Denis JACOPINI interviewé par une journaliste de Ouest France | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Denis JACOPINI interviewé par une journaliste de Ouest France				

Est-il risqué de se connecter au wifi public ?
Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français).
Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.

Denis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?
Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

Quel est le danger ? Se faire espionner ?
Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.

Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » – par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. – ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?
Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates !

Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

Peut-on se faire abuser par une fausse borne wifi ?
Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

Comment se protéger ?
En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.

Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

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 ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Source : http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/

7
Par Corinne Bourbeillon

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

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

---

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

Comment se connecter de manière sécurisée à un wifi public ? | Denis JACOPINI

En période de vacances ou lors de déplacements professionnels, nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… En juillet 2015, nous vous avions publié un article « Est-il risqué de se connecter au wifi public ? » pour vous informer des principaux risques à partager ces accès sans fil à internet avec d'autres. Cette fois, nous allons parler des solutions pour surfer sécurisé en utilisant les réseaux Wifi publics.

RAPPEL DU PRINCIPAL RISQUE

Un pirate peut se connecter tout aussi facilement que vous sur un réseau Wifi Public et espionner les données qui y transitent.

Il peut ainsi, en fonction des données qu'il récupère :

• **accéder à toutes les informations qui sortent et qui entrent de votre ordinateur** (le protocole tcp/ip n'étant pas protégé par défaut) ;

• vous voler, **crypter des documents ou exercer un chantage pour que vous puissiez les récupérer** ;

• **usurper votre identité** et **réaliser des actes illégaux ou terroristes sous votre identité ;**

• **accéder à des informations bancaires et vous spolier de l'argent**.

LA SOLUTION ?

Utiliser une connexion Wifi qui sera cryptée au moyen d'un logiciel VPN (ce ctyptage n'a aucun rapport avec les clés Wifi) .

La connexion Wifi ainsi créée étant crypté, toutes les informations qui véhiculeront (identifiants, adresses email, mots de passe, numéros de cartes bancaires…) seront illisibles pour tous les pirates qui seront connectés sur le mêle point d'accès wifi.

Vous pouvez certes partager la connexion 3G ou 4G de votre smartphone, mais l'utilisation d'un logiciel VPN est recommandé.

Un logiciel « VPN » (Virtual Private Network) est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais elle est du coup sécurisée.

Nous utilisons et conseillons le logiciel VPN HotSpot Shield.
Ce logiciel rendra vos connections Wifi publiques tranquilles.
Téléchargez et découvrez gratuitement HotSpot Shield
Notre page de présentation de HotSpot Shield

Réagissez à cet article

Formation Data protection officer (DPO)

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Formation Data protection officer (DPO)				

Le data protection officer sera obligatoire en France dans certaines entreprises le 25 mai 2018. Voici ce qu'il faut savoir sur son rôle.

D'ici le 25 mai 2018, les entreprises et les administrations qui utilisent des données à caractère personnel devront recourir aux services d'un data protection officer (DPO).
Quel est son rôle et ses obligations ?

Data protection officer : définition

Les données sont présentes en masse dans les entreprises. Ce qui peut poser des risques en matière de sécurité mais aussi de légalité. Pour aider les entreprises, un nouveau métier a le vent en poupe dans le secteur du numérique : le data protection officer (DPO).
Sa mission est la suivante : s'assurer que son employeur ou son client respecte la législation lorsqu'il utilise les données à des fins commerciales (mailing par exemple) mais aussi à des fins internes (logiciels RH). Son rôle est donc transversal, ce qui l'amène à travailler avec de nombreux départements : direction générale, marketing, développement ou encore RH. En cas de manquement à la loi, il est tenu d'alerter sa direction dans les plus brefs délais.
Son rôle est très polyvalent. En plus de connaissances en informatique et en cybersécurité, le data protection officer est tenu de posséder une grosse culture juridique, notamment en droit des nouvelles technologies de l'information et de la communication (NTIC). Aujourd'hui, des juristes spécialistes des NTIC, des informaticiens, des ingénieurs en cybersécurité peuvent exercer des fonctions de data protection officer au sein d'entreprises ou de cabinets de conseil.

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 : *Data protection officer (DPO) : définition, formation et salaire*

Phishing, repérez les faux mails et déjouez les pièges des pirates

Phishing, repérez les faux mails et déjouez les pièges des pirates

Le phishing, ou hameçonnage, a pour but de vous dérober vos données personnelles en douceur, au moyen d'un simple courriel ou d'un faux site Web, depuis un ordinateur ou un mobile. Voici quelques conseils et outils pour mieux vous protéger.

