Vous offrez aux hackers des données invisibles sans le savoir

	Vous offrez aux hackers des données invisibles sans le savoir

Empreintes digitales, données GPS des photos, réponses aux questions prétendues «secrètes»…: des données sensibles se cachent sur ce que vous publiez sur les réseaux sociaux, même si l'essentiel du risque se concentre sur des informations livrées plus directement encore…

Le « V » de la victoire pourrait être celui des hackers. Un chercheur japonais avertissait début janvier contre le danger contenu dans ce signe parfois associé aux selfies: en montrant vos doigts, vous courez le risque de vous faire voler vos empreintes digitales, prévient Isao Echizu.
Alors que les «données sont le pétrole du 21ème siècle », comme on l'entend à l'envi, nous avons une fâcheuse tendance à livrer les nôtres, intentionnellement, sur les réseaux sociaux, en négligeant bien souvent les règles de confidentialité ou l'utilisation commerciale qui est leur est destinée. Mais la vigilance se complique quand on n'a même pas conscience qu'une donnée en est une…

Attention aux données invisibles…

Permettez-moi d'emprunter vos empreintes

Avec la haute résolution des photos prises par les smartphones, une opération – assez complexe, toutefois, et loin d'être à la portée de tout le monde – peut permettre de récupérer les empreintes. « Or à l'inverse des mots de passe, les empreintes, une fois volées, ne pourront jamais être changées», rappelle à *20 Minutes* Gérôme Billois, expert cybersécurité au cabinet Wavestone.
Il note que si l'avertissement du professeur japonais a fait le tour du monde, « on connaissait le risque depuis 2014 »: un hacker avait montré lors d'une conférence qu'il était parvenu à cloner les empreintes digitales de la ministre allemande de la Défense. Depuis, les empreintes digitales sont de plus en plus utilisées, pour déverrouiller smartphones, objets connectés ou pour réaliser certains paiements.

Des photos très bavardes

Autre donnée invisible, la géolocalisation associée aux photos, la grande majorité étant prise aujourd'hui par des smartphones équipés d'une puce GPS (qui ne sert pas qu'à vous guider sur la route jusqu'à Palavas-Les-Flots). Aux images numériques sont associées tout un ensemble de métadonnées, qui «peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale», comme le précise We Fight Censorship, qui indique la marche à suivre pour nettoyer ces métadonnées.«Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage», lit-on encore.
En septembre dernier, deux étudiants de Harvard ont pu démasquer 229 dealers grâce aux coordonnées géographiques contenues dans les métadonnées associées à des photos qu'ils avaient prises et postées en ligne.

En huit tweets, tout est dit

Sur Twitter, si la géolocalisation des tweets est désactivée par défaut, beaucoup l'activent. En mai dernier, des experts du MIT et d'Oxford démontraient que huit tweets (d'utilisateurs pour lesquels la géolocalisation est activée) suffisaient à localiser quelqu'un de façon très précise. « Il est extrêmement simple pour des personnes avec très peu de connaissance technique de trouver où vous travaillez ou vivez », expliquaient-ils, à l'issue d'une expérience concluante.

Le secret imaginaire des questions secrètes

Il y a enfin ces infos que nous livrons publiquement sur les réseaux sociaux alors qu'elles contiennent parfois les réponses aux questions censées être «secrètes». «Les questions secrètes sont le talon d'Achille des réseaux sociaux, souligne Gérôme Billois. Elles vous permettent d'accéder à vos comptes en cas d'oubli de mot de passe et ce sont toujours les mêmes: Quel est le prénom de votre mère? Quel est votre plat préféré? Or toutes ces infos peuvent être retrouvées facilement sur les réseaux sociaux.»

… et surtout aux données plus évidentes, qui permettent de personnaliser le phishing

Pour les scénarios ci-dessus, qui peuvent avoir le mérite d'attirer l'attention, la probabilité d'utilisation malveillante est pourtant « faible », assure Gérôme Billois. Parallèlement, «nous passons notre temps à livrer des informations hypersensibles», et de façon bien plus directe. Or l'occupation principale des cybercriminels reste les mails de phishing, et ces données les aident à les personnaliser.
«Si le mail est pointu, que c'est votre « bonne » banque qui vous dit qu'elle a remarqué votre passage à telle heure la veille, et que toutes ces infos sont correctes parce que vous avez partagé ces données sur les réseaux sociaux, il y a toutes les chances pour que vous cliquiez sur le lien malveillant.»…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Sans le savoir, vous offrez aux hackers des données invisibles

---

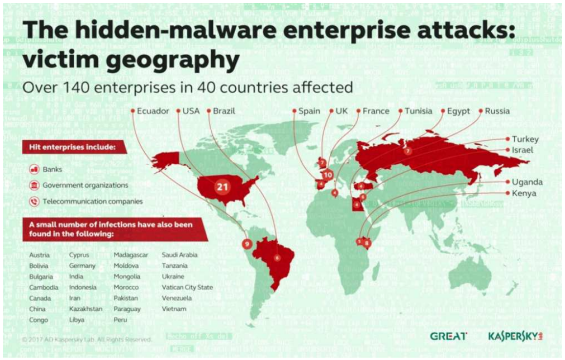
Une nouvelle menace plane sur les distributeurs automatiques de billets

Une nouvelle menace plane sur les distributeurs automatiques de billets

---

Des chercheurs en sécurité informatique ont découvert une faiblesse des DAB, difficilement détectable à ce jour.

