Un technique d’attaque informatique très répandue : Le « Watering Hole » | Denis JACOPINI

Les motivations des attaquants sont diverses. Les plus répandues sont le gain financier, la gloire personnelle, la malveillance ou encore l'espionnage.Quelle que soit la finalité de l'attaque, cette dernière passe le plus souvent par la compromission d'un système. Pour parvenir à leur fin, les attaquants disposent d'un large arsenal comprenant le contournement des mécanismes de sécurité, l'accès physique à la machine ou encore l'exploitation de vulnérabilités. Au sein de cet arsenal, l'exploitation de vulnérabilités constitue sans aucun doute le principal vecteur d'intrusion. Les méthodes d'infection employées peuvent alors prendre différentes formes :• Infection par média amovible (CD, USB, cartes SD, …)
• Infection par e-mail (pièce jointe ou un lien malicieux notamment)
• Infection via le réseau interne (fichiers partagés)
• Infection par visite d'un site Web

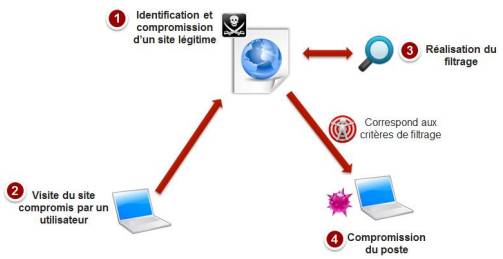
Le « Watering Hole » fait partie de la dernière catégorie : «Infection par site Web », autrement appelé «Drive-By Download». Cette dernière repose sur le principe suivant :
1. Création ou compromission d'un site Web par l'attaquant (accès à l'interface d'administration, compromission des régies publicitaires pour injecter du code au sein des publicités affichées, découverte d'une vulnérabilité de type XSS…)
2. Dépôt du malware sur le site (Ex : code JavaScript offusqué s'exécutant au chargement de la page, iframe contenant un ActiveX ou un applet Java malicieux hébergé sur un autre site, …)
3. Compromission de la machine cliente. La victime est incitée à se rendre ou redirigée de manière automatique sur le site Web hébergeant le malware. Son navigateur exécute le code malicieux et un malware est installé à son insu sur son poste de travail ou son Smartphone, très souvent de manière transparente. L'attaquant dispose alors d'un accès partiel ou complet sur l'appareil infecté.
Simple attaque de type « Drive-by Download » ?
La subtilité de cette attaque réside dans le choix des sites Web initialement compromis (cf étape 1). En effet, en fonction de la cible, le choix est principalement réalisé en fonction de la localité de l'entité ciblée ou en lien avec son métier.

Plusieurs cas concrets récents peuvent être cités en exemple :
• Professionnel : (politique/religieux/syndical…) Dans le cas d'Apple, de Microsoft ou de Facebook en février dernier, le site Web compromis était un site Web consacré au développement sur iPhone (iphoneDevSDK), site susceptible d'être visité par les développeurs des trois sociétés. La population cible peut également être plus restreinte comme l'illustre la compromission du site « http://www.rferl.org (Radio Free Europe Radio Liberty) ».
• Géographique : En Septembre 2012 lors de l'attaque VOHO[1], les cybercriminels avaient compromis un site gouvernemental local au Maryland, celui d'une banque régionale dans le Massachusetts afin de compromettre les machines de populations spécifiques résidant ou travaillant dans les localités ciblées.
• Et pourquoi pas Personnel : Il est tout à fait possible de voir le site du club de sport ou de musique où les enfants de la victime sont inscrits, être compromis…

Pourquoi utiliser cette méthode plutôt qu'une autre ?
En comparaison de l'envoi de phishing par exemple, cette méthode présente de nombreux avantages pour les attaquants :watering hole – scalable

Scalable :
Elle permet de couvrir un grand nombre de victimes « facilement ». Le «Drive-By Download» est largement utilisé dans le domaine de la #cybercriminalité permettant de compromettre un très grand nombre de machine rapidement ;
L'exploitation de vulnérabilités Java ou Adobe Flash récentes, peuvent permette de contourner les mécanismes de cloisonnement au sein des navigateurs Web et ainsi de couvrir de nombreux systèmes d'exploitation et navigateurs Web vulnérables différents
Efficace :
Couplée avec l'exploitation d'une vulnérabilité de type « 0-day », le taux d'infection peut être très élevé. Le rapport sur la campagne « VOHO »[2] publié par RSA et portant sur des attaques par « Watering Hole » recensait 32 160 machines infectées appartenant à 731 organisations pour un taux d'infection de 12%.
Discret :
Aucune action de l'utilisateur n'est nécessaire si ce n'est d'aller visiter ses sites Web habituels. L'absence de signaux rend également l'identification de la source de l'infection difficile. Enfin, la possibilité de filtrer les postes infectés (classe IP, langue du navigateur, localité …) permet de restreindre les dommages collatéraux et donc de limiter la visibilité de l'attaque.

Cette méthode présente cependant un certain nombre d'inconvénients :
• Potentiellement, une phase de reconnaissance, consistant à identifier sur quels sites se rendent les futures victimes
• Une phase de compromission de sites légitimes est nécessaire : les attaquants peuvent cependant identifier les sites vulnérables via des scans automatisés.
• Les attaquants doivent réaliser une analyse post-infection afin de déterminer, pour chaque poste compromis, quel type de profil a été infecté et si le profil correspond à la cible (société, fonction, …)



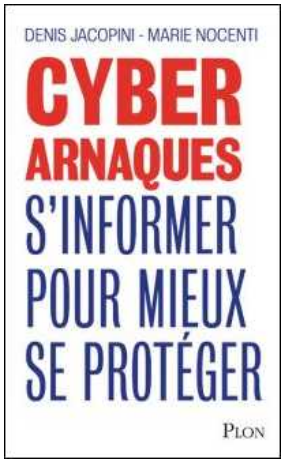
A noter que le filtrage effectué afin de réduire le périmètre des postes compromis émergent également au sein des attaques par phishing.

