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…

Quels dégâts après une attaque DDoS ?

	Quels dégâts après une attaque DDoS ?

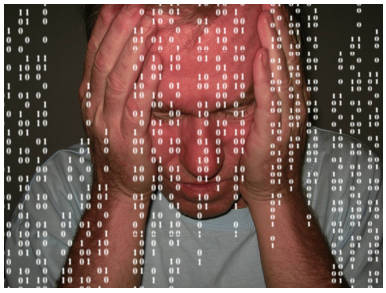
Selon les résultats d'une étude réalisée par Kaspersky Lab et B2B International, une attaque DDoS contre les ressources en ligne d'une entreprise pourrait causer un préjudice considérable, se chiffrant en moyenne entre 52 000 et 444 000 dollars selon la taille de l'entreprise. Pour de nombreuses entreprises, ce coût a un sérieux impact sur leur bilan ainsi que sur leur réputation en raison de la perte d'accès aux ressources en ligne pour leurs partenaires et leurs clients.

Ce coût total reflète plusieurs problèmes. Selon l'étude, 61 % des victimes d'une attaque DDoS ont temporairement perdu l'accès à des informations critiques ; 38 % ont été dans l'incapacité de poursuivre leur activité principale ; 33 % font état de pertes d'opportunités et de contrats. En outre, dans 29 % des cas, le succès d'une attaque DDoS a eu un impact négatif sur la cote de crédit de l'entreprise et, dans 26 % des cas, a entraîné une augmentation de ses primes d'assurance.
Les experts incluent dans le calcul des coûts moyens la réparation des conséquences d'un incident. Par exemple, 65 % des entreprises ont consulté des spécialistes en sécurité informatique, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque. Et il ne s'agit là que des frais les plus courants.
Les informations sur les attaques DDoS et les perturbations qui en résultent pour l'entreprise sont souvent rendues publiques, ce qui accentue encore les risques. 72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d'un incident, 36 % l'ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d'une attaque DDoS et près d'une sur trois a dû demander l'aide de conseillers en image.
« Une attaque DDoS qui fait mouche peut compromettre des services critiques, avec des conséquences graves pour l'entreprise. Par exemple, les récentes attaques contre des banques scandinaves (en particulier OP Pohjola Group en Finlande) a interrompu pendant quelques jours les services en ligne ainsi que le traitement des transactions par carte, un problème fréquent en pareil cas. C'est pourquoi les entreprises doivent aujourd'hui considérer la protection DDoS comme faisant partie intégrante de leur politique globale de sécurité informatique. Cet aspect est tout aussi important que la protection contre les malwares, les attaques ciblées, les fuites de données et autres », commente Tanguy de Coatpont, Directeur Général chez Kaspersky Lab France.
La technologie de Kaspersky Lab assure la continuité d'accès aux ressources en ligne de ses clients, y compris pendant les attaques DDoS complexes, prolongées ou d'un type jusque-là inconnu. Kaspersky DDoS Protection détourne le trafic client vers les centres de nettoyage de Kaspersky Lab pendant la durée de l'attaque, filtrant le trafic malveillant de sorte que le client ne reçoive que les requêtes légitimes et que ses infrastructures et services ne soient pas saturés.

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

Source : http://www.globalsecuritymag.fr/Kaspersky-Lab-et-B2B-International,20150128,50328.html par Kaspersky

Le cybervandalisme envahit internet

	**Le cybervandalisme envahit internet**

Après le piratage du site de Sony Pictures et les cyberattaques de nombreux sites internet français, le piratage est de plus en plus présent sur internet. Depuis ces événements, on entend de plus en plus parler de « cyberguerre » ou de « cybervandalisme », mais qu'en est-il vraiment ? Voici quelques réponses.

Le « cybervandalisme » plutôt qu'une « cyberguerre »

Les Etats-Unis contre la Corée du Nord, les Anonymous contre l'Etat Islamique, on pourrait assimiler le piratage informatique à une sorte de guerre virtuelle tant les conséquences sont importantes. Le piratage de Sony Pictures a d'ailleurs pris une tournure politique : Barack Obama a pris officiellement la parole sur ce sujet et a préféré associer ce phénomène à du « cybervandalisme » et non à un acte de guerre. Le hacking de Sony Pictures a été conséquent puisqu'il a retardé la diffusion du film The Interview, une comédie à propos d'un complot fictif de la CIA pour assassiner le leader de la Corée du Nord Kim Jong-Un. De nombreuses informations privées ont également été dérobées.

La lutte contre les cyberattaques ne fait que commencer, mais des moyens sont mis en place pour éviter le piratage de nombreux sites internet ou comptes Facebook. Ce concept recoupe la réflexion sur la guerre économique et la stratégie d'intelligence économique, qui accordent, entre autres, une place prépondérante à la cybersécurité et transformation numérique. L'essentiel pour dominer aujourd'hui serait de posséder l'information, avant de posséder des territoires ; et le web est une mine d'or pour partir à la recherche de données confidentielles et capitales, que ce soit en politique ou pour le lancement d'un nouveau produit.

Comment se prémunir contre les cyberattaques ?

Au travers des entreprises attaquées, c'est tout un chacun qui peut être touché. En effet, le nombre de fraudes à la carte bancaire lors d'un achat sur internet a fortement augmenté ces dernières années. Les entreprises possédant des sites internet ou boutiques en ligne doivent les sécuriser au maximum afin d'éviter toute cyberattaque. Elles stockent et protègent les données personnelles des clients pour que les hackers ne puissent y accéder. Les pirates informatiques tentent en effet de dérober les codes bancaires des internautes par l'intermédiaire de cyberattaques.

