Qui est responsable de la cybersécurité : le RSSI, le DSI, le PDG ou vous ? | Le Net Expert Informatique

La menace informatique est changeante et les décideurs IT peinent à s'adapter à un danger croissant. La cybermenace, certes significative, ne constitue qu'un élément de la sécurité de l'entreprise. Dès lors, qui devrait être responsable de la sécurité et comment les entreprises peuvent adopter une approche plus proactive face aux menaces ? Cinq experts IT donnent leur avis.

1. Faites de la sécurité la responsabilité de tous les salariés

« Le directeur général, et n'importe qui d'autre » répond David Allison à la question de savoir qui est responsable de la sécurité au sein de l'entreprise. Le responsable des systèmes métier pour Aggregate Industries estime que le PDG devrait être responsable de la sécurité, mais que chaque salarié a une responsabilité personnelle.

« La sécurité, ce n'est pas le confinement et la prévention » juge Allison, même si les pare-feu, les antivirus et les autres mesures IT doivent être considérés comme acquis. « Une grande sécurité, c'est affaire d'éducation, de sensibilisation et de responsabilité individuelle. »

Pour lui, le dirigeant de l'entreprise doit s'engager personnellement pour disposer d'une équipe en place formant le personnel dans un large éventail de domaines comme la gestion des courriels, la détection des liens suspects et l'adoption de bonnes pratiques pour les mots de passe.

« La sécurité a besoin d'être une culture diffusée au sein de l'organisation » souligne David Allison. « Le PDG met en place cette culture. Le responsable de la sécurité informatique (RSSI) définit et exécute la stratégie répondant à ce besoin – et chaque salarié est responsable de s'assurer d'adopter et de suivre les pratiques requises. »

2. Ne vous reposez pas sur des produits technologiques

Tim Holman, le président de l'ISSA, une association britannique de sécurité des SI, estime que la responsabilité au sein d'une entreprise se situe toujours au niveau des propriétaires ou des comités de direction. Certains Comex peuvent désigner un DSI, RSSI ou un directeur IT comme le responsable de la sécurité, mais ces individus ne peuvent jamais être tenus pour responsables.

« Les entreprises doivent avoir conscience de l'ampleur de la menace lorsqu'elles font du commerce sur Internet ou stockent leurs données sur le Cloud » déclare Holman. « Les entreprises peuvent charger un DSI d'implémenter une solution Cloud, mais elles resteront toujours responsables si quelque chose tourne mal. »

Face aux cybermenaces, les firmes doivent adopter une attitude proactive, et elles peuvent le faire au travers d'une simple analyse de risques, ou en suivant des standards comme IASME ou Cyber Essentials. D'après Tim Holman, la compréhension des enjeux liés à la sécurité progresse en consacrant du temps avec des dirigeants et en leur expliquant en termes simples les risques inhérents au business en ligne.

« La cybermenace ne peut pas être résolue en achetant des produits. Une approche de bon sens consistant à réduire le volume de données sensibles stockées, à éjecter les fournisseurs non-sécurisés, à restreindre l'accès aux données et à souscrire une cyber-couverture sera souvent dix fois plus efficace et dix fois moins chère que la dernière génération d'appliance de sécurité vendue par les experts de la vente. »

3- Gardez sous contrôle les périls des terminaux mobiles

David Reed, directeur des services d'information et de l'infrastructure à la Press Association (PA), juge complexe la discussion autour de la sécurité, mais est d'avis que la responsabilité commence au sommet de l'IT. « Si en tant que DSI, vous n'êtes pas en mesure de percevoir les dangers liés à la sécurité, vous ne faites pas un assez bon travail » tranche-t-il.

Un des domaines les plus importants pour Press Association est ainsi la gestion du mobile. Les journalistes de la société ont à traiter des informations extrêmement sensibles, et la menace de piratage d'un terminal, bien que sérieuse, n'est pas aussi répandue qu'une simple perte ou un vol. PA travaille avec EE pour implémenter une stratégie mobile COPE (un terminal de l'entreprise pour un usage personnel et professionnel) utilisant des Samsung S4 Mini et le système de sécurité Knox.

« Un conteneur peut être créé sur chacun des téléphones pour stocker séparément documents de travail, courriels et contacts et éléments personnels. Nos journalistes disposent principalement de deux zones sur leurs téléphones : une pour l'usage personnel et l'autre pour le travail » précise David Reed.

« Chez PA, nous aidons les journalistes en recommandant des apps. Nous avons appliqué ce principe pour les jeux du Commonwealth de 2014 en envoyant aux journalistes présents sur l'évènement un message pour télécharger l'app Team GB. L'appli était en liste blanche et installée simplement dans le conteneur. »

4- Obtenez le soutien du dirigeant pour les démarches de gouvernance

Pour Omid Shiraji, ex-DSI de Working Links, la responsabilité de la sécurité est totalement liée à l'entreprise et à la nature de ses activités. Il n'est pas persuadé de la nécessité de disposer d'un RSSI dans la majorité des organisations.

