Carole Maréchal, Telehouse France : La protection des données, un enjeu au cœur des problématiques des datacenters et prestataires Cloud

Selon IDC, 8,6 millions de datacenters auront fleuri dans le monde à l'aube 2017. Usines des temps modernes, les datacenters abritent les données de nombreuses entreprises. Comment les protéger ? La sécurité des données est aujourd'hui un des enjeux majeurs des hébergeurs.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation

Professionnelle n°93 84 03041 84).
Plus d’informations sur notre page formations.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Nouvelles menaces informatiques et évolution des protection

Nouvelles menaces informatiques et évolution des protection

Destinés au grand public, ESET Internet Security et ESET Smart Security Premium apportent 5 nouvelles fonctions.

« Le tout nouveau produit ESET Internet Security vient s'ajouter à notre portefeuille de produits primés et offre aux utilisateurs les meilleures fonctionnalités en matière de détection, de vitesse et de convivialité. Ces nouveaux produits ajoutent à nos protections multi-couches existantes un ensemble de fonctionnalités centrées sur la protection de la vie privée » explique Eduard Kesely, Product Manager chez ESET.

ESET Internet Security, une protection optimale

ESET Internet Security s'adresse aux utilisateurs nécessitant une protection complète. Aux couches de sécurité déjà disponibles dans l'antivirus, s'ajoutent 3 nouvelles fonctionnalités :

• La protection contre les attaques par script.
• La protection Webcam qui signale les processus et les applications qui tentent d'accéder à la webcam de l'utilisateur et permet de les bloquer.
• La protection du réseau domestique qui permet à l'utilisateur de connaître l'identité des appareils connectés.

ESET Smart Security Premium, un produit haut de gamme

ESET propose un nouveau produit haut de gamme, ESET Smart Security Premium, destiné aux utilisateurs avancés et TPE. En plus des trois fonctionnalités ci-dessus, ESS Premium propose :

• Un gestionnaire de mots de passe.
• Le chiffrement des données pour les protéger en cas de vol ou de perte.

ESET cumule 3 récompenses prestigieuses : Pour la 98ème fois, ESET reçoit le prix VB100. De plus, il est le seul éditeur à avoir détecté 100% des menaces lors du test SE Labs (produits grand public) catégorie protection anti-malware. Enfin, le test réalisé par AV-Comparatives sur la protection anti-spam révèle qu'ESET est le N°1 haut la main.

La gamme ESET destinée aux particuliers, en plus de améliorations citées, couvre toujours macOS®, Android™ (antivirus et contrôle parental) afin de protéger l'intégralité de la famille.

Vous pouvez retrouver l'ensemble des fonctionnalités de nos produits sur https://www.eset.com/fr/

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

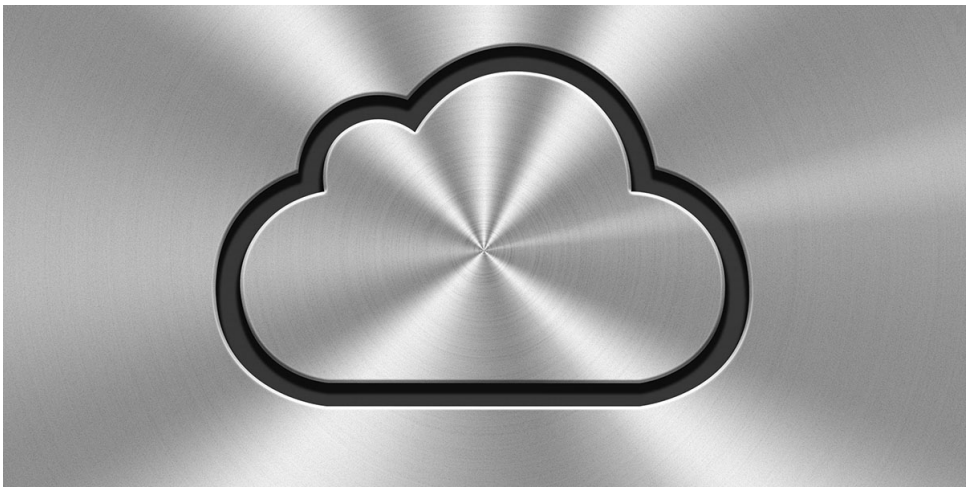
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

