Réunion de crise de 8 banques à cause d’attaques de hackers | Le Net Expert Informatique

Réunion de crise de 8 banques à cause d’attaques de hackers

De nos jours les attaques par des hackers font partie du quotidien. Souvent on reçoit des mails par des expéditeurs inconnus qui ont pour but de parvenir aux données personnelles des clients. Les banques sont souvent ciblées lors de tels envois: le système « multiline » offert par 8 banques du Grand-Duché est actuellement dans la ligne de mire.

Attention! N'ouvrez aucun fichier ou document émis par l'adresse email suivante: helpdesk@multiline.lu !
Ceci est un message obtenu directement lorsque qu'on se rend sur le site Multiline.

Multiline est un service dit « e-banking » pour professionnels et entreprises (pour leur gestion financière) proposé depuis 1992.
Bien que ce système paraisse assez sécurisé (collaboration avec Luxtrut et Cetrel) il a quand même fait l'objet de cyberattaques.
Les dégâts ont été tels que 8 banques utilisant ce système (BCEE, Banque de Luxembourg, Raiffeisen, BIL, Poste, BGL BNP Paribas, ING et Société Générale) se sont réunies en cellule de crise.
Il n'y a pas encore d'informations disponibles émanant de l'ABBL, de la Cetrel ou de Multiline.
Le situation serait sous contrôle, un communiqué officiel est attendu pour le mardi de pentecôte.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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 sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://5minutes.rtl.lu/fr/actualite/alaune/634917.html

Le Bundestag se montre incapable de surmonter une cyber-attaque | Le Net Expert Informatique

Le Bundestag se montre incapable de surmonter une cyber-attaque

Depuis quelques semaines le parlement allemand est victime d'attaques informatiques à répétition. Un phénomène qui inquiéte certains députés.

Le Bundestag est vulnérable. Depuis le début du mois de mai, les services informatiques du parlement allemand sont la cible de cyber-attaques répétées. Les députés ne sont plus en mesure de sécuriser leurs communications. Des données ont été piratées, sans qu'il soit possible d'en connaître la nature. Impossible pour l'heure de savoir si des documents confidentiels ont été volés. «Et ce n'est pas terminé», a déclaré un porte-parole, selon des propos rapportés par les médias allemands, comme Der Spiegel ou Die Zeit, qui ont notamment révélé l'affaire. Le «cheval de Troie» utilisé par les hackers n'a pas encore été neutralisé. Selon le quotidienSüddeutsche Zeitung, le BSI, chargé de la sécurité fédérale informatique, aurait même demandé une aide extérieure pour en venir à bout.
L'exaspération et l'inquiétude commencent à se répandre au Bundestag, principalement dans les rangs de l'opposition. Les députés Verts et Die Linke semblent davantage touchés par l'attaque. Mais la cible exacte des hackers reste encore inconnue. «L'incertitude demeure sur l'intensité de l'attaque et son ampleur», a expliqué le député Vert Konstantin von Notz, spécialiste des questions informatiques. «Il n'y avait encore jamais une telle attaque pendant plusieurs jours», a déploré la vice-présidente Petra Pau (Die linke). «Il y a une attente évidente pour que la protection des communications soient rétablies», a observé le responsable SPD Lars Klingbeil. Le Bundestag envisage la possibilité de devoir réinstaller totalement l'infrastructure du réseau, pour purger la menace. Toute l'activité informatique du Bundestag en serait interrompue. L'opération pourrait avoir lieu au moment des vacances parlementaires, en juillet.

20 tentatives d'intrusion par jour en 2014
Qui se cache derrière l'assaut? Pour l'instant, la seule piste connue mène vers Europe de l'Est, où sont situés des serveurs qui auraient infiltré au moins deux ordinateurs du Bundestag. Mais l'enquête de la Sécurité intérieure est toujours en cours. Toutefois, à écouter les experts, la complexité de l'attaque témoigne d'une capacité technologique dont seuls des services secrets peuvent disposer.
Il ne s'agit pas de la première attaque informatique dont est victime l'administration allemande, loin de là. Selon le BSI, les services internes du gouvernement auraient subi en moyenne 20 tentatives d'intrusion par jour l'année dernière. Des services de renseignement étrangers seraient à l'origine d'au moins une attaque quotidienne. Pour renforcer la sécurité informatique de l'Allemagne et notamment de ses entreprises, le gouvernement élabore un nouveau projet de loi. «Avec cette loi, une amélioration significative de la sécurité des communications informatiques devra être atteinte», promet le texte en préparation. Le Bundestag sera amené à en débattre.

