : Service commercial, service technique...) :
 Merci d'énumérer les services** de votre structure :

PRESTATAIRES & SOUS-TRAITANTS

Travaillez-vous avec des sous-traitants ?
 Merci d'énumérer ces sous-traitants :
 Travaillez-vous avec des prestataires qui interviennent dans vos locaux ou dans vos agences ?
 Merci d'énumérer ces prestataires :
 Avec combien de société(s) d'informatique travaillez-vous ?
 Merci d'énumérer ces sociétés d'informatique en indiquant les produits ou services pour lesquels elles interviennent et éventuellement leur pays :

VOTRE SITUATION VIS-À-VIS DU RGPD

Votre établissement échange-t-il des données avec l'étranger ?
 Si oui, avec quel(s) pays ?
 Avez-vous déjà été sensibilisé au RGPD ?
 Les personnes utilisant un équipement informatique ont-elles déjà été sensibilisées au RGPD ?
 Si vous ou vos collaborateurs n'ont pas été sensibilisés au RGPD, souhaitez-vous suivre une formation ?

VOS LOCALS

L'analyse des conditions de traitements de données dans votre local professionnel ou vos locaux professionnels fait partie de la démarche de mise en conformité.
 Disposez-vous de plusieurs bureaux, agences etc. dépendant juridiquement de votre établissement ?
 Si "Oui", combien ?
 Merci de nous indiquer l'adresse ou les adresses de vos agences (et pays si pas en France) ou des lieux dans lesquels vous et vos éventuels collaborateurs exercez

TYPE D'ACCOMPAGNEMENT SOUHAITÉ

Nous pouvons vous accompagner de différentes manières.
 A) Nous pouvons vous apprendre à devenir autonome (formation) ;
 B) Nous pouvons vous accompagner au début puis vous aider à devenir autonome ensuite (accompagnement, audit + formation) ;
 C) Vous pouvez choisir de nous confier la totalité de la démarche de mise en conformité (accompagnement) ;
 D) Nous pouvons vous accompagner de manière personnalisée (merci de nous détailler vos attentes).
 Quel type d'accompagnement souhaitez-vous de notre part (A/B/C/D = détails) ?

FIN DU QUESTIONNAIRE

Si vous le souhaitez, vous pouvez nous communiquer des informations complémentaires telles que :
 - Nombre d'agences au total (qui dépendent de l'établissement principal = qui n'ont pas leur propre numéro SIRET) ;
 - Nombre d'agences au total qui ont leur propre numéro SIRET ;
 - Nombre d'agences que votre structure a en France ;
 - Urgence de votre projet ;
 - Toute information complémentaire que vous jugerez utile pour nous permettre de mieux connaître votre projet.

Envoyer les informations saisies

Les informations recueillies sont enregistrées dans la messagerie électronique et le système informatique de l'expert pour les traitements correspondant à la gestion de vos demandes et la proposition de services correspondant à votre demande. Le lieu de traitement de stockage et de sauvegarde se situe en France et auprès d'établissements respectant le bouclier de protection des données UE-Etats-Unis (en anglais : EU-US Privacy Shield). Elles sont conservées 3 ans après notre dernier échange et sont destinées aux services internes. Une démarche de mise en conformité a été entamée en interne depuis 2018 et jusqu'à ce jour par des formations régulières, l'identification des traitements, la réalisation d'un registre des traitements, une analyse de risques sur nos traitements manipulant des données sensibles ou des données à caractère hautement personnel pour lesquels leur violation pourrait avoir de graves conséquences dans la vie quotidienne des personnes concernées et un suivi constant. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (dit RGPD (Règlement général sur la Protection des Données)), à la loi n°78-17 dite « Informatique et Libertés » du 6 janvier 1978 et à la loi n° 2018-003 du 29 juin 2018 relative à la protection des données personnelles, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant le Net Expert, Monsieur le Délégué à la Protection des Données – J les Magnolias – 84300 CAVAILLON par Recommandé avec accusé de réception. Enfin, sur le fondement des articles 111-13, 222-17, 222-18, 222-19-1, 222-22, 222-13, R-621-1, R-621-2, R-621-3, R-621-4, R-621-5, R-621-6, R-621-7, R-621-8, R-621-9, R-621-10, R-621-11, R-621-12, R-621-13, R-621-14, R-621-15, R-621-16, R-621-17, R-621-18, R-621-19, R-621-20, R-621-21, R-621-22, R-621-23, R-621-24, R-621-25, R-621-26, R-621-27, R-621-28, R-621-29, R-621-30, R-621-31, R-621-32, R-621-33, R-621-34, R-621-35, R-621-36, R-621-37, R-621-38, R-621-39, R-621-40, R-621-41, R-621-42, R-621-43, R-621-44, R-621-45, R-621-46, R-621-47, R-621-48, R-621-49, R-621-50, R-621-51, R-621-52, R-621-53, R-621-54, R-621-55, R-621-56, R-621-57, R-621-58, R-621-59, R-621-60, R-621-61, R-621-62, R-621-63, R-621-64, R-621-65, R-621-66, R-621-67, R-621-68, R-621-69, R-621-70, R-621-71, R-621-72, R-621-73, R-621-74, R-621-75, R-621-76, R-621-77, R-621-78, R-621-79, R-621-80, R-621-81, R-621-82, R-621-83, R-621-84, R-621-85, R-621-86, R-621-87, R-621-88, R-621-89, R-621-90, R-621-91, R-621-92, R-621-93, R-621-94, R-621-95, R-621-96, R-621-97, R-621-98, R-621-99, R-621-100. Sauf indication contraire ou information publique, nous nous engageons à la plus totale discrétion et la plus grande confidentialité concernant les informations que vous nous communiquez.