Les distributeurs automatiques de billets restent une cible appréciée des pirates informatiques. Selon une étude publiée par Kaspersky , une entreprise spécialisée en cybersécurité, et relayée par 01Net , les « DAB » seraient vulnérables à une attaque informatique perfectionnée et surtout, discrète. Cette attaque a été détectée 10 fois en France, rapporte Kaspersky. C'est le deuxième pays à être autant ciblé après les Etats-Unis.
La méthode est assez ingénieuse. « Alors que les virus que l'on connaît aujourd'hui écrivent des fichiers sur le disque dur du DAB, cette nouvelle génération d'attaques va s'en prendre à la mémoire vive, ce qui ne laisse aucune trace », décrit Daniel Fages, directeur technique de Stormshield, une entreprise française spécialisée, aux « Echos ». Une fois introduit dans le système, qui est peu ou prou un ordinateur, l'attaquant va pouvoir prendre le contrôle de la machine à distance, à n'importe quel moment. L'attaque a un nom : « fileless malware », ou malware « sans fichier », en bon français.



Les Etats-Unis sont particulièrement touchés par le phénomène – Kaspersky

A partir de là, tout est possible. « L'attaquant peut faire sortir des billets comme il l'entend, ou bien capturer les données des utilisateurs qui retirent des billets dans le DAB infecté », décrit Daniel Fages.

Les DAB, pas réellement protégés

Cette vulnérabilité est d'autant plus importante que les distributeurs ne sont que très rarement mis à jour aujourd'hui. Si certaines banques disposent de protection contre les virus « classiques », très souvent, elles s'en contentent. « Tant que ça marche, on ne touche pas », résume Daniel Fages.
Difficulté supplémentaire : les DAB sont produits sur un mode industriel. Une faille telle que celle-ci peut donc fonctionner sur de très nombreux appareils.

Une attaque difficile à réaliser

Néanmoins, une telle attaque n'est pas facile à réaliser. Pour infiltrer la mémoire vive du distributeur, il faut d'abord avoir infecté le réseau qui relie les DAB d'une même banque entre eux. Ce réseau, souvent interne, n'est pas directement exposé à Internet et donc à une attaque.
« Les attaquants capables d'une telle manoeuvre ont des moyens et de très bonnes connaissances techniques », estime Daniel Fages.

Une sécurité : protéger son code PIN

Qui plus est, si les attaquants décident de s'en prendre aux données des …[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Une nouvelle menace plane sur les distributeurs automatiques de billets, Banque – Assurances

Le délit de consultation habituelle de sites terroristes est réinstauré

Le délit de consultation habituelle de sites terroristes est réinstauré

Lors de de la commission mixte paritaire pour le projet de loi relatif à la sécurité publique, les parlementaires ont réinstauré le délit de consultation habituelle de sites terroristes en y ajoutant une condition supplémentaire.

Censuré par le Conseil constitutionnel, le délit de consultation habituelle provoquant directement à la commission d'actes de terrorisme ou faisant l'apologie de ces actes est en train de faire son retour dans la législation française. Une nouvelle version de l'article 421-2-5-2 du code pénal a en effet été proposée par les parlementaires lundi 13 février, trois jours à peine après le verdict des Sages de la rue de Montpensier.
C'est dans le cadre de la commission mixte paritaire, chargée de négocier la version définitive du projet de loi relatif à la sécurité publique en faisant appel à sept députés et sept sénateurs, que le nouvel article de loi a été déposé, sous l'impulsion du député Éric Ciotti et le sénateur Philippe Bas, ce dernier déclarant le jour de la censure que cette disposition est « *essentielle à la lutte antiterroriste* ».
Suivre


Philippe Bas
✔@BasPhilippe
J'ai fait rétablir en le modifiant le délit de consultation de sites terroristes à la #CMP de la loi sur la sécurité publique.
18:46 – 13 Févr 2017
•
•
3131 Retweets
•
2929 j'aime
Suivre


Eric Ciotti
✔@ECiotti
Avec Philippe Bas, nous venons de rétablir en CMP le délit de consultation des sites djihadistes annulé de façon ahurissante par le CC
17:44 – 13 Févr 2017
•
•
115115 Retweets
•
106106 j'aime
« *J'ai fait rétablir en le modifiant le délit de consultation de sites terroristes à la CMP de la loi sur la sécurité publique* », s'est félicité Philippe Bas. Plus offensif, Éric Ciotti a chargé le Conseil constitutionnel qui a « *annulé de façon ahurissante* » cet article né avec la loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
La nouvelle rédaction du texte est la suivante (les changements par rapport à la première version du texte ont été mis en gras) :
Le fait de consulter habituellement **et sans motif légitime** un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende **lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service**.
Constitue notamment un motif légitime […] la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes.
LA NOUVELLE VERSION DEMANDE DÉSORMAIS DE VÉRIFIER UNE MANIFESTATION DE L'ADHÉSION À L'IDÉOLOGIE…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le délit de consultation habituelle de sites terroristes fait son retour – Politique – Numerama

