Attaque informatique TV5 Monde – Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8 | Denis JACOPINI

	Attaque informatique TV5 Monde -Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8

A la suite de l'attaque informatique ayant visé TV5 Monte, le 9 avril dernier, pendant qu'il se trouvait à un Colloque international sur la Cybercriminalité à Montpellier organisé par Adel JOMNI, Denis JACOPINI a été interviewé par un journaliste de Canal Plus et certains propos retenus pour le JT de 20h45 sur Direct 8.

D'après-vous, pourquoi les pirates ont choisi la chaîne de télévision TV5 Monde comme cible de leur attaque informatique ?Lorsque des pirates ou des cybercriminels décident d'attaquer un système informatique, il le font principalement pour les raisons suivantes :- A la suite d'une sorte de défi qu'ils se sont lancés afin de prouver leur capacité à pirater un système qui s'est par exemple déclaré comme système inviolable…- Afin de récolter de l'argent soit en menaçant de diffuser des informations secrètes, soit en vendant les informations piratées, soit en prenant en otage un serveur en le bloquant et tout cela, contre rançon.

– Ou bien, dans le but de diffuser un message idéologique, prônant un message politique, religieux… Dans ce cas, l'objectif premier des cyber-attaquants est la diffusion à grande échelle d'un message (c.f. les deffaçages de plus de 25000 sites Internet à la suite des attentats contre Charlie Hebdo). Que le plus de personnes possibles puisse prendre connaissance d'un message en y associant une sensation de puissance, tel a été le type d'attaque contre TV5 Monde. Cette attaque, a été destinée avant tout à diffuser un message idéologique, en touchant un média à couverture mondiale pour qu'on parle le plus possible des attaquant et de leur symbole.

Quelle a été la technique utilisée lors de l'attaque des serveurs de TV5 Monde ?

Les cybercriminels utilisent généralement 2 types de méthodes pour pénétrer dans un système informatique :

– la recherche de failles

– la naïveté d'un destinataire à un e-mail

C'est un voire même plusieurs e-mails, de type phishing qui semblent être à l'origine, depuis probablement plusieurs semaines ou mois, de l'intrusion du système informatique de TV5 monde par les cybercriminels. Une fois introduits dans le système informatique, l'accès invisible ou silencieux à des informations confidentielles ou secrètes permet ensuite de trouver les clefs autorisant de se répandre dans un réseau et contaminer ainsi le plus possibles d'organes sensibles ou stratégiques.

Une fois tous ces accès ainsi possibles, il suffit de coordonner une attaque simultanée de tous ces fruits devenus véreux pour donner l'impressionnante vision d'un arbre prêt à tomber.

« Il suffit d'envoyer tous les jours un email avec un virus auprès de différentes personnes de différents services et à un moment ou un autre il va bien y a voir quelqu'un qui va l'ouvrir.

Son vrai travail va commencer lorsque quelqu'un aura mordu à l'hameçon »

Peut-on conclure que n'importe quelle chaines de télévision peuvent être victime de cyber-attaques telles que celle dont a été victime TV5 monde ?

La faille qu'ont exploité les cybercriminels dans le cadre de l'attaque informatique de TV5 monde est une faille humaine. En effet, recevoir un e-mail nous incitant à cliquer sur un lien qui va contre notre volonté et de manière complètement invisible changer dans son ordinateur un logiciel malveillant chargé, de manière tout aussi silencieuse, de prendre le contrôle de notre ordinateur est devenu le moyen d'attaque le plus utilisé.

Les systèmes informatiques des chaines de télévision sont certes équipées de moyens de protection techniques contre les virus, les codes malveillants et autres types d'attaques, mais les cybercriminels auront toujours un coup d'avance en exploitant la faille humaine, principalement par manque de connaissance ou manque de formation de la part des utilisateurs.

Existe t-il un moyen de se protéger contre ce type d'attaque ?

