

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.



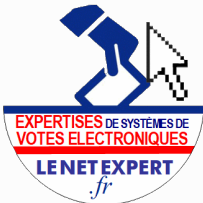
[Contactez-nous](#)



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		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 Etats-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 NextImpact – 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, circulez il n'y a rien à voir.

La question du député (publiée le 27 décembre) fait référence au piratage du parti démocrate aux Etats-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 Etats-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 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 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 assurant 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° 2010-371 du 21 octobre 2010 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

Le réseau électrique américain pénétré par des pirates Russes



Le réseau
électrique
américain
pénètre
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.



[Contactez-nous](#)

Réagissez à cet article

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.



[Contactez-nous](#)

Réagissez à cet article

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.



[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 renvoient 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 taillés 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 ; (Présentation du séminaire n°102 de 2016 à 2018)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



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

Denis JACOPINI



vous informe

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

À l'occasion des grands groupes, la majorité des entreprises françaises sous-estiment les risques de cyber-attaque ; moins de 4 sur 10 d'entre elles déclarent considérer ces « importants », ou « très importants ». 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 des Assurances.

Les décideurs d'entreprise se font de fausses idées sur la cyber-fraude. Plus de trois sur quatre sous-estiment la violence de propagation de ce fléau dans l'Hexagone, pensant que le nombre des cyber-fraudes recensées en France n'a augmenté « que » de 30% ou de 25% en 2013, alors qu'il a crû de 50% ! (Source : Anssi, Agence nationale de sécurité des systèmes d'information). Questionnée sur les cibles visées en priorité par les pirates, 55% des déclarants 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).

Statistiquement, 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 processus de cybersécurité, tandis que 50% des TPE et environ 75% des PME et des ETI se jugent bien protégées.

Deux bonnes pratiques ?

Les entreprises ayant adopté une politique de cybersécurité ont mis en place, en moyenne, trois bonnes pratiques. Les plus répandues sont le chantage régulier par l'entreprise des codes d'accès à son réseau (mesure existant dans 50% des structures), et l'installation en son sein d'une procédure d'authentification de tous les ordinateurs et commutateurs (53% des entreprises). La formation interne aux enjeux et aux implications 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 40% et 40% des sociétés) se situent la troisième place sur le podium. Deux entreprises sur trois comptent adapter en 2017 de nouvelles mesures pour lutter contre le piratage informatique qui se décomposent comme l'indique l'infographie ci-dessous.

50% 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 inclut les dirigeants de très petites structures, peu ou pas de tout concernés par ces sujets, les décideurs apparaissent bien conscients des nouveaux risques encourus par les entreprises, et décidés à les combattre. En effet, 60% des décideurs indiquent qu'ils se préoccuperont au cours des trois années à venir de lutter contre les « rançonnages » ; 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 éditeur : Vous aider à vous protéger des piratages 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'aide 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 Liberté (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement... (Autorisation de la Direction de Travail de l'Emploi et de la Formation Professionnelle n°03 84 93841 86)

Plus d'informations sur : <https://www.le-net-expert.fr/informations-cybersécurité-protection-des-donnees-personnelles>

Le Net Expert
INFORMATIQUE
Cybersécurité & Clouds

Tendances actuelles et émergentes pour la cybersécurité en 2017

Denis JACOPINI
EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ
vous informe

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

Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?



La dernière étude d'IFS sur les défis auxquels les DSI sont confrontés durant la période des fêtes de fin d'années révèle que 76% des sondés se sentent davantage préoccupés à l'approche de cette période et ce, pour plusieurs raisons : la disponibilité du personnel (41% des répondants), les risques de piratage liés à la sécurité IT (31%) ainsi que les besoins IT des collaborateurs travaillant à distance (31% également). Tout cela a un impact certain sur les processus et activités métier.