Quels sont les mécanismes de défense ?
Face à ce type de menace, il n'existe pas de solution « miracle ». Il convient donc d'appliquer des bonnes pratiques afin de limiter les risques d'infection et d'être réactif en cas de compromission :
1. [Mise à jour du parc] – On constate que les vulnérabilités exploitées sont le plus souvent liées aux technologies Java ou à Adobe Flash. A minima, il convient de maintenir à jour le parc applicatif. Cependant, cette mesure peut ne pas être suffisante (cas des 0-day). Nous recommandons donc de les désinstaller lorsqu'ils ne sont pas nécessaires.
2. [Filtrage Web] – Mettre à jour régulièrement en ajoutant automatiquement et au besoin manuellement les sites connus comme hébergeant des malwares au sien des listes noire des équipements de filtrage Web (nécessite de disposer d'un service de veille). De manière plus radicale, il est envisageable d'imposer la navigation Web pour des populations sensibles depuis des postes séparés du reste du réseau de l'entreprise.
3. [Durcissement des postes] – Des mécanismes de contournement peuvent également être mis en place. Pour Java par exemple, il est possible de configurer le niveau de sécurité sur « high » de manière à n'exécuter les applets non signés qu'après validation manuelle de l'utilisateur. Des mesures similaires peuvent être appliquées sur le plug-in Flash. Il est aussi possible de pousser des plugins comme « NoScript » afin d'interdire l'exécution de code JavaScript, Flash, Java …

Conclusion
La compromission par « Watering Hole » partage les mêmes objectifs que par « **spear-phishing** » et la même méthode d'infection que les attaques par « **Drive-by download** ».
Cette combinaison est ainsi surtout utilisée pour des attaques cherchant à s'introduire au sein d'une organisation, quel que soient les postes compromis.
Avec le temps et grâce aux campagnes de sensibilisations, les utilisateurs et en particulier les populations VIP sont de plus en plus précautionneuses quant à l'ouverture des pièces jointes aux courriels. Les attaques par « Spear-phishing » sont ainsi complétées par des attaques de type « Watering-Hole » qui ne nécessitent aucune action de la part de la victime si ce n'est de visiter ses sites Web habituels…

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : http://www.lexsi-leblog.fr/cert/watering-hole-et-cybercriminalite.html

---

Pourquoi ne pas partager

l’avertissement mettant en garde contre le pirate Jayden K. Smith ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Pourquoi ne pas partager l’avertissement mettant en garde contre le pirate Jayden K. Smith ?

Depuis le début du mois de juillet, un hoax (canular) circule sur Facebook. Il a été traduit de l'anglais et te met en garde contre un hacker nommé Jayden K. Smith. Pas de panique, c'est une mise en garde totalement fausse. Alors ignore le message, n'accepte rien et surtout, ne le repartage pas! C'est un peu soûlant.

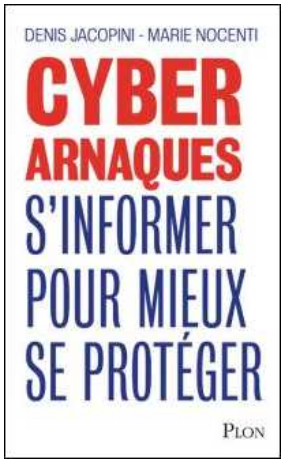
« S'il te plaît dis à tous tes contacts de ta liste messenger de ne pas accepter la demande d'amitié de Jayden K. Smith. C'est un hacker et a un système connecté à votre compte facebook. Si un de tes contacts l'accepte, tu seras aussi piraté, aussi assures toi que tous tes contacts le sachent. Merci. Retransmis tel que reçu. Gardes ton doigt appuyé sur le message. En bas, au milieu il sera dit transmettre. Appuyer dessus et cliquer sur les noms qui sont sur ta liste et cela leur sera envoyé. »
Voilà le message que vous avez peut-être reçu ce matin via Messenger. Il s'agit d'une nouvelle chaîne totalement infondée, comme l'ont fait remarquer certains médias outre-Atlantique. Le message est juste une traduction d'un texte en anglais qui est devenu viral un peu partout dans le monde la semaine dernière…[lire la suite]

L'avis de notre Expert Denis JACOPINI

Même s'il nous paraît difficile de pirater un compte Facebook par une simple lecture ou une demande d'ami, nous recommandons de ne pas partager ce message et de simplement le supprimer ou l'ignorer.
Ces canulars peuvent aussi bien prendre la forme d'un faux virus, d'une chaine de solidarité (comme ici), d'un gain hypothétique, d'une pétition ou d'une fausse information destinée à influencer l'opinion publique.
Vous pouvez aisément comprendre que les intérêts ne sont pas tous dans un but de vous arnaquer ou vous soutirer de l'argent. Certains auteurs de ces chaines recherchent la fierté d'avoir leur message qui fait le tour de la planète, d'autres de saturer les réseaux avec des messages inutiles mais les plus dangereux sont ceux qui vous demandent de cliquer ou de partage.
Même si je suis certains que vous êtes vigilants lorsqu'on vous demande de télécharger ou d'exécuter un programme, vous l'êtes certainement bien moins lorsque vous partagez un message à vos amis. L'expéditeur peut du coup disposer et utiliser de manière malveillante des informations sur eux.

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *Ne partage pas cet avertissement qui te met en garde contre le pirate Jayden K. Smith, c'est un hoax*

Comment réagir en cas de

chantage à la webcam ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

L'arnaque à la webcam touche chaque année des milliers de victimes. Cette série de conseils vous aidera à adopter les bonnes pratiques si vous devez faire face à ce type de chantage.

A quoi ressemble un cas typique de chantage à la webcam ?

La victime se rend sur un site de rencontre puis entame la conversation avec une jeune femme ou un jeune homme au physique attrayant. Après lui avoir posé quelques questions sur sa vie privée, cette personne l'invite à approfondir les échanges via une conversation vidéo plus intime. Quelque temps plus tard, un courriel ou un message Facebook apprendra à la victime que cette rencontre a été enregistrée. Le cyber-escroc menace de diffuser la vidéo de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos si la victime ne lui remet pas la somme de 200 euros sous 24h/48h.

