Utilisez cette carte pour savoir où utiliser votre drone de loisir

	Utilisez cette carte pour savoir où utiliser votre drone de loisir

Cette carte signale toutes les zones de restrictions et dinterdictions…
Le secrétaire d'Etat aux Transports, Alain Vidalies, a annoncé mardi la mise en ligne d'une carte de France interactive représentant les zones interdites ou restreintes pour l'usage de drones de loisir.
La carte est accessible à l'adresse http://www.geoportail.gouv.fr/donnees/restrictions-pour-drones-de-loisir

Outre-mer dans les prochains mois
« A la veille des fêtes de fin d'année, la mise en ligne de cette carte interactive offre une information accessible aux télépilotes pour faire voler leur drone en toute sécurité sur tout le territoire métropolitain », a déclaré Alain Vidalies dans un communiqué.

Cette carte, élaborée par la Direction générale de l'aviation civile (DGAC) avec l'Institut national de l'information géographique et forestière (IGN), définit les zones de restrictions et d'interdictions permanentes en France métropolitaine.
L'outil sera complété, dans les prochains mois, par des cartes des Outre-mer, tandis que l'intégration des zones de restrictions temporaires est à l'étude.

Réagissez à cet article

Original de l'article mis en page : Drones de loisir: Une carte interactive de France pour savoir où les utiliser

En 2017, les pirates informatiques vont mettre les bouchées doubles

En 2017, les pirates informatiques vont mettre les bouchées doubles

Les hackers vont notamment chercher à ébranler la confiance que l'on porte aux données, annonce un rapport de CyberArkBy SHOSHANNA SOLOMON

Les cyber-criminels du monde entier devraient intensifier leur activité l'année prochaine en utilisant l'intelligence artificielle et la manipulation des sources d'information pour créer des attaques plus fortes et plus dévastatrices, mettent en garde les experts de CyberArk.
En infiltrant et en manipulant les sources d'information, les pirates s'efforceront de saper la confiance des gens dans l'intégrité des données qu'ils reçoivent, utiliseront l'intelligence artificielle pour mener des cyber-attaques plus sophistiquées et augmenteront la collaboration entre eux pour déclencher un plus grand désordre, selon les prévisions cybersécuritaires pour 2017.
« L'intégrité de l'information sera l'un des plus grands défis auxquels les consommateurs, les entreprises et les gouvernements du monde devront faire face en 2017, où les informations venant de sources vénérées ne seront plus dignes de confiance », ont déclaré les experts.
« Les cyber-attaques ne se concentreront pas seulement sur une entreprise spécifique, il y aura des attaques contre la société visant à éliminer la confiance elle-même ».
Les attaquants ne se contentent pas d'accéder à l'information : ils « contrôlent les moyens de changer l'information là où elle réside et la manipulent pour les aider à atteindre leurs objectifs », affirment les auteurs.
Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)
Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)
Manipuler l'information – dans une campagne électorale par exemple – peut être un outil puissant. L'altération de contenus inédits, comme les fichiers audio, pourrait conduire à une augmentation des tentatives d'extorsion, en utilisant des informations qui peuvent ne pas être réelles ou prises hors de leur contexte.
« Il sera plus facile que jamais de rassembler des informations réelles volées dans une brèche avec des informations fabriquées, pour créer un déséquilibre ce qui rendra plus difficile pour les gens de déterminer ce qui est réel et ce qui ne l'est pas ».
L'augmentation de l'utilisation mobile, du web et des médias sociaux sont parmi les facteurs clés contribuant à l'augmentation explosive des cyber-menaces, a déclaré MarketsandMarkets, une firme de recherche basée au Texas, dans un rapport. La semaine dernière, Yahoo a subi le plus grand piratage au monde connu à ce jour, dans lequel la société a découvert une violation de sécurité vielle de 3 ans qui a permis à un pirate de compromettre plus d'un milliard de comptes d'utilisateurs.
Le marché mondial de la cyber-sécurité atteindra plus de 170 milliards de dollars d'ici 2020, selon une estimation de MarketsandMarkets, avec des entreprises qui se concentrent globalement sur les solutions de sécurité mais aussi sur les services…[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 : Les pirates informatiques vont mettre les bouchées doubles en 2017 | The Times of Israël

---

Les États peuvent-ils imposer aux FAI une obligation générale de conservation des données ?