18 mois de prison pour le pirate qui a publié des photos intimes de célébrités



Aux États-Unis, la justice a condamné à un an et demi de prison l'auteur d'une vaste campagne de phishing qui a débouché sur la diffusion de photos intimes de plusieurs dizaines de célébrités en 2014. Un an et demi de prison ferme.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Multiples vulnérabilités dans les produits Apple

Multiples vulnérabilités dans les produits Apple

…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Faille de sécurité pour le PARTI SOCIALISTE – Avertissement Public de la CNIL

Faille de sécurité pour le PARTI SOCIALISTE – Avertissement Public de la CNIL

Le 26 mai 2016, la CNIL a été informée de l'existence d'une faille de sécurité entraînant une fuite de données sur le site du Parti Socialiste. Lors d'un contrôle en ligne réalisé dès le lendemain, la CNIL a constaté que les mesures garantissant la sécurité et la confidentialité des données des primo-adhérents du PS étaient insuffisantes.

Les contrôleurs de la CNIL ont en effet pu accéder librement, par la saisie d'une URL, à la plateforme de suivi des primo-adhésions au Parti Socialiste effectuées en ligne. Ils ont notamment pu prendre connaissance des éléments suivants : nom, prénom, adresses électronique et postale, numéros de téléphone fixe et mobile, date de naissance, adresse IP, moyen de paiement et montant de la cotisation de certains adhérents.
Cette faille avait été rendue possible par l'utilisation d'une technique non sécurisée d'authentification à la plateforme. Elle a concerné plusieurs dizaines de milliers de primo-adhérents.
Alerté le même jour par la CNIL de cette faille, le PS a immédiatement pris les mesures nécessaires pour y mettre fin.
Un second contrôle réalisé cette fois dans les locaux du PS le 15 juin 2016, destiné à comprendre les raisons de la faille, a permis de constater que les mesures élémentaires de sécurité n'avaient pas été mises en œuvre initialement. En effet, il n'existait pas de **procédure d'authentification** forte au site ni **de système de traçabilité** permettant notamment d'identifier l'éventuelle exploitation malveillante de la faille.
Le contrôle a aussi permis de constater que le PS conservait sans limitation de durée les données personnelles de la plateforme, ce qui avait accru la portée de la fuite de données. La base active contenait des demandes d'adhésion effectuées depuis 2010 qui auraient dû a minima être stockées en archive.

En conséquence, la Présidente de la CNIL a décidé d'engager une procédure de sanction en désignant un rapporteur. La formation restreinte de la CNIL a prononcé un avertissement public car elle a estimé que le Parti Socialiste avait manqué à ses obligations :
• de veiller à la sécurité des données à caractère personnel des primo-adhérents, en méconnaissance de l'article 34 de la loi Informatique et Libertés ;
• de fixer une durée de conservation des données proportionnelle aux finalités du traitement en méconnaissance de l'article 6-5 de la loi Informatique et Libertés.

Enfin, la formation restreinte a décidé de rendre publique sa décision en raison de la gravité des manquements constatés, du nombre de personnes concernées par la faille et du caractère particulièrement sensible des données en cause qui permettaient notamment d'avoir connaissance de leurs opinions politiques.

Pour en savoir plus

Délibération de la formation restreinte n°2016-315 du 13 octobre 2016 prononçant un avertissement à l'encontre du PARTI SOCIALISTE
[PDF-312.22 Ko]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Faille de sécurité de données sensibles en ligne : Avertissement public pour le PARTI SOCIALISTE | CNIL

Des attaques DDoS de plus de 10 Tbit/s en vue ?

L'arsenal des attaques DDoS (Distributed Denial of Service) vient de s'enrichir d'une nouvelle arme : le LDAD.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Que faire en cas de harcèlement en ligne ?

Que faire en cas de harcèlement en ligne ?

Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

Qui sont les cyber-harceleurs ?

Un(e) internaute peut être harcelé(e) pour son appartenance à une religion, sa couleur de peau, ses opinions politiques, son comportement, ses choix de vie … Le harceleur peut revêtir l'aspect d'un « troll » (inconnu, anonyme) mais également faire partie de l'entourage de la victime (simple connaissance, ex-conjoint, camarade de classe, collègue, voisin, famille …).

A quoi ressemble une situation de cyber-harcèlement ?

