

Le recours au vote électronique en entreprise enfin facilité !

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT fr	 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
					Le recours au vote électronique en entreprise enfin facilité !

L'employeur peut maintenant décider de mettre en œuvre le vote électronique pour les élections professionnelles même en l'absence d'accord d'entreprise.

Jusqu'à présent, le recours au vote électronique pour le déroulement des élections professionnelles (délégués du personnel, membres du comité d'entreprise...) était subordonné à la conclusion d'un accord d'entreprise. Autrement dit, l'employeur n'avait pas la possibilité, en l'absence d'accord collectif, de mettre en place un tel dispositif. Une possibilité aujourd'hui offerte par la loi Travail du 8 août 2016 et dont les modalités d'application ont été fixées par décret.

Ainsi, les employeurs d'au moins 11 salariés peuvent désormais, en l'absence d'accord le prévoyant, recourir au vote électronique pour organiser les élections professionnelles au sein de l'entreprise. Attention : le décret ne précise pas si, avant de prendre une telle décision, l'employeur doit préalablement tenter de conclure un accord avec les syndicats représentatifs. Aussi lui est-il conseillé d'ouvrir de telles négociations compte tenu du risque d'annulation du scrutin qui pourrait en découler.

Il appartient alors à l'employeur de fixer les modalités du déroulement du scrutin dans un cahier des charges respectant les règles légales relatives au vote électronique. Parmi ces règles, on peut citer notamment l'obligation d'assurer la confidentialité des données transmises et la sécurité de l'adressage des moyens d'authentification ainsi que le scellement du système de vote à l'ouverture et à la clôture du scrutin. Important : le cahier des charges doit être tenu à la disposition des salariés sur le lieu de travail et, le cas échéant, figurer sur le site Intranet de l'entreprise.

Par ailleurs, lorsqu'il décide de recourir au vote électronique, l'employeur peut exclure ou autoriser le scrutin à bulletin secret sous enveloppe. Dans ce dernier cas, l'ouverture du vote à bulletin secret doit avoir lieu après la clôture du vote électronique.

Enfin, l'employeur doit informer l'ensemble des syndicats représentatifs de salariés dans l'entreprise qu'il a bien accompli la déclaration préalable du dispositif de vote auprès de la Commission nationale de l'informatique et des libertés.

Décret n° 2016-1676 du 5 décembre 2016, JO du 6

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

Notre sélection d'articles sur le vote électronique

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

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

**Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise**



Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

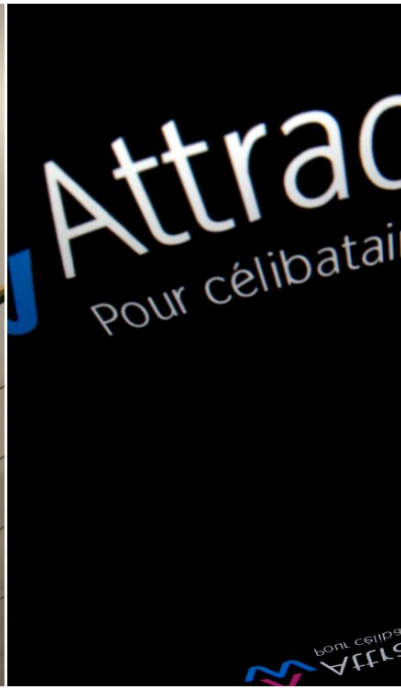
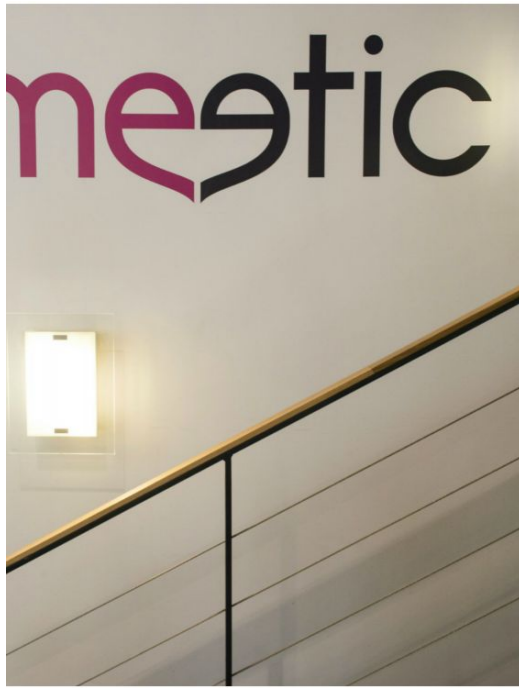
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l'article mis en page : Le recours au vote électronique en entreprise est facilité !, Social et RH – Les Echos Business