« La sécurité IT est une commodité. Vous pouvez acheter des produits et de l'expertise auprès d'un fournisseur » juge-t-il. « La même chose est vraie en ce qui concerne la sécurité des entreprises dans de nombreux cas – les processus et la gouvernance sont une marchandise que vous pouvez acheter comme un service géré. »

Omid Shiraji préférerait consacrer son budget IT limité aux opérations en première ligne, et ensuite s'appuyer sur une expertise spécifique pour l'aider à protéger ses données et guider son personnel. La société a récemment été certifiée ISO 27001 et le support du PDG s'est révélé essentiel.

« Les individus changent leur comportement car ils entendent le PDG parler des conséquences majeures des activités non protégées » déclare-t-il. « La sécurité IT est en fait le travail de chaque employé, mais le patron doit soutenir chaque initiative en matière de sécurité et de gouvernance dans l'entreprise. Et c'est ce qui s'est passé chez Working Links. »

5. Créez une culture du risque pragmatique

Julian Self, un DSI expérimenté qui a travaillé pour de nombreux acteurs de la finance, fait lui une analyse différente et estime que l'importance du RSSI dans l'entreprise continue de grandir. Selon lui, il est du ressort du DSI de promouvoir auprès des dirigeants les avantages d'un spécialiste de la sécurité.

« Dans un monde déjà hyper-connecté, et avec l'avènement de l'Internet des Objets, le travail de sécurisation des données de l'entreprise devient infiniment plus complexe avec des flux de données qui entrent et sortent de nombreux terminaux » commente Julian Self, pour qui le panorama de la menace continue d'évoluer.

« Les RSSI ne réussiront pas à moins d'avoir l'adhésion et l'engagement des métiers. Sans cela, ils seront simplement perçus comme des freins à l'activité et leurs efforts seront contournés. »

« Fondamentalement, les RSSI ont besoin de créer une prise de conscience et une culture pragmatique du risque afin que la sécurité de l'information soit appliquée de façon inconsciente dans tous les domaines de l'entreprise. Cette approche doit aller de pair avec une réponse à incidents qui soit proportionnée et sans alarmisme, et la gestion et la réaction au risque, restaurant in fine la confiance de l'entreprise. »

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.zdnet.fr/actualites/qui-est-responsable-de-la-cybersecurite-le-rssi-le-dsi-le-pdg-ou-vous-39826198.htm

---

Comment réagir face à une cyberattaque | Le Net Expert Informatique

Comment réagir face à une cyberattaque

Choc, sidération, déni… Une attaque informatique paralyse souvent les entreprises qui en sont victimes. L'idéal est donc de s'y préparer pour avoir les bons réflexes le moment venu. « Au début, une cyberattaque ne fait pas de bruit. L'entreprise continue apparemment à fonctionner normalement. Les cellules de crise classiques ont donc du mal à se mobiliser. Il faut s'adapter en prenant en compte la dimension cyber de l'attaque », remarque Gérôme Billois, expert en cybersécurité chez Solucom.

1 MONTER UNE CELLULE DE CRISE CYBER

La cellule de crise décisionnelle (direction générale, service juridique, RH, informatique, communication…) doit être secondée par une cellule de crise cyber. Idéalement, cette équipe est pilotée par le responsable sécurité des systèmes d'information (RSSI). Elle regroupe des membres de la direction informatique et les responsables des applications informatiques liées aux métiers de l'entreprise. Tous ces protagonistes doivent être sensibilisés à travers des exercices spécifiques, organisés annuellement.

« Suivant le scénario d'attaque, cela peut prendre la forme d'un exercice sur table de quelques heures à la simulation d'un début de crise », explique Gérôme Billois. Tout le monde doit être sur le pont. Les managers pour identifier les ressources à protéger, les RH pour répondre aux interrogations des collaborateurs, le service juridique pour évaluer les suites judiciaires, la communication si l'information de l'attaque a fuité…

2 DÉCONNECTER LES MACHINES INFECTÉES

Dès les premiers soupçons d'attaque, il faut réagir. Un grand industriel européen s'est mordu les doigts de ne pas avoir pris au sérieux les alertes remontées en 2012 par les autorités nationales. Résultat : le pirate a eu tout le loisir de sonder en profondeur son réseau informatique. « La crainte est qu'il ait eu accès au code source de nos outils informatiques qui permettent de gérer les infrastructures de nos clients », confie cet industriel. Il ne faut toutefois pas confondre vitesse et précipitation, prévient Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces au ministère de l'Intérieur. Les entreprises sont entre deux feux. D'une part, elles doivent isoler leur système de l'extérieur pour éviter la propagation de l'attaque. D'autre part, il faut éviter d'en effacer les traces. « Si on coupe et on efface les disques durs, les enquêteurs perdent les preuves et la possibilité de remonter aux auteurs de l'attaque », souligne le préfet.

La déconnexion peut être utile. Victime, en avril dernier, d'une attaque sévère qui a interrompu ses programmes, la chaîne de télévision TV5 Monde a agi ainsi pour limiter la casse. « Par chance, les équipes informatiques étaient présentes le soir de l'attaque. Elles ont pu déconnecter les machines infectées. Cela été salutaire. Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), l'objectif était de détruire notre société », précise Yves Bigot, le directeur général de la chaîne.

L'urgence passée, il faut rapidement faire appel à des professionnels expérimentés dans la neutralisation des attaques informatiques. L'Anssi dispose sur son site internet d'une liste de prestataires disposant du label CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques). Certains s'engagent à intervenir en moins de quatre heures.

