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

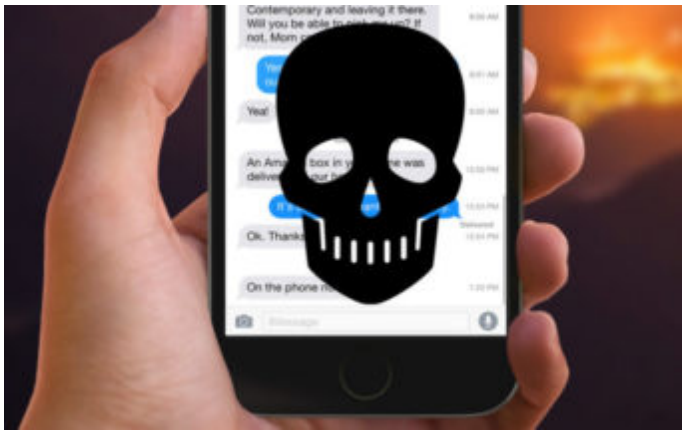
Contactez-nous

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.

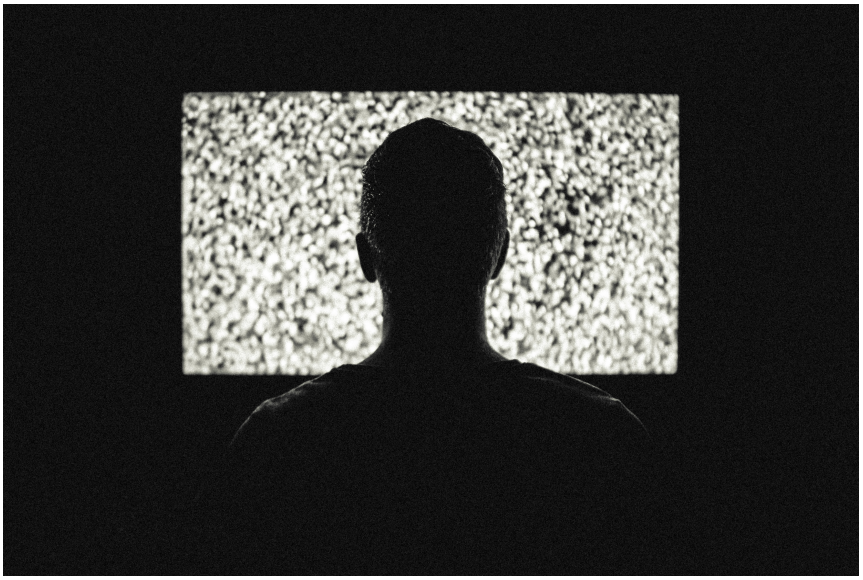
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation 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

Et si je vous remerciais par avance pour vos voeux 2017 ?

	Et si je vous remerciais par avance pour vos voeux 2017 ?

Avignon, le 29/12/2016
A force de voir les rayons remplis de cartables avant même la fin de l'année scolaire et des rayons de guirlandes et de sapins vierges dès la fin de l'été, j'ai souhaité garder le rythme et, pour ne pas vous choquer, attendre un peu pour vous souhaiter de joyeuses pâques mais déjà vous remercier pour les vœux 2017 que vous allez dans les 30 prochains jours m'envoyer.
Pour terminer, sans pour autant critiquer ni protester contre les envois en masse de messages tous aussi impersonnels les uns que les autres, je tiens par contre du coup, à vous envoyer ce message personnalisé. La preuve, il n'est que pour vous.

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

Quelles tendances en 2017 pour la sécurité du Cloud ?

Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ». Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[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 DIRTEF 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 : Sécurité du Cloud : quelles tendances en 2017 ? – Globb Security FR

Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

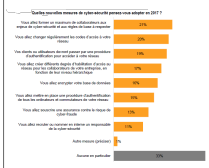
À l'exception des grands groupes, la majorité des entreprises françaises sous-estiment les risques de cyber-attaque ; moins de 4 sur 10 d'entre elles décideurs considèrent comme « important », ou « très important », le risque que leur société subisse une cyber-attaque ces prochaines années… et ce, alors que 52% des entreprises ont déjà été piratées. C'est ce que montre une enquête réalisée par le cabinet Denjean & Associés en partenariat avec Gan Assurances

Les décideurs d'entreprise se font de fausses idées sur la cyber-fraude. Plus de trois sur quatre sous-estiment la vitesse de propagation de ce fléau dans l'Hexagone, pensant que le nombre des cyber-fraudes recensées en France n'a augmenté « que » de 10% ou de 25% en 2015, alors qu'il a crû de 50% ! (Source : Anssi, Agence nationale de sécurité des systèmes d'information). Questionnés sur les cibles visées en priorité par les pirates, 50% des décideurs citent les multinationales ; et pour 23% des répondants, les organismes publics constituent le premier choix des hackers. Seulement 20% des personnes interrogées connaissent la bonne réponse : les PME concentrent dans notre pays près de 80% des cyber-attaques (source : Syntec).