Les organismes et entreprises ont prix trop de retard pour mettre en place des politiques de sécurité informatique. Quand on voit qu'en 2013, moins de 100 000 entreprises en France s'étaient mises en conformité avec la CNIL, excellent point de départ pour mettre en place des mesures de sécurité sur les données personnelles, il y a de quoi s'inquiéter sur la manière dont nos données (mot de passe y compris) sont sécurisées.

Commencer par se mettre en conformité avec la CNIL serait un bon début…

http://www.lenetexpert.fr/wp-content/uploads/2015/04/Denis-JACOPINI-interviewé-par-journaliste-Canal-plus-pour-JT-de-Direct-8.mp4

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.bfmtv.com/culture/l-attaque-contre-tv5monde-enclenchee-des-fin-janvier-877334.html

Utilisation des données personnelles dans le cas de la prospection Téléphonique – Rappel des règles | Denis JACOPINI

	**Dans le cadre de vos activités, vous pouvez être amenés à contacter par téléphone des personnes. Quelles sont les règles à respecter ?**

LE PRINCIPE : Information préalable et droit d'opposition.

La prospection par téléphone (télémarketing) est possible à condition que la personne soit, au moment de la collecte de son numéro de téléphone :

- informée de son utilisation à des fins de prospection.
- en mesure de s'opposer à cette utilisation de manière simple et gratuite, notamment par le biais d'une case à cocher.

LÉGISLATION APPLICABLE

Article 38 de la loi Informatique et Libertés du 6 janvier 1978

Articles L.34 et R.10 du code des postes et des communications électroniques.

RÉFÉRENCES UTILES

Code Déontologique du e-commerce et de la vente à distance du FEVAD

SANCTIONS

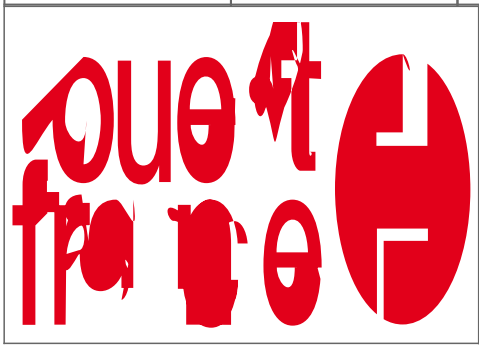
Amende de 750 € par appel
dans le cas de l'utilisation des coordonnées des personnes inscrites sur la « Liste Orange », à partir des annuaires téléphoniques (contravention de la 4e classe prévue par l'article R.10-1 alinéa 1 du code des postes et des communications électroniques).

5 ans emprisonnement et 300 000 € amende
Délit prévu par les articles 226-18 et 226-18-1 du code pénal.

Jusqu'à 300 000 € d'amende
Sanction prononcée par la CNIL, prévue par l'article 47 de la loi informatique et libertés modifiée.

Cet article vous à plu ? Laissez-nous un commentaire
(notre source d'encouragements et de progrès)

Denis JACOPINI interviewé par une journaliste de Ouest France | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Denis JACOPINI interviewé par une journaliste de Ouest France				

Est-il risqué de se connecter au wifi public ?
Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français).
Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.


Denis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?
Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

Quel est le danger ? Se faire espionner ?
Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.


Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » – par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. – ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?
Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates !


Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

Peut-on se faire abuser par une fausse borne wifi ?
Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

Comment se protéger ?
En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.


Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (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

Source : http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/

Par Corinne Bourbeillon

Denis JACOPINI au JT de TF1 : Cybercriminalité : Dans les prochaines années, ce qui arrive sur nos ordinateurs et nos téléphones risque aussi de se produire sur nos télévisions, nos voitures autonomes…

Denis JACOPINI au JT de TF1 : Cybercriminalité : Dans les prochaines années, ce qui arrive sur nos ordinateurs et nos téléphones risque aussi de se produire sur nos télévisions, nos voitures autonomes…

JT 20H – Le constat est sans appel, la cybercriminalité est devenue un phénomène massif auquel presque personne ne peut échapper. Citoyens, entreprises, et même les plus hautes instances de l'Etat ne sont pas épargnés.