3 PORTER PLAINTE ET ESTIMER LES PRÉJUDICES

« Les entreprises hésitent à porter plainte, car elles craignent que cela nuise à leur réputation. Or, sans cela, on ne peut traiter policièrement et judiciairement une affaire », déplore le « préfet cyber ». Il faut donc déposer plainte au commissariat ou à la brigade de gendarmerie locale. Certains disposent d'un investigateur en cybercriminalité qui fournira les conseils d'urgence. La seconde étape est de se rapprocher d'interlocuteurs techniques qui pourront apporter leur expertise.

Les entreprises en région parisienne doivent solliciter la Befti, la brigade d'enquête sur les fraudes aux technologies de l'information. Cette unité spécialisée conseille les entreprises victimes d'intrusion informatique ou de détournement de fonds… Les entreprises en province auront accès à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Il faut venir avec le maximum d'éléments qui vont aider les enquêteurs : le journal des connexions, la configuration des machines, les disques durs des machines infectées… « Il faut aussi estimer les préjudices subis sur la base d'éléments concrets. Cela permettra de présenter un dossier solide auprès du procureur de la République. C'est sur ce dossier qu'il décidera des suites à donner à l'enquête », explique le colonel Freyssinet, spécialisé dans la lutte contre les cybermenaces au ministère de l'Intérieur.

4 RECONSTRUIRE LA SÉCURITÉ INFORMATIQUE

Il faut agir sur les conséquences de l'attaque. Le grand industriel européen qui craignait qu'un pirate ait eu accès au code source de son outil de gestion à distance des infrastructures de ses clients n'a pas tergiversé. « Le code du produit a été totalement revu afin d'éviter la création d'un backdoor [une porte dérobée, ndlr] exploitable par les pirates. Nous avons également informé nos clients de l'attaque subie », confie-t-il. Après son attaque, TV5 Monde a remis à plat sa sécurité informatique. Elle a remplacé le matériel technique compromis et déployé des nouveaux équipements de sécurité.

Les 400 salariés suivent une formation pour apprendre les gestes de base dans ce domaine. La chaîne a imposé des mesures drastiques : suppression du Wi-Fi, interdiction de connecter des équipements électroniques personnels (tablette, smartphone…) aux ordinateurs de bureau, passage des clés USB au sas de décontamination… Soit, au total, une facture de 5 millions d'euros.

Pour soigner les machines infectées, l'Anssi préconise de réinstaller entièrement le système d'exploitation et d'appliquer tous les correctifs de sécurité avant de la reconnecter. Elle recommande de modifier les mots de passe de tous les comptes de l'entreprise sous peine de revoir débarquer le pirate informatique. L'agence incite également les entreprises victimes à communiquer avec leurs pairs. « Généralement, les pirates s'attaquent à plusieurs entreprises d'un même secteur, en réutilisant les mêmes techniques. En partageant son expérience, on renforce la sécurité collective », explique Guillaume Poupard, le directeur général de l'Anssi.

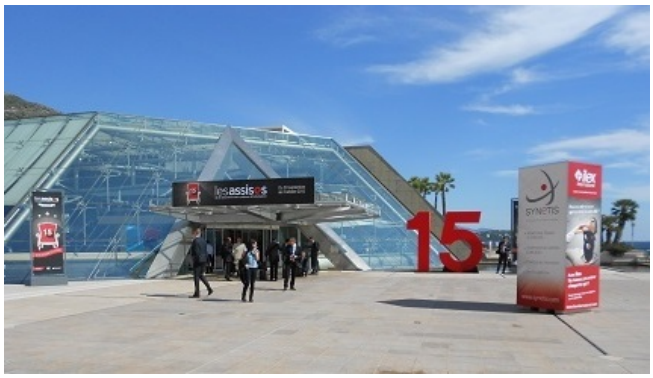
La messagerie sous écoute

Dans la panique, les membres de la cellule de crise communiquent par e-mails et s'échangent des fichiers via le réseau de l'entreprise. Grave erreur. Il y a de grandes chances pour que ces systèmes soient compromis et sous écoute. Le conseil pour communiquer en toute discrétion : ouvrir temporairement des comptes de messagerie à partir de services web. Les échanges informatiques doivent également se faire par l'intermédiaire d'un réseau de secours indépendant de celui de l'entreprise afin de garantir leur confidentialité.

Denis JACOPINI est Expert 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.usine-digitale.fr/article/comment-reagir-a-une-cyberattaque.N354821
Par HASSAN MEDDAH

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

---

Stopper les attaques informatiques avant qu'elles ne bloquent l'entreprise | Le Net Expert Informatique

Stopper les attaques informatiques avant qu'elles ne bloquent l'entreprise

Une récente étude de Gartner révèle que seulement 40 % des grandes organisations auront mis en place des plans de sécurité globaux afin de se prémunir contre les cyberattaques d'ici 2018. Cela signifie que 60 % des entreprises n'auront pas mis en place de stratégie d'ici trois ans, prenant un risque considérable face à des attaques de plus en plus sophistiquées qui pourraient atteindre un niveau supérieur au cours des prochaines années. Il ressort notamment de ce rapport que la priorité serait donnée à l'adoption de solutions de détection des attaques de manière réactive plutôt que proactive. Jean-François Pruvot, Regional Director France chez CyberArk, nous livre son analyse.