Quel réflexe adopter ?

1.

Ne répondez surtout pas à un cyber-escroc

Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, ne versez surtout pas d'argent quelle que soit la somme demandée.

2.

Verrouillez immédiatement vos comptes sociaux

Paramétrez vos comptes sociaux professionnels et vos comptes Facebook de manière à ce que le malfaiteur n'associe pas votre nom à une liste d'amis / de contacts. Ne rendez accessible votre profil Facebook qu'auprès de vos amis de confiance. Enfin, ne publiez rien de personnel sur votre mur. Des personnes mal intentionnées peuvent détourner ces informations à d'autres fins. Notre page Facebook délivre quelques conseils pour bien paramétrer vos comptes.

3.

Alertez les autorités via la plateforme du Ministère de l'Intérieur

- **Effectuez des captures d'écran** justifiant votre situation (messages reçus, contenus à effacer …). Voir la fiche pratique
- **Signalez directement l'escroquerie** sur la plateforme www.internet-signalement.gouv.fr
- **Renseignez-vous via le service Info Escroqueries** au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile ; Du lundi au vendredi de 9h à 18h)

4.

Parlez-en à une personne de confiance

La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. **Il est conseillé d'en parler avec une personne de confiance.** **Vous êtes mineur ? Des télé-conseillers sont gratuitement à votre écoute** au 0800 200 000 de 9h à 19h en semaine. Voir le site Net écoute

5.

Informez vos amis de l'escroquerie

Veillez à informer discrètement les personnes susceptibles d'être sollicitées par le cyber-escroc en mentionnant sobrement que vous êtes victime d'une escroquerie en ligne et qu'il ne faut ni ouvrir, ni partager, ni répondre à une éventuelle sollicitation provenant d'un inconnu.

6.

Effectuez régulièrement des recherches à votre nom

Vous pouvez par exemple programmer une alerte à votre nom qui vous enverra un message sur votre messagerie électronique dès qu'un contenu associé à votre nom est mis en ligne. Certains services existent iciou là.

Si la vidéo a été diffusée …

7.

Demandez systématiquement au site de dépublier le contenu gênant

Exemple : si la vidéo a été mise en ligne sur Youtube : demandez à Youtube de supprimer cette vidéo. Si le site ne répond pas à votre demande sous deux mois, adressez vous à la CNIL en suivant la procédure de notre formulaire de plainte en ligne.

8.

En parallèle, demandez au moteur de recherche de déréférencer le contenu en cause

Depuis un récent arrêt de la cour de justice européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leurs nom et prénom. Le droit au déréférencement

D'autres solutions existent

9.

Créer du contenu bien référencé à votre nom

Vous pouvez créer rapidement des contenus valorisants associés à votre nom et donc bien référencés. Il peut s'agir d'un blog consacré à une passion ou d'une page de curation de contenus (outil qui permet de sélectionner, éditer et partager des pages/liens web sur un sujet précis). Attention à ne pas communiquer d'éléments personnels.

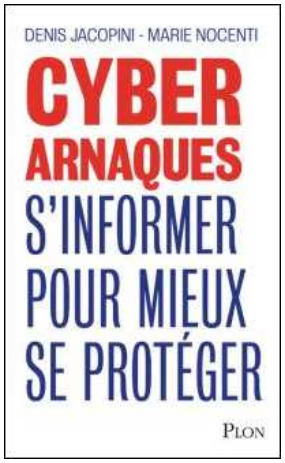
10.

Faire appel à une agence spécialisée

Certains cas peuvent nécessiter l'intervention d'une agence spécialisée dans l'effacement de contenus gênants. Soyez néanmoins vigilant sur les compétences vantées dans l'annonce. N'hésitez pas à vous rendre sur des forums pour vous renseigner sur la réputation de ces agences.

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Original de l'article remis en page : Réagir en cas de chantage à la webcam | CNIL

TCP Stealth : Un nouveau

logiciel pour se protéger des cybercriminels | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

#TCP Stealth : Un nouveau logiciel pour se protéger des cybercriminels

Les balayeurs de ports sont des programmes qui parcourent le web en recherchant les ports ouverts, donc vulnérables, sur un serveur de réseau. Dans le cadre des récentes révélations de cyber-espionnage massif, un tel logiciel aurait été utilisé. Une équipe de l'Université technique de Munich (TUM, Bavière) a développé un logiciel de défense contre ce type d'attaques.

Baptisé « TCP Stealth », ce programme peut empêcher la détection des systèmes sur le net lors d'attaques par balayage de ports, ainsi que la prise de contrôle massive de ces systèmes. Ce logiciel, gratuit, nécessite tout de même certaines connaissances en informatique et systèmes pour être utilisé. Un usage plus large nécessitera encore une phase de développement. Cet outil peut venir en complément des pare-feux, antivirus et réseaux privés virtuels qui ne protègent que partiellement face à de telles attaques.
La connexion d'un utilisateur à un serveur se fait à travers un protocole de transport fiable (TCP). Afin d'accéder au service souhaité par l'utilisateur, sa machine envoie une demande au serveur. La réponse du serveur contient parfois des données susceptibles d'être utilisées pour mener des attaques. Le logiciel développé se fonde sur le principe suivant : un nombre est partagé uniquement entre la machine d'un utilisateur et le serveur. Sur la base de ce numéro, un code secret est généré puis transmis de manière invisible au serveur lors de la mise en connexion. Si le code reçu par le serveur n'est pas correct, le système ne répond pas et ne transmet donc pas d'informations au possible pirate.
De tels moyens de défense sont déjà connus, mais le logiciel développé est présenté par les chercheurs comme un outil de protection plus fiable, car il gère également une variante de cette attaque. Il est ici question d'attaques générées lors de l'échange de données entre l'utilisateur et le serveur, mais cette fois-ci dans le cas où la connexion est déjà établie. Les données envoyées par l'utilisateur au serveur peuvent être, à ce stade, encore interceptées et modifiées. Afin d'empêcher cette attaque et suivant le même principe que précédemment, un code secret intégré au flux de données est également envoyé au serveur. Le serveur reconnaîtra alors si le contenu est conforme à l'original.