Lorsque les internautes se retrouvent sur une boutique en ligne pour acheter un billet d'avion, une voiture ou des vêtements, ils doivent avoir la possibilité de payer en toute sécurité. Si ce n'est malheureusement pas toujours suffisant, plusieurs moyens de payement alternatifs ont été développés et sont mis à la disposition de tout acheteur, afin d'éviter de dévoiler les données personnelles de leurs cartes bancaires.

Plusieurs sites comme Paysafecard.com proposent des cartes prépayées pour faciliter les paiements en ligne. Il suffit de se créer un compte pour obtenir une carte de crédit prépayée qui se recharge à tout moment. Vous pouvez mettre le montant que vous désirez et payer en ligne sur des sites partenaires. Le système 3D Secure est également un bon moyen d'éviter tout piratage lors d'un paiement en ligne. Il vous permet même d'effectuer des achats rapidement sur la toile. Ces systèmes sont donc recommandés pour pallier les attaques des hackers à petite échelle.

Le meilleur moyen également de prévenir tout piratage est de choisir avec soin son mot de passe.

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

Source : http://www.archimag.com/vie-numerique/2015/01/29/fleau-cybercriminalite-comment-se-premunir

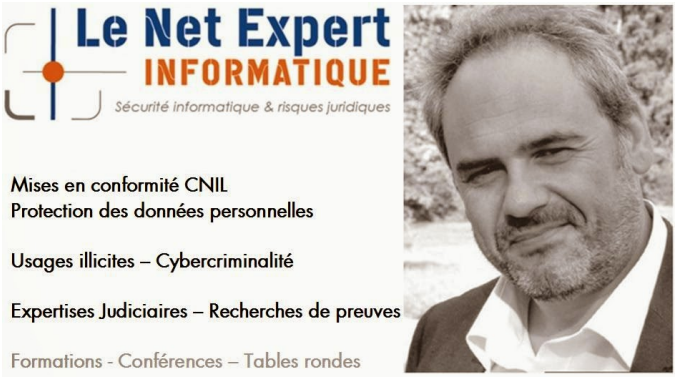
Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

	Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

La plateforme Initiative Cavare et Sorgues (ICS) accueille dans ses rangs un nouvel expert Denis JACOPINI, diplômé en droit de l'Expertise Judiciaire et en Cybercriminalité, pour sensibiliser les entreprises sur ce sujet d'actualité.

Les attaques informatiques ont toujours existé mais aujourd'hui elles sont très nombreuses.
En effet, que l'on soit une institution, une collectivité, un particulier ou une entreprise nous sommes tous des proies potentielles.
Que cela soit par méconnaissance des risques, sous-estimation des conséquences, ou bien par pure négligence, les faits sont là et nous sommes tous concernés. Piratage de serveurs, vol de données, arnaques financières en tout genre utilisant Internet… Le cyber-crime a couté plus de 327 milliards d'euros dans le monde en 2013.
Plus de 25 000 sites internet récemment défacés. Pourtant, il est possible d'enrayer ce phénomène qui semble incoercible.
Avec un peu de sensibilisation, beaucoup de bon sens et une information bien choisie, les chefs d'entreprises peuvent facilement reconsidérer l'importance de la sécurité numérique dans leurs priorités et ainsi rapidement repousser les principaux vandales du numérique.

« Nous accompagnons et finançons essentiellement des entreprises de moins de 10 salariés sur le territoire des 2 intercommunalités de l'Isle sur la Sorgue et de Cavaillon, quasiment toutes communique par l'intermédiaire entre autre d'un site internet, il nous a semblé important de les sensibiliser car il est possible d'enrayer ce phénomène » précise la directrice Anne-Laure STRETTI BOUSCARLE.
« Nous sommes très heureux que Denis JACOPINI viennent élargir les rangs des professionnels experts qui interviennent chez nous au même titre que les experts comptables, notaires, avocats, assureurs…et qu'il mette au service du plus grand nombre ses compétences pour les aider à lutter contre ces cyber-attaques».



Denis JACOPINI – Le Net Expert Informatique

Cet ancien chef d'entreprise Cavaillonnais d'une entreprise d'informatique, il a choisi après 17ans d'activité de se tourner vers son domaine de prédilection : l'expertise en sécurité informatique et en protection des données personnelles.
Diplômé en droit de l'Expertise Judiciaire et en Cybercriminalité il est à ce titre assermenté auprès des Tribunaux et spécialiste en sécurité informatique, en protection des données personnelles et en Informatique légale.
Il intervient auprès du Master II en Commerce électronique à l'Université d'Avignon, à l'Ecole de Formation des Avocats Centre Sud (EFACS), au CNFPT (Centre National de la Fonction Publique Territoriale) et est Formateur auprès de nombreux organismes dont des Centres de Gestion Agréés.
www.lenetexpert.fr

1ère session de sensibilisation le 10 février 2015 à 18 h30 dans les locaux d'ICS
Conférence débat au cours de laquelle seront évoquées les différentes techniques notamment celles qui consistent à détourner un site internet.
Inscription au préalable auprès de la plateforme
Pour vous inscrire :
Initiative Cavare et Sorgues
111 boulevard Paul Doumer 84300 CAVAILLON
Tel : 04 90 78 19 61

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

Source : Anne-Laure STRETTI BOUSCARLE

« La cyber-assurance devient une priorité pour les dirigeants d’entreprise »

	« La cyber-assurance devient une priorité pour les dirigeants d’entreprise »

Face à la recrudescence de la cybercriminalité, les dirigeants de PME et ETI s'interrogent de plus en plus sur ces nouveaux risques et la façon de s'en protéger. Le point avec Philippe Gaillard, directeur des Risques Techniques chez Axa Entreprises.