Source : http://www.lefigaro.fr/international/2015/05/22/01003-20150522ARTFIG00173-le-bundestag-se-montre-incapable-de-surmonter-une-cyber-attaque.php

---

Comment s'assurer contre le cyber-risques ? | Le Net

Expert Informatique

Comment s’assurer contre le cyber-risques ?

Diverses études montrent que les entreprises sont mal préparées pour lutter contre le hacking. Les grands assureurs affinent leurs stratégies commerciales.

Sony, Home Depot, JP Morgan, TV5 Monde, Target… Le nombre d'entreprises victimes de cybercriminalité explose. Mais les couvertures d'assurance contre ce type de méfait ne font qu'émerger. Les vols de données, espionnages et autres attaques de systèmes informatiques coûtent pourtant 300 à 1000 milliards de dollars, selon la société de sécurité informatique McAfee.
La Suisse n'est pas épargnée. Dernier exemple en date: Implenia. Selon une étude récente de l'Université de Saint-Gall (https://www.alexandria.unisg.ch/Projekte/238276), plus de 90% des entreprises ont été touchées par des attaques de hackers, l'année passée. «Les PME se sentent, à tort, à l'abri. Leur protection est insuffisante», juge son auteur, Martin Eling.
Elles semblent effectivement ne pas être préparées, comme en témoigne le sondage de KPMG auprès de 64 entreprises, présenté mercredi à la presse. Son auteur, Matthias Bossardt, parle d'un «cycle de complaisance». **Plus de la moitié des sociétés interrogées croient que leur organisation est capable de détecter des attaques. Mais 45% n'ont pas de plan pour y répondre**. Même si celles-ci ne cessent de se transformer, 79% des entreprises interrogées n'ont pas changé leurs plans, ces 12 derniers mois. 7% d'entre elles n'ont même pas pris de mesure, après une attaque.

En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise
Les entreprises ne découvrent que fort tard qu'elles sont piratées. «**En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise**», explique Manuel Meier, directeur général de la division entreprises pour Zurich Insurance. Sur le plan global, le coût du cyber-risque correspond à celui des catastrophes naturelles. Mais sa complexité est supérieure. L'incendie ou l'effraction sont plus aisés à localiser et immédiatement visibles. «La cybercriminalité, dont l'origine est souvent étrangère, change la façon d'appréhender un sinistre», analyse l'assureur.
Le thème s'est imposé aux Etats-Unis, où «un tiers des entreprises ont déjà signé un contrat de cyberassurance», affirme Manuel Meier. Le marché américain est estimé à 1,3 milliard de dollars en 2013 par le rapport «Betterley», contre 150 millions d'euros en Europe continentale.
«Le cyber-risque nous préoccupe surtout depuis cinq ans», précise Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. L'importance du cyber-risque s'est accrue fortement à la suite de l'«obligation de notification», soit le devoir d'annoncer quand une infraction s'est produite, fait valoir Manuel Meier. Le client qui a été frappé par une attaque doit être averti, par exemple si les informations contenues sur sa carte de crédit ont été violées. Aux Etats-Unis, l'entreprise est pénalisée par un risque de publicité et par un coût d'information qui peut atteindre «plusieurs douzaines de millions de francs», explique Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. Son bénéfice est réduit d'autant. Les entreprises suisses actives aux Etats-Unis, ou ayant un client américain, sont directement touchées si la filiale américaine l'est, parce que l'obligation d'annonce la touche immédiatement.
A l'origine, les entreprises parlaient de sécurité «informatique». Parce que c'est le département du même nom qui était en charge du sujet. Mais elles se sont aperçues que tout leur personnel était concerné et qu'il ne suffisait plus d'avoir un pare-feu ni de changer leurs mots de passe régulièrement.
Si le hacking s'est aussi vite répandu, c'est parce que presque tous les objets sont connectés à Internet, de la voiture à la maison, multipliant les opportunités de piratages. Les risques d'intrusion dans les systèmes informatiques dépassent les produits de consommation et frappent aussi les hôpitaux et leur responsabilité civile en cas de vol de documents.
Les assurances peuvent offrir leur service habituel de transfert de risque. Mais ce dernier ne va jamais couvrir l'ensemble des cyber-risques, même s'il contribue à la réduction des coûts économiques. «Les coûts juridiques d'une attaque sont énormes», observe Manuel Meier. Une grande partie de la couverture d'assurance se concentre sur ceux-ci. «Il arrive que la couverture d'assurance soit entièrement utilisée pour les risques juridiques et qu'il ne reste rien pour la responsabilité civile», fait valoir Carine Gantenbein. L'assurance paie les coûts d'annonce et de rétablissement des données ainsi que l'interruption d'activité. Mais elle ne couvre pas les conséquences d'un piratage, comme l'absence de transaction ou la perte de confiance. Les entreprises peuvent décider de couvrir elles-mêmes les cyber-risques dans une filiale dite «captive» ou faire appel à un réassureur. La définition du prix pose toutefois problème. Il manque encore un historique. «Les assureurs sont dans une phase d'essais et d'erreurs», analyse Manuel Meier.
En outre, les risques d'interruption d'activité conduisent à des estimations compliquées, puisque tout est interconnecté. «Les clients utilisent les mêmes nuages (clouds). Si l'un d'entre eux est attaqué, certaines entreprises ne peuvent plus livrer leurs produits», explique Zurich Insurance.