La **sanctionne** « **Attractive World** » et « **Meetic** » **Cnil**



La Cnil
sanctionne
« Attractive
World » et
« Meetic »

Meetic a indiqué qu'en s'inscrivant sur son site de rencontre, « les personnes ont conscience et sont informées que les données qu'elles fournissent sont nécessaires pour la fourniture du service auxquelles elles souscrivent » , une forme de consentement express en quelque sorte.

Après plusieurs mises en garde, réunions et rencontres avec la CNIL, les deux géants Meetic et Attractive World n'avaient pas fait mine de s'intéresser aux recommandations de l'autorité pour changer un aspect important relatif à la protection des données personnelles. La Commission nationale de l'informatique et des libertés a prononcé, fin décembre 2016, une sanction publique de 10 000 euros à l'encontre de la société Samadhi, propriétaire du site Attractive World et de 20 000 euros à l'encontre de Meetic SAS, en raison du traitement des données *sensibles* de leurs utilisateurs sans recueil de leur consentement exprès.

Il faut dire que ces sites sont de plus en plus thématiques, ciblés, en fonction de goûts ou de communautés. Un point que ne partage pas la CNIL qui déplore un manquement évident à la loi « *Informatique et Libertés* » .

Conséquence, en juillet dernier, 8 sites, et pas des moindres, ont été mis en demeure de rectifier le tir. Visiblement, deux d'entre eux n'ont pas joué le jeu. En effet, en cas d'attaque malveillante à l'encontre de ces sites, donc de piratage informatique, les données personnelles et *sensibles* peuvent se retrouver dans la nature ce qui pourrait être déplorable pour les utilisateurs qui n'ont pas donné leur consentement éclairé sur l'exploitation de leurs données privées, qui plus est, sur leurs affinités, leurs croyances, leurs avis politiques ou leurs origines ethniques.

« Les utilisateurs souhaitant s'inscrire aux sites devaient – en une seule fois – accepter les conditions générales d'utilisation, attester de leur majorité et consentir au traitement des données *sensibles* », rappelle la Cnil. « La seule inscription au **site de rencontre** ne peut valoir accord exprès des personnes au traitement de telles données qui révèlent **des éléments de leur intimité** » .

Original de l'article : « Attractive World » et « Meetic » épinglés par la Cnil

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 de formation, de sensibilisation ou d'audits 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : « Attractive World » et « Meetic » épinglés par la Cnil

Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

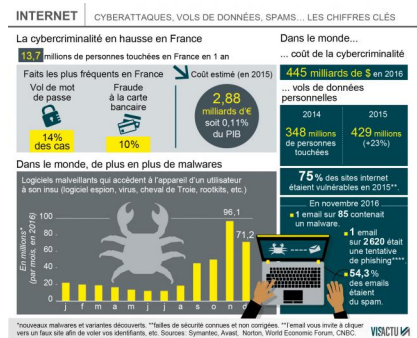


Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

Il y a les cyberattaques à l'échelle des états et il y a la cybercriminalité qui peut toucher chaque citoyen. Vols de mots de passe, demandes de rançon, vols de données personnelles... Les chiffres sont en hausse partout dans le monde mais aussi en France.

Les chiffres de la cybercriminalité ont de quoi faire peur. 13,7 millions de personnes ont été confrontées à la cybercriminalité en France en 2016, selon Norton, entreprise spécialisée dans la sécurité en ligne.

Vente de faux papiers d'identité, apologie du terrorisme, vols de mots de passe, de données personnelles, extorsion de fonds ou encore trafic d'armes : le terme cybercriminalité couvre de multiples activités illicites.



Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. | Visactu

Vol de mots de passe

En France, les actes les plus fréquents sont les vols de mots de passe (14 % des cas) et la fraude à la carte bancaire (10 % des cas). Mais entre les faits recensés et la réalité, il est très difficile de mesurer l'ampleur exacte du phénomène...

Certaines victimes ne savent tout simplement pas (encore) qu'elles ont été volées, d'autres n'ont pas porté plainte et ont préféré payer une rançon (parfois quelques centaines d'euros) pour récupérer des photos intimes par exemple.

Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. Elle en a recensé 291 000 pour le seul mois de novembre 2016 contre 1 461 000 en janvier 2015.

Gare aux malwares

Par contre, le nombre de nouveaux malwares explose. Ces logiciels malveillants qui accèdent à l'appareil d'un utilisateur à son insu (logiciel espion, virus, cheval de Troie, rootkits, etc.) dans le but de dérober des données sont partout.

Symantec dénombrait 20 millions de nouveaux malwares (et variantes) chaque mois début 2016, un chiffre qui a bondi en fin d'année pour atteindre les 96,1 millions en novembre et 71,2 millions de nouveaux malwares détectés en décembre.

Les vols de données de personnes en hausse

En novembre 2016, Symantec estimait qu'un email sur 85 contenait un malware, qu'un email sur 2 620 était une tentative de phishing (l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, mots de passe, etc.) et que plus de la moitié des emails (54,3 %) étaient non sollicités (spam).

En 2015, elle estimait que 429 millions de personnes dans le monde s'étaient faites voler des données personnelles, un chiffre en hausse de 23 % par rapport à l'année précédente.

Original de l'article : La cybercriminalité en hausse en France et dans le monde

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 de formation, de sensibilisation ou d'audits 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

Original de l'article mis en page : La cybercriminalité en hausse en France et dans le monde

Après les ransomwares, la prochaine menace est le

ransomworm



Après les
ransomwares,
la prochaine
menace est
le
ransomworm

Plusieurs spécialistes de la sécurité informatique sont formels les ransomwares vont évoluer pour s'en prendre au réseau à travers des vers.

Star de l'année 2016 dans le domaine de la sécurité informatique, le ransomware entend bien continuer sa progression et sa malfaisante économie. Pour mémoire, le groupe Symantec Security Response a recensé une moyenne de 4000 attaques quotidiennes en 2016. Aux Etats-Unis, les rançongiciels ont coûté 209 millions de dollars aux entreprises au 1^{er} trimestre 2016, constate le FBI.

Face à ce pactole, les cybercriminels vont redoubler d'ingéniosité prévoit les spécialistes de la sécurité. Interrogé par nos confrères de *MIS-Asia*, Corey Nachreiner, directeur technique de Watchguard Technologies, estime que 2017 va voir « *l'arrivée du premier ransomworm permettant une propagation plus rapide du rançongiciel* ». Imaginer la combinaison d'un Locky avec des vers connus comme CodeRed, SQL Slammer ou le plus récent et encore actif Conficker. « *Après avoir infecté une victime, la charge utile va se copier inlassablement sur chaque ordinateur du réseau local* », indique Corey Nachreiner. Et de pronostiquer « *que vous croyiez ou non à ce scénario, les cybercriminels y pensent déjà* ». Un avis partagé par Nik Poltar, CEO et fondateur d'Exabeam. « *Le ransomware constitue un gros business pour les pirates et le ransomworm peut garantir des revenus récurrents. En clair, il chiffre vos dossiers, vous payez pour les récupérer mais au passage il vous laisse des cadeaux empoisonnés.* »

Une première alerte avec Zcryptor

Et le mal a commencé. Microsoft a découvert au mois de mai dernier, une souche de ransomware baptisé Zcryptor, qui se comporte comme un ver. C'est-à-dire qu'il est capable de se déplacer d'un ordinateur Windows à un autre via des supports externes (clés USB, disque dur externe, etc.) ou des disques réseaux. A l'époque, Michael Jay Villanueva, un chercheur de Trend Micro, soulignait que « *ce ransomware est un des rares à être en mesure de se diffuser par lui-même. Il laisse une copie de lui-même sur les disques amovibles, rendant l'emploi des supports USB risqué* »...[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 de formation, de sensibilisation ou d'audits 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Après les ransomwares, la prochaine menace est le ransomworm

La Russie crée des unités d'élite de pirates informatiques



La Russie crée
des unités
d'élite
de pirates
informatiques

La Russie s'appuie sur les médias sociaux pour appeler de jeunes recrues à intégrer des « escadrons scientifiques » capables d'accéder à des systèmes et réseaux, à l'insu des cibles. Accusée par les États-Unis d'avoir influencé l'élection américaine de novembre à travers des opérations de piratage informatique, la Russie a accéléré ses recrutements de pirates bien avant ces événements, rapporte le *New York Times* en référence à une enquête du site d'information russophone Meduza. En plus de recruter dans les écoles d'ingénieurs, Moscou diffuse depuis plusieurs années des annonces sur les médias sociaux à l'attention d'étudiants et de programmeurs professionnels. Des hackers ayant maille à partir avec la justice sont également ciblés, selon Meduza.