• Happy slapping : lynchage en groupe puis publication de la vidéo sur un site
• Propagation de rumeurs par téléphone, sur internet.
• Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.
• Publication de photographies sexuellement explicites ou humiliante
• Messages menaçants, insulte via messagerie privée
• Commande de biens/services pour la victime en utilisant ses données personnelles
• …

Comment réagir ?

Ne surtout pas répondre ni se venger

Vous avez la possibilité de bloquer l'accès de cette personne à vos publications, de la signaler auprès de la communauté ou d'alerter le réseau social sur un comportement qui contrevient à sa charte d'utilisation.

Verrouiller l'ensemble de vos comptes sociaux

Il est très important de limiter au maximum l'audience de vos comptes sociaux. Des options de confidentialité existent pour « ne plus me trouver », « ne pas afficher/partager ma liste d'amis ». Il est également possible de « bannir » les amis indésirables. Sur Facebook, une option vous permet d'être avertis si un autre utilisateur mentionne votre nom sur une photo (tag).

Les paramétrages conseillés sur Facebook :

PARAMÉTRAGE POSSIBLE	CHEMIN D'ACCÈS
Limiter la visibilité de vos photos	Ce type d'option ne fonctionne que photo par photo
Limiter la visibilité de vos informations de profil	Informations générales : page du profil > encart gauche > sélectionner « amis » ou « moi uniquement »
Cacher votre liste d'amis	Page du profil > onglet « amis » > « gérer section » > « modifier la confidentialité » > « liste d'amis » ou « moi uniquement »
Cacher vos mentions « j'aime »	Page du profil > Mentions j'aime (encart gauche) > « modifier la confidentialité » > « moi uniquement »
Être prévenu si quelqu'un vous « tague »	Paramètre > journal et identification > Paramètres d'identification et de journal> « examiner les identifications »
Limiter la visibilité de vos publications	Journal > sélectionner la publication > « moi uniquement » / ou « supprimer »
Examiner votre historique	Page du profil > « afficher l'historique personnel » > supprimer au cas par cas

• Capture écran des propos / propos tenus
Ces preuves servent à justifier votre identité, l'identité de l'agresseur, la nature du cyber-harcèlement, la récurrence des messages, les éventuels complices. Sachez qu'il est possible de faire appel à un huissier pour réaliser ces captures.Fiche pratique : comment réaliser une copie d'écran ?

• Portez plainte auprès de la Gendarmerie/Police si le harcèlement est très grave
Vous avez la possibilité de porter plainte auprès du commissariat de Police, de Gendarmerie ou du procureur du tribunal de grande instance le plus proche de votre domicile.

• En parler auprès d'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.

Si quelqu'un d'autre est harcelé ?

Le fait de « partager » implique votre responsabilité devant la loi. Ne faites jamais suivre de photos, de vidéos ou de messages insultants y compris pour dénoncer l'auteur du harcèlement. Un simple acte de signalement ou un rôle de conseil auprès de la victime est bien plus efficace ! ***Le chiffre :*** *61% des victimes indiquent qu'elles n'ont reçu aucun soutien quel qu'il soit de la part d'organismes ou d'une personne de leur réseau personnel.* * Source: rapport européen sur le cyber-harcèlement (2013)

Si vous êtes victime et avez moins de 18 ans …

Composez le 3020. Il est ouvert du lundi au vendredi de 9h à 18h (sauf les jours fériés). Le numéro vert est géré par la plateforme nonauharcelement.education.gouv.fr qui propose de nombreuses ressources pour les victimes, témoins, parents et professionnels (écoles, collèges, lycées).

Si le harcèlement a lieu sur internet, vous pouvez également composer le 0800 200 000 ou vous rendre sur netecoute.fr. La plateforme propose une assistance gratuite, anonyme, confidentiel par courriel, téléphone, chat en ligne, Skype. Une fonction « être rappelé par un conseiller » est également disponible. La réponse en ligne est ouverte du lundi au vendredi de 9h à 19h.

Un dépôt de plainte est envisagé ? Renseignez vous surle dépôt de plainte d'un mineur. Celui-ci doit se faire en présence d'un ou de plusieurs parents ou d'un représentant légal. N'hésitez pas à contacter les télé-conseillers du fil santé jeune au 0800 235 236.

Un droit à l'oubli pour les mineurs. L'article 40 modifié de la loi informatique et Libertés – au même titre que futur Règlement européen sur la protection des données – consacre un droit à l'oubli spécifique pour les mineurs. Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement demander au site l'effacement des données le concernant et ce, dans les meilleurs délais. En pratique, si le responsable de traitement n'a pas effacé les données ou répondu à la personne dans un délai d'un mois, la personne concernée peut saisir la CNIL. Des exceptions existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.