Nous avons tous été victimes d'une fraude à la carte bleue ou d'un piratage de données personnelles. Un rapport officiel publié ce mercredi 20 juin par le ministère de l'Intérieur, montre l'augmentation considérable du nombre de cyberattaques. La raison: on a plus besoin d'être un hacker professionnel pour lancer une opération. Les techniques sont connues : l'hameçonnage, qui vise à obtenir frauduleusement les coordonnées bancaires, et le rançongiciel.

« Dans les prochaines années, ce qui arrive sur les ordinateurs et sur les téléphones risque de se produire aussi sur des télévisions, des voitures autonomes… »

Ce sujet a été diffusé dans le journal télévisé de 20H du 20/06/2018 présenté par Gilles Bouleau sur TF1. Vous retrouverez au programme du JT de 20H du 20 juin 2018…[lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

• **RGPD**
- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

• **CYBERCRIMINALITÉ**
- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

• **EXPERTISES**
- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (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

Source : *Cybercriminalité : une menace de plus en plus fréquente – LCI*

Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

---

Elles ont beaucoup fait parler d'elles durant la campagne présidentielle américaine : certaines pratiques malveillantes sur Internet pourraient aussi peser sur l'élection en France. Voici en quoi elles consistent.
Interview par Marina Cabiten (France Bleu)

Des pirates informatiques qui œuvrent contre Hillary Clinton, et donc en faveur de Donald Trump, le tout commandité par le Kremlin : il ne s'agit pas d'un scénario de film mais d'une accusation très sérieuse formulée par les autorités américaines lors de la campagne présidentielle. Internet est un outil puissant pour les manipulations informatiques, à différents degrés. Et la France est, selon plusieurs acteurs de la cybercriminalité, très mal préparée à ces usages détournés. Voici comment des personnes mal intentionnées pourraient perturber la campagne.

Inonder les réseaux sociaux de faux utilisateurs : l'astroturfing

Tout un chacun peut utiliser son compte Facebook ou Twitter pour s'exprimer, et éventuellement partager ses opinions politiques. Mais cette utilisation des réseaux sociaux peut être bidonnée. Ce phénomène est appelé astroturfing, du nom d'une marque de pelouse synthétique pour les stades : Astroturf. Autrement dit, il s'agit de faire prendre aux internautes du faux gazon pour de l'herbe naturelle… Comment ? **En inondant les réseaux sociaux de faux comptes automatisés, les "bots"**, qui diffusent des messages rédigés par les initiateurs de cette technique de "marketing politique" qui ne dit pas son nom, et garantit l'anonymat.
N'importe quel internaute peut créer et animer des faux comptes. Avec un peu plus de moyens financiers, il peut payer pour qu'un réseau social comme Facebook donne plus de visibilité à une page ou à un post via un algorithme qui fera apparaître le message sur davantage de "murs" d'utilisateurs, qui n'ont rien demandé. Sur Twitter, il peut acheter des "followers" (personnes qui suivent le compte) pour donner une fausse légitimité à ses comptes artificiels. Le degré ultime est de se payer un logiciel qui fait ça tout seul, voire d'employer quelqu'un pour l'exploiter. Cela existe, au sein d'entreprises privées mais parfois aussi de partis politiques. **C'est une forme de propagande de plus en plus répandue.** Le gouvernement français a annoncé récemment son intention de surveiller les réseaux sociaux pour éventuellement repérer des "mouvements" suspects de ce type.