A l'heure où les cyberattaques sont de plus en plus nuisibles, les entreprises qui stockent des données sensibles figurent parmi les principales cibles. Le fait que la plupart des sociétés n'aient pas prévu de stratégie globale de sécurité d'ici à trois ans, et ce malgré les récentes attaques perpétrées contre de grands noms, témoigne souvent d'un manque de connaissances sur la manière de hiérarchiser les priorités dans le cadre de leurs programmes de sécurité ; cela laisse présumer que le hacker se trouve déjà à l'intérieur du réseau. Selon le général chinois Sun Tzu, dans son traité de stratégie militaire « L'art de la guerre », le succès de celle-ci repose sur la préparation mais également sur une bonne connaissance du terrain. Les entreprises doivent donc impérativement identifier l'ensemble des portes permettant d'accéder au « royaume IT », en particulier les comptes administrateurs ou à hauts pouvoirs qui conduisent à l'intégralité du système et des données qu'il renferme ; il est en effet impossible de protéger un espace sans connaître son étendue et ce qu'il contient.

La mise en place d'une stratégie globale de sécurisation de ces comptes et des systèmes d'information est donc indispensable pour limiter les vols et pertes de données, et se fait en plusieurs étapes clés.

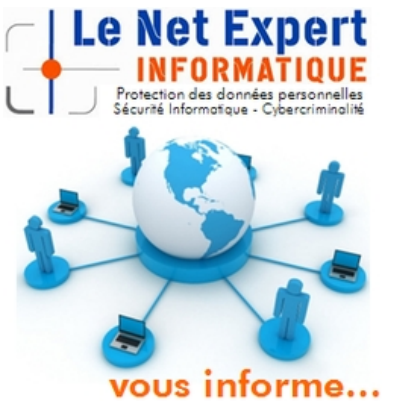
Tout d'abord, partant du constat que la menace est peut-être déjà à l'intérieur, les RSSI doivent s'équiper d'outils de détection d'activités inhabituelles dans leurs systèmes. Cela leur permettra de contenir les menaces et de se prémunir contre l'infiltration progressive et malveillante de hackers dans le réseau en stoppant leur déplacement latéral. Une fois que les mesures de sécurité sont prises pour protéger les données, les comptes à privilèges difficilement détectables restent l'accès principal aux informations pour les pirates. Il est par exemple possible de les contourner pour pénétrer dans le système à l'aide de techniques de phishing classiques ; une fois à l'intérieur, le hacker peut s'y déplacer insidieusement et y installer des logiciels malveillants qui lui permettront de collecter autant de données que nécessaires sur des périodes pouvant se compter en années, et ce sans être détecté. Les comptes à hauts-pouvoirs qui ne sont pas suivis, gérés et protégés sont en effet l'une des vulnérabilités les plus répandues dans le cas de cyberattaques.

Enfin, une fois la stratégie établie, bien qu'il ne faille pas négliger la faille humaine, il est essentiel aujourd'hui que les entreprises ne se réfugient plus derrière cette excuse pour justifier les faiblesses des systèmes. En effet, que la menace vienne de l'intérieur ou de l'extérieur, les conséquences sont les mêmes pour les entreprises encore nombreuses à ne pas posséder les bases pour sécuriser leurs données ; elles doivent en effet commencer par mettre en place des correctifs, assurer leur mise à jour régulière, et surtout veiller au renforcement des contrôles sur les comptes à privilèges et administrateurs. Il est donc essentiel d'anticiper la présence de l'ennemi dans l'organisation et d'adopter ainsi une posture de gestion des risques concentrée sur la proactivité.

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.infodsi.com/articles/158490/gestion-risques-stopper-attaques-avant-bloquent-entreprise.html

Multiples vulnérabilités dans Apple iTunes | Le Net Expert Informatique



Multiples vulnérabilités dans Apple iTunes

1 – Risque(s)exécution de code arbitraire à distance
déni de service à distance
atteinte à la confidentialité des données

2 – Systèmes affectés
Apple iTunes version antérieure à 12.3

3 – Résumé
De multiples vulnérabilités ont été corrigées dans Apple iTunes. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données.

