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 SYSTÈMES DE VOTES ELECTRONIQUES 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

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

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

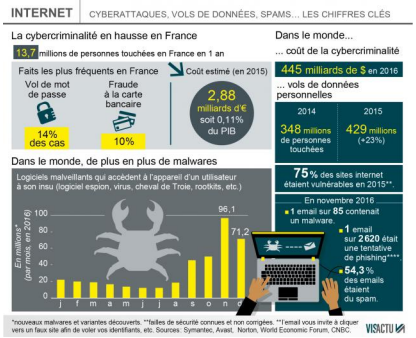
---

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 personnelles 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

---

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

---

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 médiaux 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 évènements, 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 Vkontakte. Dans le spot vidéo ci-dessous, on devine un homme diposant 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 *« patchs, 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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

---

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.

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

Contactez-nous

Réagissez à cet article

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 Pietrasanta, 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 recompter 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 ministère 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, circuler 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 Etats 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 nombreuses 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 Etats-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 Etats 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
Délibération n° 2010-371 du 21 octobre 2010 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° 2010-371 du 21 octobre 2010.
Contactez-nous
[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 solution 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 rapport 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 spécialistes du vote électronique assurent qu'« Il est facile de pirater l'élection américaine »

Des spécialistes du vote électronique assurent qu'« il est facile de pirater l'élection américaine »

Deux chercheurs de l'université du Michigan ont participé aux recomptages dans certains Etats après le scrutin de novembre.

L'élection présidentielle américaine de novembre a-t-elle été piratée ? Depuis l'intrusion de hackers dans les serveurs du Parti démocrate, la question taraude les Etats-Unis. Sans aller aussi loin, le président Barack Obama a dénoncé des *« cyberactivités qui avaient pour but d'influencer l'élection »*. Sur cette base, il a fait déclarer, jeudi 29 décembre « persona non grata », aux Etats-Unis, trente-cinq diplomates de l'ambassade de Russie à Washington et du consulat à San Francisco.
Pour leur part, après avoir participé aux opérations de recomptage des voix qui ont eu lieu dans certains Etats dans les semaines suivant le scrutin, Alex Halderman et Matt Bernhard, chercheurs de l'université du Michigan, spécialistes du vote électronique, en sont arrivés à la conclusion que l'élection n'a probablement pas été piratée. Mais que celle de 2020 pourrait bien l'être. C'est ce qu'ils ont expliqué lors du Chaos Computer Congress, grand-messe des hackers, qui se tient du 27 au 30 décembre à Hambourg, en Allemagne.

« Nous savions que des attaques sans précédent avaient été lancées pour interférer dans l'élection. Nous savions aussi qu'il était possible pour un attaquant de changer suffisamment de votes dans les machines à voter pour changer le résultat du scrutin », rappelle M. Halderman. Mais *« le recomptage a conforté l'idée que l'élection a été fiable »,* déclare M. Bernhard.

« Il est plus facile de pirater l'élection présidentielle américaine que je ne le pensais », reconnaît toutefois M. Halderman, qui avertit : *« Même si l'élection de 2016 n'a pas été piratée, l'élection de 2020 pourrait bien l'être. Nous faisons face à de plus en plus d'attaquants étatiques. Nous avons besoin de défenses efficaces pour les empêcher de mettre à mal le cœur de notre démocratie. »*

Quels contrôles sur d'éventuels piratages ?

M. Halderman, qui tente depuis des années de rendre le vote électronique plus fiable, a été convié, un peu plus d'une semaine après l'élection, à participer à une conférence téléphonique avec l'équipe de campagne de Hillary Clinton. Lors de cette discussion, à laquelle participait John Podesta, le directeur de campagne de Mme Clinton, plusieurs universitaires ont tenté de convaincre les vaincus de demander un recomptage des voix.

« De manière choquante, même dans ces circonstances, aucun Etat n'allait vérifier les traces en papier du scrutin électronique pour savoir si piratage il y avait », raconte M. Halderman, aux yeux de qui seule cette comparaison entre votes décomptés électroniquement et traces papier de ces votes pouvait permettre de s'assurer des résultats.

Mais l'équipe de campagne de la candidate démocrate est plus que réticente. Comme le temps presse – la loi fédérale impose aux Etats de finaliser leurs résultats le 13 décembre – l'un des collègues de M. Halderman suggère une alternative : demander à la candidate du Parti écologiste, Jill Stein (elle a obtenu un peu plus de 1 % des voix au niveau national), de requérir un recomptage dans certains Etats où le résultat a été très serré.

Où des contrôles ont-ils été réalisés ?