Quand des sites partisans se font passer pour des organes de presse : les « fake news »

L'expression "Fake news", qui se traduit littéralement par « fausses informations », est très en vogue depuis la présidentielle américaine et vient de la diffusion sur Internet de prétendus articles de presse, qui ne sont en réalité pas rédigés par des journalistes. Des articles contenant des informations non vérifiées, parfois erronées, voire carrément mensongères dans le but bien précis de manipuler l'opinion.
La mécanique est la même que pour l'astroturfing, tout faire pour que ces "fake news" soient largement vues sur Facebook et les autres réseaux sociaux ou forums. Selon les calculs du site Buzzfeed, les articles relayant de fausses informations **(comme le faux soutien du pape François à Donald Trump, ou la révélation imaginaire de ventes d'armes par Hillary Clinton à l'organisation Etat islamique)** ont suscité 8,7 millions d'interactions sur Facebook durant la campagne américaine, contre 7,3 millions pour les articles de la presse traditionnelle.
En France récemment, plusieurs médias ont fait part de leur volonté de lutter contre ce phénomène, allant même pour certains jusqu'à nouer un partenariat avec Facebook et Google. ***"Le problème c'est que la rumeur court toujours beaucoup plus vite que la rectification ou la suppression du contenu"***, objecte Denis Jacopini, diplômé en cybercriminalité et sécurité de l'information, ***"laissant s'installer dans l'esprit de l'électeur ces fausses affirmations."***

De vrais contenus, mais dérobés et diffusés sans autorisation : le vol de données

La menace la plus sophistiquée reste le vol d'informations numériques. C'est l'exemple des pirates informatiques (hackers) qui ont récupéré près de 20.000 courriels de responsables du parti d'Hillary Clinton. Ils sont entrés dans les serveurs du parti démocrate dès l'été 2015, accumulant ces données parfois embarrassantes sans que personne ne s'en aperçoive, pour les publier au moment opportun pour déstabiliser le camp démocrate. Une cyberattaque venue de Russie pour aider Donald Trump à gagner l'élection, affirme la CIA dans un rapport révélé par la presse américaine. ***"Aucun parti politique français n'est actuellement protégé contre une telle malveillance"***, assure Denis Jacopini.
Selon le Canard Enchaîné (numéro du 8 février 2017), **les services secrets français s'inquiètent de cyberattaques russes** durant la Présidentielle, qui auraient pour but d'aider la campagne de Marine Le Pen. De son côté, le secrétaire général du mouvement « En Marche ! » Richard Ferrand a affirmé publiquement que les pirates russes visent particulièrement Emmanuel Macron et ont déjà attaqué à plusieurs reprises son site web.

Réagissez à cet article

Source : *Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle*

Denis JACOPINI questionné par un journaliste de l’Express | Le Net Expert Informatique

	Denis JACOPINI questionné par un journaliste de l’Express

Le site d'actualité de jeux vidéo Nintendojo.fr a faussement annoncé mercredi 1er avril avoir été bloqué par le ministère de l'Intérieur. Une blague douteuse qui, par l'absurde, révèle néanmoins certains écueils de la loi Cazeneuve. Explications.

Voici l'écran qui s'affiche ce mercredi lorsque l'on tente de se connecter au site Nintendojo.fr

Ministère de l'Intérieur

Enfin, les détracteurs de la loi Cazeneuve tiennent leur martyr! Jugez donc: Nintendojo.fr, un simple site consacré à l'actualité des jeux Nintendo, est inaccessible ce mercredi. Il renvoie vers une page du ministère de l'Intérieur qui explique que le contenu a été bloqué. Une mesure qui est autorisée depuis le vote de la loi Cazeneuve fin 2014, avec de premiers cas en mars dernier, mais en principe réservée aux sites terroristes ou pédophiles.

Rassurez-vous tout de suite. « Il s'agit d'une blague de mauvais goût et ça nous a bien fait rigoler », explique à L'Express Mortal, l'administrateur du site. Il ne faut donc pas voir la main du ministère de l'Intérieur derrière ce faux blocage, mais un poisson d'avril qui aura trompé des dizaines d'internautes et quelques sites d'information.

Pourquoi ce gag?

« Ce n'est pas un geste politique, mais nous estimons quand même que la loi qui permet le blocage de certains sites internet est mauvaise, justifie Mortal, qui se revendique de la Quadrature du Net, association de défense des libertés sur internet hostile au dispositif. On avait envie de piquer les gens pour que ça éveille un peu les consciences sur le sujet. Cela pourrait arriver pour de vrai à d'autres demain, c'est ça le problème », tranche-t-il.