Le logiciel est disponible au téléchargement à l'adresse suivante : https://gnunet.org/knock.
Les personnes intéressées peuvent également participer à son développement.
Christian Grothoff, chercheur à la TUM, faculté d'architecture des réseaux et services
email : knock@gnunet.org

[block id="24761" title="Pied de page HAUT"]

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Sources : « TUM-Forscher entwickeln Abwehrsystem gegen Cyberangriffe », dépêche idw, communiqué de presse de la TUM – 15/08/2014- http://idw-online.de/pages/en/news599759
Rédacteurs :
Aurélien Filiali, aurelien.filiali@diplomatie.gouv.fr – http://www.science-allemagne.fr
Références
: http://www.bulletins-electroniques.com/actualites/76579.htm

---

Wifi gratuit: Attention à vos données personnelles !

Wifi gratuit: Attention à vos données personnelles !

Les utilisateurs de réseaux de wifi du monde entier ne sont pas à l'abri du danger. D'après une enquête réalisée par Norton by Symantec, la grande majorité des internautes de l'Hexagone adoptent des comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les Français parmi les mauvais élèves

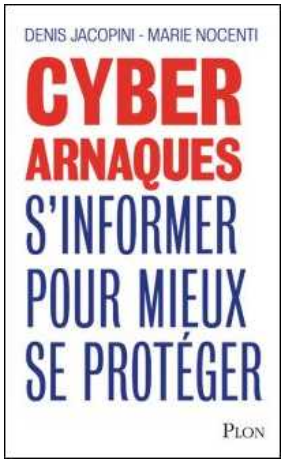
Un sondage a été réalisé par Norton by Symantec sur un échantillon de 1 000 personnes environ dans chacun des 15 pays supervisés, dont la France et les Etats-Unis. L'enquête a tenté de mettre en avant les dangers d'une **connexion à des réseaux de wifi gratuit**. Il a été révélé que les internautes prennent de très gros risques pour leur sécurité et leur confidentialité par le biais du troc connexion-information. Ce dernier se manifeste sous plusieurs formes : adresse email à fournir, coordonnées, géolocalisation à accepter ou encore publicité à voir. Selon l'étude, la quasi-totalité des internautes de l'Hexagone (87%) ne cesse de multiplier les comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les comportements dangereux des mobinautes

L'étude a mis en avant le comportement des internautes du monde entier. Ainsi, 43% des sondés sont impatients de se connecter à peine installés au restaurant, au café, à l'hôtel, dans un magasin ou même chez un ami. Plus encore, l'envie est si pressante que 25% avouent avoir déjà tenté de se connecter sans la permission du propriétaire du réseau. Les 7% ont déjà tenté de pirater ou deviner le mot de passe (7%), rapporte *LCI*. Pour avoir une bonne **connexion**, 55% des personnes enquêtées accepteraient de fournir n'importe quelle information…[lire la suite]

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : http://www.linfo.re/magazine/high-tech/722259-wifi-gratuit-halte-a-vos-donnees-personnelles »>Wifi gratuit: attention à vos données personnelles! – LINFO.re – Magazine, High-Tech

Pourquoi le vol de données personnelles devient-il de plus en plus commun ? | Denis JACOPINI

Des pirates informatiques Russes viennent de réaliser « le casse du siècle » en récoltant 1,2 milliard de comptes utilisateurs (identifiants et mots de passe associés) et plus de 500 millions d'adresses e-mail, provenant de 4200 000 site Internet d'entreprises de toute taille. NetIQ, fournisseur de solutions de #sécurité informatique, ne s'étonne pas de la multiplication de ce type de hack. Geoff Webb, Senior Director, Solution Strategy chez NetIQ, explique pourquoi le vol de données personnelles devient de plus en plus commun :

« Dans ce type de cas, la faute ne repose pas uniquement sur les hackers. Il faut aussi prendre en compte le comportement des entreprises et celui des utilisateurs finaux face à la sécurisation des accès.

Commençons par les hackers. De nos jours, il n'est pas nécessaire d'avoir un groupe sophistiqué et étendu de pirates informatiques expérimentés pour perpétrer les plus gros cyber-crimes. Aujourd'hui une simple recherche Internet permet à quiconque de rapidement trouver toutes les informations nécessaires pour pénétrer les systèmes informatiques vulnérables. Les pirates informatiques ont même cartographié toutes les vulnérabilités de la toile, et le tout est disponible en ligne. De plus, avec l'avènement du cloud, les hackers ont une porte d'entrée supplémentaire pour accéder aux données des entreprises. On entend régulièrement parler dans nos médias de la sécurité, ou plutôt du manque de sécurité lié au cloud.

Continuons avec les entreprises. Le cloud n'est pas le cœur du problème. Le problème de fond est que les entreprises ne mettent pas assez l'accent sur la sécurité des accès, que ça soit au niveau des accès cloud, aux applications d'entreprise, ou aux applications Web. Tant que les entreprises n'auront pas assimilé le caractère critique de la protection des mots de passe, ce type de hack continuera de se multiplier.

Enfin, il faut s'intéresser au comportement des utilisateurs finaux, qui ne facilitent pas la tâche des entreprises en matière de sécurité des mots de passe. En effet, de nombreuses études l'ont révélé récemment, par souci de facilité, les mots de passe utilisés sont souvent très (trop) simples. Les utilisateurs utilisent les mêmes mots de passe pour accéder à leurs comptes bancaires, messagerie électronique qu'elle soit personnelle ou professionnelle, et compte Facebook, par exemple. Ce comportement est une aubaine pour les cybercriminels. En laissant aux utilisateurs finaux le choix de leurs mots de passe, nous confions tout simplement une étape cruciale dans le processus de sécurisation des données à ceux qui sont les moins qualifiés et surtout les moins préoccupés par la sécurité informatique. Vous comme moi, nous n'avons pas envie d'avoir à nous souvenir de mots de passe compliqués et différents pour chaque compte que nous devons utiliser au quotidien. C'est donc bien notre propre comportement en tant qu'utilisateur qui constitue le plus gros risque.