Les chercheurs et les équipes de Mme Clinton identifient trois Etats où un recomptage pourrait être intéressant : le Wisconsin, le Michigan et la Pennsylvanie. Ces trois Etats du nord du pays, où Mme Clinton était censée l'emporter, ont été arrachés par M. Trump. Ils comptent pour 46 grands électeurs, soit davantage que l'écart qui sépare les deux candidats dans le collège électoral. M. Trump a conquis ces Etats avec moins de 0,8 point d'avance, soit moins de 78 000 votes en tout. Autrement dit, si ces trois Etats avaient basculé du côté de Mme Clinton, cette dernière l'aurait emporté.

Les avocats de M. Trump ayant multiplié les recours, aucun recomptage total ne sera finalement réalisé dans aucun de ces trois Etats. En Pennsylvanie, il n'a jamais vraiment commencé. Au Michigan, il aura duré trois jours. Cette comparaison entre résultats et traces écrites a tout de même permis, selon M. Halderman et M. Bernhard, d'écarter le spectre d'une fraude généralisée. Aucune preuve de trucage n'a été découverte…[lire la suite]

Original de l'article mis en page : « Il est facile de pirater l'élection américaine », assurent des spécialistes du vote électronique

---

Le réseau électrique américain pénétré par des pirates Russes

Le réseau électrique américain pénétré par des pirates Russes

Washington – Des pirates informatiques russes sont parvenus à pénétrer le réseau électrique américain via un fournisseur du Vermont, une cyberattaque sans conséquence sur les opérations de cette entreprise mais qui a pu révéler une « vulnérabilité », rapporte vendredi le Washington Post.

« Un code associé à l'opération de piratage informatique baptisée Grizzly Steppe par l'administration Obama a été détecté à l'intérieur du système d'un fournisseur d'électricité du Vermont », écrit le quotidien sur son site Internet, sans indiquer de date.
Se référant à des responsables américains non identifiés, il souligne que ce si code *« n'a pas été activement utilisé pour perturber les opérations du fournisseur* […] *la pénétration du réseau électrique national est importante parce qu'elle représente une vulnérabilité potentiellement grave ».*
Les autorités américaines ignorent à ce stade quelles étaient les intentions des Russes, poursuit le *Washington Post*, supputant qu'ils pourraient avoir tenté de porter atteinte aux activités du fournisseur –non identifié par les sources du journal– ou qu'il pourrait simplement s'agir d'un test de faisabilité.
Selon le journal, le Vermont compte deux importants fournisseurs d'électricité : Green Mountain Power et Burlington Electric.
Les pirates russes auraient envoyé des emails pour piéger les destinataires, leur faisant révéler leurs mots de passe.
En décembre 2015, 80 000 habitants de l'ouest de l'Ukraine avaient été plongés plusieurs heures dans le noir à la suite d'une cyberattaque d'une ampleur inédite. Les Russes avaient été désignés comme en étant les auteurs, ce qu'ils avaient nié…[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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

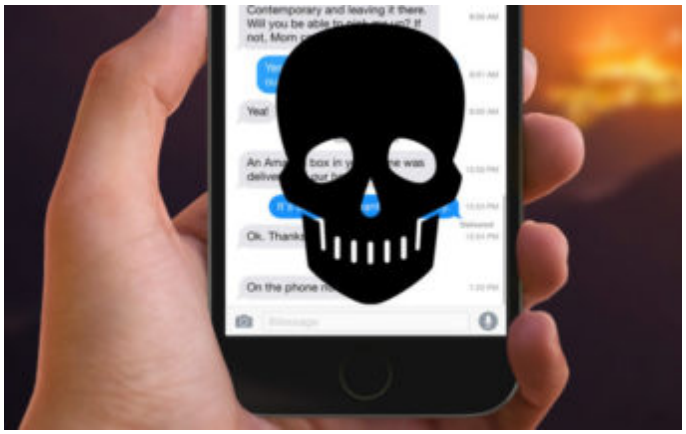
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Des pirates russes ont pénétré le réseau électrique américain | Le Devoir

---

Alerte : Un hack par MMS bloque l’application Messages de votre iPhone



Alerte : Un hack par MMS bloque l’application Messages de votre iPhone

---

Un nouveau hack iPhone permet de bousiller à distance l'application Messages, qui permet d'envoyer et de recevoir les textos et MMS. Il s'agit d'un fichier .vcf (une fiche contact) corrompue, qui semble complètement faire flipper votre application Message, qui freeze, avant devenir complètement inutilisable. Même un redémarrage de l'iPhone ne vient pas à bout du problème qui touche tous les iPhone sous toutes les versions d'iOS 9 et d'iOS 10, y compris les versions bêta.