Quelles sanctions encourues par l'auteur de ces violences en ligne ?

L'auteur de tels actes est susceptible de voir sa responsabilité engagée sur le fondement du Droit civil, du Droit de la presse ou du Code pénal. **Quelques exemples de sanctions :**
• Une injure ou une diffamation publique peut être punie d'une amende de 12.000€ (art. 32 de la Loi du 29 juillet 1881).
• Pour le droit à l'image, la peine maximum encourue est d'un an de prison et de 45.000 € d'amende (art. 226-1, 226-2 du Code pénal).
• L'usurpation d'identité peut être punie d'un an d'emprisonnement et de 15.000€ d'amende (art. 226-4-1 du Code pénal).

Quels sont les recours auprès de la CNIL ?

La qualification et la sanction de telles infractions relève de la seule compétence des juridictions judiciaires. En parallèle de telles démarches, **vous pouvez demander la suppression de ces informations à chaque site ou réseau social d'origine, en faisant valoir votre droit d'opposition**, pour des motifs légitimes, sur le fondement de l'article 38 de la loi du 6 janvier 1978 modifiée dite « Informatique et Liberté ». Le responsable du site dispose d'un délai légal de deux mois pour répondre à votre demande. La majorité des sites propose un bouton « signaler un abus ou un contenu gênant ». Si aucun lien n'est proposé, contactez directement par courriel ou par courrier le responsable du site en suivant la procédure expliquée sur notre site.
Par ailleurs, **si ces informations apparaissent dans les résultats de recherche à la saisie de vos prénom et nom, vous avez la possibilité d'effectuer une demande de déréférencement auprès de Google en remplissant le formulaire**. En cas d'absence de réponse ou de refus, vous pourrez revenir vers la CNIL en joignant une copie de votre demande effectuée auprès du moteur de recherche incluant le numéro de requête Google.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Réagir en cas de harcèlement en ligne | CNIL

ESET sensibilise les TPE aux risques informatiques et au RGPD

ESET sensibilise les TPE aux risques informatiques et au RGPD

Par manque de sensibilisation à la sécurité informatique, les TPE qui ne disposent de moyens humains dédiés, s'exposent à un risque plus élevé pouvant avoir de graves conséquences pour leur entreprise.

« Récemment, un cabinet médical s'est adressé à nous après s'être retrouvé infecté par un ransomware causant la perte de l'ensemble des données de ses patients. Il n'avait pas installé de solutions de sécurité car il n'en voyait pas l'utilité. Il devient urgent que les TPE prennent conscience de l'importance des données qu'ils détiennent », explique Benoît Grunemwald, Directeur des Opérations chez ESET France.
Avec l'arrivée du RGPD (2018) les TPE devront, au même titre que les grands comptes, s'approprier le texte qui vise à protéger les données personnelles qu'ils détiennent. A ce titre, des mesures imposées par le règlement européen devront être mises en place sous peine de sanctions.
La première démarche consiste à réaliser une cartographie des données et attribuer un niveau de sensibilité aux informations (voir pièce jointe). Pour appliquer les mesures, l'expert juridique viendra en soutien des actions entreprises par la société. Il restera alors la mise en place des systèmes de sécurité.
Les experts ESET ont mis au point un produit accessible aux besoins des TPE, ne nécessitant pas une connaissance accrue des systèmes de sécurité : ESET Smart Security Premium.
Au-delà des fonctions primaires qu'il propose (antivirus, anti-phishing, protection contre les attaques par script, antispam…), nos experts ont ajouté 3 fonctions permettant d'accompagner ces entreprises dans la mise en place de systèmes de sécurité répondant aux exigences du RGPD :
• Le chiffrement des données pour éviter les fuites éventuelles
• La protection du réseau domestique afin de connaître l'identité des appareils connectés
• Le gestionnaire de mots de passe afin de protéger tous les accès par des mots de passe efficaces
…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