On ne peut empêcher un hacker d'agir, mais on peut le stopper aux portes de l'entreprise en ayant des solutions de sécurité globale prenant en compte toutes les potentielles portes d'entrée. C'est pourquoi il est impératif que des solutions de gestion des identités et des accès soient intégrées dans les projets de sécurité des entreprises, au même titre que peut l'être la sécurisation des réseaux, ou des terminaux. »

[block id="24761" title="Pied de page HAUT"]

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Références : http://www.globalsecuritymag.fr/1-2-milliard-de-mots-de-passe,20140806,46775.html

---

Sécurisez votre MAC avec Security Growler | Denis JACOPINI

Sécurisez votre MAC avec Security Growler

Security Growler est un soft pour OSX qui se loge dans la barre de menu et qui vous alertera via le Centre de Notifications en cas d'événements suspects liés à la sécurité de votre Mac.

Security Growler vous alerte lorsqu'il y a des tentatives de connexions SSH (ou des connexions réussies)…

Lorsque des connexions TCP entrantes ou sortantes ont lieu… (FTP, SMB, AFP, MySQL, PostgreSQL, partage iTunes, VNC)

Lorsqu'une commande utilisant « sudo » est lancée…

Lorsqu'un scan de ports déboule sans crier gare…

…etc., etc.

Security Grawler permet de ne plus être en aveugle sur sa propre machine et d'être averti du moindre truc louche. Indispensable donc ! De plus, Security Growler est très économique : il consommera moins de 0,01% de votre CPU et jamais plus de 15 Mb de RAM. Et si vous utilisez Prowl, vous pourrez faire suivre les alertes sur votre iPhone / iPad.
À télécharger ici.

[block id="24761" title="Pied de page HAUT"]

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

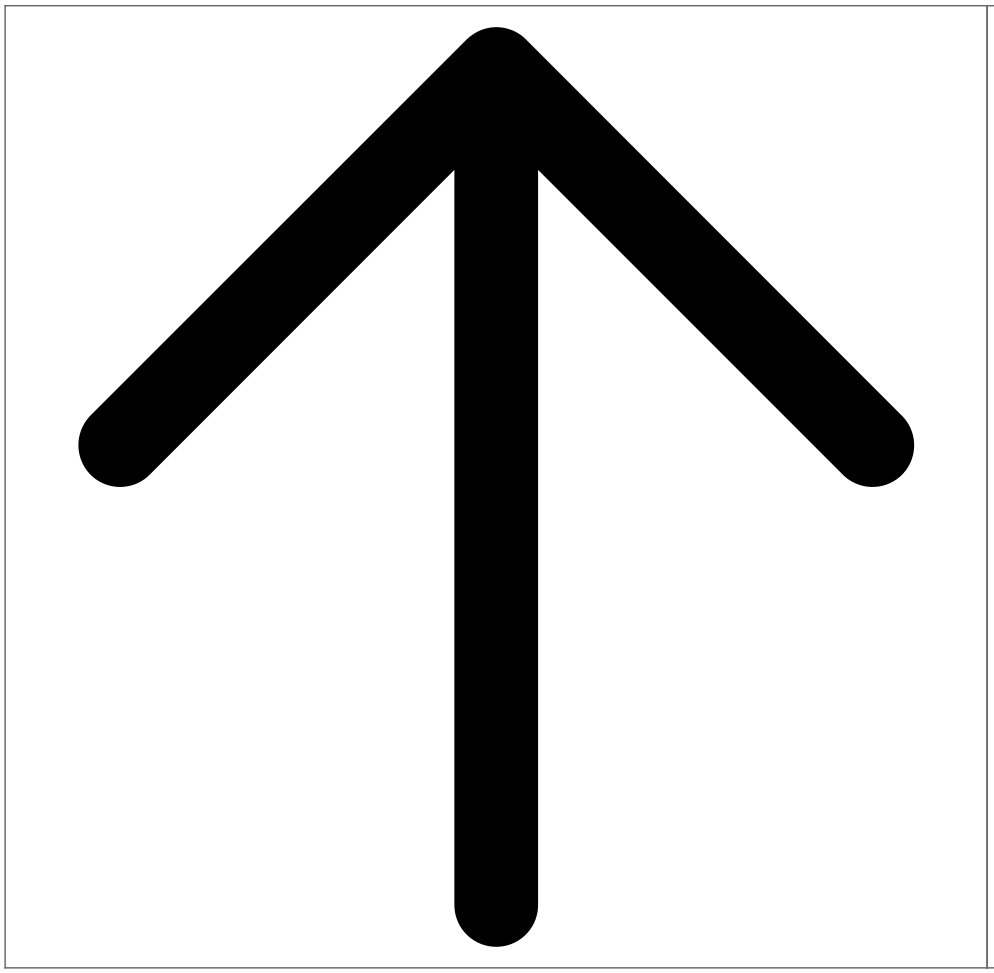
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques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

[block id="24760" title="Pied de page BAS"]

Source : *Security Growler – Soyez aware sur la sécurité de votre Mac – Korben*

---

3 nouvelles techniques de diffusion de phishing et virus identifiées | Denis JACOPINI



3 nouvelles techniques de diffusion de phishing et virus identifiées

Alors qu'auparavant le spam était essentiellement source de désagréments et de baisse de productivité, il sert également aujourd'hui à véhiculer des virus et des attaques par phishing très dangereuses.

