Un nouveau logiciel malveillant cible les iPhone | Le Net Expert Informatique

	Un nouveau logiciel malveillant cible les iPhone

Décidément, les terminaux à la pomme intéressent de plus en plus les pirates. Après la découverte le 4 février par les experts du cabinet de sécurité informatique Trend Micro du premier logiciel espion baptisé « XAgent » exploitant des failles sur les téléphones Apple non débridés (dits « non jailbreakés »), c'est au tour de l'unité de recherche 42 de l'entreprise de sécurité informatique Palo Alto Networks de publier dimanche 4 octobre une alerte sur un nouveau logiciel malveillant (malware) affectant les iPhones du commerce.

Baptisé « YiSpecter », il attaque sans distinction les iPhone du commerce vendus avec le système d'exploitation officiel iOS d'Apple et ceux qui ont été débridés. Apple, qui a reconnu l'existence de ce malware, a indiqué lundi 5 octobre que les utilisateurs d'iOS 8.4 et d'iOS 9 étaient désormais protégés. La particularité de ce programme – qui serait actif depuis plus de 10 mois à Taïwan et en Chine continentale d'où il proviendrait – est d'utiliser des failles que l'on pensait impossible à exploiter, et de se propager de façon inédite, selon Palo Alto Networks.

Un fonctionnement et une propagation inédits

Détournant certaines interfaces de programmation propres au système d'exploitation iOS, cette nouvelle forme de logiciel malveillant ne laisse rien présager de bon pour l'avenir des terminaux mobiles à la pomme selon la firme de sécurité à l'origine de la découverte : « C'est le premier malware que nous avons vu en circulation qui abuse les API [interfaces de programmation] privées dans le système iOS pour mettre en œuvre des fonctionnalités malveillantes. »

En se propageant seul soit grâce à « Lingdun », un ver informatique sous Windows (qui se charge d'envoyer des liens malicieux de téléchargement d'YiSpecter à tous ses contacts), soit par le piratage des connexions WiFi des boîtiers des fournisseurs d'accès à Internet, cette nouvelle variante de malware inquiète la société californienne. Ses quatre composants, tous authentifiés par des certificats d'entreprises réels émanant de sociétés comme Verisign ou Symantec, s'installent de façon furtive sur les iPhone, en masquant ses programmes, mais aussi en dupliquant les noms et les logos des icônes système (Game Center, Météo, Notes, PassBook, Téléphone, etc.), piégeant même les utilisateurs les plus avertis.

Une fois installé, YiSpecter peut télécharger, installer et lancer des applications de l'App Store, mais aussi les modifier, par l'affichage de publicités en plein écran par exemple. Il permet également de collecter les données des utilisateurs, notamment celles utilisées dans le navigateur Internet Safari. S'il est découvert, sa suppression par méthode classique ne fonctionnera pas car il se réinstalle automatiquement après un redémarrage système. Enfin, peu d'espoir du côté des antivirus, qui ne détectent toujours pas sa présence sur les terminaux infectés.

Des malwares aux origines peu claires

Certains indices repérés par Palo Alto Networks font converger les soupçons vers « YingMob », une entreprise chinoise de publicité mobile ayant pignon sur rue, qui aurait programmé et diffusé ce malware à des fins publicitaires, n'hésitant pas à en faire sa promotion au grand jour. Mais la complexité et les méthodes de propagation de YiSpecter cachent peut-être des visées plus opaques.

Déjà le mois dernier, 344 applications iOS officielles présentes dans l'App Store, la boutique d'applications d'Apple, avaient été retirées en urgence car infectées par le malware « XcodeGhost », découvert le mercredi 16 septembre par les équipes sécurité du groupe chinois Alibaba. L'origine de ce malware est encore incertaine, mais les méthodes utilisées sont très similaires aux techniques de programmation qu'emploie la CIA – selon des documents publiés en mars par The Intercept.

Tout début septembre, c'était le logiciel malveillant « KeyRaider » également découvert par la société Palo Alto Networks, qui faisait parler de lui : selon la société de sécurité, plus de 225 000 comptes et identifiants Apple auraient été dérobés, uniquement sur des iPhone et iPad débridés.

La société de sécurité américaine est également à l'origine de la chute d'un mythe : c'est elle qui annonçait il y a moins d'un an, en novembre 2014, la découverte, toujours en Chine, de « Wirelurker », le tout premier malware pour iPhone touchant des téléphones non débridés. Depuis, il ne se passe pas un mois sans qu'une nouvelle alerte concernant les terminaux mobiles d'Apple ne soit lancée.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.lemonde.fr/pixels/article/2015/10/07/un-nouveau-logiciel-malveillant-cible-les-iphone_4784509_4408996.html

Que peuvent faire les entreprises en attendant un Safe Harbor II | Le Net Expert Informatique

Que peuvent faire les entreprises en attendant un Safe Harbor II

La décision de la CJUE étant d'application immédiate, depuis le 6 octobre 2015, tous transferts vers les Etats-Unis fondés sur le Safe Harbor sont invalides. Marc d'Haultfoeuille (Avocat Associé) et Nadège Martin (Avocat Of Counsel) de l'Equipe Technologie & Innovation de Norton Rose Fulbright, explique quoi faire en attendant un Safe harbor II.