Les États peuvent-ils imposer aux FAI une obligation générale de conservation des données ?

Dans un arrêt, la Cour de justice de l'Union européenne considère que les États ne peuvent pas imposer une « conservation généralisée et indifférenciée » des données de connexion. Celle-ci doit se faire de façon «ciblée, limitée et avec des garde-fous.

L'accès aux données de connexion ne peut pas être « open bar ». Tel est, en somme, le sens de l'arrêt que la Cour de justice de l'Union européenne vient de rendre ce mercredi 21 décembre. Pour les magistrats, il n'est pas possible d'imposer aux fournisseurs d'accès à Internet une « *conservation généralisée et indifférenciée* » des données de connexion de leurs clients. Celle-ci doit être extrêmement ciblée et fortement délimitée pour éviter des dérives. Rappel des faits.
C'était le 8 avril 2014. Dans son mémorable arrêt *Digital Rights Ireland*, la Cour de justice de l'Union européenne manifestait sa volonté jurisprudentielle de protéger les droits des internautes, en invalidant la directive européenne de 2006. Celle-ci obligeait les États membres à exiger des opérateurs qu'ils conservent un journal des données de connexion de leurs clients pour que la police et la justice puissent y avoir accès.
S'appuyant sur la Charte des droits fondamentaux de l'Union européenne, la cour jugeait que cette obligation était disproportionnée et offrait un cadre insuffisant pour la protection de la vie privée et des données personnelles des citoyens européens. Grâce à cet arrêt, plusieurs États ont suspendu ou révisé leur législation pour intégrer l'avis de la cour suprême communautaire. D'autres nations ont en revanche choisi de ne pas bouger, à l'image de la France.

CC Harald Deischinger

Sollicité dans le cadre de deux affaires jointes (C-203/15 Tele2 Sverige et C-698/15 Secretary of State for Home Department/Tom Watson e.a), l'avocat général de la Cour de justice de l'Union européenne, le Danois Henrik Saugmandsgaard Øe a considéré au mois de juillet que les États membres avaient bien le droit d'exiger la conservation de toutes les métadonnées mais uniquement s'ils se conforment aux impératifs fixés par l'arrêt *Digital Rights Ireland*.
Une analyse que la Cour de justice de l'Union européenne a refusé de suivre. Dans un arrêt rendu le 21 décembre, l'institution communautaire n'a en effet pas suivi l'avocat général. Elle déclare que les États ne peuvent pas imposer aux fournisseurs d'accès à Internet une obligation générale de conservation de données, que ces données soient relatives au trafic ou qu'elles concernent la localisation. Pour le dire autrement, l'accès aux données n'est plus « open bar »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Les États ne peuvent pas imposer aux FAI une obligation générale de conservation des données – Politique – Numerama

---

Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?

Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?

Suite à une nouvelle panne de courant, la compagnie nationale d'électricité de l'Ukraine enquête pour savoir si une attaque de cyberpirates est à l'origine du problème.
Des experts en sécurité cherchent à savoir si la panne de courant qui a affecté ce week-end certains quartiers de la capitale ukrainienne, Kiev, et la région environnante provient d'une cyberattaque. Si ce dernier point venait à être confirmé, il s'agirait du deuxième black-out causé par des pirates informatiques en Ukraine, après celle qui s'est produite en décembre 2015.