Globalement, 70% des entreprises s'estiment bien protégées contre la cyber-fraude. Une statistique qui recouvre des disparités : 100% des grands groupes affichent leur confiance dans leurs process de cybersécurité, tandis que 58% des TPE et environ 75% des PME et des ETI se jugent bien protégées.

Quelles bonnes pratiques ?

Les entreprises ayant adopté une politique de cybersécurité ont mis en place, en moyenne, trois bonnes pratiques. Les plus répandues sont le changement régulier par l'entreprise des codes d'accès à son réseau (mesure existant dans 56% des structures), et l'instauration en son sein d'une procédure d'authentification de tous les ordinateurs et commutateurs (53% des entreprises). La formation interne aux enjeux et aux précautions de base en matière de cybersécurité, et la création de différents degrés d'accès au réseau pour les collaborateurs selon leur niveau hiérarchique (respectivement pratiquées par 45% et 44% des sociétés) se disputent la troisième place sur le podium.
Deux entreprises sur trois comptent adopter en 2017 de nouvelles mesures pour lutter contre le piratage informatique qui se décomposent comme l'indique l'infographie ci-dessous.



90% des entreprises françaises sont disposées à investir chaque année pour se protéger efficacement contre la cyber-fraude, et 60% sont même prêtes à y consacrer un budget supérieur ou égal à 1% de leur chiffre d'affaires. Parmi les différentes catégories d'entreprises, les PME et les ETI se montrent les plus enclines à réaliser un effort financier conséquent : les trois-quarts d'entre elles acceptent de dépenser chaque année pour leur cybersécurité entre 1% et 2% de leur chiffre d'affaires.
Si l'on exclut les dirigeants de très petites structures, peu ou pas du tout concernés par ces sujets, les décideurs apparaissent bien conscients des nouveaux risques encourus par les entreprises, et décidés à les combattre. En effet, 66% des décisionnaires indiquent qu'ils se préoccuperont au cours des trois années à venir de lutter contre les « ransomwares » ; 70% disent qu'ils s'attacheront à sécuriser les données mises sur le cloud ; et 70% déclarent qu'ils veilleront à prévenir les risques liés aux objets connectés…

Original de l'article mis en page : Les entreprises françaises sous-estiment les risques de cyber-attaque

---

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 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

100 000 emplois en Tunisie grâce aux smart-cities et objets connectés

100 000 emplois en Tunisie grâce aux smart-cities et objets connectés

La Tunisie se met au numérique pour son développement économique. Avec la régression de l'une des principales sources de revenu qu'est le tourisme, la Tunisie ambitionne d'optimiser son économie avec le projet « Tunisie Numérique 2020 ».
Le numérique, dans l'économie de la Tunisie, représente déjà 11% de taux de croissance annuelle et 7% du PIB, devant le secteur du tourisme. Avec les initiatives privées, le gouvernement travail à faire progresser ce chiffre.
« C'est la première fois que le secteur public se dit : « Je ne vais pas tout faire tout seul et il y a des secteurs que je connais mal », « De notre côté, nous sommes conscients qu'après la révolution, le rôle de la société civile devient plus important et c'est pourquoi nous mettons notre savoir-faire au service de la Tunisie », a expliqué l'entrepreneur, éditeur du logiciel Badredine Ouali, qui préside également le partenariat public-privé Smile Tunisia.
D'ici 2020, le gouvernement tunisien vise créer 100 000 emplois en misant sur les smart-cities ou les objets connectés.

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 : Tunisie: 100 000 emplois grâce aux smart-cities et objets connectés | Africa Top Success

Tendances actuelles et émergentes pour la cybersécurité en 2017

Tendances actuelles et émergentes pour la cybersécurité en 2017

Original de l’article mis en page : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 – Global Security Mag Online