L'e-mail reste la porte d'entrée préférée des hackers sur les réseaux d'entreprise. Ainsi, près de 90% des e-mails envoyés sur les adresses de messagerie professionnelles sont des spam. Alors qu'auparavant ces spam étaient essentiellement source de désagréments et de baisse de productivité, ils servent également aujourd'hui à véhiculer des virus et des attaques par phishing très dangereuses, qui gagnent continuellement en intensité et en intelligence.
Plusieurs finalités à ces attaques : voler des données (identifiants personnels, coordonnées bancaires, propriété intellectuelle, etc.), et de l'argent (via des trojan banking par exemple ou des cryptolocker et demandes de rançons) mais également infiltrer des réseaux pour mener des attaques ultérieures de plus grande envergure et développer des réseaux de botnets de plus en plus puissants pour diffuser encore plus de spam, virus et phishing.

3 nouvelles techniques identifiées

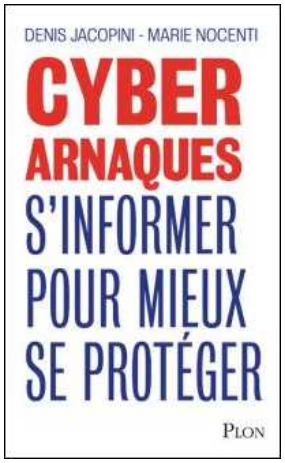
> Des vagues qui utilisent des adresses IP non reconnues
Les cybercriminels se servent de réseaux de botnets/spambots (réseaux de PC zombies) dont ils ont considérablement développé la puissance ces derniers mois. Grâce à ces réseaux, les cybercriminels sont en mesure d'envoyer régulièrement des vagues massives et intenses de spam – jusqu'à plusieurs millions de spam simultanément pour les plus gros réseaux. La force de ces campagnes de spam massives est qu'elles sont basées sur des réseaux de PC bénéficiant d'adresses IP non reconnues, que les outils de filtrages antispam classiques par signatures ou réputation ne sont pas en mesure d'identifier comme spam dans un premier temps.
L'utilisation d'adresses IP non blacklistées permet aux spam, et potentiellement aux virus et phishing de franchir les systèmes de filtrage – traditionnels basés sur les signatures ou réputation- qui ont besoin de temps pour identifier et blacklister ces nouvelles adresses. Pour les hackers, cela suppose toutefois de renouveler leurs réseaux de PC zombies non identifiés entre chaque attaque. On observe ainsi une période de 6 à 10 jours entre chaque très grosse vague de spam. Entre-temps les hackers se livrent surtout à de petites attaques pour infecter de nouveaux postes et ainsi faire croître leur réseau de PC zombies. Le seul moyen de bloquer efficacement ces vagues est d'utiliser le filtrage heuristique qui permet d'analyser le contenu des e-mails plutôt que de se baser uniquement sur son origine (réputation) ou sa propagation sur les réseaux et l'internet (signature).

> Des virus à tout faire (polymorphes)
Illustration de la nouvelle ère de l'industrialisation du hacking, les virus sont également de plus en plus intelligents. Alors qu'auparavant chaque virus était programmé pour une action précise, les virus actuels sont commandés à distance. Après avoir pénétré le réseau le plus discrètement possible, un virus actuel peut être commandé à distance et être utilisé au besoin par exemple comme actif d'un spambot de grande envergure voire même pour une attaque de cryptolockage.

> Activation des liens URL de phishing après le passage du filtre
En matière de phishing (phishing ciblé), les cybercriminels font également preuve de plus en plus d'intelligence pour faire évoluer leurs techniques. Ainsi, certains cybercriminels envoient des e-mails de phishing utilisant des liens URL activables à distance, une fois les outils de filtrage franchis. Cette technique permet aux e-mails de phishing de franchir le filtrage sans être détectés puisque les liens URL renvoient vers un contenu totalement légitime. Ce n'est qu'une fois les barrières franchies que les hackers vont les activer pour les faire renvoyer vers des sites de phishing frauduleux.
Cette technique de plus en plus utilisée est très efficace mais cependant encore peu répandue car elle n'est techniquement pas à la portée de tous les hackers.

Le hacking s'est fortement industrialisé ces dernières années. Les techniques utilisées pour diffuser du spam massivement et des virus sont de plus en plus intelligentes et dangereuses pour les entreprises. Pour se protéger mieux, l'éducation et la formation des utilisateurs sont des axes primordiaux d'où l'importance de rappeler quelques règles de base :
• N'ouvrir les pièces jointes suspectes (fichiers .zip, .xls ou .doc.) que si l'expéditeur est confirmé.
• Supprimer le message d'un expéditeur suspect inconnu sans y répondre.
• Refuser de confirmer l'accusé de réception dans le cas d'un expéditeur inconnu suspect. Cela risquerait de valider et diffuser l'adresse e-mail de l'utilisateur à son insu.
• Remonter les emails identifiés comme spam auprès de son service informatique. Ils seront ensuite transmis à l'entreprise chargée de la protection des messageries pour une prise en compte dans la technologie de filtrage.
• Et en cas de doute, contacter son service informatique.

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : http://www.journaldunet.com/solutions/expert/62660/diffusion-de-phishing-et-virus—3-nouvelles-techniques-identifiees.shtml

Les 6 conseils pour se protéger des Cryptovirus (Ransomwares)

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Les 6 conseils pour se protéger des Cryptovirus (Ransomwares)

Alors que l'ANSSI vient d'annoncer un MOOC pour aider les entreprises à bien se protéger suite aux dernières attaques informatiques comme WannaCry, on réalise que la sécurité d'une entreprise doit être avant tout l'affaire de tous ses employés, et pas simplement des équipes dédiées au sein du service informatique. Après tout, la capacité de résistance de toute organisation dépend de son maillon le plus faible.

Une partie des financements devrait avoir pour objectif d'aider les entreprises à développer un programme de sensibilisation aux pratiques de cybersécurité spécialement adapté aux problématiques des PME. En effet, contrairement à leurs homologues des grandes entreprises, les dirigeants des PME sont généralement davantage impliqués dans des décisions d'ordres variés ce qui influe directement sur leur capacité à consacrer le temps ou l'attention nécessaires à la sécurité des systèmes d'information.
Tout programme conçu pour sensibiliser les employés aux méthodes de protection des menaces devrait en premier lieu viser à développer les connaissances des meilleures pratiques à tous les échelons hiérarchiques. Thibaut Behaghel, Spécialiste Produits International au sein du gestionnaire de mots de passe LastPass, nous explique à quoi pourrait ressembler un tel programme pour les petites et moyennes entreprises, et qu'elles devraient en être les priorités.