Faites appel à votre bon sens et restez sur vos gardes

Lorsque vous recevez un mail censé provenir d'un portail gouvernemental ou bancaire, demandez-vous pourquoi vous le recevez et scrutez attentivement cette correspondance avant de cliquer sur le moindre lien ! Examinez l'intitulé et surtout l'adresse de l'expéditeur. Impensable que le centre des impôts vous écrive avec une adresse @free.fr ! L'inspection des éventuelles fautes d'orthographe et l'exactitude de vos infos personnelles doivent également susciter la méfiance. En cas de doute sur l'authenticité du message reçu de votre banque ou d'un organisme officiel, prenez le temps de le contacter par téléphone. Sachez en outre que les grandes entreprises disposent de plus en plus souvent de services dédiés à la protection des données de leurs clients. Certaines proposent même depuis leur site Internet de transmettre le mail suspect ou frauduleux, c'est le cas chez EDF notamment…[lire la suite]

Denis JACOPINI : Face au développement incoercible de la cybercriminalité, suivez **nos formations** pour anticiper les prochains piratages et prochaines arnaques dont vous risquez bien de vous retrouver la cible. Nous partons du principe que le meilleurs moyen de se protéger des pirates, c'est non seulement de connaître leur mode opératoire mais de **savoir reconnaître les symptômes.** Découvrez nos nouvelles formations : les 30 plus dangereuses arnaques sur Internet

---

NOTRE MÉTIER :

• FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO

• EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES

• AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT

• MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dansl e but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

Réagissez à cet article

Source : *Phishing, repérez les faux mails et déjouez les*

Phishing, repérez les faux mails et déjouez les pièges des pirates

Phishing, repérez les faux mails et déjouez les pièges des pirates

Le phishing, ou hameçonnage, a pour but de vous dérober vos données personnelles en douceur, au moyen d'un simple courriel ou d'un faux site Web, depuis un ordinateur ou un mobile. Voici quelques conseils et outils pour mieux vous protéger.

Faites appel à votre bon sens et restez sur vos gardes

Lorsque vous recevez un mail censé provenir d'un portail gouvernemental ou bancaire, demandez-vous pourquoi vous le recevez et scrutez attentivement cette correspondance avant de cliquer sur le moindre lien ! Examinez l'intitulé et surtout l'adresse de l'expéditeur. Impensable que le centre des impôts vous écrive avec une adresse @free.fr ! L'inspection des éventuelles fautes d'orthographe et l'exactitude de vos infos personnelles doivent également susciter la méfiance.

En cas de doute sur l'authenticité du message reçu de votre banque ou d'un organisme officiel, prenez le temps de le contacter par téléphone. Sachez en outre que les grandes entreprises disposent de plus en plus souvent de services dédiés à la protection des données de leurs clients. Certaines proposent même depuis leur site Internet de transmettre le mail suspect ou frauduleux, c'est le cas chez EDF notamment…[lire la suite]

Denis JACOPINI : Face au développement incoercible de la cybercriminalité, suivez **nos formations** pour anticiper les prochains piratages et prochaines arnaques dont vous risquez bien de vous retrouver la cible. Nous partons du principe que le meilleurs moyen de se protéger des pirates, c'est non seulement de connaître leur mode opératoire mais de **savoir reconnaître les symptômes.**

Découvrez nos nouvelles formations : les 30 plus dangereuses arnaques sur Internet

---

NOTRE MÉTIER :

• FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
• EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
• AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
• MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dansl e but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

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 ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Phishing, repérez les faux mails et déjouez les pièges des pirates – SFR News*

Cybersécurité : quand les collectivités prennent la mesure du problème

	Cybersécurité : quand les collectivités prennent la mesure du problème

---

A l'heure où la cybersécurité est un enjeu croissant pour les acteurs publics, les collectivités semblent se prendre enfin en main. La ville de Marseille a mis en place une initiative pour tester ses défenses. Dans le même temps, la région Hauts-de-France a, elle, été choisie pour être le théâtre d'une expérimentation de l'ANSSI.