L'incident a affecté les systèmes de commande d'automatisation d'un relais de puissance près de Novi Petrivtsi, un village situé au nord de Kiev, entre samedi minuit et dimanche. Cela a entraîné une perte de puissance complète pour la partie nord de Kiev sur la rive droite du Dniepr et la région environnante…

75 minutes pour rétablir le courant

Les ingénieurs d'Ukrenergo, la compagnie d'électricité ukrainienne, ont commuté l'équipement de commande en mode manuel et commencé à rétablir la puissance par palier de 30 minutes, a dit Vsevolod Kovalchuk, directeur d'Ukrenergo, dans un billet posté sur Facebook. Il a fallu 75 minutes pour restaurer toute la puissance électrique dans les zones touchées de la région, où les températures descendent jusqu'à -9 en ce moment. Une des causes suspectées est « une interférence externe à travers le réseau de données » a déclaré sans plus de précision Vsevolod Kovalchuk. Les experts en cybersécurité de la société étudient la question et publieront très bientôt un rapport.
Parmi les causes possibles de l'accident figurent le piratage et un équipement défectueux, a déclaré Ukrenergo dans un communiqué. Les autorités ukrainiennes ont été alertées et mènent une enquête approfondie. En attendant, les premières conclusions, tous les systèmes de commande ont été basculés du mode automatique au manuel, a indiqué la compagnie.

Un Etat derrière les attaques sophistiquées

Si un piratage venait à être confirmé, ce serait la seconde cyberattaque en un an contre le réseau électrique ukrainien. En décembre dernier, juste avant Noël, des pirates informatiques avaient lancé une attaque coordonnée contre trois compagnies d'électricité régionales ukrainiennes. Ils avaient réussi à couper l'alimentation de plusieurs sous-stations, provoquant des pannes d'électricité qui ont duré entre trois et six heures et touché les résidents de plusieurs régions.
A l'époque, les services de sécurité ukrainiens, le SBU, avaient attribué l'attaque à la Russie. Bien qu'il n'y ait aucune preuve définitive liant ces attaques au gouvernement russe, les cyberattaquants avaient utilisé un morceau de malware d'origine russe appelé BlackEnergy, et la complexité de l'attaque suggère l'implication d'un État. La semaine dernière, des chercheurs du fournisseur de sécurité ESET ont alerté la communauté au sujet d'attaques récentes contre le secteur financier ukrainien menées par un groupe qui partage de nombreuses similitudes avec le groupe BlackEnergy…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une cyberattaque suspectée de causer un black-out en Ukraine – Le Monde Informatique

---

Que nous réserve la CyberSécurité en 2017 ?

	**Que nous réserve la CyberSécurité en 2017 ?**

La fin de l'année c'est aussi et surtout la période des bilans. Dans cet article, nous mettrons en évidence les cinq tendances les plus importantes tendances à venir. Qu'elles se maintiennent ou évoluent durant l'année 2017, une chose est sûre, elles risquent de donner du fil à retordre aux professionnels de la cybersécurité.

1 : intensification de la guerre de l'information
S'il y a bien une chose que la cybersécurité nous a apprise en 2016, c'est que désormais, les fuites de données peuvent être motivées aussi bien par la recherche d'un gain financier ou l'obtention d'un avantage concurrentiel que pour simplement causer des dommages dus à la divulgation d'informations privées. À titre d'exemples, le piratage du système de messagerie électronique du Comité National Démocrate (DNC) américain qui a conduit à la démission de Debbie Wassermann Schultz de son poste de présidente ; ou encore, la sécurité des serveurs de messagerie qui a miné la campagne présidentielle américaine de la candidate Hillary Clinton dans sa dernière ligne droite. Il est également inexcusable d'oublier que Sigmundur Davíð Gunnlaugsson, le Premier ministre islandais, a été contraint de démissionner en raison du scandale des Panama Papers.
Les évènements de ce type, qui rendent publiques de grandes quantités de données dans le cadre d'une campagne de dénonciation ou pour porter publiquement atteinte à un opposant quelconque d'un gouvernement ou d'une entreprise, seront de plus en plus fréquents. Ils continueront de perturber grandement le fonctionnement de nos institutions et ceux qui détiennent actuellement le pouvoir.