Qu'est-ce-que le cyber-risque aujourd'hui ? Comment -a-t-il évolué ces dix dernières années ?
Le cyber-risque prend de plus de plus de place dans notre quotidien. Pourtant les cyber- attaques et virus au sens large ne sont pas vraiment nouveaux. Jusqu'aux années 2000, les cyber-attaques étaient principalement des virus ou des vers informatiques qui étaient le résultat d'une sorte de compétition entre jeunes prodiges de l'informatique qui tentaient de pénétrer des systèmes prestigieux connus pour être inviolables. Autour des années 2005, les cyber-attaques ont évolué et se sont dirigées vers les Etats et les défenses nationales. Depuis 2010, on observe une recrudescence de ces attaques. Elles sont de plus en plus complexes, et prennent des formes de plus en plus variées. On commence à voir de l'espionnage industriel, des attaques entre concurrents, de l'extorsion et de la fraude. C'est toute cette évolution qui fait que les entreprises, quelle que soit leur taille, sont victimes de plus en plus de cyber-attaques. En cinq ans, la cybercriminalité s'est accélérée en nombre, et transformée en complexité et en variété d'objectifs.

Quels sont les cyber-attaques le plus souvent répertoriées ?
Il existe trois grandes catégories de cyber-attaques.
Le sabotage, qui peut soit être une vengeance envers un tiers, soit une compétition entre sociétés mal intentionnées à l'instar de ce qui pouvait donner lieu autrefois à un incendie volontaire de la part d'un mauvais concurrent.
Seconde catégorie, l'espionnage, qui consiste à aller chercher de l'information dans les autres entreprises, que ce soit de l'information commerciale ou technologique. Dans ce cas, ce sont les directions générales et les équipe de R&D qui sont les plus ciblées.
Troisième catégorie : la criminalité ou la piraterie qui consistent à voler des données ou à paralyser un système en espérant avoir une rançon en échange. Il est important de savoir que ces cyber-attaques agissent dans la durée. D'abord, elles se préparent longtemps à l'avance, car lorsqu'il s'agit d'espionnage par exemple, les criminels doivent commencer par chercher à comprendre la culture et les points sensibles de l'entreprise qu'ils visent. A la suite de cela, ils injectent un logiciel malveillant dans le système informatique de l'entreprise et le font évoluer pour se rapprocher progressivement de la cible finale. Entre le moment où se font les premières intrusions dans l'entreprise et le moment où est découverte cette action malveillante, il se passe bien souvent un an, voire plus.

Pouvez-vous nous donner un exemple type de cyber-attaque ?
Aujourd'hui, la plupart des comités de direction des grandes entreprises sont sur le réseau Linkedin. La technique utilisée par un cybercriminel pour pénétrer dans le système de l'entreprise est assez simple. Il repère des personnes qui travaillent sur un sujet sur lequel il y a eu un séminaire par exemple ; il envoie un mail piégé aux personnes susceptibles d'avoir été présentes à ce séminaire en leur faisant croire qu'il y participait également. Dans ce mail, il y a une pièce jointe qui annonce par exemple un compte rendu du séminaire. De fait, parmi les personnes réceptionnaires de cet email, il y a en a qui ont réellement participé à ce séminaire. Pour ceux et celles qui ouvrent la pièce jointe, le virus pénètre aussitôt dans leur système informatique. Le mal est fait. Le virus paralyse ensuite l'ordinateur de la personne qui aura ouvert la pièce jointe ; ladite personne appelle alors son help desk, qui bien souvent intervient à distance sur les ordinateurs. Pour prendre la main, l'expert informatique en charge de réparer l'ordinateur saisit le mot de passe administrateur. Il est aussitôt enregistré par le virus qui peut ensuite, tout doucement, progresser dans le système informatique de l'entreprise ciblée jusqu'à parvenir par exemple au serveur de la direction générale ou celui de la R&D.

Comment réagissent les dirigeants de PME-PMI face à la cybercriminalité ?
Il y a encore deux ans, les dirigeants de PME-PMI ne s'inquiétaient pas vraiment des cyber-attaques. Mais depuis douze mois, face aux dernières attaques médiatiques qu'ont pu connaître de grands groupes, l'inquiétude est en train de monter fortement. Selon notre dernier baromètre de juin 2014, sur 500 chefs d'entreprises interviewés, 46% placent le cyber-risque parmi leurs préoccupations majeures. Ce qui était un quasi non sujet il y a encore un an tend à devenir une priorité. D'autant plus que les PME et ETI sont mal protégées et donc deviennent des cibles très vulnérables. Par ailleurs, elles peuvent être des sous-traitants de grosses entreprises et par conséquent être une porte d'entrée pour les cybercriminels qui visent ces grands groupes.

Comment les entreprises peuvent-elle se protéger des cyber-attaques ?
Une bonne protection doit être équilibrée et reposer sur trois piliers. Le premier, c'est bien évidemment la technologie pour empêcher les virus de pénétrer les systèmes informatiques, pour les détecter et les traiter. Cela est nécessaire mais totalement insuffisant ! Le second, c'est l'information et la formation des salariés. Il est primordial de sensibiliser les collaborateurs aux bonnes pratiques afin d'éviter les comportements qui mettent l'entreprise en danger. En troisième lieu, il faut travailler sur la résilience de l'entreprise pour limiter les effets d'une possible attaque notamment en anticipant les capacités de rebond et de continuité d'activité. Les entreprises doivent admettre que, quoi qu'elles fassent, elles peuvent être attaquées. A l'instar d'une porte blindée, si un voleur veut pénétrer dans les lieux, et qu'il peut y mettre les moyens, il finira bien par entrer. Donc, partant du principe que toute entreprise sera attaquée à un moment ou un autre, il est important de proposer des solutions qui aident l'entreprise à limiter les dégâts et redémarrer au plus vite.