L'une de ces annonces a été publiée sur le réseau social russe V Kontakte. Dans le spot vidéo ci-dessous, on devine un homme disposant d'une arme et d'un ordinateur portable. On peut y lire ce message : « si tu es diplômé de l'enseignement supérieur, si tu es un spécialiste des technologies, nous t'offrons des opportunités, des équipements techniques de pointe, des capacités de calcul puissantes, du matériel dernier cri, un véritable entraînement au combat ». Sans oublier le logement tout confort.

Former des « escadrons scientifiques »

Dans une autre annonce citée dans l'enquête, les autorités russes sont à la recherche d'informaticiens ayant des connaissances des « *patches, vulnérabilités et exploits* », explique Meduza, le site d'information russophone basé à Riga (Lettonie). La recherche de talents ne s'arrête pas là. Moscou se tournerait également vers des « *hackers ayant des problèmes avec la loi* ». Le gouvernement russe leur proposant une remise de peine en échange de leur engagement au service de la Russie...[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 de formation, de sensibilisation ou d'audits 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Comment la Russie crée des unités d'élite de pirates informatiques

L'association Donne-Moi un Logement victime d'un piratage informatique



L'association
Donne-Moi un
Logement victime
d'un piratage
informatique

Fin décembre, l'association limousine Dessine-moi un logement (DML) a été victime d'un pirate informatique qui s'est attaqué à sa boîte mail.

Ce dernier a pris le contrôle de la messagerie de sa coordinatrice et a récupéré les contacts de l'association.

Des messages ont été envoyés implorant de l'aide et parlant de « situation délicate » et d'« affaire confidentielle ».

Le pirate demande d'envoyer en urgence des recharges PCS Mastercard, un moyen de paiement très prisé des escrocs. Il ne faut évidemment pas répondre à ce message.

L'association DML, spécialisée dans le logement social d'urgence, déplore cette attaque au moment des fêtes de fin d'année et doit maintenant entièrement reconstituer son carnet d'adresses électroniques.

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 de formation, de sensibilisation ou d'audits 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : L'association Donne-Moi un Logement victime d'un piratage informatique – Limoges (87000) – Le Populaire du Centre

Le site du FBI victime d'une faille Zero Day



Un pirate du nom de Cyberzeist s'est introduit, fin décembre, sur un serveur du site du FBI. Il aurait exploité une faille zero day du système de gestion des contenus (CMS) du site....[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 de formation, de sensibilisation ou d'audits 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 sur cette page.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Un logiciel malveillant russe découvert dans un ordinateur américain



Un logiciel
malveillant
russe
découvert
dans un
ordinateur
américain

Au lendemain de la passe d'armes diplomatique entre les Etats-Unis et la Russie, une entreprise américaine a fait savoir qu'un logiciel malveillant avait été découvert dans un de ses ordinateurs. Les autorités ont été alertées.

Nouvel élément dans la « guerre » que se mènent les Etats-Unis et la Russie ces derniers jours. Un programme malveillant associé à l'opération de piratage informatique russe, surnommée Grizzly Steppe par l'administration Obama, a été détecté dans un ordinateur portable lié à une compagnie d'électricité de l'Etat du Vermont. Celui-ci n'était cependant pas connecté au réseau électrique, a fait savoir l'entreprise Burlington Electric Department (BED).

« Nous avons pris aussitôt des mesures pour isoler l'ordinateur portable et avons alerté les autorités fédérales au sujet de la découverte », a dit l'entreprise BED, compagnie qui distribue l'électricité à Burlington dans le Vermont. « Notre équipe coopère avec les autorités fédérales pour remonter la piste de ce programme malveillant et empêcher toute autre tentative visant à s'introduire dans les ordinateurs du réseau électrique. Nous avons informé les autorités de l'Etat et coopérerons pleinement à l'enquête », a-t-elle ajouté.