2 : l'ingérence de l'État-nation
Nous avons assisté cette année à une augmentation des accusations de violations de données orchestrées par des États-nations. À l'été 2015, l'administration Obama a décidé d'user de représailles contre la Chine pour le vol d'informations personnelles relatives à plus de 20 millions d'Américains lors du piratage des bases de données de l'Office of Personnel Management. Cette année, le sénateur américain Marco Rubio (républicain, État de Floride) a mis en garde la Russie contre les conséquences inévitables d'une ingérence de sa part dans les élections présidentielles.
Il s'agit là d'une autre tendance qui se maintiendra.
Les entreprises doivent donc comprendre que si elles exercent ou sont liées de par leur activité à des secteurs dont les infrastructures sont critiques (santé, finance, énergie, industrie, etc.), elles risquent d'être prises dans les tirs croisés de ces conflits.

3 : la fraude est morte, longue vie à la fraude au crédit !
Avec l'adoption des cartes à puces – notamment EMV (Europay Mastercard Visa) – qui a tendance à se généraliser, et les portefeuilles numériques tels que l'Apple Pay ou le Google Wallet qui sont de plus en plus utilisés, les fraudes directes dans les points de vente ont chuté, et cette tendance devrait se poursuivre. En revanche, si la fraude liée à des paiements à distance sans carte ne représentait que de 9 milliards d'euros en 2014, elle devrait dépasser les 18 milliards d'ici 2018.
Selon l'article New Trends in Credit Card Fraud publié en 2015, les usurpateurs d'identité ont délaissé le clonage de fausses cartes de crédit associées à des comptes existants, pour se consacrer à la création de nouveaux comptes frauduleux par l'usurpation d'identité. Cette tendance devrait se poursuivre, et la fraude en ligne augmenter.
Le cybercrime ne disparaît jamais, il se déplace simplement vers les voies qui lui opposent le moins de résistance. Cela signifie, et que les fraudeurs s'attaqueront directement aux systèmes de paiement des sites Web.

4 : l'Internet des objets (IdO)
Cela fait maintenant deux ans que les experts prédisent l'émergence d'un ensemble de risques inhérents à l'Internet des objets. Les prédictions sur la cybersécurité de l'IdO ont déjà commencé à se réaliser en 2016. Cela est en grande partie dû à l'adoption massive des appareils connectés d'une part par les consommateurs, mais aussi par les entreprises. En effet, d'après l'enquête internationale portant sur les décideurs et l'IdO conduite par IDC, environ 31 % des entreprises ont lancé une initiative relative à l'IdO, et 43 % d'entre elles prévoient le déploiement d'appareils connectés dans les douze prochains mois. La plupart des entreprises ne considèrent pas ces initiatives comme des essais, mais bien comme faisant partie d'un déploiement stratégique à part entière.
Cette situation va considérablement empirer. L'un des principaux défis de l'IdO n'est pas lié à la sécurisation de ces appareils par les entreprises, mais plutôt au fait que les fabricants livrent des appareils intrinsèquement vulnérables : soit ils sont trop souvent livrés avec des mots de passe par défaut qui n'ont pas besoin d'être modifiés par les utilisateurs, soit la communication avec les appareils ne requiert pas une authentification de niveau suffisant ; ou encore, les mises à jour des firmwares s'exécutent sans vérification adéquate des signatures. Et la liste des défauts de ces appareils n'en finit pas de s'allonger.
Les entreprises continueront d'être touchées par des attaques directement imputables aux vulnérabilités de l'IdO, que ce soit par des attaques par déni de service distribué (attaques DDoS), ou par le biais d'intrusions sur leurs réseaux, rendues possibles par les « faiblesses » inhérentes de l'IdO.

5 : bouleversements de la réglementation…[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 DIRECCTE 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 Contacter-nous

Réagissez à cet article

Original de l'article mis en page : Les grandes tendances 2017 de la cybersécurité, Le Cercle

---

Les mails de Clinton piratés par des «hackeurs russes», stratégie de diversion ?

Les mails de Clinton piratés par des «hackeurs russes», stratégie de diversion ?

Les Etats-Unis utilisent la Russie comme un «ennemi commode», dont l'existence est indispensable pour entretenir leur complexe militaro-industriel, explique Jean-Robert Raviot, professeur des études russes.

