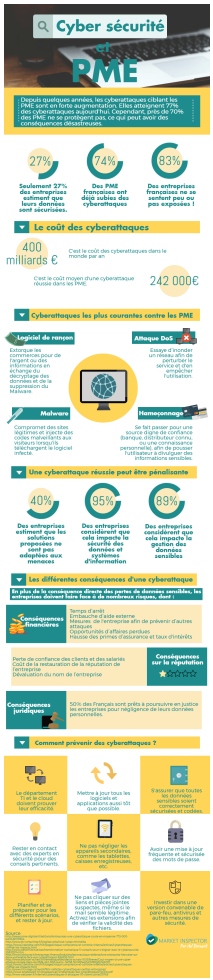
Votre PME est-elle protégée des cyberattaques?

	Votre PME est-elle protégée des cyberattaques ?

Bien que la plupart des PME ne se sentent pas ou peu concernées, ce sont bien elles les premières victimes des cyberattaques. En effet, elles sont moins équipées en systèmes de sécurité et sont donc bien plus susceptibles d'être hackées.
Une PME non préparée aux risques des cybermenaces peut souffrir de **conséquences désastreuses**. Dans beaucoup de cas, ces entreprises n'ont rien préparé et ne savent pas comment réagir face à ces problèmes. Ces attaques résultent alors souvent en la **perte de données**, de **clients** et de **revenue**, sans compter les coûts supplémentaires de la **réparation du système**, etc.
Le type d'attaques les plus subies par les entreprises reste la **demande de rançon** (par ransomware), à 80%. Se place ensuite les attaques par **déni de service** (40%), les **attaques virales** généralisées (36%), et la **fraude externe** à 29%.
Market Inspector vous a alors décrypté le sujet en infographie, afin d'en apprendre plus sur le risque des cyberattaques sur les PME et comment s'en défendre simplement.



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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Votre PME est-elle protégée des cyberattaques? | Market-Inspector*

Les entreprises du CAC 40 sont la cible de cyberattaques

Les entreprises du CAC 40 sont la cible de cyberattaques

Renault n'est pas la seule entreprise dans le viseur des cyberterroristes. Les champions de la défense et les géants de la Bourse peaufinent leur bouclier.
par Guerric PONCET

« En 2016, de gros industriels ont été touchés et des géants du CAC 40 ont pris conscience qu'ils pouvaient disparaître du jour au lendemain à cause d'une cyberattaque », nous confie Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). « Je veux dire que, si leur piratage était dévoilé, ils étaient *OPAbles* le lendemain », précise-t-il. En effet, la révélation d'une telle attaque ferait immédiatement chuter le cours de la Bourse…
Nos champions de la cybersécurité, Airbus, Thales, Capgemini et Orange en tête, sont sollicités de toutes parts par les comités exécutifs. Mais leurs tarifs sont souvent hors de portée des PME : dans le cyber, la défense coûte cent fois le prix de l'attaque. Et, quand bien même, le budget ne fait pas tout : JP Morgan, Yahoo !, Adobe, Visa ou encore Sony ont beau avoir alloué des centaines de millions de dollars à leur sécurité informatique, ils ont tous vécu des intrusions gravissimes. « Il est impossible de créer un cyberbouclier infaillible », tranche Guillaume Poupard, pour qui il faut avoir « une bonne gouvernance avant même de parler technique ». « Jusqu'à présent, nous avons stoppé les attaques majeures qui nous visaient, mais, si l'une d'elles réussissait, ce serait une catastrophe, avec des conséquences sur la souveraineté économique de la France et, très rapidement, sur la sécurité des populations », nous glisse, sous le couvert de l'anonymat, le responsable de la sécurité informatique d'une entreprise classée « opérateur d'importance vitale » (OIV).
Des exercices de crise sont régulièrement menés pour anticiper et limiter les dégâts que créerait assurément une cyberattaque chez un OIV – panne générale dans la production électrique, paralysie des transports, implosion des télécoms… Des agents de l'Anssi jouent aux hackers, tentent de déjouer les systèmes de sécurité… et y parviennent : « La dernière fois, ils ont pris le contrôle d'une partie de notre système assez facilement, ils auraient pu créer des accidents graves », reconnaît, lui aussi en toute discrétion, le responsable informatique d'un autre OIV. Nous voilà rassurés…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cyberguerre : le CAC 40 dans le viseur – Le Point*