Ce que les entreprises peuvent faire en attendant un Safe Harbor II

Force est d'admettre que la décision du 6 octobre 2015 par laquelle la Cour européenne de justice (CJUE) a déclaré invalide la décision Safe Harbor, sème un trouble auquel il n'existe aucune réponse juridique unanimement valable pour l'ensemble des entreprises concernées. Cette situation tient au fait qu'au-delà du contenu de cette décision, dont la portée demeure encore difficilement mesurable en l'absence de positionnement officiel des autorités de protection des données, d'autres paramètres doivent être pris en compte : le transfert est-il déjà effectif ? quelles sont ses finalités ? la loi nationale impose-t-elle des formalités préalables ?

AUDIT DES TRANSFERTS EN COURS

La décision de la CJUE étant d'application immédiate, depuis le 6 octobre 2015, tous transferts vers les Etats-Unis fondés sur le Safe Harbor sont invalides. Il est ainsi recommandé d'identifier rapidement les contrats et formalités déclaratives existants (ces transferts étaient soumis à simple notification auprès de la CNIL) afin de disposer des détails pertinents sur ces transferts.

Cet audit est nécessaire à l'identification des solutions alternatives envisageables à plus ou moins court terme, en l'état de la loi Informatique et Libertés ou sur la base des mesures qui pourraient être annoncées dans l'intervalle par la CNIL. A plus long terme, la décision Safe Harbor II en cours de discussion devrait être une solution pertinente mais il est difficile de prévoir sous quels délais elle sera adoptée.

DES DÉLAIS À ANTICIPER POUR LES TRANSFERTS À COURT TERME

La situation s'avère plus délicate pour les contrats en voie de conclusion pour lesquels le transfert était censé être fondé sur le Safe Harbor. En effet, sauf à pouvoir remplacer ce fondement par une exception légale ou des BCRs également soumis à simple notification préalable auprès la CNIL, les parties devront non seulement conclure des clauses contractuelles types (CCT) mais le responsable de traitement devra solliciter l'autorisation préalable de la CNIL au transfert. Or, obtenir cette autorisation peut prendre jusqu'à deux mois, voire plus, selon la loi. De plus, au vu des motifs de la décision rendue par la CJUE, le traitement de ces demandes par la CNIL est susceptible d'en être complexifié et en tout état de cause, allongé. Ces projets seront ainsi, pour beaucoup, dépendants des orientations qui seront prises par les autorités de protection des données.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

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

Source : http://www.usine-digitale.fr/article/ce-que-les-entreprises-peuvent-faire-en-attendant-un-safe-harbor-ii.N356084

Le secret professionnel des avocats menacé par la Loi renseignement ? | Le Net Expert Informatique

 Le Conseil de l’ordre des avocats de Paris va saisir la Cour européenne des droits de l’Homme (CEDH) contre la loi controversée sur le renseignement. | AFP	Le secret professionnel des avocats menacé par la Loi renseignement ?

Le Conseil de l'ordre des avocats de Paris va saisir la Cour européenne des droits de l'Homme (CEDH) contre la loi controversée sur le renseignement.

« Nous allons saisir la CEDH contre cette loi qui repose à nos yeux sur deux mensonges d'État », a expliqué vendredi le bâtonnier de Paris Pierre-Olivier Sur, confirmant une information du site Next INpact.

« Le premier mensonge, c'est que cette loi ne vise pas simplement à protéger la société contre le terrorisme, elle concerne toute la matière pénale. Le second, c'est qu'il n'y a pas dans le texte de véritable juge pour protéger les libertés publiques car le seul juge habilité à le faire, c'est le juge judiciaire. Et le législateur a choisi un juge administratif, très éloigné des questions de liberté », a-t-il fait valoir.

« Ce secret professionnel a une valeur sacrée »

Pour le représentant des avocats parisiens, la loi sur le renseignement porte également atteinte « au secret professionnel des avocats ».

« Ce secret professionnel a une valeur sacrée. Il ne place pas l'avocat au-dessus des lois mais on doit prendre en compte la spécificité de son travail, ne pas aller chercher, en fracturant le secret, des renseignements sur des actes qu'il aurait pu commettre et qui, par capillarité, risque de nuire à la défense de son client. Il faut donc que les premiers actes d'investigation soient particulièrement contrôlés, notamment par le président du TGI », a-t-il fait valoir.