4 – Solution
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 – Documentation
Bulletin de sécurité Apple HT205221 du 16 septembre 2015
https://support.apple.com/fr-fr/HT205221
Référence CVE CVE-2010-3190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3190
Référence CVE CVE-2014-8146
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8146
Référence CVE CVE-2015-1152
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1152
Référence CVE CVE-2015-1153
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1153
Référence CVE CVE-2015-1157
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1157
Référence CVE CVE-2015-1205
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1205
Référence CVE CVE-2015-3686
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3686
Référence CVE CVE-2015-3687
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3687
Référence CVE CVE-2015-3688
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3688
Référence CVE CVE-2015-3730
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3730
Référence CVE CVE-2015-3731
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3731
Référence CVE CVE-2015-3733
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3733
Référence CVE CVE-2015-3734
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3734
Référence CVE CVE-2015-3735
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3735
Référence CVE CVE-2015-3736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3736
Référence CVE CVE-2015-3737
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3737
Référence CVE CVE-2015-3738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3738
Référence CVE CVE-2015-3739
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3739
Référence CVE CVE-2015-3740
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3740
Référence CVE CVE-2015-3741
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3741
Référence CVE CVE-2015-3742
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3742
Référence CVE CVE-2015-3743
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3743
Référence CVE CVE-2015-3744
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3744
Référence CVE CVE-2015-3745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3745
Référence CVE CVE-2015-3746
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3746
Référence CVE CVE-2015-3747
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3747
Référence CVE CVE-2015-3748
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3748
Référence CVE CVE-2015-3749
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3749
Référence CVE CVE-2015-5755
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5755
Référence CVE CVE-2015-5761
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5761
Référence CVE CVE-2015-5789
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5789
Référence CVE CVE-2015-5790
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5790
Référence CVE CVE-2015-5791
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5791
Référence CVE CVE-2015-5792
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5792
Référence CVE CVE-2015-5793
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5793
Référence CVE CVE-2015-5794
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5794
Référence CVE CVE-2015-5795
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5795
Référence CVE CVE-2015-5796
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5796
Référence CVE CVE-2015-5797
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5797
Référence CVE CVE-2015-5798
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5798
Référence CVE CVE-2015-5799
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5799
Référence CVE CVE-2015-5800
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5800
Référence CVE CVE-2015-5801
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5801
Référence CVE CVE-2015-5802
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5802
Référence CVE CVE-2015-5803
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5803
Référence CVE CVE-2015-5804
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5804
Référence CVE CVE-2015-5805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5805
Référence CVE CVE-2015-5806
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5806
Référence CVE CVE-2015-5807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5807
Référence CVE CVE-2015-5808
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5808
Référence CVE CVE-2015-5809
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5809
Référence CVE CVE-2015-5810
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5810
Référence CVE CVE-2015-5811
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5811
Référence CVE CVE-2015-5812
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5812
Référence CVE CVE-2015-5813
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5813
Référence CVE CVE-2015-5814
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5814
Référence CVE CVE-2015-5815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5815
Référence CVE CVE-2015-5816
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5816
Référence CVE CVE-2015-5817
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5817
Référence CVE CVE-2015-5818
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5818
Référence CVE CVE-2015-5819
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5819
Référence CVE CVE-2015-5821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5821
Référence CVE CVE-2015-5822
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5822
Référence CVE CVE-2015-5823
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5823
Référence CVE CVE-2015-5874
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5874
Référence CVE CVE-2015-5920
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5920
Gestion détaillée du document

18 septembre 2015
version initiale.
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-398

«Vous avez tous des secrets à protéger» | Le Net Expert Informatique

	«Vous avez tous des secrets à protéger»

«Sauvegardez vos données, protégez votre connexion internet, ne vous séparez pas de votre matériel dans les aéroports». Autant de conseils donnés, jeudi soir, lors de la première réunion de sensibilisation des entreprises ariégeoises à l'intelligence économique. Car si les nouvelles technologies participent aux échanges et au développement des entreprises, elles sont aussi une aubaine pour les prédateurs économiques. Maîtriser les communications d'informations stratégiques est donc primordial pour les chefs d'entreprise. Les risques encourus ? Le vol des «recettes secrètes» des productions ariégeoises, le piratage de site internet…

En Ariège, Marie Lajus, la préfète, a désigné Marie-Hélène Guilbaud chef du pôle interministérielle et modernisation. C'est elle, avec le concours de la CCI, l'UPAP et Ariège expansion qui a organisé cette soirée d'échanges à laquelle une vingtaine de dirigeants de PME ariégeoises, élus, officiels de la gendarmerie et de la police se sont rendu.

Derrière le pupitre, plusieurs intervenants : consultant privé, agents de la direction générale de la sécurité intérieure et extérieure, et de la direction de la protection et de la sécurité de la défense. Et pour appuyer leurs propos, l'expérience de plusieurs chefs d'entreprises ariégeoises. Eric Rumeau, directeur de Mapaero a ainsi expliqué comment l'entreprise, qui a aujourd'hui plusieurs antennes à l'étranger, «a pris la question de la sécurité à bras-le-corps», en organisant «des réunions mensuelles avec leurs commerciaux», en fournissant «des clés USB maison».

Quatre thématiques étaient développées lors de ce premier rendez-vous : la veille stratégique ; la mobilité, quels risques pour l'entreprise ? ; les signes de radicalisation au sein de l'entreprise ; et le label SUREN (outil d'évaluation de la sûreté des entreprises, une action de service public).

L'objectif pour tous les acteurs est clair. Dans un espace économique mondialisé et concurrentiel, pour les entreprises, il est essentiel d'adopter une attitude active vis-à-vis de l'information, de mieux comprendre leur environnement, d'améliorer leur surveillance afin de prendre des décisions.