2 employés sur 10 pirateraient leur entreprise

2 employés sur 10 pirateraient leur entreprise

21 % des employés de bureau britanniques pirateraient leur entreprise s'ils avaient les compétences requises. Une enquête révèle les informations susceptibles d'être piratées par les employés : leurs salaires, leurs jours de congés, les commérages, les informations RH sensibles.

L'entreprise CyberArk, spécialiste de la protection d'organisations face aux cyberattaques ayant réussi à pénétrer dans le périmètre réseau, a dévoilé les résultats d'une enquête révélant ce que les employés feraient s'ils étaient capables d'accéder anonymement aux données sensibles de leur entreprise, notamment les salaires, les jours de congé ou des informations confidentielles liées aux ressources humaines. Ce sondage rappelle l'importance de contrôler les accès aux comptes à privilèges, afin d'éviter que les cyber-pirates internes et externes ne puissent obtenir un accès libre et illimité aux actifs les plus précieux de l'entreprise...[lire la suite]

Réagissez à cet article

Source : *2 employés sur 10 pirateraient leur entreprise – Data Security BreachData Security Breach*

Protégez-vous contre la cybercriminalité, les experts mettent en garde les business et le public Seychellois

Protégez-vous contre la cybercriminalité, les experts mettent en garde les business et le public Seychellois

Suite à la cyber-criminalité, une vigilance extrême a été conseillée aux hommes et femmes d'affaires et le public général aux Seychelles qui procèdent à des transactions monétaires en ligne.

Les experts aux Seychelles ont avertis, mercredi, lors d'une conférence de presse, que les messageries électroniques de certains hommes d'affaires sont piratées par des criminels internationaux très bien organisés, et des informations personnelles sont volées afin de détourner des transactions financières de leurs destinations d'origine.

Un représentant de l'Association des banquiers (la ***Bankers Association***), Norman Weber, explique que pour prévenir la perte d'argent par ce genre d'interception, il est de la responsabilité de l'homme d'affaire de vérifier l'authenticité des détails qui lui sont envoyés.

« Il est important de connaître le fournisseur avec lequel vous avez affaire. Si vous recevez, par email, de nouvelles instructions relatives à un transfert bancaire, cela ne coûte pas plus que ça de vérifier l'information par un appel », a exprimé N Weber.

Une autre arnaque populaire, qui a attiré l'attention de la police, concerne de faux profils sur les réseaux sociaux, généralement sur Facebook, que les criminels utilisent pour offrir des prêts attractifs à leurs potentielles victimes. Les membres du public ont été conseillés de ne pas entrer en contact avec ces arnaqueurs sur Facebook.

Avant que vous receviez le prêt « vous devrez payer les frais juridiques et administratifs. Au moment où vous vous rendrez compte [qu'il s'agit d'une arnaque] vous aurez déjà perdu beaucoup d'argent. » a déclaré le directeur de la cellule de renseignement financier des Seychelles (la **Financial Intelligence Unit** FIU), Philip Moustache.

P. Moustache a expliqué que ce qui rend ces transactions financières si difficiles à tracer, c'est qu'elles ne passent pas par les banques, l'arnaqueur demande que les transactions passent par **Western Union** ou Moneygram.

La police a annoncé mercredi qu'ils avaient reçu huit cas signalés cette année, où des locaux avaient été victimes de fraudes sur Internet et avaient perdu de grosses sommes d'argent. L'année dernière, 18 cas similaires ont été signalés.

Jusqu'à présent, il n'y a pas eu de cas rapportés relatifs à des transactions faites sur PayPal ou eBay.

« Les enquêtes réalisées ont montré que ces activités sont menées par des personnes dans des pays étrangers et que pour cette raison, il est presque impossible pour la police locale de lutter contre ce type de criminalité, comme nous n'avons pas juridiction dans ces pays », a déclaré Reginald Elizabeth, Commissaire de Police.