** - Exemple de services : Service commercial, Service technique, Service pédagogique, Service administratif et financier...

[Bouton pour envoyer les informations]

ou bien, envoyez un e-mail à rgpd@ro-ba-se|netexpert.fr

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



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

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique,

Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

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

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



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

Réagissez à cet article

Source : Denis JACOPINI

Attaques informatiques : Comment s'en protéger ?

 Attaques ,informatiques, : Comment s'en protéger ?

Les cyberattaques se faisant de plus en plus nombreuses et sévères, les entreprises doivent apprendre à s'en protéger. Pour cela, les directions juridiques et de l'informatique peuvent s'appuyer sur l'expertise de la police judiciaire et des experts en data protection.

Tous les quinze jours en moyenne, une attaque sévère – où des données sont exfiltrées – est découverte. Face à ce constat, le tribunal de commerce de Paris a réuni quatre tables rondes d'experts de la sécurité informatique, des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les entreprises. Julien Robert, directeur de la sécurité chez SFR, résume les trois facteurs agissant sur la sécurité : les utilisateurs, car ce sont eux qui choisissent les données qu'ils utilisent et partagent, les fournisseurs d'accès et l'encadrement d'un data center externe fortement conseillé.

Prévention

« *Il est difficile d'agir lorsque l'attaque a déjà eu lieu* », précise Sylvie Sanchis, chef de la Befiti (1) de la police judiciaire de Paris. Le moyen le plus efficace dont disposent les entreprises pour se protéger est donc la prévention. Il faut avant tout investir dans la sécurité informatique. Si certaines sociétés sont réticentes en raison du coût, il est important de rappeler qu'il sera toujours moindre que celui engendré par une attaque.

Tous les salariés doivent par ailleurs être formés car certaines intrusions sont rendues possibles par leur comportement, sans qu'ils en soient conscients, notamment par leur exposition sur Internet.

Les modes opératoires

Les modes opératoires d'exfiltration des données se diversifient et se sophistiquent au fil des années. Certains se veulent discrets afin que l'entreprise ne prenne connaissance de l'attaque que très tardivement, d'autres relèvent du chantage ou de la demande de rançon.

L'attaque peut venir d'un mail qui, à son ouverture, téléchargera un virus sur l'ordinateur de l'employé. Les données peuvent également être extraites grâce au social engineering, pratique qui exploite les failles humaines et sociales de la cible, utilisant notamment la crédulité de cette dernière pour parvenir à ses fins (arnaque au patron). Quant aux ransomwares, il s'agit de logiciels malveillants permettant de rançonner l'entreprise pour qu'elle récupère ses données. Dans ce cas, Anne Souvira, chargée de mission aux questions liées à la cybercriminalité au cabinet du préfet de police de Paris, précise que « *même si l'entreprise paye, il est très rare de récupérer toutes les données.* » Si elle peut être tentée de payer la rançon sans prévenir les autorités compétentes pour une somme modique, il n'y a aucune garantie de récupérer les données et les traces de l'attaque seront perdues. D'autres techniques de chantage sont utilisées, comme lorsque l'on se voit menacer d'une divulgation des vulnérabilités du système.

L'importance de porter plainte

La réaction à adopter, la plus rapide possible, fait partie de la sécurité informatique : « *C'est un travail de réflexion en amont qui permettra d'adopter la bonne stratégie* », selon Ciryil Piat, lieutenant-colonel de la gendarmerie nationale. Suite à une cyber-attaque, la plupart des entreprises sont réticentes à porter plainte, par peur d'une mauvaise réputation ou par scepticisme vis-à-vis de la réelle utilité de cette procédure. Alice Cherif, chef de la section « cybercriminalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'investigation qui permettront de remonter au cybercriminel. « *Toute autre alternative est bien moins efficace et fait perdre un temps précieux à l'entreprise ainsi que des éléments d'investigation.* »

L'utilité du cloud

L'une des façons de sécuriser ses données est de les confier à un tiers spécialiste qui les stockera en ligne sur un cloud. « *Il s'agit d'un système complexe connecté sur Internet, où les données sont stockées sur des disques durs physiques situés dans des salles d'hébergement, les fameux data centers* », explique Julien Levrard, chef de projet sécurité chez OVH. Le cloud rend l'accès plus difficile aux malfaiteurs d'autant qu'ils ignorent la localisation de la donnée. Vigilance et prévention : les maîtres mots en matière de cybercriminalité.

Article original de Emilie Smelten

(1) Brigade d'enquête sur les fraudes aux technologies de de l'information



Réagissez à cet article

Original de l'article mis en page : Cybercriminalité : comment se protéger ? – Magazine Decideurs