

Formations RGPD Protection des données personnelles et en Cybercriminalité

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



NOS SERVICES :

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

VOTRE PROFIL :

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

LES SUJETS DE FORMATION :



Consultez notre catalogue

COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

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

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

Durée : 1 jour

LES ARNAQUES INTERNET À CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Durée : 1 jour

COMMENT BIEN UTILISER LE CLOUD

Durée : 1 jour

COMMENT PROTÉGER VOTRE IDENTITÉ ET VOTRE VIE PRIVÉE SUR INTERNET

Durée : 1 jour

DÉCOUVREZ 50 LOGICIELS GRATUITS À CONNAÎTRE ABSOLUMENT

Durée : 1 jour

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

Durée : 1 jour

RGPD : ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

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

COMMENT BIEN UTILISER LES DONNÉES DANS LE CLOUD

Durée : 1 jour

À LA DÉCOUVERTE DU DARKNET (LE WEB CLANDESTIN)

Durée : 1 jour

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Durée : 2 jours

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

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

Durée : 2 jours

Remarque :

Un sujet peut être traité en quelques heures mais aussi en quelques jours.

Malgré un minimum de théorie à connaître, nous pouvons réaliser un mélange de ces thèmes afin de vous proposer un contenu personnalisé en fonction des thèmes et durées globales souhaités.

EN FORMAT CONFÉRENCE :

QUE NOUS RÉSERVE LA CYBERCRIMINALITÉ DANS LES 12 PROCHAINS MOIS ?

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

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

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

FONCTIONNEMENT :

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

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



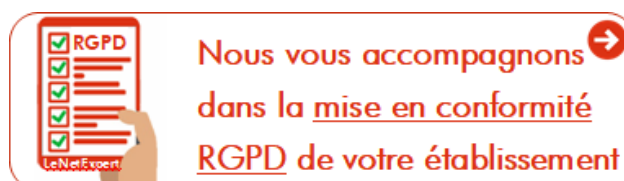
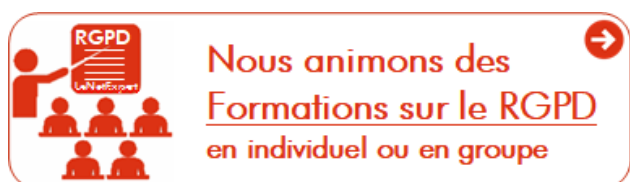
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

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

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

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



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

Dispositif biométrique d'accès à la cantine : quelles formalités à la CNIL ? | Denis JACOPINI



Dispositif biométrique
d'accès à la cantine :
quelles formalités à la
CNIL ?

Les dispositifs biométriques utilisant le contour de la main des élèves pour gérer l'accès à la cantine scolaire sont couverts par une autorisation unique adoptée par la CNIL.

Les établissements qui souhaitent installer ce type de dispositifs doivent faire une déclaration simplifiée, en sélectionnant dans l'onglet « Finalité » l'autorisation unique AU-009.

Le responsable du dispositif s'engage ainsi à se conformer aux caractéristiques décrites dans ce texte.

Les autres dispositifs biométriques (réseaux veineux, empreintes digitales, reconnaissance faciale, etc.) doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

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.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D5FEF7DD5664BF01E19E95AF8AF7782F>

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


Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
		<p>Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris</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.

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 » 3+1 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.



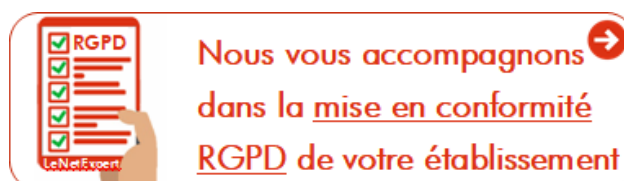
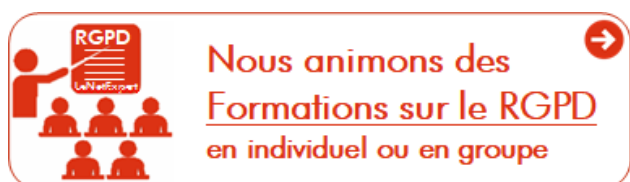
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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)

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

Sans formation en cybersécurité le risque humain reste toujours le plus fort

	Sans formation en cybersécurité le risque humain reste toujours le plus fort
---	---

Le risque humain figure toujours parmi les failles principales dans les affaires de cybersécurité. Les entreprises redoublent donc d'effort pour sensibiliser davantage leurs collaborateurs. La tâche est ardue.