Existe-t-il des assurances qui protègent les entreprises de la cybercriminalité ?
Axa Entreprises est l'assureur d'une PME sur trois en France ; nous mettons un point d'honneur à les accompagner pour répondre à leurs besoins. Face aux cyber-risques, nous avons conclu un partenariat avec le département cyber sécurité du Groupe Airbus, qui est la référence dans le domaine.
Pour les ETI et les grandes entreprises, nous proposons de réaliser un audit de risques, mené par un ingénieur d'Axa et un ingénieur d'Airbus qui interviennent en binôme. Cet audit donne lieu à un diagnostique complet de la situation de l'entreprise face aux cyber-risques. Sur cette base, en fonction des situations, nous pouvons proposer une solution d'assurance qui combine deux volets complètement imbriqués : un contrat d'assurance qui couvre toutes les conséquences des cyber-attaques ainsi qu'un accompagnement dans le temps en ingénierie pour aider l'entreprise à maitriser son risque cyber et à l'améliorer.
Pour les PME, nous avons élaboré une approche simplifiée. Aussi bâtie en collaboration avec l'expertise du groupe Airbus, cette approche repose sur un questionnaire très simple, accessible à tous. A partir des réponses à ce questionnaire, nous pouvons réaliser une mesure du risque cyber et ainsi proposer une offre d'assurance avec des garanties et un tarif adaptés. Sur cette même base un diagnostic cyber est remis au client d'AXA Entreprises pour l'accompagner dans ses actions de prévention contre les risques cyber. Les PME ayant rarement les contacts nécessaires, se trouvent bien souvent démunies quand survient un sinistre cyber. Par conséquent, au-delà des garanties de dommage, de responsabilité civile, de protection des données personnelles et d'accompagnement à la gestion de crise, la valeur de l'offre d'assurance réside beaucoup dans sa capacité à proposer un accompagnement global de proximité de l'entreprise, en amont et en aval, avec des services pragmatiques, rassurants et réactifs.

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

Source :
http://www.latribune.fr/loisirs/la-tribune-now/20150128tribd355efe7a/la-cyber-assurance-devient-une-priorite-pour-les-dirigeants-d-entreprise.html

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/

La cybercriminalité à l’encontre des entreprises s’industrialise

	La cybercriminalité à l’encontre des entreprises s’industrialise

Un écosystème professionnalisé de cybercriminels mène la danse.
Pas d'électrochoc dans les entreprises après l'affaire Sony : les investissements restent insuffisants.
Sony débordé par les cybercriminels
Phishing, escroquerie, espionnage, vol de secrets industriels… Si ces phénomènes ne sont pas nouveaux, la cybercriminalité ne s'est jamais aussi bien portée.
Bernard Cazeneuve n'a pas manqué de rappeler la réalité de cette menace au Forum international de la cybersécurité, qui s'est tenu à Lille la semaine dernière. « Des attaques de plus en plus sophistiquées touchent principalement les entreprises et visent à leur voler des données stratégiques, parfois en très grande quantité », a fait valoir le ministre de l'Intérieur. Si le phénomène est difficile à chiffrer, il connaît une montée en puissance. Pourquoi ? « La technologie explose. Il y a de plus en plus d'applications. Plus on développe vite, plus le risque de bugs augmente», explique Jean-Michel Orozco, président de CyberSecurity chez Airbus Group (ex-Cassidian).
Au quotidien, les entreprises doivent lutter contre la petite délinquance, peu sophistiquée mais rentable. « Les entreprises ont été fortement touchées par les "cryptolockers" », explique Eric Freyssinet, chef de la division de lutte contre la cybercriminalité de la Gendarmerie nationale. Des pirates bloquent des PC, et exigent des rançons pour les débloquer. Bien sûr, celui qui paie ne récupère pas pour autant ses données.
« Les anciennes menaces s'industrialisent. Les banques, par exemple, souffrent beaucoup d'attaques en déni de service [rafale d'attaques dont le but est de bloquer les systèmes] ou de phishing », explique Michel Van Der Berghe, à la tête d'Orange Cyberdefense. Plus élaboré, « le "spearphishing" permet d'envoyer des e-mails ultraciblés personnalisés par secteur identifié, l'armement, le transport… » dit Eric Freyssinet. C'est grâce à un e-mail très bien personnalisé que la Syrian Electronic Army a réussi, ces derniers jours, à pirater « Le Monde ».

Des PME très exposées
Les PME sont particulièrement exposées aux faux placements, où la victime verse de l'argent à un tiers soi-disant spécialisé dans les placements à haut rendement. Selon la gendarmerie, ce type d'attaque représente les « trois quarts des escroqueries » qui concernent les entreprises. Plus connue, « l'arnaque au président » consiste à extorquer de l'argent à une entreprise en se faisant passer pour son dirigeant. Parmi les victimes, Michelin, qui a perdu 1,6 million d'euros.
L'espionnage – de secrets industriels ou commerciaux –, un fléau auquel font face les entreprises depuis deux ou trois ans, ne requiert pas non plus de techniques ultrasophistiquées. « Un mot de passe faible, type 1 2 3 4 5 6, sur un équipement de réseau ou une application peut suffire », estime Stanislas de Maupeou, directeur-conseil cybersécurité chez Thales. Dans ce cas-là, la difficulté consiste surtout à identifier les intrusions.