Comme il est difficile de mener une enquête dans ces pays, lorsque Interpol est impliqué, la piste de l'argent est devenue froide et l'argent a été retiré du compte bancaire.

La Banque Centrale des Seychelles (la CBS) travaille en étroite collaboration avec la police et l'Association des banquiers afin de mettre en place un programme de sensibilisation du public concernant ces transactions.

Le Premier Sous-Gouverneur de la Banque Centrale, Christopher Edmond, a informé que « la banque cherche un consultant en cyber-sécurité afin de réaliser une évaluation de ses systèmes en place, afin de s'assurer que ces fraudes n'aient pas lieu dans la juridiction des Seychelles. »…[lire la suite]

Réagissez à cet article

Source : *Protégez-vous contre la cybercriminalité, les experts mettent en garde les business et le public Seychellois. – Seychelles News Agency*

« La plupart des crypto virus viennent de Russie et d’Ukraine»

	« La plupart des crypto virus viennent de Russie et d’Ukraine»

Lors du salon Viva Technology, qui se déroulait à Paris du 15 au 17 juin, Ondrej Vlcek, directeur technique de la société Avast, l'un des antivirus les plus populaires du monde, animait une conférence sur «le commerce des malwares». Alors qu'une nouvelle attaque d'un logiciel malveillant appelé WannaCry a touché la planète en mai dernier, comment se prémunir d'une telle menace à l'avenir? Quelles sont les bonnes pratiques à adopter pour minimiser les risques?

Ondrej Vlcek : C'est le nom d'une catégorie de malwares («logiciels malveillants») qui réclament une rançon. Généralement, une fois qu'un rançongiciel est installé, le hacker s'empare du disque dur des victimes avec tous leurs fichiers personnels et demande de l'argent pour rendre les fichiers – sans quoi il les supprime. Une fois que l'ordinateur est infecté, le rançongiciel commence à chiffrer les fichiers, c'est-à-dire à les transformer afin qu'ils ne soient plus lisibles et que l'on ait besoin d'un mot de passe ou d'une clé de chiffrement pour y avoir accès. Il existe aujourd'hui de nouvelles variantes : en plus de crypter le disque dur, le rançongiciel peut aussi menacer l'utilisateur de faire fuiter les fichiers volés sur tout l'Internet.

Les vieux virus étaient beaucoup moins agressifs : ils détournaient votre ordinateur et l'utilisaient simplement pour envoyer des spams ou vous obliger à cliquer sur des pubs afin de générer de l'argent. Ils pouvaient aussi détourner votre ordinateur pour vous espionner et connaître vos mots de passe et identifiants. Là, une fois que la machine est infectée, vos fichiers personnels sont immédiatement modifiés et l'on vous réclame tout de suite de l'argent pour y accéder.

WannaCry est particulièrement inquiétant, car c'est un rançongiciel « auto-répliquant ». Qu'est-ce que cela signifie ?

Normalement, la plupart des logiciels malveillants aujourd'hui nécessitent l'action de l'homme : vous devez cliquer sur un lien, ouvrir une pièce jointe associée à un message électronique ou faire quelque autre exécution manuelle. Ici, tout est entièrement automatisé, c'est-à-dire que si vous avez un ordinateur vulnérable ou pas à jour, WannaCry peut l'infecter sans avoir besoin d'aucune interaction humaine, sans même que vous soyez devant votre ordinateur.

Quelles conséquences cela peut-il avoir sur l'ampleur de WannaCry ?

Cela rend sa propagation beaucoup plus rapide, car le fait de devoir cliquer sur un lien peut prendre des jours ou des semaines. Concernant WannaCry, le monde entier a été infecté en deux heures, le logiciel passant d'un ordinateur à l'autre.

Savons-nous aujourd'hui d'où viennent tous ces logiciels malveillants ? Et quelles sommes d'argent sont impliquées dans ces attaques ?