Cela fait quelques années qu'au sein des entreprises, les principes de cybersécurité ne sont plus l'apanage des seuls experts (DSI, RSSI, responsables techniques). En effet, pour se prémunir contre les vulnérabilités d'origine humaine, les entreprises, avec plus ou moins de détermination, ont développé des processus de sensibilisation auprès de leurs collaborateurs, comité exécutif compris. « La mise en place de cette politique de sécurité doit être compréhensible par tous. Elle ne doit donc pas être écrite dans un jargon technique de spécialiste, explique Franck Greverie, Corporate Vice-president des activités cybersécurité chez Capgemini. Surtout les collaborateurs doivent apprendre à comprendre les risques qu'ils font courir à leur entreprise s'ils ne la respectent pas ». La sensibilisation passe donc pas une communication pédagogique sur des sujets tels que la gestion des mots de passe, le phishing, l'ingénierie sociale, l'utilisation d'applications qui ne sont pas à jour, etc. et les conséquences liées à ces attaques et au non respect des procédures.

Alterner des sessions de formations obligatoires avec des ateliers de mise en situation

De façon concrète, cette éducation peut prendre la forme de modules de formations obligatoires, de journées de démonstrations de piratage en comités restreints ou encore de mises en situation. En complément de ces événements de sensibilisation ponctuels, le niveau de maturité des collaborateurs doit être entretenu et mis à jour, par une communication interne régulière. « L'intranet, par exemple, représente un outil adapté pour aider les entreprises à planifier une campagne de sensibilisation à long terme », suggère Franck Greverie. Les pouvoirs publics ont également leur rôle à jouer. « En septembre 2015, certaines entités de l'Etat associées au CIGREF (une association rassemblant les patrons informatiques des grandes entreprises) annonceront conjointement une campagne de sensibilisation de grande ampleur », révèle l'expert.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://bfmbusiness.bfmtv.com/actualite/eduquer-tous-les-collaborateurs-a-la-cybersecurite-de-facon-simple-et-recurrente-891740.html>

Par Eddy Dibar

RGPD : Vous voulez vous mettre en conformité ? Voici

comment faire

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

LE NET EXPERT
AUDITS & EXPERTISES

EXPERTISES DE SYSTEMES DE
VOTES ELECTRONIQUES
LE NET EXPERT

RGPD
CYBER
LE NET EXPERT
MISES EN CONFORMITE

SPY DETECTION
Services de détection
de logiciels espions

LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

RGPD : Vous voulez mettre en conformité ? Voici comment faire

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 (la partie pédagogique de la démarche). Ensuite, 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 et formateur depuis 1998, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15845), en tant que praticien de la mise en conformité et formateur, je vous accompagne

« 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 :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » (nous vous apprenons et vous poursuiviez le maintien de la mise en conformité tout en ayant la sécurité de nous avoir à vos côtés si vous en exprimez le besoin) ;
- ou « 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 DPO : « 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 Organisme / 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 cliquez 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... :

VOTRE ACTIVITÉ

Détails sur votre activité :

Êtes-vous soumis au secret professionnel ?

Oùui MonOJe ne sais pas

Votre activité dépend-elle d'une réglementation ?

Oùui MonOJe ne sais pas

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 TOUTS 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 ?

Oùui MonOJe ne sais pas

Quel(s) est(sont) ce(s) site(s) Internet ?

Avez-vous des données dans le Cloud ?

Oùui MonOJe ne sais pas

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 ?

0

1

Nombre de services** dans votre structure (exemple : Service commercial, service technique...) :

0

1

Merci d'énumérer les services** de votre structure :

PRESTATAIRES & SOUS-TRAITANTS

Travaillez-vous avec des sous-traitants ?

Oùui MonOJe ne sais pas

Merci d'énumérer ces sous-traitants :

Travaillez-vous avec des prestataires qui interviennent dans vos locaux ou dans vos agences ?

Oùui MonOJe ne sais pas

Merci d'énumérer ces prestataires :

Avec combien de société(s) d'informatique travaillez-vous ?

0

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 ?

Oùui MonOJe ne sais pas

Si oui, avec quel(s) pays ?

Avez-vous déjà été sensibilisé au RGPD ?

Oùui MonOJe ne sais pas

Les personnes utilisant un équipement informatique ont-elles déjà été sensibilisées au RGPD ?

Oùui MonOJe ne sais pas

Si vous ou vos collaborateurs n'ont pas été sensibilisés au RGPD, souhaitez-vous suivre une formation ?