De la difficulté de distinguer « vrai » et « faux » blocage

Qu'on le juge drôle ou pas, le poisson d'avril de Nintendojo.fr pose de sérieuses questions sur le principe même de bloquer certains sites Internet. Est-il possible pour un internaute face à une page qui affiche le fameux message du ministère de l'Intérieur de savoir avec certitude que le site a été bloqué? « La réponse est simple: c'est non », estime **Denis Jacopini**, consultant en cybersécurité. Point de vue partagé par plusieurs observateurs interrogés ce mercredi.

« **Rien est impossible, poursuit l'analyste. Cela peut être un vrai message, bien sûr. Mais cela peut aussi être une blague de l'administrateur du site, ou l'oeuvre d'un hacker qui a modifié le site**« , avance-t-il.

Qu'en pense l'Intérieur? Contactés par L'Express, les services du ministère n'ont pas donné suite à nos sollicitations. A ce jour, les services de la Place Beauvau n'ont pas mis en place de dispositif pour informer sur de telles situations. Il ne serait pas étonnant, dans ce contexte, de voir fleurir les farces voire de réelles arnaques du même tonneau dans les semaines qui viennent.

Attention, arnaques à prévoir…

Dans le cas de Nintendojo.fr, l'artifice était plutôt élaboré. Le message affiché sur la page d'accueil du site reprenait, aussi bien graphiquement qu'au niveau du contenu, celui affiché en cas de blocage. Ce n'est pas tout. Un utilisateur de Twitter a comparé le code HTML de la page vers laquelle redirigeait Nintendojo.fr avec celui d'une page affichée via un site réellement bloqué par l'Intérieur, et ils étaient bien identiques.

Mais Nintendojo.fr est allé encore plus loin. « Nous avons vraiment procédé à un blocage DNS » (domain name system, nom de domaine) explique Mortal. Ce qui a pu donner l'illusion a certains que le site avait bel et bien été « bloqué ». « Techniquement, le dispositif de censure fait appel à un résolveur DNS menteur, c'est-à-dire qu'il ne renvoie pas le résultat correct, mais un mensonge tel que demandé par le gouvernement », explique nextinpact.com.

Concrètement, le gouvernement n'efface pas les sites bloqués: l'internaute qui essaye de s'y connecter est simplement redirigé vers la fameuse page ministérielle. Un mécanisme que Nintendojo.fr a plutôt bien singé ce mercredi.

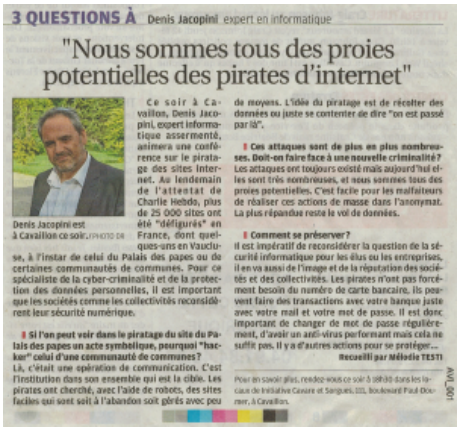
« On aurait pu faire encore plus sophistiqué »

Les bons connaisseurs, eux, ont néanmoins pu déjouer la supercherie en testant d'autres DNS. Ils ont alors observé que tous renvoyaient vers la page du ministère de l'Intérieur, ce qui n'aurait pas été le cas pour un « vrai » blocage gouvernemental. En situation réelle, les fournisseurs d'accès à Internet (FAI) bloquent le site concerné au fur et à mesure, ce qui prend du temps. De plus, il existe des DNS publics, gérés par d'autres acteurs du Web (par exemple, Google), qui peuvent ne pas faire l'objet de blocage. Changer de résolveur DNS est d'ailleurs précisément l'une des solutions pour ceux qui souhaitent contourner la censure.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://lexpansion.lexpress.fr/high-tech/les-vraies-questions-que-pose-le-faux-blocage-de-nintendojo-par-le-gouvernement_1667195.html

Nous sommes tous des proies potentielles des pirates d’Internet



3 QUESTIONS À Denis Jacopini expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites Internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Denis Jacopini est à Cavaillon ce soir. PHOTO DR

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes?

Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité?

Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver?

Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger...

Recueilli par Mélodie TESTI

Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de l'Initiative Causse et Sorgues, 111, boulevard Paul-Doumer, à Cavaillon.

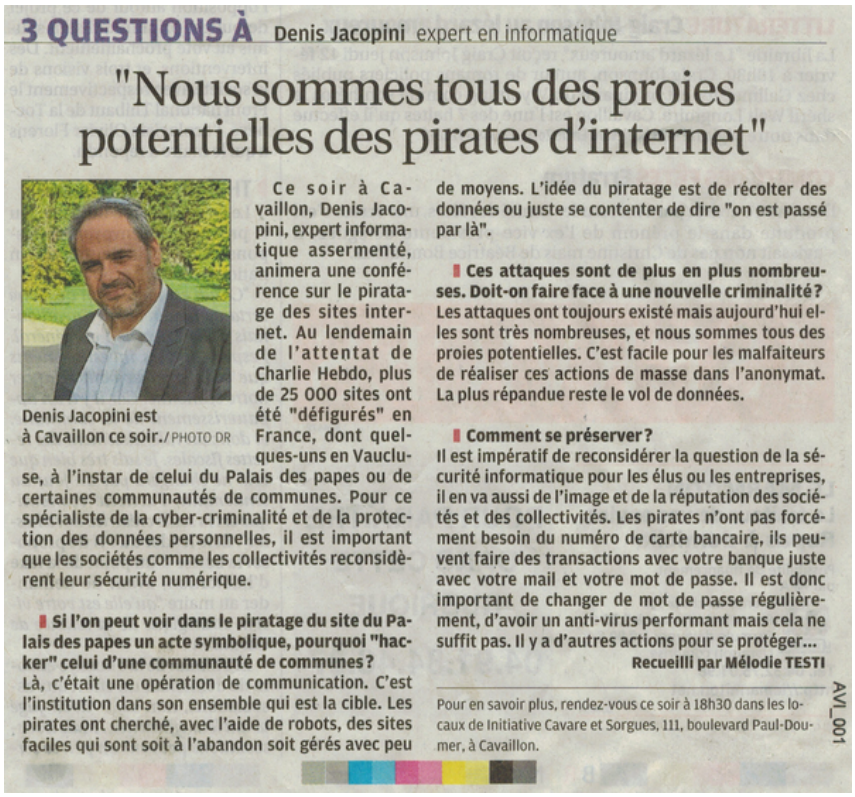
AVI_001

Nous sommes tous des proies potentielles des pirates d’Internet

A la suite des attentats de Paris à Charlie Hebdo le 7 janvier 2015, plus de 25000 sites Internet ont été « défigurés » en France. Dans le but de continuer à sensibiliser les chefs d'entreprises et Elus qui ne connaissent ou ne maîtrisent pas encore bien le sujet, le 10 février 2015, Denis JACOPINI a animé une conférence à Cavaillon.

Victime d'actes illicites, les cibles de la cybercriminalité se sentent démunies face à ce risque incoercible. Après un état des lieux, la conférence à dévoilé les principales raisons pour lesquelles la cybercriminalité sévit aussi facilement.

Enfin, des solutions de bon sens ont été présentées, concernant à la fois la mise en place de mesures de sécurité, mais aussi le respect de la loi informatique et libertés chargée d'encadrer l'usage et la protection des données personnelles, des données à caractère personnel.



3 QUESTIONS À Denis Jacopini expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"

Denis Jacopini est à Cavaillon ce soir./PHOTO DR

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes?

Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité?

Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver?

Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger...