Cellules « N-Tech » : la gendarmerie aussi s'arme face à la cybercriminalité

Pas facile de lutter contre ces attaques à grande échelle. Car, en face, on a affaire, non pas à des groupements organisés, mais à un écosystème criminel. « Sur le "dark Web", on trouve des publicités pour des attaques en kit. Il y a même des réductions ! » explique Michel Van Der Berghe. « Ceux qui vendent les virus ne sont pas ceux qui les collectent. Deux personnes différentes à deux bouts de la France peuvent se mettre d'accord pour développer un virus. Elles communiquent sur Tor, sur certains forums ou sur des messageries instantanées comme Jabber », explique le lieutenant-colonel.
De leur côté, les entreprises restent insuffisamment armées. Le piratage massif de Sony, victime d'un vol à grande échelle de données, n'a pas créé d'électrochoc. Chez Thales, un seul client exerçant dans le même domaine que Sony, et expliquant qu'il ne pourrait supporter une attaque d'une telle ampleur, a appelé, chez Airbus aucun.

Pas seulement des moyens
Beaucoup de dirigeants n'ont pas encore fait grand-chose. « Les moyens seuls ne suffisent pas. Il faut aussi un plan, avec une gouvernance qui sait quoi faire en cas de problème », détaille Jean-Michel Orozco, d'Airbus CyberSecurity, qui estime qu'un grand groupe devrait dépenser entre 8 et 11 % de son budget informatique en sécurité. On est loin du compte. « Aujourd'hui, on est à 3 ou 4 %. Or, en cas de problème, si l'on doit remonter entièrement un système, cela peut coûter 20 % du budget IT », estime Stanislas de Maupeou, qui rappelle qu'au regard des outils existants, la lutte contre le fléau est à la portée de tous.

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

Source : http://www.lesechos.fr/tech-medias/hightech/0204110358637-la-cybercriminalite-a-lencontre-des-entreprises-sindustrialise-1087050.php
Par Sandrine Cassini

Le NFC est-il vraiment utile pour le paiement ?

Le NFC est-il vraiment utile pour le paiement ?

Un sondage rapporte que les Français ne considèrent pas le NFC comme utile pour réaliser des paiements. Les banques se sont pourtant massivement dirigées vers cette technologie, notamment avec leurs cartes de paiement.

Régler un achat en passant simplement sa carte sur une borne ne semble pas intéresser outre mesure les Français. En dehors des défauts et qualités inhérents au NFC, un sondage réalisé par Odoxa pour le compte du Syntec Numérique, montre que l'utilité de cette technologie reste encore à démontrer.
Selon l'étude réalisée en janvier dernier auprès d'un échantillon de 1 008 personnes représentatif de la population, pas moins de 57% des sondés « trouvent le paiement sans contact inutile. Ce désintérêt pour le sujet semble toucher toutes les catégories de population interrogée ».
L'institut nuance ce résultat par le fait que certaines personnes interrogées vivent en milieu rural et ne disposent pas de moyens d'utiliser le NFC au quotidien. Malgré ce point, le désintérêt envers ce type de technologie, en particulier pour le paiement, est clairement affirmé.
Cette étude (.pdf) vient s'ajouter à d'autres sondages montrant des résultats identiques. En février dernier, une analyse réalisée par Statista expliquait que seulement 22% des Français étaient à l'aise avec le paiement sans contact. Ces derniers précisaient qu'ils préféreraient de loin l'usage traditionnel de la carte de paiement (insertion dans la fente d'un terminal puis code à taper).

Le paiement NFC n'a pas décollé en France
La carte à puce semble donc avoir encore de beaux jours devant elle. C'est pourquoi les banques se sont massivement dirigées vers le NFC en proposant à leurs clients des cartes compatibles avec la technologie. Le succès n'est, malgré tout, pas au rendez-vous puisque les transactions réalisées par ce biais ne représentent qu'une infime partie du volume global.
Le sondage réalisé pour le Syntec Numérique confirme ce mouvement. Il indique que 44% des personnes interrogées ont connaissance de la fonction paiement sans contact de leur carte bancaire, mais seulement 15% l'ont déjà utilisée. Pire, 29% des sondés affirment ne pas se servir de cette option tout en sachant que leur carte est compatible NFC.
Pour tenter d'inverser la tendance, les professionnels entendent communiquer davantage sur l'intérêt de la technologie. Dans ce cas, ils devront également informer des risques que peut représenter le NFC en termes de sécurité.

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

Source : http://pro.clubic.com/e-commerce/paiement-en-ligne/actualite-751153-nfc.html
Etude : http://www.syntec-numerique.fr/sites/default/files/cp_sondage_odoxa_paiement_sans_contact_22janv2015.pdf

Risques informatique : « Jusque-là, on nous prenait pour des paranos »

	Risques informatique : « Jusque-là, on nous prenait pour des paranos »

Non, même au Forum international de la cybersécurité, les experts ne hurlent pas à la cyberguerre. Leur secteur reconnu, ils restent modérés sur la menace… tout en profitant des récentes attaques.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)

Se balader dans les travées du FIC, le Forum international de la cybersécurité qui se tenait à Lille ces 20 et 21 janvier, a de quoi faire flipper.
Partout, des bannières en rouge et noir ; l'une avec un gros masque d'Anonymous, l'autre reconstituant une scène de crime, rubans policiers jaunes barrant l'accès, non pas à des corps mais à des serveurs.

Des bannières aperçues sur les stands du FIC 2015 (Andréa Fradin/Rue89)

Des écrans diffusant des films où clignotent « Heartbleed », « Stuxnet » (noms des dernières vulnérabilité et attaque célèbres), dans des environnements rappelant les nanars hollywoodiens dans lesquels de petits-génies-mais-méchants-hackers lancent une opération hyper sophistiquée contre une banque, ou un organisme gouvernemental.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)

En plus de l'ambiance anxiogène, s'étalent aussi tout autour de moi des termes imbitables, des anglicismes techniques qui rappellent un peu les pubs pour le shampoing, où pro-vitamine B5 et revitalisants sont remplacés par « Net HSM » et « audit de SSI ».