Cette saisine intervient quelques jours après celle de l'Association de la presse judiciaire (APJ) qui estimait, elle, que la loi sur le renseignement menaçait la liberté de la presse et le secret des sources.

Ecoutes, caméras, logiciel-espion…

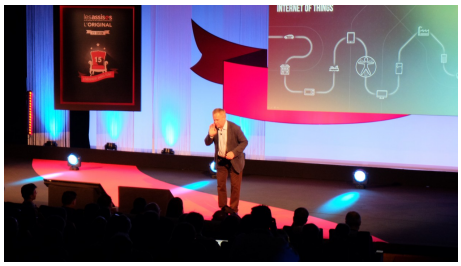
De la prévention d'attentats à l'espionnage économique, le texte définit un large éventail des missions des services de renseignement ainsi que le régime d'autorisation et de contrôle de techniques d'espionnage (écoutes, pose de caméra ou de logiciel-espion, installation chez les opérateurs de télécommunications de dispositifs pour collecter les données de connexion, etc.).

Fin juin, le Parlement a adopté définitivement la loi à une large majorité gauche-droite, mais avec des voix dissidentes dans presque chaque groupe.

Face à la controverse, François Hollande a saisi le Conseil constitutionnel. Ce dernier a validé la loi en juillet estimant notamment que « le législateur (avait) prévu des garanties suffisantes pour qu'il ne résulte pas » du texte contesté « une atteinte disproportionnée au droit au respect de la vie privée, au droit de la défense et au droit à un procès équitable, y compris pour les avocats et les journalistes ».

Source :
http://www.ouest-france.fr/loi-renseignement-le-secret-professionnel-des-avocats-menace-3752413

La progression impressionnante de la cybercriminalité | Le Net Expert Informatique



La progression impressionnante de la cybercriminalité

En 10 ans, le nombre d'attaques a explosé. De la simple intrusion au sabotage, les criminels exploitent toutes les failles des systèmes d'information.

Le chiffre impressionne. En effet si l'on en croit Eugène Kasperky – fondateur et PDG de la société éponyme spécialisée dans la sécurité des systèmes d'information – il y aurait eu en 2014, 237 millions d'attaques informatiques, contre 500 000 en 2004.
Cette vertigineuse croissance d'actes de malveillances tient bien sur à l'extension d'Internet dans le monde, qui compte désormais plus de 3 milliards d'utilisateurs. Cette progression provient également de la professionnalisation des pirates. De simples hackers, il y a encore une dizaine d'années, certains sont aujourd'hui des ingénieurs pointus recrutés par des Etats ou par des mafias qui ont fait du cyber-espace leur nouveau terrain d'action.

Windows et Android parmi les systèmes les plus piratés

Eugène Kaspersky met enfin en avant la faiblesse de la sécurisation des systèmes technologiques: « un ordinateur sur 20 doté d'un système Microsoft est infecté et les attaques sur les mobiles équipés du système Android se sont multipliées depuis 2011, notamment lorsqu'ont été lancés des services bancaires sur smartphone ». Le système d'Apple limite lui les dégâts: « il y a moins d'ingénieurs dans le monde pour concevoir des logiciels pour les machines Apple. Les pirates doivent avoir les mêmes problèmes de recrutement que nous » souligne, amer, le PDG russe qui distingue trois grands types de menaces informatiques: « la cybercriminalité qui veut récupérer de l'argent ; le cyber-espionnage qui s'intéresse aux données et enfin le cyber-sabotage qui cherche à tuer ».

Poursuivre les efforts de sensibilisation et de formation du public et des salariés

Des dangers qui ne vont que s'accroitre avec la multiplication des objets connectés et le développement des « smart » (Cities, building, voitures…). « Ce qui est particulièrement à redouter c'est le cyber-espionnage qui va s'attaquer aux infrastructures publiques comme les transports, les réseaux d'eau, d'électricité ».
Face à ce tableau noir, pas de miracle. Les entreprises, les Etats, les individus doivent être vigilants: « il faut être prêt pour la prochaine génération d'attaques. Il faut poursuivre les efforts de sensibilisation et de formation ». Dont acte…

Source :
http://bfmbusiness.bfmtv.com/entreprise/la-progression-impressionnante-de-la-cybercriminalite-919455.html
Par Florence Puybareau

Invalidation du « Safe Harbor » : quels sont les changements auxquels on doit s’attendre ? | Le Net Expert Informatique

La justice européenne a invalidé, mardi 6 octobre, l'accord « Safe Harbor » qui encadrait le transfert de données personnelles de l'Union européenne vers les Etats-Unis.