Pour ce qui concerne les rançongiciels, la plupart viennent de Russie et d'Ukraine (concernant WannaCry, la piste nord-coréenne semble la plus probable, ndlr). Nous avons des indications qui nous laissent penser que la majorité des rançongiciels aujourd'hui sont déployés de façon à ce qu'ils n'affectent pas les personnes vivant en Russie. La raison est qu'il existe en Russie une loi qui rend la création de rançongiciels illégale lorsqu'ils peuvent avoir un impact sur des citoyens russes, mais techniquement légale, d'une certaine manière, lorsqu'ils infectent des gens hors de Russie. L'année dernière, une estimation publiée par le FBI chiffrait le coût de ces cyberattaques à plus d'un milliard de dollars. Cette année, ce montant va probablement doubler et monter à plus de deux milliards de dollars.

Peut-on neutraliser ce type de logiciels malveillants ?

Il y a deux enjeux. Le premier, c'est la prévention. Très important : utiliser un système d'exploitation à jour afin de ne pas être trop vulnérable. Il faut aussi installer un logiciel antivirus de qualité. Enfin, il vaut mieux faire des sauvegardes régulièrement, car vous pouvez ainsi récupérer vos fichiers en cas d'attaque. Je fais des sauvegardes tous les jours et je recommande à tout le monde de faire de même.

La majorité des sauvegardes se font automatiquement, mais il faut être prudent sur ce point parce que, si le rançongiciel est installé sur l'ordinateur depuis un certain temps – un jour ou deux – la sauvegarde peut aussi enregistrer les fichiers infectés qui écraseront les anciennes versions saines.

Le second enjeu apparaît lorsque l'infection s'est produite : que peut-on faire ? En fait, quasiment la moitié des rançongiciels peuvent être supprimés et décryptés sans payer la rançon, car le chiffrement n'est pas bien installé, et possède des failles. Nous ou d'autres entreprises spécialisées dans la cybersécurité sommes capables d'accéder à l'algorithme de chiffrement et de décrypter les fichiers. Mais s'il est installé correctement, il n'y a aucune chance. Avec les ordinateurs d'aujourd'hui, décrypter les fichiers prendrait des centaines d'années.

Mon conseil : si vous êtes attaqué et qu'il n'y a pas de moyen de décrypter le disque dur aujourd'hui, ne supprimez pas vos fichiers infectés pour autant si vous en avez vraiment besoin. Bien que l'outil de décryptage pour ce rançongiciel en particulier ne soit pas disponible pour le moment, il peut l'être dans six mois, un mois ou même une semaine…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cybercriminalité: «La plupart des rançongiciels viennent de Russie et d'Ukraine» – Technologies – RFI*

Alerte : Mettez à jour votre

Windows quelle que soit sa version.

Alerte : Mettez à jour votre Windows quelle que soit sa version.

Windows se met à jour en amont de potentielles cyberattaques, a annoncé Microsoft sur son blog officiel. Exceptionnellement, tous les OS sont concernés, de Windows 10 à XP en passant par Vista. Ces correctifs sont accessibles différemment selon votre situation et votre OS.

Comme à son habitude, **Microsoft** propose sa mise à jour mensuelle de ses **OS Windows** 10, 8.1 et 7. Seulement, cette fois-ci, même Windows XP et Vista auront droit eux aussi à une mise jour exceptionnelle, dans le but de lutter contre les **cyberattaques** potentielles semblables à celles ayant eu lieu récemment, comme Adylkuzz et le ransomware Wannacry.

Microsoft met à jour tous ses OS Windows, de 10 à XP, pour contrer de nouvelles cyberattaques

La cyberattaque Wannacry avait particulièrement touché Windows 7 et Windows XP, poussant Microsoft a faire des mises à jour correctives rapidement. Il avait même proposé des patchs de sécurité pour XP, exceptionnellement.

C'est sur son blog Windows que Microsoft donne des explications. Selon eux, des menaces ont été identifiées et il subsiste un risque d'attaque menée par « des organisations gouvernementales ». Ces attaques seraient semblables à Wannacry, qui exploitait une faille qui était utilisées par la NSA pour l'espionnage.