Pour plus d'information, consulter le site internet de la délégation interministérielle à l'intelligence économique www.intelligence-economique.gouv.fr ou le site de l'agence nationale de la sécurité des systèmes d'information www.ssi.gouv.fr

---

Source :

http://www.ladepeche.fr/article/2015/09/26/2185316-vous-avez-tous-des-secrets-a-proteger.html

L’essor du chiffrement inquiète le renseignement anglais | Le Net Expert Informatique

L’essor du chiffrement inquiète le renseignement anglais

Dans une interview à la BBC, le patron du renseignement intérieur britannique (MI5) a exprimé ses inquiétudes à l'égard de l'évolution des technologies de chiffrement. Selon lui, les entreprises technos ont le devoir éthique d'informer les autorités de menaces potentielles.

Le gouvernement britannique n'en démord pas et veut ses backdoors : dans une interview donnée à la BBC, le dirigeant du MI5, les services de sécurité de la Grande-Bretagne, évoque à nouveau le débat autour des technologies de chiffrement qui se développent à destination du grand public.

Pour Andrew Parker, directeur du MI5, les services de police ont de plus en plus de mal à obtenir des informations en ligne et les entreprises du secteur technologique devraient selon lui informer les agences de renseignement des potentielles menaces détectées via leurs outils. Il explique au micro de la BBC que les services de police sont confrontés à la difficulté croissante d'obtenir « les relevés de communications des utilisateurs suspectés d'activités terroristes, et ce même en disposant d'un mandat de justice. »

Haro sur le chiffrement

Une critique déjà entendue fréquemment et qui fait écho au développement d'outils de chiffrement de bout-en-bout, mouvement qui gagne en intensité dans l'industrie des nouvelles technologies et des services en ligne suite aux révélations d'Edward Snowden.

Et la problématique n'est cantonnée Outre-Manche, où David Cameron a annoncé son intention de légiférer sur le sujet. Aux États Unis, on a ainsi pu voir les dirigeants du FBI exprimer une demande similaire, évoquant la possibilité de mettre en place des backdoors connues des seuls services de renseignement afin de pouvoir accéder aux données échangées sur les plateformes de messagerie en ligne. En France, c'est le procureur de la République de Paris qui s'y colle : celui-ci avait signé en août une tribune dans le New York Times déplorant l'essor du chiffrement et l'obstacle que celui-ci constituait dans les enquêtes judiciaires.

Face à cette offensive, les défenseurs de la cryptographie s'inquiètent tout particulièrement des conséquences que pourrait apporter la mise en œuvre d'une telle volonté politique : pour Bruce Schneier, expert américain de la cryptographie, s'appuyer sur ce type de procédé viendrait immanquablement contredire le principe même de la cryptographie, supposé garantir la sécurité des échanges entre les destinataires. De plus, et l'affaire récente des clefs d'accès aux cadenas TSA le rappelle bien : les backdoors ne sauraient garantir que la personne qui les utilise est bien un représentant des forces de l'ordre, laissant la possibilité à des cybercriminels ou à des pays étrangers de les exploiter.

Source :
http://www.zdnet.fr/actualites/le-renseignement-anglais-s-inquiete-lui-aussi-de-l-essor-du-chiffrement-39825120.htm

---

Des hackers dupent Apple et

infectent des millions d’iPhone | Le Net Expert Informatique

	Des hackers dupent Apple et infectent des millions d’iPhone

Pour la première fois, des pirates ont réussi à diffuser des applications malveillantes sur le magasin AppStore, en trafiquant le langage de codage utilisé par les développeurs.

Après ses ordinateurs Mac, c'est au tour des iPhone et iPad d'Apple de se frotter aux virus. Le groupe à la pomme croquée a confirmé à Reuters que son magasin d'applications AppStore a été victime de sa toute première faille de sécurité majeure. Jusqu'à présent, l'AppStore était réputé comme ultra-sûr puisqu'Apple inspecte minutieusement chaque appli avant de la proposer aux téléchargements (à l'inverse du Play Store de Google), afin d'éviter les logiciels malveillants mais aussi imposer sa chape de plomb sur le sexe.

Sauf que des pirates malins ont trouvé une parade pour échapper à la vigilance de la pomme. Les hackers sont remontés jusqu'à la source de toutes les applis, le langage de codage Xcode, pour diffuser auprès des développeurs naïfs une version compromises (intitulée XcodeGhost). Toutes les applis créées avec cet outil pouvant dès lors de se transformer en logiciel malveillant. Un porte-parole d'Apple souligne auprès de Reuters :

Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps ».

La version compromise de Xcode a été identifiée comme hébergée sur un serveur chinois. Les développeurs ont préféré celle-ci puisqu'elle s'avérait beaucoup plus rapide à télécharger que le logiciel officiel hébergé sur le serveur d'Apple.

Des centaines de millions d'iPhone exposés

Selon la firme de sécurité Palo Alto Networks Inc, 39 applications malicieuses ont été découvertes et certaines sont particulièrement populaires, dont :

– l'incontournable appli de discussion instantanée WeChat,
– le très utilisé enregistreur de cartes de visites CamCard,
– Didi Chuxing, le concurrent chinois d'Uber,
– l'unique appli pour acheter des billets de train en Chine Railway 12306.

Au total, plusieurs centaines de millions d'utilisateurs pourraient avoir été victimes d'un vol de données tels que des mots de passe, estime l'entreprise, même si aucun cas n'a pour l'heure été constaté.