Si ce marché se situe avant tout aux Etats-Unis, en raison des coûts juridiques, il devrait s'étendre à l'Europe. L'Union européenne débat aussi de l'introduction du devoir d'obligation», indique Manuel Meier. Le temps à cet effet est réduit, sous peine de sanctions supplémentaires. L'UE pourrait mettre en œuvre cette obligation en 2016. La sanction atteindrait 5% du chiffre d'affaires ou jusqu'à 100 millions d'euros.

Le marché suisse de la cyberassurance est encore minuscule, selon l'étude de l'Université de Saint-Gall, réalisée sur mandat du courtier Kessler. Il s'élève à 5 millions de francs. Mais Martin Eling est d'avis qu'il devrait décupler en cinq ans. Dans le monde, le marché devrait quintupler pour s'élever à 10 milliards de dollars.

Les assureurs répondent à ces défis en offrant une combinaison de services de prévention (pare-feu, logiciels) et de protection. C'est une chasse gardée des grands groupes internationaux. Les acteurs actifs dans ce domaine sont AIG Europe Limited, Allianz Global Corporate & Specialty AG (AGCS), Chubb Insurance Company of Europe SE, Zurich et Axa Winterthur. Les grands groupes suisses doivent souvent signer des accords de partenariat. Axa Winterthur travaille par exemple avec Nexos AG, tandis que Zurich Insurance collabore avec Kudelski.

Axa Winterthur offre des mesures de préventions et de couverture de sinistres spécifiques. Dans le cas d'une perte de données, Axa assume la réinstallation du système d'exploitation et des programmes ainsi que la récupération des données. En cas de perte de chiffre d'affaires, à l'image d'une boutique en ligne dont le système est bloqué à la suite d'une attaque et indisponible pendant trois jours, l'assureur verse le manque à gagner, déduit de la franchise.

Auprès de Zurich Insurance, l'assurance cyber-risque est définie selon le principe des modules. La composante de base est toujours la responsabilité civile, laquelle peut s'accompagner de la récupération des données et des coûts d'annonce, s'il y a des clients américains et dès 2016 européens. Elle offre aussi la couverture du risque de chantage. Le prix dépend du nombre de données sensibles et de la branche. Une petite banque est bien plus chère qu'une PME industrielle. Le tarif d'une couverture correspond à 0,6% du chiffre d'affaires, mais des changements sont fréquents. Les statistiques sont encore insuffisantes.

Au sein des entreprises, le travail de sensibilisation intègre chaque employé, selon Carin Gantenbein. Les PME n'ont pas les moyens d'établir de tels processus. L'assureur offre à ses clients des conseillers pour les sinistres, la communication et l'analyse des processus.

Pour les personnes privées, il existe une assurance cybermobbing pour les privés. L'assureur se charge d'éliminer certaines histoires répandues sur le Web. Un privé n'obtiendra pas satisfaction s'il téléphone à Google pour changer un site, explique Manuel Meier.

Et dans cinq ans? Si l'obligation de notification est introduite dans l'Union européenne, la Suisse suivra, promet le directeur de Zurich Insurance. Le marché en deviendra plus transparent. On en parlera davantage, la perception sera supérieure. Et l'offre d'assurance sera élargie.