En quoi consiste Safe Harbor et que dit la Cour de justice de l'Union européenne (CJUE) ?
En Français « sphère de sécurité », le « Safe Harbor » est une décision de la Commission européenne, datant de 2000, qui affirme que le transfert de données personnelles d'Europe vers les Etats-Unis est possible car ce pays présente des garanties suffisantes pour la protection de la vie privée.
Très controversé, cet accord a notamment été mis à mal par les révélations d'Edward Snowden, en 2013, sur les programmes de surveillance de masse de la NSA. Les adversaires du Safe Harbor, dont Max Schrems, un Autrichien qui a déposé plusieurs plaintes contre Facebook, estimaient que ces révélations montraient que les données personnelles des Européens n'étaient en fait pas protégées lorsqu'elles étaient stockées aux Etats-Unis.
Dans son arrêt rendu mardi, la CJUE estime que le Safe Harbor n'est pas conforme au droit européen, pour plusieurs raisons détaillées sur une trentaine de pages. La Cour a notamment estimé que les recours possibles pour les citoyens européens estimant leurs droits malmenés étaient beaucoup trop faibles. Elle juge également que les programmes de surveillance de masse des Etats-Unis sont incompatibles avec une protection adéquate des droits des citoyens européens.

Cela veut-il dire que Facebook ne peut plus fonctionner en Europe, ou va devoir stocker les données des citoyens européens en Europe ?
Non : l'arrêt invalide un accord très générique. Facebook peut continuer à fonctionner comme il le faisait jusqu'à aujourd'hui, mais l'entreprise – tout comme Google ou tout autre entreprise qui stocke des données de citoyens européens aux Etats-Unis – ne peut plus s'abriter, en cas de procédure, derrière le fait qu'elle fait partie du Safe Harbor et que ses flux de données entre l'Europe et l'Amérique sont présumés légaux.
Facebook affirme en fait ne pas s'appuyer uniquement sur le Safe Harbor, mais « sur d'autres méthodes recommandées par l'Union européenne pour transférer légalement des données de l'Europe vers les Etats-Unis ».
Il existe en effet d'autres normes de transfert de données, comme par exemple les « clauses contractuelles type » ou les « règles internes d'entreprise » (dans le cas de transfert de données entre filiales), le Safe Harbor étant le cadre juridique simplifié et « par défaut ». Certaines entreprises du numérique utilisent déjà ces cadres juridiques alternatifs.
La Commission craint d'ailleurs que la décision de la CJUE ne favorise la multiplication de contrats spécifiques établis entre des entreprises et des pays européens, au détriment d'un cadre générique européen. Frans Timmermans, le vice-président de la Commission, a d'ailleurs annoncé que des « lignes directrices » à destination des autorités de protection des données seraient publiées afin d'éviter un « patchwork avec des décisions nationales ».
Par ailleurs, sans aller jusqu'à ces procédures juridiques, la loi européenne – plus spécifiquement l'article 26 de la directive de 1995 sur la protection des données personnelles – prévoit qu'un transfert vers un pays tiers peut être autorisé dans plusieurs cas. Par exemple, pour assurer la bonne exécution du contrat commercial (dans le cas d'une réservation d'hôtel par exemple, où les coordonnées du client sont nécessaires) ou lorsque intervient le consentement explicite de l'internaute à ce que ses données soient transférées.

Le Safe Harbor va-t-il être renégocié ?
La renégociation de cet accord était déjà en cours avant l'arrêt de la Cour. Malgré l'expiration de plusieurs dates butoirs, les négociateurs ont récemment affirmé qu'ils faisaient des progrès dans les discussions. Mais il sera difficile d'obtenir rapidement un accord qui puisse satisfaire les exigences de la CJUE : cette dernière rappelle dans son arrêt que, pour obtenir un régime de ce type, un pays doit faire la preuve qu'il offre des garanties de protection de la vie privée comparables à celles en vigueur au sein de l'UE.
Cela signifie qu'il faudrait des changements majeurs dans le droit américain pour qu'un nouvel accord ne soit pas, à son tour, invalidé par la Cour.

Que se passe-t-il dans l'immédiat ?
Plus de 4 000 entreprises étaient soumises à l'accord Safe Harbor. Nombre d'entre elles, particulièrement les plus petites, se retrouvent brusquement, au moins jusqu'à l'adoption d'un nouvel accord Safe Harbor, dans un vide juridique.
Les grands acteurs du Web, eux, sont dans l'attente. L'annulation du Safe Harbor semble les avoir pris de court. Dans un communiqué, l'association professionnelle Digital Europe, qui regroupe tous les grands acteurs du secteur (d'Apple à Toshiba en passant par Google, à l'exception de Facebook), « demande de toute urgence à la Commission européenne et au gouvernement américain de conclure leurs négociations pour parvenir à un nouvel accord "Safe Harbor" aussi vite que possible ».
« Nous demandons également à la Commission européenne d'expliquer immédiatement aux entreprises qui fonctionnaient sous le régime du Safe Harbor comment elles doivent opérer pour maintenir leurs activités essentielles durant ce vide juridique », poursuit l'association.
Facebook a, de son côté, estimé également qu'il « fallait impérativement que les gouvernements européens et américain donnent des méthodes légales pour le transfert des données et règlent toutes les questions de sécurité nationale ».