La firme de sécurité chinoise Qihoo360 affirme elle avoir détecté pas moins de 344 applis compromises. Plusieurs ont été retirées de l'AppStore par Apple, mais le groupe refuse de donner le nombre exact d'applications concernées. Un porte-parole affirme à « l'Obs » : *Nous prenons la sécurité très au sérieux et iOS [le système de l'iPhone et l'iPad, NDLR] est conçu pour être fiable et sécurisé. Pour protéger nos clients, nous avons supprimés les applications de l'AppStore que nous savons créées avec cet outil contrefait. »*

Sur son blog, WeChat affirme que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

Les iPhone, « des cibles de choix »

Selon Ryan Olson de Palo Alto Networks Inc, « l'information n'est toutefois pas à prendre à la légère », puisque cela montre que l'AppStore peut être compromis par des hackers qui ciblent les développeurs. Pis, cela pourrait donner des idées à d'autres et il sera difficile de s'en prémunir, estime-t-il.

L'iPhone ne serait-il plus aussi sûr qu'à ses débuts ? « Avec l'augmentation des parts de marché d'Apple, le nombre de cibles augmente et l'intérêt des cybercriminels augmente », pointe Laurent Heslault, responsable des stratégies de sécurité chez Symantec. Gérome Billois, administrateur du Club de la sécurité de l'information français (Clusif), renchérit :

Surtout que les utilisateurs d'Apple sont connus pour avoir des revenus plus élevés, faisant d'eux des cibles de choix ».

Surtout que les utilisateurs d'iPhone – et plus largement de smartphones – n'ont pas encore pris pleinement conscience des risques de piratage sur ces mini-ordinateurs. Rien que l'an dernier, l'entreprise de sécurité Symantec a découvert 6,3 millions d'appli malicieuses capables d'infecter les terminaux.

Apple n'est donc pas beaucoup plus sûr que ses concurrents. Le rapport annuel de Symantec pointe que 84% des vulnérabilités découvertes le sont sur iPhone (contre 11% pour Android). Le plus souvent, elles sont exploitées pour infecter l'appareil, dérober des informations personnelles (mots de passe, comptes bancaires…), afficher des publicités, ou encore envoyer des SMS surtaxés. Laurent Heslault interroge :

Il y a des centaines de milliers d'applications gratuites disponibles, croyez-vous qu'il y ait autant de philanthropes ? »

La vigilance est donc de rigueur avant de cliquer sur un lien, entrer ses identifiants sur un site, etc. Même prudence lorsqu'une fenêtre pop-up s'ouvre sur l'iPhone, réclamant l'identifiant et le mot de passe iCloud. Si elle n'a pas de raison de s'ouvrir (par exemple lors de la consultation de ses e-mails), alors il n'y a pas de raison de lui donner les informations.

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://tempsreel.nouvelobs.com/tech/20150921.OBS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html
Par Boris Manenti

Des applications malveillantes dans l’App Store | Le Net Expert Informatique

Des pirates ont trouvé le moyen de faire entrer des applications malveillantes dans la boutiques d'Apple. Ils ont pour cela convaincu des développeurs d'utiliser une version modifiée de Xcode, introduisant ainsi des malwares sur l'App Store.

Pour minimiser les risques d'infection des terminaux mobiles, les éditeurs de plateformes recommandent (ou imposent) l'utilisation de leurs boutiques d'applications officielles. Il est malgré tout possible d'éviter les mécanismes de contrôle mis en place par exemple par Google et Apple.

Et Apple vient d'ailleurs d'en faire les frais. La firme a confirmé officiellement à Reuters avoir dû retirer plusieurs apps de l'App Store suite à la découverte d'une faille de sécurité. Des pirates ont trouvé une solution pour échapper à la vigilance de l'éditeur.

Xcode corrompu pour pénétrer l'App Store

Pour concevoir des applications pour iOS et OS X, les développeurs ont recours aux outils de développement d'Apple regroupés au sein du logiciel Xcode. Les pirates ont ainsi mis au point une version modifiée de Xcode, diffusée ensuite auprès de développeurs d'apps. Les applis réutilisant cet outil se transformaient dès lors en malwares.

Présenté sous la dénomination XcodeGhost, ce malware a pu faire son entrée sur l'App Store. Plusieurs applications populaires ont été compromises par cette méthode dont la messagerie WeChat, CamCard ou le concurrent chinois d'Uber, Didi Chuxing.

WeChat a précisé dans un billet de blog que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

« Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps » déclare un porte-parole d'Apple auprès de Reuters. Le malware XcodeGhost est présenté par la société de sécurité Palo Alto Networks comme particulièrement nuisible et dangereux.

L'éditeur de sécurité précise également que la version compromise de Xcode a été identifiée sur un serveur en Chine. Et si elle a été utilisée par les développeurs, c'est probablement car elle s'avérait plus rapide à télécharger que le logiciel officiel hébergé chez Apple.