De tous, les plus inquiets quant à la disponibilité du personnel à la période des fêtes de fin d'année sont les français. 62% d'entre eux déclarent qu'il s'agit de l'une de leurs plus grandes préoccupations au cours de la saison des fêtes de fin d'année. À l'opposé, près de la moitié des répondants américains (48%) citent le piratage informatique.

Du côté des « besoins », 42% des décideurs IT sont en demande d'un budget plus important. La migration vers le Cloud (18%) et le recrutement de personnel IT (16%) sont également cités dans le top 3 de leurs besoins. Par ailleurs, un quart des répondants américains et suédois (respectivement 26% et 25%) souhaitent, à court terme, une accélération de la migration vers le Cloud, alors qu'ils ne sont que 11% et 14% en Australie et Allemagne à privilégier cet enjeu.

« Ce qui ressort clairement de notre étude est que de nombreux décideurs IT ont des craintes légitimes pour la période des fêtes de fin d'année : disponibilité du personnel, risque de piratage informatique, commente Mark Boulton, CMO d'IFS. Il est essentiel que toutes les entreprises, quelle que soit leur taille, se préparent à affronter les problèmes qui pourraient survenir et soient en mesure d'accompagner, à distance, leurs collaborateurs ». L'IoT et la migration vers le Cloud faisant partie des solutions possibles.

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 : Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?

Quels changements en Cybersecurité pour 2017 ?



Quels
changements
en
Cybersecurité
pour 2017 ?

Yahoo, Twitter, Spotify, Amazon, eBay, CNN... l'année 2016 aura été fructueuse en attaques informatiques majeures. Si, les conséquences sont limitées, elles prouvent que les hackers sont tenaces et créatifs. Faut-il s'attendre à un nouveau type d'attaque en 2017 ?

Historiquement, les cyber-pirates ont focalisé leur attention sur les grandes entreprises. Ces sociétés ont donc été les premières à adopter les nouvelles technologies, via des solutions souvent à peine testées. Résultat : elles peuvent plus facilement être compromises, via certaines failles qui n'ont pas encore été repérées par les fabricants. En conséquence, ce sont les grandes sociétés qui attirent les hackers en quête de nouveaux défis et subissent les attaques de grande ampleur.

En parallèle, par effet pyramidal, ces mêmes technologies sont progressivement adoptées par les moyennes entreprises puis, en bas de pyramide, par les PME. Lorsque le deuxième échelon de la pyramide est atteint, les technologies sont plus sécurisées grâce au retour d'expérience. Les hackers les délaissent donc bien souvent pour se concentrer sur des technologies plus récentes.

Mais 2017 devrait marquer un tournant : en effet, ce sont aujourd'hui ces entreprises de taille moyenne qui – dans un souci d'accélérer leur transformation numérique – adoptent en premier les nouvelles technologies. Elles s'équipent donc plus rapidement que les grands groupes – qui ont un processus plus lourd et laisse moins de place à la flexibilité. En adoptant, par exemple, l'IoT et les technologies de l'industrie 4.0, ces sociétés "mid market" sont en train de devenir la cible privilégiée des hackers.

Type d'attaque : Des ransomwares liés à l'IoT

Après des années d'observation, on assiste enfin au déploiement à grande échelle de l'IoT. Chambres froides, kiosques, usines, voitures, et même machines de nettoyage industriel, tout cela sera bientôt connecté dans un souci de performance et de monitoring. Espérons qu'ils soient également sécurisés.

Le déploiement de ces dispositifs connectés n'est pas sans risque : leur intégrité peut être compromise si la sécurité n'est pas pensée d'une nouvelle manière. Certaines rumeurs prétendent même que des hackers se sont déjà servis de l'IoT pour attaquer une entreprise et lui demander une rançon. Nous risquons donc de voir une augmentation de ce type d'attaques dans un avenir proche. Par conséquent, l'année 2017 sera certainement la première où une entreprise admettra de façon publique qu'elle a été confrontée à ces cyber-attaques par rançon....[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 : Cybersécurité : quels changements pour 2017 ?