Quelles seront les conséquences plus larges de cette décision ?
Si l'arrêt de la CJUE ne porte que sur le Safe Harbor, il dénonce avec des mots très durs les programmes de surveillance de masse de la NSA américaine, présentés comme incompatibles avec les droits fondamentaux garantis par le droit européen.
Le jugement pourrait aussi influencer deux dossiers européens brûlants dont les négociations arrivent dans leur dernière ligne droite : l'accord « parapluie » sur l'échange de données personnelles pour la coopération policière, entre Europe et Etats-Unis, et le projet de règlement sur les données personnelles.
La commissaire européenne à la justice, Vera Jourova, a indiqué que l'arrêt de la Cour confortait la position de la Commission, notamment sur la nécessité d'avoir « des garde-fous solides » en matière de protection des données.
Washington s'est dit « déçu » par la décision de la justice européenne, estimant qu'elle créait une « incertitude pour les entreprises et les consommateurs à la fois américains et européens et met en péril l'économie numérique transatlantique qui est en plein essor ».

Source : http://www.lemonde.fr/pixels/article/2015/10/06/safe-harbor-que-change-l-arret-de-la-justice-europeenne-sur-les-donnees-personnelles_4783686_4408996.html

Réponse sur incidents et bonnes pratiques | Le Net Expert Informatique

	Réponse sur incidents et bonnes pratiques

Les 2/3 des cyberattaques mettent plusieurs mois à être détectées et près de 70% le seraient par des tiers ! Aujourd'hui c'est un fait, plus personne n'est à l'abri d'une cyberattaque, il est donc indispensable de se mettre en ordre de marche pour être prêt à réagir en cas d'attaque. La mise en place d'une politique de réponse sur incident de sécurité permet, en effet, de détecter la cyberattaque le plus tôt possible, de réagir très rapidement pour la contrer et de réduire ainsi au maximum les impacts d'image et business. Econocom nous livre son expertise en la matière, aux côtés de Maître Garance Mathias, à l'occasion de la 15ème édition des Assises de la Sécurité.

En 2014, 81% des entreprises ont déjà fait l'objet d'une cyberattaque, constate Marc Cierpisz, Directeur de l'offre Cybersécurité chez Econocom. 66% de ces attaques ont été découvertes après plusieurs mois, et 69% d'entre elles ont été découvertes par des tiers. Il observe, de plus, une difficulté à arrêter ce type d'attaque ; une incertitude plane quant aux délais de détection et de traitement de ce type d'incident.
La réponse sur incident est à la fois un défi technique, organisationnel et juridique pour les entreprises. L'enjeu est aussi de savoir s'adapter aux circonstances particulières.
Concernant les mesures techniques, il s'avère que la sécurité périmétrique reste inadaptée ou inefficace, car le SI est aujourd'hui de plus en plus diffus. La mise en place de firewalls n'a, par exemple, pas empêché TV5 Monde de se faire pirater. Il existe une grande diversité à l'heure actuelle des moyens de réaction : audits (test d'intrusion, tableaux de bord…), détection (SIEM, SOC, CERT, veille…). Toutefois, on constate beaucoup de manquements à ce niveau-là, à la fois en termes de budgets et de ressources adéquates, même si les enjeux de sécurité sont de mieux en mieux compris.
Au niveau juridique, le droit n'a pas encore clairement défini de manière intrinsèque la notion d'incident de sécurité, contrairement aux fuites de données, explique Me Garance Mathias. L'approche devra donc passer par une définition précise des incidents de sécurité et des responsabilités avec les différents prestataires.
Un cadre réglementaire existe néanmoins, avec la Loi Informatique et Libertés notamment mais pas seulement. Le projet de règlement européen relatif à la protection des données personnelles, le règlement eIdas, ou encore les différentes réglementations sectorielles, viennent compléter et complexifier les obligations relatives à la protection de l'information et au traitement des incidents. Le projet européen concernant la protection des données à caractère personnel va venir imposer l'obligation de déclaration pour le CIL des incidents de sécurité, ce qui changera la donne surtout dans un pays où la fuite de données se fait soi-disant plus « rare » qu'ailleurs. Le bénéfice d'être assuré sera certainement demain de plus en plus prégnant.

Les réponses juridiques diffèrent sur le plan civil et pénal, et les sanctions aussi. Le risque est bien réel pour les entreprises, en termes de dommages et intérêts bien sûr, d'atteinte à l'image et à la réputation également. Les illustrations jurisprudentielles varient, quant à elles, selon le fait que l'entreprise ait effectué ou non préalablement des audits de sécurité par exemple… La question est de savoir comment démontrer s'il y a eu un défaut de sécurisation ou non. Les incidents de sécurité ont mis globalement en avant un manque de sécurisation des systèmes d'information, qu'il faudra donc renforcer si les entreprises ne veulent pas être sanctionnées.