Source : http://www.letemps.ch/Page/Uuid/01ccdc38-f4e7-11e4-bb1f-074820583190/Les_solutions_des_assureurs_face_au_cyber-risques
Par Emmanuel Garessus

87% des actes cybercriminels commis en France sont du fait

de hackers made in France | Le Net Expert Informatique

87% des actes cybercriminels commis en France sont du fait de hackers made in France

Une étude révèle que 87% des actes cybercriminels commis en France sont du fait de hackers made in France. Russes, Africains, Chinois ou Coréens seraient moins offensifs qu'on ne le pense.

La dernière étude de ThreatMetrix va secouer les idées reçues sur la cybercriminalité en France. Selon ce rapport, qui porte sur le 1er trimestre 2015, « la plus grande cyber-menace ayant pesé sur les entreprises françaises durant cette période aurait pour origine l'hexagone ».

L'étude précise que 87% des attaques sont commises depuis la France. Pour les auteurs du rapport, il ne s'agit pas de pointer la performance de la cyberdélinquance made in France, mais de noter que désormais, les attaques menées dans chaque pays sont pilotées dans leur frontière. Ce constat est « en rupture avec les tendances dominantes où la grande majorité des cyberattaques avaient pour origine la Russie, l'Asie ou l'Afrique. »
Ainsi, la France n'est donc pas une exception, mais elle exprime une véritable tendance. En Grande-Bretagne, 75% des actes cybercriminels proviennent d'Irlande ou d'Angleterre, 81% en Allemagne, 54% aux Pays-Bas, 94% en Italie et 85% en Russie.
Sur les attaques, ThreatMetrix a constaté que l'usurpation d'identité (spoofing) est devenue la plus courante. Lors des fêtes de Noël, le cabinet a dénombré 11.4 millions de tentatives de transactions frauduleuses.

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 sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://bfmbusiness.bfmtv.com/entreprise/les-hackers-francais-sont-les-rois-du-cybercrime-en-france-888210.html
Par Pascal Samama

Affaire United : selon le

FBI, un hacker a modifié en vol la puissance d’un réacteur – Le Monde Informatique | Le Net Expert Informatique

	Un hacker a modifié en vol la puissance d’un réacteur

Selon une note du FBI, en trois ans, le chercheur en sécurité Chris Roberts a réussi à pirater une vingtaine de fois les systèmes informatiques d'avions de ligne. Le dernier en date, sur un vol d'United Airlines entre Denver et Chicago, a entraîné son interpellation à la sortie de l'avion le 15 avril 2015.

Le FBI soupçonne aujourd'hui le chercheur en sécurité Chris Roberts, fondateur et CTO de One World Labs, d'avoir modifié la puissance d'un des réacteurs du vol d'United Airlines du 15 avril dernier entre Denver vers Chicago. M. Roberts avait été interpellé par le FBI à sa descente d'avion suite à un tweet suggérant qu'il avait scanné les systèmes informatiques (EICA) d'un Boeing 737. Cette arrestation et la saisie de tout son matériel informatique semblent faire suite à des dysfonctionnements relevés par United Airlines. Interrogé par le FBI, le chercheur, justement spécialisé dans les failles de sécurité des systèmes embarqués en aéronautique, a indiqué avoir réussi à accéder une vingtaine de fois aux systèmes informatiques d'avions de ligne.

Le 17 avril, l'agence fédérale américaine a obtenu un mandat pour perquisitionner les locaux du chercheur. Dans sa demande de mandat, le FBI révèle des informations provenant des trois interrogatoires de M. Roberts. Il n'a pas encore été accusé d'un crime, même si United Airlines l'a interdit de vol sur ses avions. On ne sait pas encore si l'incident impliquant le moteur de l'avion a eu lieu ou si l'avion aurait pu être en danger à la suite de celui-ci.

Un tweet dévastateur

Dimanche dernier, M. Roberts a écrit sur Twitter que «au cours des cinq dernières années, mon seul but a été d'améliorer la sécurité des avions … compte tenu de la situation actuelle, on m'a conseillé de ne pas en dire plus. » La défense du chercheur en sécurité est assurée par Nate Cardozo, un avocat travaillant avec l'Electronic Frontier Foundation. M. Cardozo a déclaré que son client n'était pas disponible pour commenter autre chose que ce qu'il a écrit sur Twitter.