Oùui MonOJe ne sais pas

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 ?

Oùui Mon

Si "Oui", combien ?

0

Merci de nous indiquer l'adresse ou les adresses de vos agences (et pays si pas en France) du 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 du début jusqu'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 pas 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

[block id="24086" title="Mentions légales formulaires"]

* = Données à Caractère Personnel

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

ou bien, envoyez un e-mail à rgpd@ro-ba-sej.net/expert.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
?

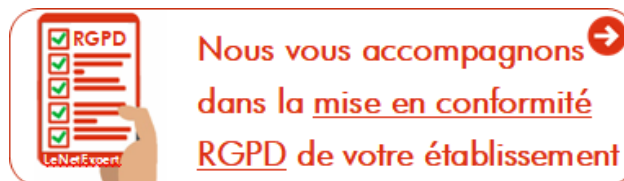
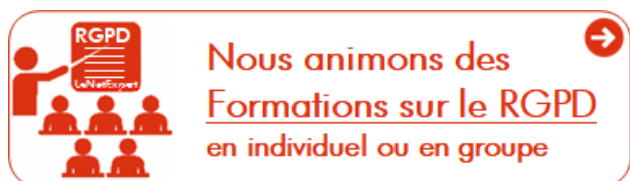
Contactez-nous

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)

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

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 Bofiti (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 Caryl 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 Levraud, 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 Smetten
(1) Brigade d'enquête sur les fraudes aux technologies de de l'information



David JACOPIN est Expert Informatique accrédité spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, ransom, piratages, fraude, arnaques Internet...) et juridiques (investigation numérique, droit des données, droit des consommateurs, droit de la vie privée...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Commissariat Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Le Net Expert
INFORMATIQUE
Conseil et Expertise en matière de Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

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

Demande de Devis pour un audit RGPD

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



LE NET EXPERT
AUDITS & EXPERTISES



EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES
LENETEXPERT
fr



RGPD CYBER
LE NET EXPERT
MISES EN CONFORMITÉ



SPY DETECTION
Services de détection de logiciels espions



LE NET EXPERT
FORMATIONS



LE NET EXPERT
ARNAQUES & PIRATAGES



RGPD
LeNetExpert

Demande de Devis pour un audit RGPD

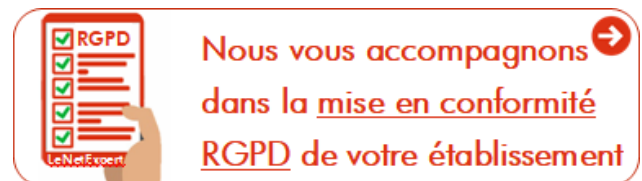
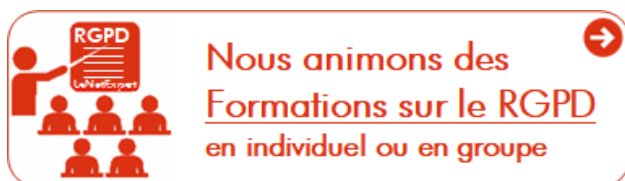
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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)

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

Source : Denis JACOPINI

Devis pour la mise en

conformité avec le RGPD de votre établissement

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>.fr</i>	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
		Devis pour la mise en conformité avec le RGPD de votre établissement			

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.

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 et formateur depuis 1998, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15845), en tant que praticien de la mise en conformité et formateur, je vous accompagne dans toutes vos démarches de mise en conformité avec le RGPD20.

« 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 inclue 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 :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » (nous vous apprenons et vous poursuivez le maintien de la mise en conformité tout en ayant la sécurité de nous avoir à vos cotés si vous en exprimez le besoin) ;
- ou « 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).

contactez-nous 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 DPO : « **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.

[Cliquez ici pour accéder à notre formulaire de demande d'informations](#)

6 conseils pour éviter la contamination du réseau par des ransomwares | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité		<h2>6 conseils pour éviter la contamination du réseau par des ransomwares</h2>			
 vous informe...					

6 conseils pour éviter la contamination du réseau par des ransomwares Une étude réalisée par Bitdefender aux États-Unis montre que les APT (Advanced Persistent Threats), le spear phishing et les ransomware sont les types d'incidents les plus craints dans les entreprises.

Cette étude montre, en effet, qu'en termes d'importance, les APT (techniques complexes d'intrusion réseau) sont en tête des préoccupations : 19,7% des managers interrogés les estiment difficiles à gérer.