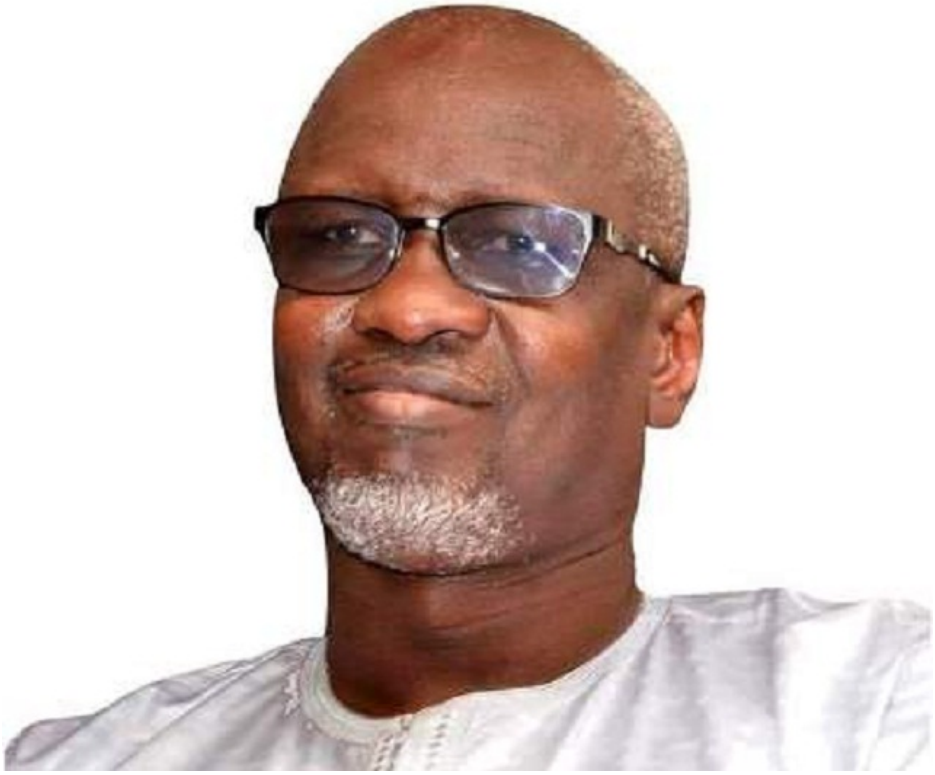
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La sécurité Internet

Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie



Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie

L'enquête sur le piratage de la plate-forme de transfert d'argent de la Poste se poursuit. Après avoir entendu plusieurs responsables de la boite, la section de recherches de Colobane (Dakar) a reçu hier dans ses locaux le directeur général, Ciré Dia. D'après le quotidien sénégalais L'Observateur qui donne l'information dans sa livraison du jour, un important arsenal technique a été mis à contribution pour remonter la filiale.

En s'introduisant dans le système de transfert international du réseau, les cybercriminels avaient emporté près de 400 millions de francs CFA. Un coup dur pour la société qui traverse actuellement des moments difficiles selon L'Enquête qui fait état de problèmes de recouvrement des montants dus par les sociétés de transfert d'argent au groupe, des montants estimés entre 4 et 5 milliards CFA.

Réagissez à cet article

Original de l'article mis en page : Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie hier | CIO MAG

Pourquoi les objets connectés sont un danger pour l’Internet ?

Pourquoi les objets connectés sont un danger pour l’Internet ?

Plusieurs grands sites Internet ont vu leurs services perturbés vendredi soir suite à une attaque contre une partie de l'infrastructure du réseau global. Cette attaque est particulièrement inquiétante car elle n'est que la dernière manifestation d'un phénomène en plein essor : le piratage d'objets connectés mal sécurisés pour constituer des réseaux offensifs. Un fléau qu'il sera difficile d'endiguer.

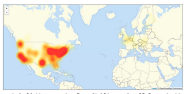
Une attaque de grande ampleur a eu lieu vendredi 21 octobre 2016, mettant hors service pendant quelques heures plusieurs grands sites Internet comme Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr. Ces sites n'étaient pas directement sous le coup d'une attaque, ils ont été les victimes collatérales d'une attaque contre Dyn, une entreprise dont les services font d'elle une infrastructure critique d'Internet : Dyn gère un service DNS (système de noms de domaine), qui permet de corréler un nom de domaine (comme « usine-digitale.fr ») en une adresse IP et vice versa.