Pour contrer tout problème, Microsoft met donc à jour ses OS en amont. Sont concernés Windows 10, 8.1, 7 bien entendu, mais également XP et Vista qui ne bénéficient pas d'un support habituellement.

Pour effectuer ces mises à jour préventives, vous n'avez rien à faire si vos paramètres sont dans leur configuration initiale et que vous utilisez une version récente de Windows. En revanche, vous devez vous rendre sur la page de support de Microsoft si vous utilisez Vista ou XP, pour savoir si vous êtes concerné par les attaques et faire les mises à jour en cas de besoin.

Et en cas de problème malgré la mise à jour, n'hésitez pas à vous rendre sur le site du gouvernement dédié à la cybermalveillance…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cyberattaque : un risque imminent force Microsoft à lancer une mise à jour critique de Windows 10 à Windows XP*

Cybercriminalité : Rien n’est plus facile que de couper Internet

Cybercriminalité : Rien n’est plus facile que de couper Internet

---

Rien n’est plus facile que de couper Internet : il suffit de sectionner des câbles. Ils sont simplement enterrés, voire posés sur le fond des océans.
L’imaginaire populaire associe souvent Internet aux satellites, mais 99,8 % du trafic intercontinental passe par les 366 câbles sous-marins répartis sur la planète. « Grâce à la fibre optique, les capacités de ces câbles sont des millions de fois supérieures à ce que nous savons faire avec les satellites », explique Jean-Luc Vuillemin, directeur des réseaux internationaux d’Orange, dont la filiale Orange Marine a posé un sixième du million de kilomètres aujourd’hui déployé dans le monde…[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 d’expertises, d’audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Cyberattaque, pourquoi les câbles sous-marins sont le maillon faible – Le Point*

L’humain, maillon faible de la cybersécurité

L’humain, maillon faible de la cybersécurité

« Le Facteur Humain 2017 » indique que les cybercriminels se reposent de plus en plus sur l'humain plutôt que sur les failles logicielles pour installer des programmes malveillants, dérober des informations confidentielles et transférer des fonds.
Pas vraiment une nouveauté, le **piratage informatique** s'est toujours d'abord reposé sur le facteur humain. Le **social engineering** en est une preuve. Dans son rapport, Proofpoint spécialiste en sécurité et conformité, a interrogé plus de 5000 entreprises en 2016. Bilan, les indicateurs sur les attaques par le biais des emails, mobiles et réseaux sociaux, donne une tendance des clients de cette société.

« C***ette tendance d'exploitation du facteur humain, qui a vu le jour en 2015, s'accélère, et les cybercriminels multiplient désormais les attaques générées par les clics des utilisateurs plutôt que par des logiciels d'exploitation vulnérables, conduisant ainsi les victimes à exécuter elles-mêmes les attaques*** », a déclaré Kevin Epstein, Vice-Président du centre d'opération des menaces de Proofpoint. « ***Il est essentiel que les entreprises mettent en place une protection avancée pour arrêter les cybercriminels avant qu'ils puissent atteindre leurs potentielles victimes. La détection anticipée des contenus malveillants dans la chaîne d'attaques permettra de les bloquer, de les canaliser et de les supprimer plus facilement.*** »…[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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *L'humain, maillon faible de la cybersécurité – Data Security BreachData Security Breach*

Cybersécurité : quand les collectivités prennent la mesure du problème

	Cybersécurité : quand les collectivités prennent la mesure du problème

A l'heure où la cybersécurité est un enjeu croissant pour les acteurs publics, les collectivités semblent se prendre enfin en main. La ville de Marseille a mis en place une initiative pour tester ses défenses. Dans le même temps, la région Hauts-de-France a, elle, été choisie pour être le théâtre d'une expérimentation de l'ANSSI.