Pour de nombreuses collectivités locales, la cybersécurité reste encore aujourd'hui un enjeu abstrait. A quelques exceptions près, ces dernières ne sont pas armées pour résister à des attaques très virulentes et aveugles. Et pourtant, les offensives font de plus en plus mal. En témoignent les dégâts causés en mai dernier par le rançongiciel WannaCry, qui a paralysé plus de 200 000 machines à travers près de 150 pays, dont des opérateurs d'importance vitale en France.
L'ampleur de l'offensive n'a fait que confirmer ce que tout le monde savait depuis longtemps : personne n'est à l'abri. Des solutions commencent toutefois à être mises en place par les collectivités elles-mêmes. Un changement de paradigme plus que nécessaire.

Marseille joue la carte prévention

La ville de Marseille a ainsi inauguré le 6 juin une initiative visant à permettre à la municipalité de tester l'efficacité de ses défenses à tous les niveaux. Concrètement, une vingtaine d'étudiants issus de l'école Polytech – l'initiative étant réalisée en partenariat avec l'Université Aix-Marseille – cherchera les éventuelles failles dont la municipalité n'aurait pas connaissance.
Les sites web, applications mais aussi les objets connectés seront passés au crible par ces « hackers éthiques ». Pour ce faire, ces derniers utiliseront SafeGouv, un service proposé par la start-up Net Guard…[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 : *Cybersécurité : quand les collectivités prennent la mesure du problème*

Vote électronique : Confidentialité et sécurité des données a confirmé le Conseil d’Etat | Le Net Expert Informatique

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Vote électronique : Confidentialité et sécurité des données a confirmé le Conseil d’Etat				

Le Conseil d'Etat a été amené, dans un arrêt du 11 mars 2015 n° 368748, à se prononcer sur la confidentialité et la sécurité des données à l'occasion de l'organisation d'un vote électronique pour les élections professionnelles de délégués du personnel.

En l'espèce, la CNIL, saisie d'une plainte d'un syndicat, prononce un avertissement à l'encontre d'une société n'ayant pas pris toutes précautions utiles pour préserver la sécurité et la confidentialité des données à caractère personnel lors de l'élection des délégués du personnel organisée par voie électronique avec recours aux services d'un prestataire extérieur. La société et le prestataire forment un recours en annulation de cette délibération devant le Conseil d'Etat.

Le Conseil d'Etat rejette la requête et retient qu'il résulte des dispositions du Code du travail, « dont l'objectif est de garantir la sincérité des opérations électorales par voie électronique, que l'utilisation d'un système de vote électronique pour l'élection des délégués du personnel est subordonnée à la réalisation d'une expertise indépendante lors de la conception initiale du système utilisé, à chaque fois qu'il est procédé à une modification de la conception de ce système ainsi que préalablement à chaque scrutin recourant au vote électronique ».

Dès lors, « à supposer même que le système de vote électronique en litige n'ai fait l'objet d'aucune modification de sa conception depuis sa précédente utilisation par l'entreprise, […] une expertise indépendante était requise préalablement à sa mise en place pour les élections professionnelles organisées par la société requérante ».

Par ailleurs, « il résulte de [l'article R. 2324-5 du Code du travail sur la confidentialité des données transmises] que la transmission aux électeurs des identifiants et mots de passe leur permettant de participer au vote doit faire l'objet de mesures de sécurité spécifiques permettant de s'assurer que les électeurs en sont les seuls destinataires ». Ainsi, « c'est à bon droit que la CNIL a estimé que la transmission par simple courriel de ces données aux électeurs méconnaissait les obligations » découlant de ce même article.

En outre, le Conseil d'Etat rappelle, conformément à un arrêté ministériel du 25 avril 2007, que « le respect de ces dispositions implique nécessairement que le chiffrement des bulletins de vote soit ininterrompu », et ce dès l'émission du vote sur le poste de l'électeur jusqu'à sa transmission au fichier dénommé « contenu de l'urne électronique ».

Enfin, si l'employeur a recours à un prestataire extérieur pour l'organisation du vote électronique, il reste malgré tout responsable de ce traitement de données. Le Conseil d'Etat précise ainsi que « la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de préserver la sécurité des données ». Cela ne méconnaît pas « le principe constitutionnel de responsabilité personnelle, dès lors que ces sous-traitants ont agi sur instruction du responsable de traitement ».

Le Conseil d'Etat a ainsi estimé que la sanction de la CNIL visant à rendre public l'avertissement était proportionnée au regard de la nature et de la gravité des manquements constatés, et sa publication appropriée « à la recherche de l'exemplarité ».

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Source : http://www.snaless.org/vote-electronique-confidentialite-et-securite-des-donnees_juri_2855.php