La France, ses fromages, sa cybersécurité…
Les noms des entreprises de sécurité informatique, et des produits qu'elles vendent, sont tout aussi carabinés : Stormshield Network Security, Arkoon, Netasq, TrustWay Proteccio, Prim'x Technologies… Sur scène, les représentants de ces sociétés défilent tout sourire, manipulant à merveille, et sans sourciller, ces intitulés barbares.
Tous viennent de recevoir un label des mains de la secrétaire d'État en charge du numérique Axelle Lemaire – le label « France cybersécurité » –, « l'AOC » en la matière, se réjouit un homme. Qui ajoute :
« La France était connue pour ses fromages et ses vins, elle le sera désormais pour la cybersécurité. »

Les lauréats du label France cybersécurité (Andréa Fradin/Rue89)

Des hommes, revenons-y, il n'y a d'ailleurs que ça sur scène : sur vingt lauréats, costumes sombres, coupe sage, seule une femme est montée recevoir le fameux trophée en verre dont je ne comprends pas l'utilité.

Des képis partout
Tout ce petit monde, en revanche, semble très bien comprendre. Et très bien se connaître. Dans les salles et les travées du FIC, tout aussi masculines, on se donne du « tu », on vanne sur des termes techniques tout aussi alambiqués que l'intitulé des sociétés auxquelles on appartient, on connaît le travail du voisin installé sur le siège d'à côté. Et ce, même quand son badge indique un mystérieux « ministère de la Défense ».

Des militaires, au FIC 2015, à Lille (Andréa Fradin/Rue89)

C'est d'ailleurs l'une des particularités de cet événement annuel : aux côtés des ingénieurs et informaticiens d'Airbus, Thales, Orange, Atos, et bien d'autres petites entreprises inconnues du grand public, figurent des policiers, des militaires, des gendarmes. C'est d'ailleurs eux, en grande partie, qui sont à l'origine du Forum : co-organisé par la Gendarmerie nationale, le FIC a été fondé par un général d'armée, Marc Watin-Augouard.

Des gendarmes, au FIC 2015, à Lille (Andréa Fradin/Rue89)

La cybersécurité, arme et bouclier des temps modernes, se niche quelque part à la frontière entre intérêts étatiques et objectifs de grands groupes industriels. Dans ce drôle de territoire, on parle le même langage, on opine sur les mêmes remarques.
Je ne comprends pas la moitié des références, je ne parviens pas à déchiffrer les sigles et acronymes qui pullulent ici.

« J'en veux quand même aux journalistes… »
Pas facile, vu comme ça, de saisir le petit monde de la sécurité informatique. Pourtant, il est au cœur de l'actualité.
Il y a bien sûr #OpFrance, l'opération menée ces derniers jours contre des sites internet français par des attaquants se revendiquant d'organisations islamistes. Il y a aussi eu cet incident, chez un hébergeur, qui a fait sauter bon nombre de sites d'informations en France. Et avant ça : Sony Pictures piraté, photos intimes de stars dérobées, vols de comptes et de mots de passe… Pas une semaine sans qu'une attaque informatique ne fasse les gros titres de la presse. Même chose dans les discours des hommes politiques :

« Pas un forum international sans que le mot cyber ne soit prononcé », résume le patron de l'Anssi, l'agence gouvernementale précisément en charge de la cybersécurité de la France, Guillaume Poupard.

Et l'effet se ressent directement sur le secteur.
Tous, au FIC, me confient n'avoir jamais vu une telle affluence, un tel intérêt des profanes (journaliste, grand public, politiques, petites entreprises qui débarquent sur Internet) pour leur matière.

Sur scène, un expert lance :
« Il faut parler le langage normal des entreprises […]. Etre ergonomique, simple d'utilisation ! »

Entre deux ateliers, deux autres chambrent la presse :
« J'en veux quand même aux journalistes, et à leur traitement de cette actualité…
– Il faut leur expliquer en moins de deux syllabes ! »

Les effets de la petite phrase de Cazeneuve
Cet impératif, le ministre de l'Intérieur Bernard Cazeneuve l'a lui-même sommé en ouverture du Forum, par une petite phrase par la suite énormément commentée :
« La lutte contre les cybermenaces ne peut plus être réservée au cénacle élitiste de quelques experts. »

Le stand Hexatrust, au FIC 2015, à Lille (Andréa Fradin/Rue89)

Pour le secteur, c'est à la fois une aubaine et une malédiction. Une aubaine, car l'ouverture de ces thèmes au grand public leur assure une visibilité dont ils n'ont jamais bénéficié. Une reconnaissance aussi. Dans les allées, nombreux sont ceux qui m'ont confié :

« Jusque-là, on nous prenait pour des paranos. »

Les cyberattaques, souvent invisibles, sont une menace floue, impalpable. Les échos que la presse et le monde politique donnent aux incidences directes et concrètes de ce risque le rendent forcément plus immédiat.

Et facilite aussi le business : gros bonnets du CAC 40 et PME de la région sont venus faire le tour des exposants du FIC.

Des clients : « Ça ne m'arrivera jamais ! »
Bien sûr, les réticences existent toujours :
« Les clients nous disent : "Ça ne m'arrivera jamais !"
– Ils ne voient pas en quoi ils sont concernés jusqu'à ce que ça touche un concurrent direct. »
Et les contrats, contrairement à ce que souhaitait Axelle Lemaire (« J'espère que les contrats se signent ! ») ne se font pas en un tournemain. Certains représentent un investissement de dizaines, de centaines de milliers d'euros, voire de millions pour un « package complet » sécurisant tous les postes d'une grosse boîte :
« Il faut entre 12 et 24 mois pour signer un contrat. »
Mais oui, l'intérêt est là.