Pour de nombreuses collectivités locales, la cybersécurité reste encore aujourd'hui un enjeu abstrait. A quelques exceptions près, ces dernières ne sont pas armées pour résister à des attaques très virulentes et aveugles. Et pourtant, les offensives font de plus en plus mal. En témoignent les dégâts causés en mai dernier par le rançongiciel WannaCry, qui a paralysé plus de 200 000 machines à travers près de 150 pays, dont des opérateurs d'importance vitale en France.
L'ampleur de l'offensive n'a fait que confirmer ce que tout le monde savait depuis longtemps : personne n'est à l'abri. Des solutions commencent toutefois à être mises en place par les collectivités elles-mêmes. Un changement de paradigme plus que nécessaire.

Marseille joue la carte prévention

La ville de Marseille a ainsi inauguré le 6 juin une initiative visant à permettre à la municipalité de tester l'efficacité de ses défenses à tous les niveaux. Concrètement, une vingtaine d'étudiants issus de l'école Polytech – l'initiative étant réalisée en partenariat avec l'Université Aix-Marseille – cherchera les éventuelles failles dont la municipalité n'aurait pas connaissance.
Les sites web, applications mais aussi les objets connectés seront passés au crible par ces « hackers éthiques ». Pour ce faire, ces derniers utiliseront SafeGouv, un service proposé par la start-up Net Guard…[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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

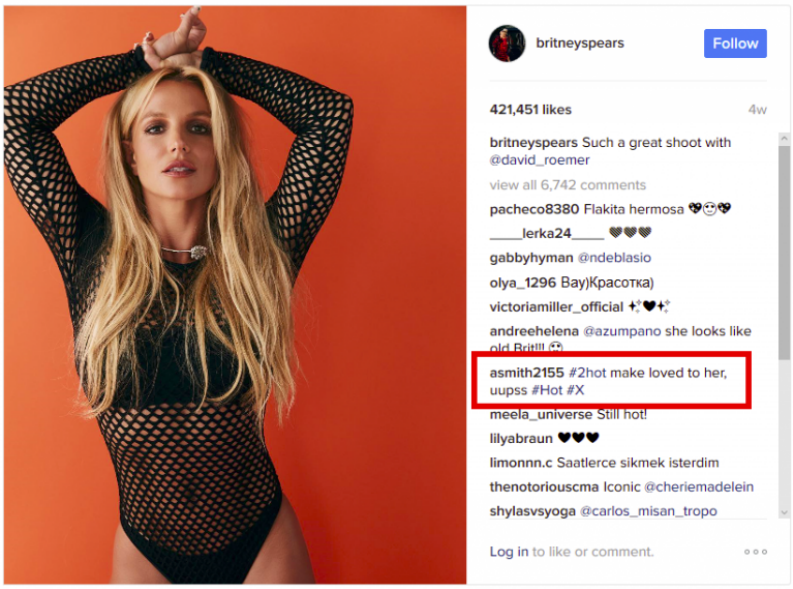
Source : *Cybersécurité : quand les collectivités prennent la mesure du problème*

L'Instagram de Britney Spears, une planque pour les hackers russes

L'Instagram de Britney Spears utilisé par des hackers russes pour planquer l'adresse de leur serveur c&c

---

Un groupe de pirates russes a utilisé le compte officiel de Britney Spears sur Instagram pour cacher la direction de leurs serveurs de commandes et contrôle.



Vivons heureux, vivons cachés ! Cet adage s'applique parfaitement aux cybercriminels. Encore faut-il trouver la bonne planque ! Des chercheurs d'Eset, éditeur de sécurité, viennent de détecter une des cachettes d'un groupe de pirates russes, Turla. Ce dernier œuvre depuis 2007 et est à l'origine dun rootkit sophistiqué Uburos, créé en 2014. Spécialisé dans le cyberespionnage, Turla est soupçonné d'être d'origine russe ou pour le moins russophone. Ses techniques de piratage sont très élaborées, mais la découverte d'Eset est particulièrement originale.
Les chercheurs ont en effet déniché une backdoor dans les commentaires publiés sur le compte officiel de Britney Spears sur Instagram. Ce trojan donne des informations de localisation des serveurs de commandes et contrôle du groupe Turla.
…[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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *L’Instagram de Britney Spears, une planque pour les hackers russes*