RT France : Barack Obama a donné vendredi passé sa dernière conférence de presse en tant que président, où il a évoqué la Russie et les hackers russes qui auraient piraté les comptes du Parti démocrate américain alors que, selon la déclaration du procureur général des Etats-Unis, il n'y a pas de preuve de l'origine de ces attaques. Pourquoi alors accuser la Russie ?

Jean-Robert Raviot (J.-R. R.) : Il faut chercher la réponse dans une logique qui n'est pas proprement en Russie, mais plutôt à Washington. C'est à dire qu'on assiste aujourd'hui à un tir de barrage contre Donald Trump de la part du Parti démocrate et d'un certain nombre de gens qui soutenaient la candidature de Hillary Clinton. Dans cette affaire il y a trois points qui soulèvent question pour moi. Premièrement, sur un plan technique – pourquoi est-ce que ce hacking, s'il est avéré qu'il a été repéré par la CIA, n'est-il pas rendu public ? Et surtout, pourquoi la NSA, qui en principe devrait avoir une vision assez claire des opérations de hacking sur le territoire américain, ne s'est-elle pas prononcée ?

Le fait d'accuser le Kremlin et les hackers russes d'avoir monté cette opération, permet de détourner l'attention du fond des mails

Je crois qu'il faut remarquer que personne de la NSA n'a donné son avis sur la question. Pour moi, ça met déjà un gros doute sur la réalité de ce hacking, sur la preuve qu'on peut avoir que des hackers russes ont agi pour prendre possession de ces mails de Podesta et ceux de Clinton. C'est un point technique, mais qui me semble important quand-même. Parce que cette question n'est pas résolue, et personne ne la pose vraiment.

On a cherché à discréditer Bernie Sanders. C'est ça le problème

Le deuxième point, comme je l'analyse, c'est la volonté de brouiller un peu l'information. Le fond de l'affaire c'est ce qu'il y a dans ces mails, et la preuve, que du côté de Hillary Clinton, on a cherché à discréditer Bernie Sanders. C'est ça le problème. On voit très clairement dans ces mails une opération interne du Parti démocrate visant tout simplement à mettre de côté Bernie Sanders, à lui mettre des bâtons dans les roues dans cette campagne électorale et dans cette primaire. C'est très clairement avéré. Le fait d'accuser la Russie ou le Kremlin ou les hackers russes d'avoir monté cette opération, permet de détourner l'attention du fond des mails.

Barack Obama exige un rapport sur le piratage, dont les résultats ne seraient pas rendus publics

Du coup, plus personne ne parle de la réalité de ce qui est dit dans ces mails, et du fait qu'ils ne sont pas rédigés par les hackers, mais par les gens qui ont tenu ces correspondances. Je dirais, c'est un moyen de détourner l'attention du grand public sur un problème qui n'est pas le même. C'est comme le vieux proverbe chinois : «Le sage montre la lune, et l'idiot regarde le doigt qui montre la lune». C'est absolument une stratégie de diversion.

La volonté c'est de se servir d'un ennemi assez commode, parce que c'est l'ennemi historique de la guerre froide – ça permet de mobiliser des récits qui sont déjà écrits et qui résonnent dans les têtes des gens

Le troisième point c'est la véritable volonté de la part d'un groupe dirigeant actuellement aux Etats-Unis, qui est autour d'Obama, autour du Parti démocrate, de Hillary Clinton et leurs soutiens, d'essayer de ramasser un maximum d'arguments. Pour l'instant, je pense qu'il y a des gens qui préparent l'impeachment de Trump. Je pense que c'est un peu rapide de dire ça – pour le moment, il n'est pas encore investi, on ne peut pas faire la destitution de quelqu'un qui n'est pas encore investi. Mais je pense que l'objectif c'est de faire une campagne, de tenter d'orienter le vote des grands électeurs et de faire en sorte qu'ils ne votent pas pour Trump.

RT France : Pourquoi ont-ils choisi Vladimir Poutine et la Russie, et non pas la Chine, par exemple, en guise de bouc émissaire ?