Le stand du ministère de l'Intérieur, au FIC 2015, à Lille (Andréa Fradin/Rue89)

Mais l'ouverture est pour certains synonyme de trahison. D'abandon de la connaissance éclairée au profit d'intérêts commerciaux, ou de récupération politique, forcément trop simplistes.

« Bienvenue au Fric ! Euh, au FIC ! »
Un participant note le fossé existant entre les prises de parole en plénière, investie par les politiques, et les ateliers, où l'on parle concret : comment fait-on une enquête lors d'une attaque utilisant malgré elle des milliers de machines infectées par un logiciel malveillant ? Comment la coopération entre les agences chargée de la cyberdéfense s'établit en Europe et dans le monde ?

Un autre, pourtant lui-même exposant, se rappelle :
« Avant ce n'était pas comme ça. Au début, il n'y avait que des képis. Aucun sponsor, aucune marque. C'était plus confidentiel mais moins marketing. Le salon n'a jamais été aussi grand que cette année. »

Au FIC 2015, à Lille (Andréa Fradin/Rue89)

Au matin du 20 janvier, juste avant les préliminaires officiels menés par Bernard Cazeneuve, Pierre de Saintignon (vice-président du conseil régional du Nord-Pas-de-Calais) provoquait l'hilarité de la salle en lançant :
« Merci pour votre présence à cette septième édition du Fric ! Euh, du FIC ! »

Lapsus révélateur de l'un des paradoxes qui traverse le secteur : tous reconnaissent bien sûr qu'il faut faire du business. Mais en aparté, chacun concède aussi que parfois, ça va trop loin :
« Certains en font des tonnes pour vendre leurs produits ! »
« Il faut démystifier, il y a de l'expertise, mais comme partout ! Ça ne sert à rien d'utiliser des mots compliqués, la cybersécurité, c'est simple ! »

Le petit dernier du business de la peur
D'eux-mêmes aussi, ils reconnaissent le business de la peur, souvent reproché au secteur. Cette méthode commerciale, que les initiés désignent aussi par l'acronyme FUD, pour « Fear, Uncertainty and Doubt » (« peur, incertitude et doute »), est classique dans les professions qui vendent des solutions censées protéger de tel ou tel danger.

Elle consiste à grossir le danger en question, à le rendre plus imminent, plus inévitable et plus dommageable qu'il ne l'est vraiment. On le retrouve partout : dans le business des alarmes, des assurances, et désormais de la cybersécurité.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)
Dans les boîtes de sécurité informatique, personne ne nie le problème, ou n'esquive la question quand je l'aborde. Certains reconnaissent même en faire un peu, ironisant sur le service marketing qui fait parfois un peu de buzz sur une attaque. Beaucoup affirment, quand je souligne dans un sourire que les discours alarmistes profitent à la bonne santé du secteur, que ce n'est pas si simple. Tel cet exposant :
« C'est positif dans une certaine mesure : s'il y a une peur, alors il peut y avoir une prise de conscience.
Mais il y a aussi le risque que les gens aient trop peur, et disent : "Finalement, vos produits ne servent à rien, puisque les attaques passent de toute manière." »

Malaise autour du mot « cyberguerre »
L'exemple de la prétendue cyberguerre est à ce titre saisissant : là encore, très peu de participants au FIC utilisent ou légitiment ce terme, que l'on retrouve pourtant de plus en plus souvent dans les médias. Au contraire, la grande majorité se montre très prudente avec ce concept. Et l'ambiance générale ne laisse pas franchement penser à un état de siège.

Au stand des principaux intéressés, les représentants de la Défense sont assez mal à l'aise dès que j'aborde le sujet. Et me dirigent vers la parole officielle, celle du contre-amiral Arnaud Coustillière, officier général de la cyberdéfense, cette « quatrième armée pour un quatrième espace », depuis 2011. Ce dernier ne parle pas de cyberguerre, et se refuse à tout catastrophisme.

Un autre ajoute : « De la peur, procède la paralysie. »

Le stand du ministère de la Défense, au FIC 2015, à Lille (Andréa Fradin/Rue89)

De même, tous s'accordent à minimiser les attaques de ces derniers jours, qualifiées de « simples graffitis » par le directeur de l'Anssi. Les experts en rigolent, assurent que ces attaques sont consubstantielles au Web. De même, ou presque, que les solutions pour s'en protéger. Certains vont jusqu'à dire :

« A la limite, si des sites tombent sous ces attaques, tant pis pour eux. Ils l'ont bien cherché, ils ne se sont pas protégés. »

Extrait d'une vidéo diffusée au FIC 2015, à Lille (Andréa Fradin/Rue89)

Pourtant, ce sont bien ces attaques qui font la une des journaux, de même que ce sont bien elles qui se retrouvent citées en exemple dans le discours politique. Le décalage entre les confidences de ceux qui vivent de la cybersécurité et l'image qui en ressort dans le grand public me déstabilise.

« Human after all »
Ce n'est d'ailleurs pas le seul grand écart : bien loin de l'image des attaques hyper complexes élaborées dans des cervelles de cybercriminels machiavéliques, bien loin des termes techniques qu'ils choisissent eux-mêmes pour désigner leurs produits et leurs sociétés, les experts en cybersécurité s'attachent à m'expliquer que leur domaine n'a finalement rien de compliqué.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)
Qu'au-delà des solutions techniques, du modus operandi des cyberattaques, la cybersécurité se rapporte avant tout à l'humain, au bon sens, et à la gestion des risques :

« La gestion des risques, on en fait tous les jours. Quand on traverse la route, on fait de la gestion de risques : on regarde à droite, à gauche, on détermine s'il est dangereux de traverser à ce moment-là. Pareil avec les incendies. C'est la même chose ici. »

Et que les intrusions informatiques, même les plus spectaculaires, relèvent le plus souvent d'imprudence humaine : le fait de brancher une clé USB trouvée par hasard dans son entreprise, le fait de ne pas protéger d'un mot de passe les caméras de son réseau de surveillance (souvenez-vous de notre enquête à ce sujet…).