En ce qui concerne l'incident de moteur, l'agent spécial Mark S. Hurley a écrit dans la demande de mandat que M. Roberts a indiqué qu'il avait connecté son PC portable au système de divertissement en vol (In Flight Entertainment System ou IFE) de l'avion United Airlines en utilisant le Seat Electronic Box (SEB), qui se trouve sous certains sièges passagers. Après le piratage du système IFE, il a accédé aux autres systèmes de l'avion, précise l'agent spécial. M. Roberts « a déclaré qu'il avait modifié le code du Thrust Management Computer (TMC) de l'avion pour modifier la puissance des moteurs », ajoute M. Hurley. « Il a déclaré qu'il a commandé avec succès le système pour consulter et modifier les commandes de vol (CLB ou climb command). Un des moteurs de l'avion a commencé à augmenter sa puissance, « entrainant un mouvement latéral ou sur le côté de l'avion lors d'un de ces vols », précise le mandat de perquisition. L'agent Hurley écrit encore que M. Roberts a précisé qu'il avait compromis 15 à 20 fois des systèmes IFE de 2011 à 2014. Selon l'agent spécial, les systèmes IFE compromis sont fabriqués par Thales et Panasonic (les moniteurs vidéo installés à l'arrière de sièges passagers), .

Un boitier SEB forcé sous le siège passager

Les problèmes judiciaires de Chris Roberts ont vraiment commencé le 15 avril quand il a écrit un tweet suggéré qu'il sondait les systèmes d'un Boeing 737/800 d'United Airlines lors d'un vol Denver/Chicago. Il a ensuite poursuivi son voyage de Chicago vers Syracuse (dans l'état de NY). Entretemps le département Cyber Security Intelligence d'United Airlines qui avait vu ce tweet faisant référence au système EICAS, a envoyé une équipe de sécurité interpeller M. Roberts à sa sortie de l'avion pour le remettre au FBI.
Après son interpellation, un agent spécial a examiné la cabine de première classe où avait voyagé M. Roberts vers Chicago. Les boitier SEB sous les sièges 2A et 3A montraient des signes d'effraction. « Le SEB sous le siège 2A a été endommagé » indique le mandat de perquisition. « L'enveloppe extérieure de la boîte a été ouverte d'environ 1,27 cm, et une des vis de fixation était manquante ». Redevenu très prudent, M. Roberts a affirmé aux agents du FBI qu'il n'avait pas compromis le réseau de l'avion sur le vol à destination de Chicago, selon le mandat. En février et mars dernier, le FBI avait déjà interrogé Chris Roberts qui avait également affirmé avoir réussi à pirater les systèmes IFE à bord d'avions.
Cette affaire devrait en n'en pas douter, impacter le monde de la sécurité aérienne dans les prochains mois, voire années, et aboutir au renforcement des règles dans ce domaine.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemondeinformatique.fr/actualites/lire-affaire-united%C3%82%C2%A0-selon-le-fbi-un-hacker-a-modifie-en-vol-la-puissance-d-un-reacteur-61170.html
Par Serge Leblal avec IDG NS

Alerte: Nouveaux courriels de phishing au nom d'Apple

(iTunes) | Le Net Expert Informatique

Des fraudeurs envoient des courriels au nom d'Apple (iTunes) afin de s'emparer des données d'accès à votre compte.
Par ces courriels, les destinataires sont informés que leur compte n'a pas pu être validé et que celui-ci a été bloqué. Les escrocs demandent de suivre un lien et de fournir des données personnelles (nom d'utilisateur et mot de passe) sous prétexte de pouvoir réactiver leur compte.

Le SCOCI conseille :
1. Effacez le courriel !
2. Si vous soupçonnez quelqu'un d'être en possession de vos données d'accès à votre compte, veuillez immédiatement prendre contact avec le support d'Apple.
3. Soyez prudents avec tous les courriels qui vous demandent de cliquer sur un lien Internet pour contrôler vos données personnelles. En règle générale, ceci est l'œuvre de fraudeurs.
4. Contrôlez toujours l'adresse Internet (URL) sur laquelle vous êtes redirigés (cf. rectangle rouge sur l'image). De manière générale, si vous devez vous connecter à un compte en ligne, inscrivez l'URL vous même dans votre navigateur plutôt que de cliquer sur un lien qui vous est transmis par courriel.
5. Signalez ces cas au SCOCI par le biais de son formulaire d'annonce en ligne afin que nous puissions analyser ces courriels et faire fermer au plus vite les sites frauduleux.

En cas de doute sur une usurpation d'identité ou de doute sur une arnaque, n'hésitez pas à contacter Denis JACOPINI expert informatique assermenté.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/2015/2015-05-15.html

---

Sécurité : il est urgent de

ne plus négliger le facteur humain ! | Le Net Expert Informatique

	Sécurité : il est urgent de ne plus négliger le facteur humain !