UNE ATTAQUE BASIQUE MAIS SURPUISSANTE GRÂCE AUX OBJETS CONNECTÉS

Ce qui est notable ici, c'est qu'il ne s'agissait pas d'une attaque sophistiquée, soigneusement mise en oeuvre par un groupe d'experts. Non, il s'agissait d'une attaque par déni de service distribué (DDoS) – autrement dit une attaque ayant pour but de rendre un service indisponible en le noyant d'informations inutiles – s'appuyant principalement sur le botnet Mirai, qu'a identifié le cabinet d'analyse Flashpoint. Les botnets ne sont pas nouveaux, il s'agit de réseaux de machines dont un malware a pris le contrôle et qui peuvent être utilisés à tout moment pour mener une attaque coordonnée. Traditionnellement, les machines infectées étaient des ordinateurs dont les mises à jour de sécurité n'avaient pas été faites. Mais les progrès en matière d'antivirus et de solutions d'atténuation d'attaques DDoS limitent aujourd'hui sérieusement l'intérêt d'utiliser un botnet constitué d'ordinateurs (long et difficile à mettre en place) pour ce type d'opération (peu rentable car les rançons sont désormais rarement payées).

MIRAI, COMMENT ÇA MARCHE ?

La différence avec Mirai, c'est qu'il s'attaque aux objets connectés. Son *modus operandi* est on ne peut plus simple : il parcourt Internet en cherchant à se connecter à toutes les adresses telnet qu'il trouve avec une liste de 62 logins/mots de passe par défaut (dont le classique admin/admin). Une fois l'appareil infecté, Mirai en bloque certains ports pour empêcher qu'on en reprenne le contrôle. Le malware est basique, rapide, efficace, et surtout disponible gratuitement pour quiconque souhaite s'amuser avec, car son créateur en a rendu le code public. De plus, contrairement aux ordinateurs, un botnet d'objets connectés n'a aucune utilité réelle autre qu'effectuer des attaques par déni de service. Le fait que les objets connectés ont tendance à être allumés 24h/24 et 7j/7 facile aussi cet usage.



Impact de l'attaque contre Dyn, établie par Level3 Communications

CAMÉRAS ET ENREGISTREURS NUMÉRIQUES EN CAUSE

Le résultat est une arme dont la puissance est absolument démesurée par rapport à son accessibilité. En septembre 2016, le blog du journaliste spécialisé Brian Krebs avait été frappé par une attaque record atteignant un débit de 620 Gb/s. Une semaine plus tard, c'est l'hébergeur français OVH qui avait été visé, avec une puissance de frappe estimée à 1,5 Tb/s. L'attaque contre Dyn, survenue un mois plus tard, semble être à nouveau montée d'un cran. Quels sont les objets connectés utilisés par Mirai ? On y trouve beaucoup de caméras de surveillance et d'enregistreurs numériques (DVR), principalement fabriquées par une seule entreprise : Hangzhou XiongMai Technology. A noter que d'autres botnets pourraient également avoir participé à l'attaque. On connaît l'existence d'au moins un autre malware au fonctionnement similaire à Mirai, baptisé Bashlight.

PAS DE SOLUTION EN L'ÉTAT

Le problème est que ces appareils sont pratiquement impossible à protéger en l'état. Pour une partie d'entre eux, les identifiants sont codés « en dur » dans le firmware et ne sont pas modifiables. Et même pour les autres, le fait qu'ils utilisent le protocole telnet (en ligne de commande, sans interface graphique) les rend difficile à configurer pour les utilisateurs. D'après une analyse de Flashpoint, plus de 515 000 objets connectés seraient aujourd'hui vulnérables et susceptibles d'être incorporés dans un botnet. Certains experts ont proposé des solutions radicales, notamment de développer un malware plus rapide que Mirai, capable d'infecter un objet connecté vulnérable avant lui lors d'un redémarrage de ce dernier, et de le saboter pour le mettre définitivement hors service. Une mesure aussi drastique qu'illégale, mais qui souligne à quel point la situation désempare l'industrie.

Il y a eu beaucoup de mises en garde face au danger que représente l'Internet des Objets, mais, comme souvent, celles-ci n'ont servi à rien. Puisqu'il est clair que l'essor des objets connectés n'est pas prêt de s'arrêter, il est impératif que les acteurs majeurs de cette industrie mettent en place des normes et des bonnes pratiques au plus tôt, faute de quoi l'Internet des Objets continuera à scléroser l'Internet tout court, et ce de plus en plus souvent.

Original de l'article mis en page : Le retour des botnets ou pourquoi les objets connectés sont un danger pour l'Internet