De l'eau qui file entre nos doigts
Finalement, je m'attendais à des cris d'orfraie sur la menace permanente et la guerre imminente, mais passés les visées marketing et politiques, j'ai avant tout eu droit à des discours modérés. Je m'attendais à être noyée sous la technique, mais passés les slogans publicitaires, j'ai eu du bon sens.

Entre impératifs commerciaux, récupération politique et réputation à tenir, le monde de la cybersécurité ne fait finalement que jongler avec ses paradoxes. Et en même temps, comment pourrait-il se débarrasser de ces forces contradictoires ? Etat, industriels, experts : les corps qui composent l'univers cybersécuritaire existent parce qu'ils prétendent pouvoir apporter une solution à un problème pourtant fondamentalement insolvable.

Dans les cyberattaques, Etats et individu isolé jouent désormais à armes égales. Avec Anonymous et d'autres, la notion d'organisation nébuleuse n'a jamais eu autant de sens. Et quand une enquête s'ouvre enfin pour déterminer l'origine d'une action malveillante, il est quasiment impossible de remonter à la source : une preuve a beau avoir été obtenue (une adresse IP, par exemple), cette dernière peut en fait s'avérer être une fausse piste. Et toute l'énergie mobilisée pour l'identifier (contacter le pays d'origine, attendre un accord de coopération qui ne vient parfois jamais…) doit être regénérée pour se déporter sur un autre pays, où l'on pourra peut-être encore faire chou blanc.

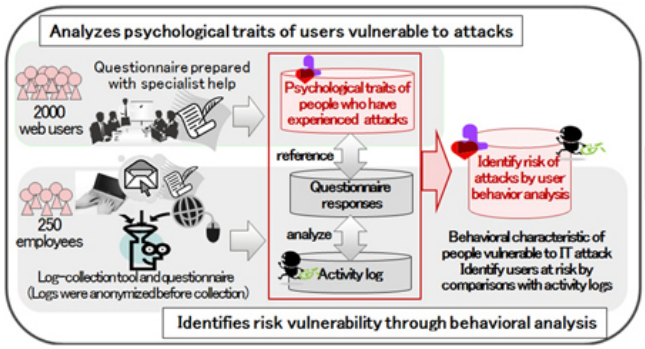
La cybersécurité revient donc un peu à essayer d'attraper de l'eau entre ses doigts. A appréhender un espace de pur mouvement, sans frontières, avec des termes, des codes, des normes forcément déjà obsolètes et inadéquates. C'est un ouvrage sans cesse détricoté, c'est Sisyphe en réseau. Et bien sûr, les acteurs qui s'évertuent à trouver des réponses ne peuvent se présenter sous ce jour.

Bruce Schneier, pape de la cybersécurité américain et guest star du FIC 2015, déclarait lors de sa conférence :
« La résilience est la clé de la sécurité informatique. […] Comment on se débrouille ? Comment on s'adapte ? Comment on survit ? »
C'est drôle : la résilience, cette capacité d'adaptation aux altérations, est précisément ce qui définit Internet.

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

Source : http://rue89.nouvelobs.com/2015/01/23/forum-cybersecurite-jusque-prenait-paranos-257257
Par Andréa Fradin

Une solution pour identifier des utilisateurs vulnérables aux cyber-attaques ?



Une solution pour identifier des utilisateurs vulnérables aux cyber-attaques ?

La société Fujitsu a annoncé avoir développé une technologie permettant d'identifier les utilisateurs vulnérables aux cyber-attaques, ayant des comportements potentiellement « à risque » donc vulnérables aux cyber-attaques. La solution est basée sur l'analyse des activités des utilisateurs sur leur ordinateur.

Cette technologie permettrait de créer des mesures de sécurité plus adaptées, comme l'affichage de messages individualisés d'alertes aux utilisateurs qui cliquent souvent sur les liens ou e-mails suspicieux, ou augmenter le niveau de menace lié aux e-mails envoyés entre départements d'une même entreprise par des utilisateurs propices à être infectés par des virus.
Jusqu'ici, un des problèmes des logiciels de sécurité est de ne pas pouvoir contrôler l'erreur humaine, comme la propension d'un utilisateur à cliquer sur les liens malveillants dans des e-mails, ou sur des sites infectés. Cette technologie permettrait d'y remédier.
Afin de développer cette solution, Fujitsu a utilisé un questionnaire en ligne, réalisé avec des experts en psychologie sociale, afin d'identifier les traits psychologiques des personnes vulnérables à trois types d'attaques : les infections par un virus, les arnaques et les fuites d'information. La société s'est également intéressée aux activités des utilisateurs pour les e-mails, l'accès internet ainsi qu'aux actions de la souris et du clavier.
Cette technologie a été présentée en détail lors du 32ème Symposium sur la Cryptographie et Sécurité de l'Information qui se tient depuis le 20 Janvier dans la ville de Kita-Kyushu.
http://www.bulletins-electroniques.com/actualites/77686.htm
http://ajw.asahi.com/article/business/AJ201501190057
http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0119-01.html

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

Source :
http://www.infohightech.com/une-solution-pour-identifier-des-utilisateurs-vulnerables-aux-cyber-attaques/