Dans sa dernière étude intitulée « Le Facteur Humain », Proofpoint indique que les pirates ont, l'an denier, décidé d'opérer au niveau des entreprises, et non plus auprès du grand public. Ils se sont donc concentrés sur les processus de partage d'informations utilisés par les cadres, tout en privilégiant la sophistication des attaques, et non plus leur volume.

Les résultats de cette étude prouve que le comportement des utilisateurs, et pas uniquement les failles d'un système ou d'un logiciel donné, a une incidence significative sur la sécurité des entreprises. « Le facteur humain constitue l'un des éléments clés des programmes de sécurité, alors qu'il est souvent celui que l'on néglige le plus, indique Nick Hayes, Christopher McClean et Claire O'Malley. C'est bien là le problème. En effet, les solutions de sécurité se révèlent fondamentales si vous souhaitez protéger votre environnement de travail, mais ne sont d'aucune utilité si des actions humaines viennent les affaiblir ».
Malgré cela, de nombreuses entreprises adossent leur sécurité uniquement sur des technologies avec passerelle et n'optent pas pour des solutions de blocage, de protection contre les attaques ciblées, de détection et de gestion des menaces (qui sont toutes basées sur les utilisateurs plutôt que sur l'infrastructure).
L'étude révèle également que les cadres constituent une cible privilégiée. L'an dernier, ils ont été deux fois plus ciblés qu'en 2013, et leurs clics sur des liens dangereux ont doublé. Du côté des services, ce sont ceux dédiés à la vente, aux finances et à l'approvisionnement (chaîne logistique) qui ont été plus touchés. Proofpoint note que les attaques se produisent surtout pendant les heures de travail. La plupart des messages malveillants étant envoyés lors des heures de travail, principalement le mardi et le jeudi matin. Le mardi constitue la journée la plus critique, avec 17 % de clics de plus que les autres jours.
Au final, même si les utilisateurs sont plus vigilants, les cybercriminels sont aussi capables de s'adapter rapidement. Ainsi, le nombre de mails intégrant des pièces jointes douteuses, et non plus des URL (notifications, avertissements à caractère financier), s'est multiplié. L'an dernier, durant certains jours, Proofpoint a même constaté une augmentation de 1 000 % du volume des pièces jointes malveillantes. Cette année, la donne est différente, les fausses sollicitations par mail faisant état de réception de fax ou de messages vocaux, voire d'alerte à caractère financier (facture, relevés de comptes, etc.).
« Il existera toujours une personne qui cliquera sur un lien, et permettra ainsi aux menaces de se propager auprès des utilisateurs, confirme Kevin Epstein, Vice-Président en charge de la gouvernance et de la sécurité avancée chez Proofpoint. L'approche de Proofpoint est efficace car nos systèmes sont capables d'identifier les individus concernés, de localiser ces derniers et de déterminer les actions en cours. Ainsi, nous permettons aux organisations de se protéger activement, ainsi que de prendre, en temps réel, les mesures adéquates ».

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

Source :
http://www.infodsi.com/articles/155558/securite-est-urgent-plus-negliger-facteur-humain.html

Arnaque aux faux virement : Vol de 15 millions d’euros à Intermarché | Le Net Expert Informatique

Arnaque aux faux virement : Vol de 15 millions d’euros à Intermarché

Après Ryanair et de centaines d’autres entreprises, c’est au tour d’Intermarché d’être victime de l’arnaque dite « au président », une escroquerie aux faux ordres de virement internationaux (FOVI). 15 millions d’euros auraient été dérobés par ce biais.

Tout a commencé par une prise de contact avec un salarié au siège du groupe fin avril, situé dans le XVe arrondissement de Paris, en se faisant passer pour le PDG. Les cyber-escrocs sont alors parvenus à le convaincre d’opérer plusieurs virements vers des comptes bancaires étrangers, situés en Pologne.
D’après les informations de l’enquête en cours, les escrocs ont ainsi pu détourner plus de 15 millions d’euros en l’espace de quelques jours en s’en prenant à l’enseigne de grande distribution Intermarché. Une fois la supercherie découverte, l’enseigne a tenté de récupérer ses fonds mais en vain. Une enquête a été ouverte par le parquet de Paris avant d’être confiée à la direction centrale de la police judiciaire (DCPJ).
De nombreuses investigations sont actuellement en cours afin d’interpeller les auteurs de cette arnaque au « président » mais cela est complexe du fait que la coopération entre états est obligatoire et décisive.
Rappelons que ce type d’escroquerie a fait plus de 700 victimes en France durant les trois dernières années, pour un préjudice estimé à 350 M€.