Parmi les mesures à mettre en place en entreprise pouvant réduire ces incidents de sécurité, elle cite entre autres :
– La politique interne à l'entreprise : la charte informatique est essentielle, mais combien la font signer aux employés… pourtant celle-ci permettrait de responsabiliser les utilisateurs ; la politique de sécurité en elle-même ; la politique contractuelle avec les prestataires, les sous-traitants… ; ou encore la sensibilisation des différentes acteurs ;
– Ensuite, des mesures de sécurité spécifiques doivent venir renforcer cette politique interne selon l'activité de l'entreprise : OIV, secteur médical, assurance, banque…

La cadre juridique est donc là, mais il est aussi à venir. On connaît déjà les textes, donc on n'est pas dans l'incertitude, que ce soit dans le secteur de la santé, ou dans le domaine de la protection des données à caractère personnel, conclut-elle.

La réponse n'est pas que technique ou juridique. Plusieurs défis se posent au niveau de l'organisation en matière de réponse à incident, reprend Marc Cierpisz :
– Identifier un incident de sécurité ;
– Etablir les objectifs de toute opération d'enquête et de nettoyage ;
– Analyser les informations relatives aux incidents ;
– Déterminer ce qui s'est réellement passé ;
– Identifier les réseaux et systèmes compromis ;
– Déterminer les informations divulguées à des tiers ;
– Etc.

Quelles démarches convient-il de mettre en place ? « Le bon stratège se prépare à tout, même au pire… »
– Concernant la partie renseignement sécuritaire, il convient en premier lieu d'évaluer la criticité de l'entreprise, d'analyser la menace sécuritaire du SI, les risques IT et métiers, d'examiner les implications des personnes, des processus, de créer un cadre de contrôle approprié, d'examiner l'état de préparation dans la réponse aux incidents de sécurité…
– Au niveau de la réponse sur incident, il faut déjà identifier les incidents de sécurité, définir les objectifs que l'on veut couvrir et les mesures à prendre quand on a qualifié les incidents de sécurité, récupérer les systèmes, les données et la connectivité…
– Le suivi post-intervention est également fondamental pour remettre en état l'entreprise : il s'agit ici d'enquêter sur l'incident de manière plus approfondie, de le signaler aux parties prenantes, d'effectuer un examen a posteriori, de réagir et de prendre les bonnes décisions, de communiquer et de s'appuyer sur les leçons apprises, de mettre à jour les informations clés, les contrôles et les processus, d'effectuer une analyse de tendance… L'objectif est que ça ne se reproduise pas.

Parmi les erreurs les plus fréquentes, les entreprises sous-estiment encore trop souvent les conséquences d'une attaque et les risques : « on traitera quand ça arrivera… » Pourtant 117 339 attaques seraient recensées chaque jour. On constate globalement une mauvaise estimation des risques, la destruction des preuves, une absence de plan de réponse à incident, de gestion de crise et de prise en compte de la réponse à incident dans les PCA, ou encore une mauvaise gestion de la e-réputation et de la communication. Pourtant, quand on subit un crash c'est violent, parfois même comme un accident de voiture.

Un certain nombre de bonnes pratiques doivent être mises en place au sein des organisations, comme la définition d'un plan de réponse à incident, la constitution d'une équipe dédiée, la définition d'un corpus documentaire, la préservation des preuves… Un plan de communication doit également être mis en œuvre. Il est essentiel d'identifier une autorité centrale en charge de cette communication, avec les médias par exemple. L'entreprise doit être impliquée en la matière, car « mieux elle va maitriser sa communication, mieux elle va gérer sa sortie de crise ». Enfin, en cas de gestion de crise, elle devra mettre en place une cellule de « war room », mais aussi gérer les relations avec les différents organismes et autorités concernés (CNIL, ANSSI…).

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.globalsecuritymag.fr/Reponse-sur-incident-des-enjeux,20151001,56316.html

---

TOP 10 des méthodes de hacking les plus utilisées | Le Net Expert Informatique

TOP 10 des méthodes de hacking les plus utilisées

BalaBit présente en exclusivité lors de la 15è édition des Assises de la Sécurité, les résultats d'une étude menée auprès des participants de la Black Hat en août dernier, conférence de référence mondiale en matière de sécurité de l'information.

BalaBit a interrogé 349 professionnels de la sécurité afin de définir le top 10 des méthodes de hacking actuellement les plus populaires. Cette étude offre aux entreprises l'opportunité de mieux connaître leurs ennemis en identifiant les méthodes et les vulnérabilités les plus utilisées par les hackers lorsqu'il s'agit de s'attaquer à leurs données sensibles. Cette base de connaissance est la première étape fondamentale pour toute entreprise souhaitant mettre en place une stratégie de sécurité IT efficace, et cela quelque soit son secteur d'activité.