Recueilli par Mélodie TESTI

Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de Initiative Cavare et Sorgues, 111, boulevard Paul-Doumer, à Cavaillon.

AVI_001

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.horizon2020.gouv.fr/pid29774/securite.html

---

Cyber-attaques : Denis

Jacopini, expert, alerte – Article dans Midi Libre Gard…

13

	Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…

Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.Après les attentats du 7 janvier, de nombreux sites internet d'institutions locales ou religieuses en France ont été piratés par des groupes de hackers se présentant comme des islamistes, dont celui du palais des Papes à Avignon, victime d'un "défaçage" (remplacement de la page d'accueil du site) par un groupe dénommé Fallaga team . Ces phénomènes de piratage ne sont pas nouveaux et s'accentuent. Ils sont imputables à différents types de malfaiteurs et se matérialisent de manière très différente. Décryptage des cyber-attaques avec Denis Jacopini, expert judiciaire près la cour d'appel de Nîmes et des juridictions du Gard, du Vaucluse, de l'Ardèche et de la Drôme. Denis Jacopini : « Les chefs d'entreprise ne sont pas assez sensibilisés. » DR Qu'est-ce qu'une cyber-attaque ? C'est une attaque informatique utilisant les réseaux de télécommunication et cela existe depuis qu'Internet s'est répandu dans le…

Bagnols

Midi Libre | midilibre.fr
MERCREDI 11 FÉVRIER 2015 | 3

Cyber-attaques : « Les sociétés ne se protègent pas »

Entretien | Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.

Contexte

Qu'est-ce qu'une cyber-attaque ?

« On peut stopper le phénomène si on change les mentalités »

Il semble impossible, quelle que soit la structure attaquée, de s'en prémunir.

A-t-on une idée du nombre de victimes que font ces attaques ?

Mais cette lutte coûte cher pour de petites structures comme une mairie !

GROS PLAN

La e-reputation

Gard : 20 faits de piratage de sites en 2014 et cinq en 2015

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.midilibre.fr/2015/02/11/cyber-attaques-les-societes-ne-se-protegent-pas,1123222.php

Denis JACOPINI est intervenu au Salon du numérique 2015 le 3 février et a coanimé une conférence avec Orange

Denis JACOPINI est intervenu au Salon du numérique 2015 le 3 février et a coanimé une conférence avec Orange

Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.

Imaginez maintenant que ce professionnel c'est vous, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !
Comment ne pas être ce professionnel négligeant en protégeant le patrimoine le plus précieux de votre entreprise : Votre réputation
Cette conférence était présentée par Denis JACOPINI (Le Net Expert Informatique) et Eric Wiatrowsi (Orange Business Services)

Présentation pdf de Denis JACOPINI Le Net Expert Informatique
Présentation pptx de Hervé JUHEL Crédit Agricole
Les infos pratiques du salon
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Denis JACOPINI Intervient au Salon du numérique 2015 le 3 février et coanime une conférence avec Orange

	Denis JACOPINI Intervient au Salon du numérique 2015 le 3 février et coanime une conférence avec Orange

10h00 – 10h45 – Cybercriminalité, protection des données personnelles et Réputation
Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.
Imaginez maintenant que ce professionnel c'est vous, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !
Venez découvrir, comment ne pas être ce professionnel négligeant en protégeant le patrimoine le plus précieux de votre entreprise : Votre réputation
Présenté par Denis JACOPINI (Le Net Expert) et Eric Wiatrowsi d'Orange

Le 3ème Salon du Numérique en Vaucluse c'est Mardi 3 février 2015 de 9 h à 20 h à la salle polyvalente de Montfavet – Rue Félicien Florent, 84000 Avignon

Entrée libre, inscription obligatoire ! 600 m² – 35 stands – 16 conférences – Le rendez vous incontournable du numérique pour votre entreprise.

Entrée gratuite, inscription obligatoire
http://www.salon-du-numerique.fr/reservez-votre-place

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Programme et infos pratiques : http://www.salon-du-numerique.fr/le-programme/