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 sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.undernews.fr/banque-cartes-bancaires/arnaque-aux-faux-virement-vol-de-15-millions-deuros-a-intermarche.html

Propriétaires de sites WordPress : attention aux »script-kiddies » pro-Etat Islamique | Le Net Expert Informatique

Le FBI alerte sur les attaques continues de défacement visant des sites Internet. Les victimes ont en commun d'utiliser des plugins WordPress vulnérables. Quant aux auteurs, ils utilisent le nom de l'EI par souci de visibilité.

En janvier, suite aux attentats en région parisienne, de très nombreuses attaques de défacement de sites Web avaient été constatées. Ces opérations de cybervandalisme étaient revendiquées par des partisans des islamistes radicaux, et notamment de l'Etat Islamique (Daesh).
« La très grande majorité de ces attaques sont des défigurations de sites Internet (ou défacement), ou des dénis de service (DDoS) qui exploitent les failles de sécurité de sites vulnérables » précisait alors l'Anssi.

Des cibles choisies pour leur usage de plugins WordPress
De telles attaques se poursuivent et pas seulement en France. Et elles ont souvent une cible de prédilection : les sites WordPress. Les Etats-Unis, par l'intermédiaire du FBI, viennent d'ailleurs de publier un bulletin de sécurité concernant ces attaques.
Certes, note le FBI, ces « défacements traduisent un faible niveau de sophistication » mais ils s'avèrent néanmoins coûteux en raison des pertes d'activité et des dépenses qu'ils génèrent afin de réparer les systèmes infectés.
Quant aux victimes de ces intrusions, elles sont très diverses. Et pour cause puisque les attaquants ciblent moins les propriétaires des sites que la plateforme technique de ceux-ci. Les victimes ont un point commun : l'utilisation de plugins WordPress vulnérables.

Les pirates pas membres de Daesh
« Le FBI estime que les auteurs ne sont pas des membres de l'organisation terroriste Etat Islamique. Ces individus sont des hackers exploitant des méthodes relativement simples afin d'exploiter des vulnérabilités techniques et utilisent le nom ISIS pour gagner plus de notoriété que l'attaque sous-jacente aurait autrement recueilli. »
C'était déjà l'analyse publiée par ZDNet en janvier. « Nous n'avons constaté aucune excentricité ou coordination dans les attaques, ni de déni de service bien outillé » confiait Loïc Guézo, expert en sécurité chez Trend Micro. « Le résultat est surtout visuel, c'est une volonté de communiquer » par des défacements.
Quant au profil des attaquants, il était « plutôt celui de personnes avec des compétences de base, au sens de la gestion du PC et de certains outils » ajoutait-il. Ils s'apparenteraient ainsi à des « script kiddies » plutôt qu'à des hackers chevronnés.

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

Source : http://www.zdnet.fr/actualites/proprietaires-de-sites-wordpress-attention-aux-script-kiddies-pro-etat-islamique-39817644.htm
Par Christophe Auffray

L'impressionnant arsenal high-tech contre les survols

de drones | Le Net Expert Informatique

 Un drone près de Paris Dominique Faget/ AFP	**L'impressionnant arsenal high-tech contre les survols de drones**

Détection radar, systèmes laser, brouillage GPS, prise de contrôle des aéronefs à distance… Industriels et pouvoirs publics ont lancé les grands travaux pour répondre aux survols de centrales nucléaires et de sites sensibles.

Ce fut un impressionnant ballet de camions, de grues, de radars et d'équipements de pointe. Une débauche de technologies de repérage et de neutralisation des drones. Fin mars, les champions français de la défense (Airbus Defence and Space, Thales, Sagem) et une quinzaine de PME ont répondu présent à l'invitation du SGDSN (Secrétariat général de la défense et la sécurité nationale) pour exposer leurs technologies sur le terrain militaire de Captieux (Gironde). Une première réplique technologique aux 68 survols de sites sensibles recensés depuis le 10 septembre 2014, dont 29 au-dessus de sites nucléaires et 8 concernant des sites militaires.
Où en est-on vraiment dans la lutte contre ces survols ? Côté enquête, c'est un peu le point mort : quasiment aucun auteur de survol interdit n'a été interpellé, même si les soupçons se portent désormais clairement sur des geeks fabriquant leurs propres engins dans le cadre de concours avec d'autres amateurs, et sur des groupes écologistes désirant prouver la vulnérabilité des centrales nucléaires françaises, comme l'a rapporté Challenges le 30 avril.