Attaquant interne ou externe ? Pas si évident…

Les menaces sont différentes et plus sophistiquées aujourd'hui et la frontière entre les menaces internes et externes est devenue très étroite. La majorité des attaquants externes tentent de pénétrer le réseau, d'acquérir des niveaux d'accès basiques et d'utiliser leurs droits pour petit à petit remonter jusqu'à des niveaux d'accès privilégiés. Dans la plupart des cas, ils restent invisibles dans le réseau pendant plusieurs mois, puisqu'ils parviennent à s'identifier comme des utilisateurs internes.

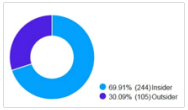
Qu'en est-il des utilisateurs internes malveillants ? : Sont-ils conscients des conséquences de leurs actes lorsqu'ils partagent leurs identifiants ou lorsqu'ils cliquent sur des liens de phishing – dans ce cas, la fuite de données est-elle le résultat d'actions intentionnelles ou accidentelles ? Doivent-ils être considérés comme malveillants seulement si leur action était intentionnelle ? Cela a t-il vraiment beaucoup d'importance si la fuite de données est très grave ?

70% des personnes interrogées considèrent les menaces internes comme les plus risquées

54% des personnes interrogées déclarent avoir très peur des hackers qui pénètrent au sein du réseau de l'entreprise via leur pare-feu, alors même que 40% d'entre elles déclarent qu'un pare-feu n'est pas assez efficace pour empêcher les hackers d'entrer.

Les participants ont également été interrogés sur les attaquants – internes ou externes – qu'ils considèrent les plus à risques :

> Les résultats soulignent un point important en vue de la définition d'une stratégie de défense efficace : 70% des personnes interrogées considèrent que les utilisateurs internes présentent le plus de risques (et seulement 30% estiment que les attaquants externes posent plus de risques).



Une chose est sûre : les attaquants externes cherchent à devenir des utilisateurs internes, et les utilisateurs internes les aident pour y parvenir – accidentellement ou intentionnellement.

Quelque soit la source de l'attaque, la liste des 10 méthodes de hacking les plus populaires -présentées ci-dessous – démontre qu'il est crucial pour les entreprises de savoir ce qu'il se passe sur leur réseau en temps réel. Qui accède à quoi ; est-ce le bon utilisateur derrière l'identifiant et le mot de passe ou est-ce un attaquant externe utilisant un compte compromis ?

Le top 10 des méthodes de hacking les plus utilisées :

1. Ingénierie sociale (ex : phishing).
2. Compromission de comptes (sur la base de mots de passe faibles par exemple).
3. Attaques web (ex : injection SQL/de commandes).
4. Attaques de clients de l'entreprise ciblée (ex: contre des destinataires de documents, navigateurs web).
5. Exploits avec des mises à jour de serveurs connus (ex: OpenSSL, Heartbleed).
6. Terminaux personnels non sécurisés (manque de politique de sécurité BYOD).
7. Intrusion physique.
8. Shadow IT (utilisation personnelle de services Cloud à des fins professionnelles).
9. Attaque d'une infrastructure outsourcée en ciblant un fournisseur de services externe.
10. Attaque de données hébergées sur le Cloud (via l'IaaS, le PaaS).

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.programmez.com/actualites/balabit-presente-un-top-10-des-methodes-de-hacking-les-plus-utilisees-23280

La Chaire de Cyberdéfense et

Cybersécurité Saint-Cyr Sogeti Thales | Le Net Expert Informatique

La Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales

2% de la surface de la terre sont occupés par les villes. Or, d'ici 2050, elles accueilleront 70% de la population mondiale et seront à l'origine de 80% des émissions de CO_2.

Au-delà de ces questions démographiques, entrent également en ligne de compte des contraintes énergétiques, budgétaires, écologiques et technologiques.
La métropole intelligente, pour répondre aux défis de demain, a commencé à développer le numérique dans ses services. La ville réseau mettant en œuvre des infrastructures communicantes et durables pour le confort des citoyens devient ainsi une réalité.
Dans ce cadre, quid de la prévention des risques ? des données personnelles ou des aspects juridiques des smart cities ?

La chaire Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales a le plaisir de vous convier au :
Colloque Cybersécurité et villes intelligentes
Jeudi 15 octobre 2015
9h30-17h00
Musée de l'Armée
Hôtel National des Invalides, amphithéâtre Austerlitz.
L'inscription est obligatoire auprès de
invitations@chaire-cyber.fr

Consultez le programme

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source : http://www.chaire-cyber.fr/

Qui protège le mieux ses données personnelles ? | Le Net Expert Informatique

Qui protège le mieux ses données personnelles ?