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… ;

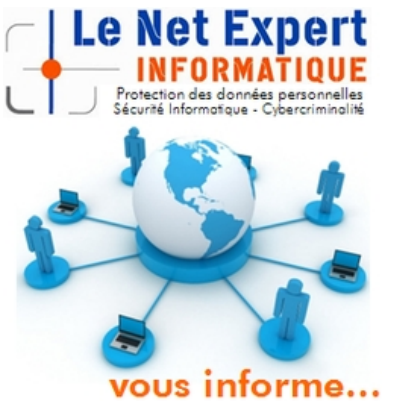
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

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

Contactez-nous

Source : http://www.zdnet.fr/actualites/apple-contraint-de-supprimer-des-apps-malveillantes-de-l-app-store-39825174.htm

Savoir profiter des erreurs des Cybercriminels | Le Net Expert Informatique



Savoir profiter des erreurs des Cybercriminels

L'affaire Ashley Madison semble le prouver une fois de plus, les cybercriminels commettent des erreurs qui peuvent leur nuire. Détecter ces fautes et savoir les utiliser sont des éléments essentiels dans la gestion des crises cyber.

DES ATTAQUES DONT LES OBJECTIFS SONT SOUVENT DIFFICILES À CERNER

L'actualité le montre trop régulièrement, les actes cybercriminels se multiplient et visent tous types d'organisation. Certains sont revendiqués et leurs objectifs sont rapidement connus. C'est le cas pas exemple de l'attaque visant le site Ashley Madison où les motivations sont explicites.

Mais dans la plupart des cas, les objectifs de l'attaquant sont beaucoup plus difficiles à identifier ! Il est pourtant crucial de le faire pour pouvoir réagir au mieux et protéger rapidement ce qui n'a pas encore été touché par l'attaque.

Une des clés pour mieux comprendre une attaque consiste à exploiter les erreurs des attaquants. En effet, malgré leur niveau de compétences potentiellement élevé, les pirates restent des humains et commettent souvent des erreurs. Des fautes qu'il est possible d'exploiter pour mieux comprendre l'attaque et la contrer, mais aussi pour identifier ceux à son origine.

UTILISER LES ERREURS DES ATTAQUANTS POUR MIEUX LES COMPRENDRE

Le cas récent d'Ashley Madison semble être un bon exemple, même s'il faudra attendre les investigations complètes pour confirmer tous les éléments. Les attaquants auraient diffusé les données volées via BitTorrent en utilisant un serveur loué chez un hébergeur aux Pays Bas. Ils auraient cependant oublié de sécuriser ce serveur, en particulier ils n'ont pas mis de mot de passe sur les interfaces d'administration web. Même si cela ne permet pas de les identifier directement, il s'agit d'une piste de premier choix pour les forces de l'ordre en charge des investigations. Il faut cependant rester prudent car cela peut aussi être une forme de diversion réalisée par les attaquants. Affaire à suivre !

Autre exemple, le cas « Red October ». C'est l'affaire d'une vaste opération de cyber espionnage qui a commencé en mai 2007 et qui a été découverte par le cabinet Kaspersky quelques années plus tard. Le cabinet a réussi à identifier, bloquer et neutraliser le logiciel malveillant en utilisant une faille de l'attaque. En effet, les noms de domaines pour les serveurs d'exfiltration qui étaient utilisés dans le code malveillant n'avaient pas été réservés par les attaquants. Cela a permis à Kaspersky de simuler un de ces serveurs et de voir qui était infecté et quelles données étaient capturées.

Parfois, ces erreurs permettent même d'identifier les auteurs de l'attaque, comme ce fut le cas avec la traque de la personne derrière le malware PlugX.

Nos consultants ont d'ailleurs eux aussi rencontré ce genre de situation dans le cadre d'une attaque ciblée chez un de nos clients. Les pirates avaient en effet « oublié » la présence d'un keylogger sur les serveurs internes utilisés pour l'exfiltration des données, ce qui a permis à nos experts d'identifier quelles données étaient ciblées et où elles étaient envoyées. Nous avons même pu récupérer le login et le mot de passe utilisés par les attaquants. Le concept de « l'arroseur arrosé » remis au goût du jour.

SAVOIR TIRER PARTI DE CES INFORMATIONS POUR MIEUX GÉRER LA CRISE

Les informations obtenues grâce à ces erreurs sont très précieuses, elles permettent ensuite d'adapter la réponse à l'incident. D'autant plus que les attaquants utilisent parfois des mécanismes de diversion « bruyants » (redémarrage de machines, effacement de fichiers, forte activité CPU, voir déni de service…) afin de détourner l'attention des vrais données qu'ils visent. Une compréhension « métier » des objectifs de l'attaque permet d'éviter de se focaliser sur ces pièges.

Il est même souvent intéressant de laisser l'attaque se dérouler pour mieux la comprendre.

Les réflexes face aux incidents de sécurité « classiques » (déployer des signatures antivirales, réinstaller des serveurs…) sont donc aujourd'hui largement révolus. Il faut adopter une approche dynamique de la crise, s'intéresser à son objectif métier et utiliser les erreurs des attaquants pour être plus pertinent, en pouvant même envisager des réponses « actives » à l'attaque. Un challenge pour les équipes de réponses à incidents, qui doivent adapter leurs méthodologies et leurs réflexes, mais un objectif crucial pour lutter contre ces attaques

---

Source :

http://www.solucominsight.fr/2015/08/attaques-ciblees-profiter-des-erreurs-des-attaquants-pour-mieux-les-comprendre-et-les-contrer/