1.Respecter les principes de bases
En matière de sécurité, il existe un certain nombre de principes de base à suivre pour toutes les organisations, à commencer par la mise en place de règles concernant la longueur, la complexité et la durée de validité des mots de passe…[lire la suite]

2.Gérer les accès des utilisateurs
Quel que soit le nombre d'employés de votre entreprise, il est essentiel que chacun d'entre eux n'ait accès qu'aux informations et aux données qu'il est autorisé à consulter…[lire la suite]

3.Définir une politique de sécurité
Toute organisation devrait créer une politique détaillant les mesures de sécurité prises à la fois au niveau de l'entreprise elle-même, et par l'ensemble de ses employés…[lire la suite]

4.Former les salariés
Une fois la politique de sécurité mise en place, il est nécessaire de former les employés afin qu'ils en connaissent les règles et qu'ils sachent comment les respecter…[lire la suite]
5.Sécuriser les réseaux sans fil
Les PME doivent utiliser des mots de passe administrateurs et d'accès aux réseaux forts, et choisir des protocoles de chiffrement éprouvés (WPA2 et AES)…[lire la suite]

6.Savoir reconnaître le phishing
En cas de doute, il ne faut prendre aucun risque. Les entreprises doivent montrer à leurs employés comment repérer et signaler des e-mails suspects…[lire la suite]

[lire la suite]

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

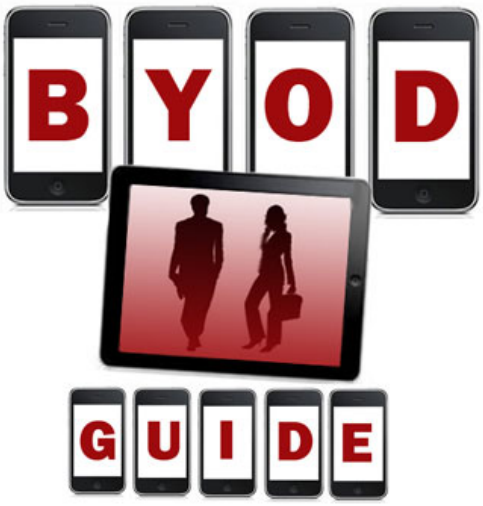
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Ransomware : les 6 conseils pour se protéger*

BYOD Matériel personnel au travail et matériel professionnel à la maison : 12 points pour une bonne sécurité | Denis JACOPINI



BYOD Matériel personnel au travail et matériel professionnel à la maison : 12 points pour une bonne sécurité

Si l'on parle souvent des avantages et des désagréments du BYOD, la base reste après tout d'adopter la politique qui correspond aux besoins de l'entreprise. Cela permet ainsi de savoir si l'on applique un BYOD total ou un CYOD (Choose Your Own Device) voire un COPE (Corporate Owned, Personally Enabled).

Et pour arriver aux bonnes conclusions, il faut se poser les bonnes questions.

1. Le BYOD : mais pour qui ?

C'est en premier lieu une question fondamentale. Faut-il permettre le BYOD à l'intégralité des employés, ou juste certains métiers, uniquement les cadres voire seulement les principaux dirigeants ? Répondre à cette question est primordial avant de mettre en place une bonne politique de BYOD, car de cette réponse découleront bien des conséquences.

Il faut toutefois bien avoir en tête que si tout le monde n'est pas autorisé à pratiquer le BYOD, cela n'empêchera pas certains d'amener leurs appareils sans prévenir qui que ce soit, ce qui pourrait créer quelques complications par la suite. Intégrer une telle donnée est indispensable.

2. Quels appareils ?
Une fois le personnel concerné enfin déterminé, il convient de se poser une question équivalente sur les appareils. Faut-il tous les accepter ? Se limiter à une marque ou un système d'exploitation particulier ? Aujourd'hui, même si les Androphones et les iPhone captent la majeure partie du marché, cibler les appareils acceptés est aussi un élément majeur qui simplifiera la vie du DSI et du patron.

Par exemple, n'autoriser que des appareils sous iOS dont la dernière version a été installée impliquera une gestion moins complexe que de permettre tous les Androphones, vieux comme récents, qui ne fonctionneront même pas sous la même version d'Android et qui comptent des dizaines de marques différentes. Et la logique est similaire pour les tablettes tactiles.

3. Quelles applications ?
On connaît désormais qui pourra exploiter le BYOD et quels appareils seront concernés. Très bien. Reste désormais à régler la question tout aussi fondamentale des logiciels. Quelles applications seront acceptées ? Certaines bien spécifiques devront-elles être installées ? Seront-elles extérieures à l'entreprise ou programmées en interne spécifiquement pour les employés ? Est-il utile ou non de passer par une interface multi-OS et multi-écran à la Exo U ?

Là encore, afin de mettre en place une bonne politique de BYOD, toujours en fonction des besoins de l'entreprise, cibler les applications autorisées est primordial. Mais là encore, le risque que l'employé utilise d'autres applications est réel et doit être pris en compte. Plus on impose de limite et plus les

mauvaises surprises sont multipliées. L'avantage de laisser une liberté totale est donc que les parades à cette liberté seront calculées.

4. Impliquer toutes les branches de l'entreprise

Une fois les trois premiers points enfin réglés, si l'on souhaite que la politique de BYOD se passe pour le mieux, il faut impliquer toutes les branches de l'entreprise. Que ce soit les ressources humaines, les juristes, évidemment le DSI, etc. Pourquoi ? Tout simplement, et c'est toujours la même chose, pour une question de besoin, mais aussi ici de précision.

Le responsable des RH apportera forcément un regard différent du DSI, qui lui-même ne pensera pas aux mêmes problématiques que le juriste. L'un insistera pour que les règlements quant au BYOD traient bien des différences entre les données privées et professionnelles. Un autre pensera à l'aspect technique, tandis que son voisin préviendra des différents risques de plaintes.