La récente affaire Ashley Madison a démontré une nouvelle fois les nombreuses failles de nos systèmes informatiques et la négligence des utilisateurs à confier leurs données personnelles à tous types de sites. Newmanity au travers de son étude a voulu étudier le comportement des français face à cette polémique et les résultats s'avèrent des plus surprenants ! Homme, femme, qui a le plus peur pour ses données personnelles ?

L'échantillon
Enquête réalisée auprès d'un échantillon de Français recrutés par téléphone puis interrogés par Internet les 31 août et 1er septembre 2015. Echantillon de 1183 personnes, représentatif de la population française âgée de 18 ans et plus. La représentativité de l'échantillon est assurée par la méthode des quotas appliqués aux variables suivantes : sexe, âge, profession du chef de famille et profession de l'interviewé après stratification par région et catégorie d'agglomération.

Ce qu'il faut retenir de l'étude
La majorité des actifs Français déclarent faire plus attention à leurs données numériques dans le cadre personnel, plutôt que dans le cadre professionnel > Les hommes déclarent protéger davantage leurs données que les femmes.
Les Français expriment plus de méfiance à l'égard des appareils mobiles (Smartphones, Tablettes) que des ordinateurs > La déconnexion des comptes est une habitude peu fréquente pour les Français

Les hommes plus méfiants que les femmes
Selon les actifs français, les données numériques les plus préoccupantes sont celles issues d'une utilisation personnelle : 69% d'entre eux déclarent y être plus vigilants contre 28% dans le cadre professionnel. Et ce sont les femmes qui sont les moins regardantes (34%) sur la protection de leurs données dans le cadre personnelles contre 73% des hommes qui scrutent méticuleusement la moindre trace sur la toile !
Paradoxalement, les manipulations de base permettant de limiter les problèmes de sécurité en matière de données numériques sont encore assez peu utilisées :
Se déconnecter d'une boîte mail : Moins de 6 actifs sur 10 se déconnectent systématiquement de leur boite mail personnelle lorsqu'ils la consultent depuis le bureau, et cette proportion tombe à 48% lorsque l'utilisation se fait sur ordinateur personnel.
Suppression de l'historique de navigation : Que ce soit sur leur ordinateur personnel ou professionnel, moins de 4 Français sur 10 suppriment leurs données de navigation tous les jours ou au moins une fois par semaine. D'ailleurs, près de 3 actifs sur 10 ne suppriment jamais leur historique de navigation sur leur ordinateur professionnel. Des gestes pourtant simples qui permettraient une meilleures protection de la vie privée de tout un chacun.

Les appareils mobiles suscitent plus de méfiance
Près de la moitié des Français détenteurs d'équipements numériques n'en n'ont pas confiance, signe d'une certaine méfiance alors que les affaires de piratage de données personnelles (Orange, Ashley Madison…) font régulièrement la Une de l'actualité. Dans le détail, que ce soit à l'égard des ordinateurs personnels ou professionnels, les cadres et les femmes qui semblent être les plus confiants. A l'inverse, les hommes et les CSP 'employés' et 'ouvriers' sont nettement plus réservés.
Il est à noter que cette méfiance devient défiance lorsqu'il s'agit de tablettes ou de smartphones. Ces équipements mobiles sont marqués par le peu de confiance qui leur est accordé en matière de sécurité de données transmises : Seulement 37% des Français détenteurs d'une tablette numérique lui font confiance et à peine plus d'un tiers (34%), en ce qui concerne les possesseurs de smartphones.

Source : http://www.economiematin.fr/news-internet-securite-utilisateurs-protection-donnees
Par Stéphane Petibon

Le site Web des universités de Montpellier piraté par un groupe pro-palestinien | Le Net Expert Informatique

Le site Web des universités de Montpellier piraté par un groupe pro-palestinien

L'attaque s'est déroulée pendant quelques heures ce samedi. Des hackers se revendiquant de l'opération « Save Gaza » ont pris en main le site des Universités de Montpellier comme l'a repéré le site H24.Dans un message écrit à la fois en anglais et en français, ils dénoncent l'aide américaine au gouvernement d'Israël, accusé de « contrôler le monde, l'armée, l'économie et les cerveaux ».

« Save Gaza »

Dans un long paragraphe, les auteurs du piratage accusent les deux « gouvernements monsters » d'être « à l'origine de l'hypnose dont souffre la race humaine ». Le texte se conclut sur une adresse aux français: « Si être un vrai « Français », comme vous le dites, c'est d'être soumis, alors personne n'a à le cacher, nous ne sommes pas français, et bien heureux et vous nous considériez différents de vous ».

Le groupe affiche en conclusion son objectif: « The Intruders Will Transform The World », traduit en français par « Les Intruders changeront le monde ».

Source :
http://www.bfmtv.com/societe/le-site-web-des-universites-de-montpellier-pirate-par-un-groupe-pro-palestinien-919637.html