Un seul cas connu

Le département américain de la Sécurité intérieure avait informé les compagnies d'électricité, jeudi 29 décembre, de l'existence du programme malveillant utilisé dans Grizzly Steppe. « Nous avons rapidement passé au crible l'ensemble des ordinateurs de notre système. Nous avons détecté le programme malveillant dans un seul ordinateur portable de Burlington Electric Department, non relié à la grille électrique de notre société », a indiqué la BED...[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 de formation, de sensibilisation ou d'audits 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



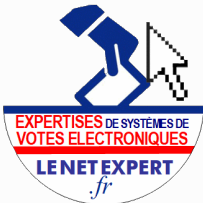
[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Cyberattaque : un logiciel malveillant russe découvert dans un ordinateur américain – LCI

Sécurité des vote électronique en France, comme aux USA ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITÉ	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI vous informe UNE CARTE BANCAIRE ANTI-FRAUDE ? LCI		Sécurité des vote électronique en France, comme aux USA ?			

L'année 2017 sera une grosse année de scrutins, avec l'élection présidentielle en avril-mai et les législatives en juin. Et comme depuis une dizaine d'années qu'un ministre de l'Intérieur, Nicolas Sarkozy, a poussé l'introduction d'ordinateurs de vote en France, des communes vont encore obliger leurs électeurs à voter sur ces machines dont ils ne peuvent contrôler eux-mêmes l'intégrité (en 2012, une soixantaine de communes pour 1,5 million d'électeurs).



Photo: machine à voter utilisée à Stains (Seine-Saint-Denis) aux élections départementales le 22 mars 2015. Chris93/Wikimedia Commons/CC by-sa

Un député socialiste, Sébastien Pierratras, vient à cette occasion de poser au gouvernement une question écrite sur « la sécurisation du vote électronique ». Il demande notamment :

« Au-delà d'un risque connu sur la fiabilité des machines et sur la difficulté de recueillir les voix, la menace de piratage informatique par des puissances étrangères est hélas d'actualité. Si la menace concerne principalement les partis politiques, à l'instar du piratage des ordinateurs du Parti démocrate aux États-Unis, la possibilité d'une attaque des machines à voter n'est plus à exclure. Aussi, il souhaiterait savoir ce que le ministre de l'Intérieur, en charge des élections, compte mettre en place pour assurer la sécurisation du vote lors des élections présidentielle et législatives 2017 et s'il envisage de recourir à un moratoire sur l'utilisation de ces machines électroniques au nom d'un principe de précaution. »

Une position oubliée du PS en 2007

Cette question a été repérée par Nextinpact – qui ironise sur le moratoire « pourtant en vigueur depuis quasiment dix ans », mais il ne s'agit que d'un moratoire sur l'installation du vote électronique dans de nouvelles communes, pas sur son usage dans les villes où il est déjà en place, si c'est dans ce sens que l'entend le député.

Le Parti socialiste, qui en 2007 (quand François Hollande en était premier secrétaire) demandait la suspension du vote électronique, l'a maintenu contre vents et marées depuis son retour au pouvoir en 2012, et indiqué en 2014 encore sa position: ni extension ni abandon (une commune peut choisir de revenir au vote papier, mais au niveau national rien n'est imposé). Donc en 2017, ce sera, encore, circolez il n'y a rien à voir.

La question du député (publiée le 27 décembre) fait référence au piratage du parti démocrate aux États-Unis, en pleine actualité puisque c'est une des raisons de l'expulsion de 35 diplomates russes que vient de décider Barack Obama.

L'opacité du vote électronique en soi est aussi un problème crucial: avant l'élection de novembre aux États-Unis, un informaticien spécialiste de la sécurité, Bruce Schneier, mettait en garde contre les risques de piratage des machines de vote électronique.

USA: toutes les machines peuvent être piratées

Un reportage de Pixels/Le Monde, depuis le Chaos Computer Congress cite deux chercheurs de l'université du Michigan, Alex Halderman et Matt Bernhard, qui ont participé aux recomptages de certains États après le scrutin. S'ils pensent, sans en être certains, que le vote de novembre n'a pas été piraté, ils pointent les nombreuses vulnérabilités du système de vote américain:

- « Première faiblesse : les machines à voter. Plus de 50 modèles différents existent et, selon les chercheurs, toutes peuvent être piratées. De nombreux machines à voter ont été étudiées, par des chercheurs indépendants, et dans tous les cas, il a été prouvé que la machine était vulnérable à l'injection de programmes informatiques malveillants faussant les résultats », explique M. Halderman.
- Les responsables des élections objectent que ces machines ne sont pas connectées à Internet et sont donc protégées. Cela ne fait aucune différence, explique M. Bernhard, puisque est insérée dans chaque machine, et avant chaque scrutin, une carte mémoire contenant les paramètres du vote. C'est aussi dans cette carte que sont stockés les résultats. Or, les ordinateurs qui paramètrent ces cartes sont fréquemment connectés à Internet. »
- Autre faiblesse, l'absence de contrôle a posteriori: plus de 70% des votes aux États-Unis ont une trace en papier. « Il faudrait comparer les votes contenus dans les cartes mémoires et la trace en papier, mais malheureusement la plupart des États ne le font pas. « Un peu comme en France: le meilleur moyen de prétendre que le vote électronique a bien marché, c'est de ne surtout pas vérifier après coup.[lire la suite]

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

Délégation n° 2018-371 du 21 octobre 2018 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

Vous avez un doute sur la sécurité de vos machines à voter ?

Vous souhaitez un expert indépendant spécialisé en votes électroniques pour expertiser le système de vote électronique que vous avez choisi ?

Nous pouvons expertiser leur sécurité en rapport avec la délibération de la CNIL n° 2018-371 du 21 octobre 2018.

Contactez-nous

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

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

Vous souhaitez organiser des élections par voie électronique ?

Cliquez ici pour une demande de chiffrage d'expertise



Vos expertises seront réalisées par **DENIS JACOPINI** :

- « Expert en Informatique assermenté et indépendant ;
- « spécialisé dans la sécurité (diplômé en cybersécurité et certifié en Analyse de risques sur les Systèmes d'Information = ISO 27005 Risk Manager «) ;
- « ayant suivi la formation délivrée par la CNIL sur le vote électronique ;
- « qui n'a aucun accord ni intérêt financier avec les sociétés qui créent des solutions de vote électronique ;
- « et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi respecte l'ensemble des conditions recommandées dans la Délibération de la CNIL n° 2018-853 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybersécurité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l'article mis en page : Vote électronique: en France, aux USA, tout baigne? Hum... – ZDNet

Des sites de piratage bientôt bannis du net par les USA ?



Des sites de piratage bientôt bannis du net par les USA ?

Les États-Unis ont toujours pris très au sérieux les menaces de la cybercriminalité, que ce soit à l'égard de l'économie du pays ou bien à l'égard de la sécurité nationale.

L'Oncle Sam ne lésine pas sur les moyens pour traquer sans relâche les présumés pirates informatiques. Tout récemment, le gouvernement américain a rendu publique la liste regroupant des sites considérés comme ayant des liens à des affaires de piratage.

Au fil des années, de nouvelles méthodes de piratage, plus sophistiquées les unes que les autres, apparaissent. Alors, *aux grands maux les grands remèdes* ! Des trackers notoires sont depuis des années dans le collimateur des États-Unis. C'est le cas, parmi tant d'autres, de **The Pirate Bay** ou **ExtraTorrent**. La Maison Blanche, selon des sources plausibles, inclut également dans sa liste de sites à abattre certains hébergeurs de fichiers. Parmi les noms cités figurent notamment *Rapidgator*, mais aussi *Uploaded*. Mais ces plateformes sont déjà connues, ou du moins, soupçonnées d'être mêlées à des activités d'espionnage. Ce qui est surprenant dans cette affaire, c'est surtout le fait que les États-Unis se penchent aussi sérieusement sur des sites de ripping tels que YouTube-MP3.

Jusqu'à preuve du contraire, les sites européens ne sont pas dans le collimateur des États-Unis

C'est en tout cas ce que laissent entendre des pistes sérieuses qui se penchent sur la cybercriminalité. Ce serait vraiment sidérant de la part du gouvernement américain puisqu'il n'y a pas un seul pays européen où **les sites pirates ne pullulent pas**. En France, pour des raisons qu'on ne connaît pas, Zone-Téléchargement ne figure pas dans la liste noire des États-Unis. À noter tout de même que cette plateforme fait partie des plus gros acteurs du marché français.

Un grand nombre de sites de streaming sont **également dans le viseur de la Maison Blanche**. C'est le cas notamment de *Putlocker*, *Primewire* ou encore *123movies*... Comme pour la drogue, une grande partie des moyens financiers déployés par le gouvernement américain est destinée à la répression.

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 de formation, de sensibilisation ou d'audits 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les États-Unis révèlent les noms des sites de piratage qu'ils souhaitent bannir du net – MeilleurActu