5. Mettre en place une infrastructure réseau suffisante

Vous savez qui utilisera quoi et comment. Vous pouvez donc prévoir (à peu près) quel sera le trafic qui sera utilisé dans votre entreprise tous les jours. Et qui dit BYOD dit généralement une utilisation bien plus forte des réseaux mobiles, que ce soit en Wi-Fi ou en 3G/4G. Une augmentation qu'il faut donc prévoir si vous voulez éviter que vos employés commencent sérieusement à s'agacer des débits.

Sachant que certains employés peuvent avoir deux, trois voire

quatre appareils en même temps connectés, il est capital de mettre en place l'infrastructure suffisante pour assurer un réseau de qualité. Augmenter ses débits fixes et obtenir des routeurs Wi-Fi puissants sera probablement indispensable. Il faudra de plus s'assurer que les forfaits mobiles des employés soient suffisamment volumineux.

6. Simplifiez, soyez clair et prévoyez

Lorsque vous allez commencer à mettre au point vos règles de politique de BYOD, il faut à la fois penser à la simplifier tout en prévoyant le futur. Faire simple, être direct et clair permet d'éviter les failles et les abus de ces dernières. Utiliser les mots justes et précis, c'est s'assurer que les règles seront bien appliquées.

Enfin, il faut absolument prévoir. Le marché évolue à grande vitesse et vos règles du jour ne seront peut-être pas viables dans trois ans ou peut-être même moins. Il faut donc là encore ne pas être trop spécifiques aux produits du moment et généraliser afin d'englober les appareils et les applications du futur.

7. Lasécurité

C'est l'évidence même, on ne cesse d'en parler, c'est généralement la priorité numéro un des entreprises (BYOD ou non), la sécurité est un point majeur à régler. Elle dépendra évidemment des sujets 1, 2 et 3 évoqués dans notre précédent article, à savoir ceux rapportés aux utilisateurs de BYOD, aux appareils autorités et aux applications permises.

La sécurité pour le BYOD, ce sont des règles de bonnes

conduites et des règles techniques. Que ce soit par rapport au cloud, à à l'accès aux données sensibles selon les réseaux utilisés, aux mises à jour des logiciels, aux mots de passe, aux protections, à la perte de l'appareil, etc. Tout doit être réglé au millimètre et prévoir toutes les catastrophes possibles est indispensable.

Et surtout, la sécurité implique un rapport de confiance entre l'employé et sa direction. La pire des situations seraient que l'employé se soit rendu compte qu'il a subi un vol de données et qu'il ne dise rien. La transparence et la rapidité sont ainsi indispensables pour assurer un maximum de sécurité.

8. La question des données personnelles

Outre le plan sécuritaire, celui du droit et du respect des données privées doit aussi être réglé. S'arranger pour séparer les données privées/personnelles des données professionnelles dans les appareils est ainsi plus que conseillé. L'entreprise doit le faire pour ses employés mais aussi pour elle-même, ne serait-ce que pour éviter quelques désagréments et plaintes dans le futur.

9. Avoir la mainmise sur l'appareil

Certes, dans le cadre du BYOD, le PC portable, le smartphone ou la tablette appartient à l'employé. Néanmoins, comme pour les données personnelles, dès lors que le professionnel s'intègre dans l'appareil, l'entreprise a donc un droit de regard.

Il faut donc bien faire comprendre à l'employé que son appareil personnel peut être surveillé et que l'entreprise

peut avoir accès à certaines données, y compris personnelles. Clarifier ce point dès le départ évite ainsi les mauvaises surprises.

10. Quelles solutions MDM ?

MDM, signifie Mobile Device Management, que l'on peut traduire en gestion des terminaux mobiles. Les solutions MDM sont indispensables pour toutes les entreprises (surtout les grandes) qui disposent d'une flotte importante d'appareils, qu'ils appartiennent ou non à l'employé par ailleurs.

Dans le cadre strict du BYOD, les solutions MDM ont souvent l'avantage d'être multiplateforme et sont l'une des armes pour sécuriser son réseau et ses données. Elles permettent en effet d'identifier les terminaux mobiles connectés, de les activer et les désactiver comme on le souhaite, d'installer des applications à distance, de les mettre à jour, de bloquer les appareils à distance ou des applications spécifiques, de géolocaliser les appareils, d'imposer des mots de passe ou même le chiffrement des données, etc. En somme, un BYOD sans MDM paraît presque impensable.

11. En cas de casse ou de vol

Même si l'appareil n'appartient pas à l'entreprise, il faut néanmoins prévoir le cas où ce dernier casserait, tomberait en panne ou tout simplement serait volé. Les données présentes sur l'appareil ou disponibles à distance peuvent être sensibles et prévoir une telle éventualité est obligatoire quand on sait que les cas de casses et de vols sont nombreux.

Bien entendu, un système de blocage à distance est

indispensable en cas de vol, tout comme le fait de chiffrer ses données. Pour la casse, moins il y a de données stockées directement dans l'appareil (sans copie en ligne), moins la situation sera catastrophique.

12. En cas de départ

Enfin, on n'y pense pas toujours, mais si l'employé vient avec son appareil, il repart évidemment avec en cas de départ, de fin de contrat ou de licenciement. C'est un point crucial à ne pas manquer dès le début de la politique de BYOD.

Il faut ainsi prévoir à l'avance le futur départ de l'employé et par conséquent le rapatriement de toutes les données qu'il détient, en sus de leur suppression sur son ou ses appareils. Dans le même esprit, il faudra donc l'empêcher d'avoir accès via ses appareils aux réseaux et serveurs de l'entreprise. Cela peut là encore éviter certains désagréments.

[block id="24761" title="Pied de page HAUT"]

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

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

[block id="24760" title="Pied de page BAS"]

Source : http://www.zdnet.fr/actualites/12-points-a-traiter-pour-une-bonne-politique-de-byod-1-2-39804195.htm