200.000 drones en France
Les experts évoquent des vols programmés à l'avance, à l'aide de points GPS, ce qui évite aux auteurs de se faire repérer, aucune liaison radio n'étant établie entre le drone et son « pilote ». D'autres survols auraient eu lieu avec des ailes volantes en FPV (First Person View), un système de lunettes ou de jumelles permettant au pilote de diriger le drone en immersion, grâce à des caméras embarquées.
Côté réglementaire, le SGDSN n'envisage pas de durcissement drastique des textes. « Il n'est pas sûr que des sanctions plus dissuasives soient la meilleure des solutions : la justice ne prononce jamais les peines maximales », estime-t-on au sein de l'organisme. L'idée est plutôt de mieux informer les propriétaires de drones, qui sont estimés à 200.000 environ en France (dont 2.000 à 2.500 drones professionnels), sur les risques et obligations liées à leur engin. Des formations sur internet, préalables à l'autorisation de vol, sont notamment envisagées.

La neutralisation, maillon faible
Côté réponse technologique, la machine se met aussi peu à peu en marche. Les tests de Captieux, pilotés par l'Onera (Office national d'études et de recherches aérospatiales), ont permis de recenser les technologies disponibles, et d'identifier les trous dans la raquette. « Nous avons constaté que le point faible, plus que la détection ou l'identification, était la neutralisation des drones, explique-t-on au SGDSN. En gros, les systèmes de détection permettent de repérer un drone à 4 km, de l'identifier à 2 km, mais de ne le neutraliser qu'à 350 mètres. » Les pistes des jets de matière (eau par exemple), ou des interceptions par filets ont été écartées, au moins à court terme, au profit de technologies de « leurrage » ou de brouillage GPS.
A l'issue d'un appel d'offres express consacré à la détection et l'interception de petits drones, l'Agence nationale de la recherche (ANR) a sélectionné début avril deux projets sur les 24 présentés. Le premier, baptisé Angelas et piloté par l'Onera, rassemble notamment Thales, Exavision, Telecom Sud Paris, EDF et le CEA. Peu disert sur les détails, le communiqué évoque « l'identification à portée de quelques kilomètres d'UAS [drones] de moins de 25 kilos en toutes conditions d'environnement » et des technologies d'imagerie laser 2D et 3D, voire des détecteurs d'optique pointées, ces systèmes laser permettant, à l'origine, de repérer les snipers grâce au renvoi de la lumière diffusée (le fameux effet « œil de chat »). Un démonstrateur est prévu à un horizon de 18 mois.

Prise de contrôle à distance
Le second projet, appelé Boréades, est piloté par l'industriel CS (ex-Compagnie de signaux). Il rassemble le spécialiste des systèmes optroniques (fusion de l'optique et de l'électronique) et infrarouges HGH, et celui du traitement des signaux Spectracom. La localisation des drones serait effectuée par un système optronique : un capteur optique dérivé d'une solution déjà en service dans la surveillance maritime, le SeaScope 360 de la société CS ; et un capteur infrarouge longue portée de HGH.

La neutralisation sera effectuée grâce à une tourelle pointant vers les drones. Deux types d'action sont prévus : un « brouillage sélectif des données de télécommandes », et un « leurrage électronique des données GPS ». En clair, le drone est trompé sur sa position exacte. Le projet envisage même la « prise de contrôle » de l'engin et son « atterrissage forcé ». Un démonstrateur est prévu dans les 12 mois, le consortium visant une « commercialisation aisée » grâce à un « coût maîtrisé et des risques limités ».

Moyens limités
La mise en place de ces démonstrateurs, puis de véritables prototypes et systèmes clé en main, s'annonce ardue : le programme de l'ANR n'est doté que d'un million d'euros, trois millions avec la participation des industriels, une somme limitée par rapport aux « centaines de millions de dollars » investis par les Etats-Unis sur le sujet, de l'aveu-même du SGDSN. L'autre difficulté, c'est que la ribambelle de technologies envisagées par les deux consortiums sera difficile à faire rentrer dans une offre commerciale à prix compétitif. Comme l'identification de leurs auteurs, la réponse technologique aux survols de drones s'annonce comme un sacré casse-tête.

Source : http://www.challenges.fr/transports-et-defense/20150506.CHA5563/l-impressionnant-arsenal-high-tech-contre-les-survols-de-drones.html