J.-R. R. : *Parce que la Russie, je dirais, a été désignée comme l'ennemi principal non seulement des Etats-Unis, mais aussi de l'Alliance atlantique. Rappelez-vous, quand en juillet 2016, au sommet de Varsovie de l'OTAN,* ***on a désigné la Russie comme menace principale****, alors que le djihadisme apparaît à peine dans le texte. C'est quand-même incroyable. La volonté c'est de se servir d'un ennemi qui existe, un ennemi qui est assez commode, parce que c'est l'ennemi historique de la guerre froide – ça permet de mobiliser des récits qui sont déjà écrits et qui résonnent dans les têtes des gens. C'est un ennemi familier, en quelque sorte. En même temps, l'image de Poutine permet d'associer cette image à un homme fort, anti-Obama, par sa personnalité, on peut facilement l'opposer aux dirigeants occidentaux. Et puis, ça résonne aussi assez bien dans le contexte de la guerre en Syrie et surtout de la guerre qu'on veut mener. C'est la narration de cette guerre qu'on veut imposer, c'est-à-dire, un soutien certainement des forces anti-Assad et anti-régime, de continuer ces opérations de «regime change», qui ont commencé en 2003, tout en s'appuyant sur le pays qui s'y oppose pour l'instant militairement, d'une manière directe…****[lire la suite]***

Réagissez à cet article

Original de l'article mis en page : Les «hackeurs russes», une stratégie de diversion pour oublier le contenu des mails de Clinton – RT en français

---

5 à 10% du budget d'une entreprise devrait être consacrée à la cybersécurité

5 à 10% du budget d'une entreprise devrait être consacrée à la cybersécurité

La sécurité a un cout mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique.

Toutes les entreprises sont des cibles potentielles mais les secteurs des nouvelles technologies, des systèmes d'information, des médias, du transport et de logistique, de la grande distribution sont exposés à des pertes financières lourdes.

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 : Les 5 chiffres à connaître de la cybersécurité – BeRecruited

La Poste livrera ses colis par drones dans le Var

Dans le Var, après deux ans d'essais, La Poste a obtenu de Direction Générale de l'Aviation Civile (DGAC) le droit d'ouvrir une ligne commerciale régulière de 15 km pour la distribution de colis par drones. Elle se situera entre Saint-Maximin-La-Sainte-Baume et Pourrières.…[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.

Réagissez à cet article

La Poste livrera ses colis par drones dans le Var

La Poste livrera ses colis par drones dans le Var

Dans le Var, après deux ans d'essais, La Poste a obtenu de Direction Générale de l'Aviation Civile (DGAC) le droit d'ouvrir une ligne commerciale régulière de 15 km pour la distribution de colis par drones. Elle se situera entre Saint-Maximin-La-Sainte-Baume et Pourrières.…[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

Vote électronique aux élections professionnelles

Le Décret n° 2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise est publié.

Désormais, le chef d'une entreprise employant au moins 11 salariés peut recourir au vote électronique pour ses élections professionnelles et ce même en l'absence d'un accord collectif.
Il peut dorénavant décider de fixer lui-même les modalités du vote électronique, sous réserve de respecter les conditions fixées par le décret du 5 décembre 2016.
L'employeur d'au moins 11 salarié peut ainsi décider de recourir au vote électronique pour les élections partielles se déroulant en cours de mandat.
Il choisit, dans ce cas, si le vote électronique interdit ou pas le vote à bulletin secret sous enveloppe.
Le chef d'une entreprise employant au moins 11 salariés doit établir un cahier des charges respectant les dispositions réglementaires relatives au vote électronique et le tenir à la disposition des salariés sur le lieu de travail et sur l'intranet de l'entreprise.
Attention : pendant le déroulement du scrutin, aucun résultat partiel n'est accessible.
Seul, le nombre de votants peut, si l'employeur le prévoit, être révélé au cours du scrutin.
Par **Carole Vercheyre-Grard**
Avocat au Barreau de Paris
Source juritravail.com
[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 aux élections professionnelles