Les ransomware arrivent en seconde position (13,7%) avec les rootkits. Ces derniers préoccupent plus les DSI que les menaces 0-day.

Le Spear Phishing (des e-mails soigneusement préparés, destinés à des individus spécifiques au sein de l'entreprise) sont mentionnées par à peu près 13% des personnes interrogées. Reste qu'il s'agit là d'une des techniques les plus utilisées pour pénétrer la sécurité de l'entreprise et diffuser des malwares.

Quant aux incidents générés par le BYOD (Bring Your Own Device, l'utilisation de son appareil personnel dans le cadre du travail) et aux vulnérabilités zero-day, ils semblent moins inquiétants, puisque 11,3% des personnes interrogées voient le BYOD comme un risque potentiel pour leur entreprise, tandis que 10,3% des managers pensent que les attaques zero-day sont sources de menaces pour la sécurité de leur entreprise.

BitDefender fait donc 6 recommandations pour que les entreprises puissent limiter les risques d'infection :

1. Mettre en garde les employés contre les nouvelles menaces et leur expliquer comment déceler un e-mail de spear phishing et d'autres attaques d'ingénierie sociale.
2. Installer, configurer et maintenir à jour la solution de sécurité de l'entreprise.
3. Bloquer l'exécution de certains programmes vecteurs d'infections, comme par exemple des logiciels de téléchargement illégal ou de P2P au bureau.
4. Utiliser un pare-feu pour bloquer les connections entrantes vers des services qui n'ont pas lieu d'être publiquement accessibles via Internet.
5. S'assurer que les utilisateurs aient les droits les plus faibles possible pour accomplir leurs missions. Lorsqu'une application requiert des droits d'administrateur, il faut être certain que l'application soit légitime.
6. Activer la restauration système afin de retrouver les versions précédentes des fichiers qui ont été chiffrés, une fois que la désinfection a eu lieu.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.itrmobiles.com/index.php/articles/157764/6-conseils-eviter-contamination-reseau-ransomwares.html> :

Quelles sont les mentions obligatoires sur un site internet ? | Denis JACOPINI

	Quelles sont les #mentions obligatoires sur un site internet ?
---	--

Tous les sites internet édités à titre professionnel, qu'ils proposent des ventes en ligne ou non, doivent obligatoirement indiquer les mentions légales suivantes :

- pour un entrepreneur individuel : nom, prénom, domicile
- pour une société : raison sociale, forme juridique, adresse de l'établissement ou du siège social (et non pas une simple boîte postale), montant du capital social
- adresse de courrier électronique et numéro de téléphone
- pour une activité commerciale : numéro d'inscription au registre du commerce et des sociétés (RCS)
- pour une activité artisanale : numéro d'immatriculation au répertoire des métiers (RM)
- numéro individuel d'identification fiscale : numéro de TVA intracommunautaire
- pour une profession réglementée : référence aux règles professionnelles applicables et au titre professionnel
- nom et adresse de l'autorité ayant délivré l'autorisation d'exercer quand celle-ci est nécessaire
- nom du responsable de la publication
- coordonnées de l'hébergeur du site : nom, dénomination ou raison sociale, adresse et numéro de téléphone
- pour un site marchand, conditions générales de vente (CGV) : prix (exprimé en euros et TTC), frais et date de livraison, modalité de paiement, service après-vente, droit de rétractation, durée de l'offre, coût de la technique de communication à distance
- numéro de déclaration simplifiée Cnil, dans le cas de collecte de données sur les clients

Avant de déposer ou lire un cookie, les éditeurs de sites ou d'applications doivent :

- informer les internautes de la finalité des cookies,
- obtenir leur consentement,
- fournir aux internautes un moyen de les refuser.

La durée de validité de ce consentement est de 13 mois maximum. Certains cookies sont cependant dispensés du recueil de ce consentement.

Le manquement à l'une de ces obligations peut être sanctionné jusqu'à un an d'emprisonnement, 75 000 € d'amende pour les personnes physiques et 375 000 € pour les personnes morales.

Remarque : Depuis l'entrée en application du RGPD, Règlement Général sur la Protection des Données), vous devez également prévoir des mentions relatives à la protection des données à caractère Personnel ainsi que prévoir des précautions relatives à la demande de consentement des internautes à utiliser leurs coordonnées.

Consultez notre dossier consacré à la demande de consentement

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://vosdroits.service-public.fr/professionnels-entreprises/F31228.xhtml>