Dans la vidéo Youtube que vous pouvez voir en fin d'article, @Vicedes3 montre un nouveau hack à distance des iPhone assez embarrassant. En fait, l'ouverture d'une fiche contact viciée envoyée par MMS suffit à rendre l'application Messages, vitale pour envoyer et recevoir des messages, complètement inutilisable. Le redémarrage du terminal, voire même un hard reset n'y feront rien.
Nous vous recommandons donc de ne pas vous amuser à l'essayer sur votre iDevice. Pour que vous compreniez ce qui se passe, ce fichier .vcf est en fait extrêmement lourd, et excède des limites de taille qu'Apple a tout simplement omis de définir. Du coup, ce fail devrait être relativement simple à corriger. Apparemment, toutes les versions d'iOS 9 et 10, même les bêtas les plus récentes sont concernées par ce problème.
Personne n'ayant eu auparavant l'idée d'exploiter la taille des fiches contact, la faille serait ainsi tout simplement passée inaperçue pendant tout ce temps. La seule manière de réellement se protéger, c'est de ne surtout pas ouvrir les fiches contact reçues depuis des sources autres que vos contacts de confiance. Ce n'est pas en soit un virus, donc si vous le recevez, c'est que quelqu'un vous fait une mauvaise blague…[lire la suite]

Original de l'article mis en page : iPhone : ce nouveau hack par MMS bousille votre application Messages

---

Le boîtier connecté d'Amazon,

témoin-clé d’une affaire de meurtre aux États-Unis ?

Le boîtier connecté d’Amazon, témoin-clé d’une affaire de meurtre aux États-Unis ?

CLUEDO. Qui a tué le docteur Lenoir ? À l’heure de la maison connectée, il suffira peut-être de le demander aux objets domotiques qui enregistrent silencieusement nos faits et gestes, et pourraient ainsi contribuer à blanchir ou accabler un suspect aux yeux de la justice.…[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.

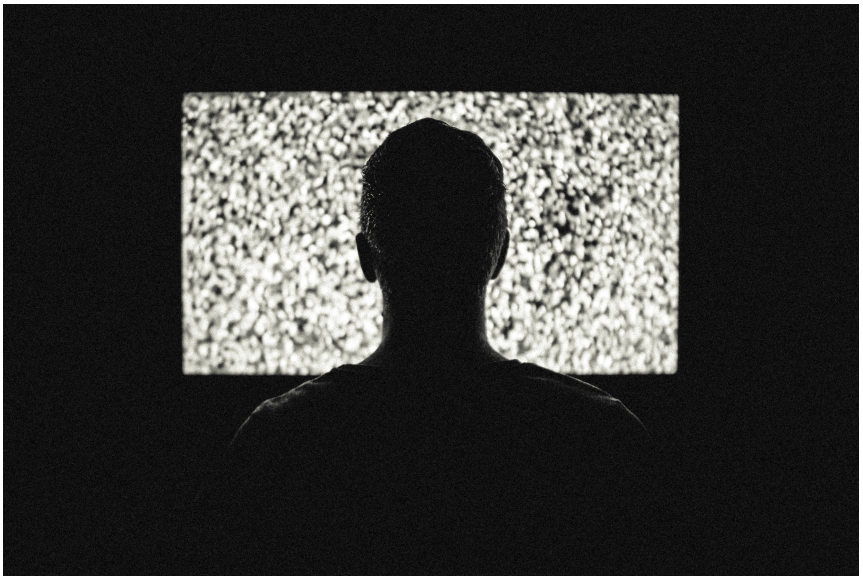
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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

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

Contactez-nous

Réagissez à cet article

Ça y est, les ransomwares qui désactivent les téléviseurs connectés arrivent !



Ça y est, les ransomwares qui désactivent les téléviseurs connectés arrivent !

L'infection d'un téléviseur LG par un malware, racontée sur Twitter par un ingénieur informatique, rappelle la vulnérabilité des téléviseurs connectés face à ces logiciels malveillants. Et la difficulté de s'en débarrasser.

Les réserves des experts en sécurité informatique au sujet des téléviseurs connectés fonctionnant avec Android, qui seraient vulnérables aux mêmes malwares que ceux diffusés sur les smartphones, remontent à loin. L'incident raconté par Darren Cauthon prouve que ces craintes étaient justifiées.

À Noël, cet ingénieur informatique a découvert que le téléviseur connecté LG de l'un de ses proches était victime d'un ransomware que l'on trouve plus communément sur smartphone. Ce dernier est connu sous le nom de Cyber.Police, FLocker, Frantic Locker ou encore Dogspectus.

Le téléviseur aurait été infecté par une application de streaming. À la moitié du film, l'appareil s'est arrêté pour finalement rester bloqué sur la page d'accueil du ransomware. L'ingénieur ne sait néanmoins pas si l'application venait du PlayStore ou d'un tiers. Ce qui pourrait, dans le cas d'une application de piratage, expliquer que le ransomware se soit introduit si facilement sur le téléviseur.

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Un ransomware désactive un téléviseur connecté LG — Tech — Numerama