Ressources pour la collecte et la vérification d’informations à destination des journalistes

Ressources pour la collecte et la vérification d’informations à destination des journalistes

Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification

Présentation de Samuel Laurent, éditeur délégué du Monde, partenaire de First Draft
L'éditeur délégué du Monde présente à First Draft ses travaux en matière de lutte contre la désinformation en ligne et ses projets…[Lire la suite]

Lancement de CrossCheck : à l'approche des élections françaises, les rédactions s'associent pour lutter contre la désinformation
CrossCheck réunit les compétences des secteurs des médias et des technologies pour s'assurer que fausses déclarations soient rapidement détectées et corrigées…[Lire la suite]

Outils pour renforcer la confiance envers les journalistes
Fort de son expérience dans le paysage journalistique américain, Josh Stearns nous présente des outils pour que journalistes et rédactions regagnent la confiance de leur audience…[Lire la suite]
Outils et ressources : Hearken, Engaging News Project, Coral ProjectNews Voices Engaged Newsroom Toolkit

Guide pour la vérification visuelle des vidéos
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des vidéos des internautes…[Lire la suite]

Guide pour la vérification visuelle des photos
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des photos mises en ligne par des tiers…[Lire la suite]

Utiliser Google Earth pour vérifier des images comme un pro
Google Earth offre bien plus que des images satellites…[Lire la suite]

Réseaux sociaux et contenus viraux : comment les développeurs des rédactions peuvent-ils faciliter la démystification ?
Les nouveaux projets de vérification doivent tenir compte des leçons clés tirées des procédés de « fact-checking » (vérification par les faits) ayant faits leurs preuves, tout en les adaptant aux écosystèmes des réseaux sociaux…[Lire la suite]
Savoir où chercher : sources d'image pour la géolocalisation
Trouver d'autres photos ou vidéos d'un lieu peut être un des meilleurs moyens de vérifier le lieu où a été capturé un contenu. Voici où chercher…[Lire la suite]
10 façons de mieux couvrir le terrain pour les journalistes locaux
Combiner le reportage traditionnel sur le terrain et les possibilités offertes par les services numériques modernes peut faire la différence entre un bon et un très bon journaliste…[Lire la suite]
Respecter la source : l'importance du témoin dans la couverture de l'actualité en temps réel
Les témoins sont des personnages clés dans de nombreux événements majeurs se produisant aux quatre coins du monde…[Lire la suite]
Comment se protéger face aux contenus traumatisants ?
Sam Dubberley, cofondateur de Eyewitness Media Hub, détaille certains des résultats principaux d'une étude récente portant sur les traumatismes indirects dans les rédactions…[Lire la suite]

Réagissez à cet article

Original de l’article mis en page : First Draft News FR – Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification

---

Des douzaines de banques internationales attaquées par un nouveau logiciel malveillant

Des douzaines de banques internationales attaquées par un nouveau logiciel malveillant

---

Selon Symantec, plus d'une centaine d'organisations issues de 31 pays ont été victimes de tentatives de cyberattaques depuis octobre dernier. Les cyber attaquants ont utilisé des sites Web compromis ou des attaques par « point d'eau » pour infecter des cibles présélectionnées. L'analyse est toujours en cours mais ces attaques pourraient être liées au groupe Lazarus.

C'est le cas d'une banque polonaise qui a décelé un logiciel malveillant sur un certain de ses ordinateurs et a partagé des indicateurs de compromis (COI) avec d'autres institutions. Ces dernières ont ainsi pu découvrir qu'elles avaient également été exposées. Aucune preuve ne laisse penser que des fonds ont été dérobés.

Inconnu jusque-là, le logiciel malveillant utilisé dans ces attaques a été repéré par la détection générique de Symantec, conçue pour bloquer tous les fichiers considérés comme malveillants. Depuis octobre 2016, Symantec a ainsi bloqué plusieurs attaques effectuées par le même kit que celui qui a infecté les banques polonaises contre les ordinateurs de ses clients : 14 au Mexique, 11 en Uruguay et 2 en Pologne. L'analyse de cette attaque est toujours en cours, mais certaines chaînes de code analysées dans le malware partagent des similitudes avec celles utilisées par Lazarus, le groupe de cybercriminels derrière les attaques de Sony…[lire la suite]

Original de l'article mis en page : Des douzaines de banques

internationales attaquées par un nouveau logiciel malveillant

---

5 leçons à retenir pour une Cybersécurité efficace

	5 leçons à retenir pour une Cybersécurité efficace

---

Les équipes ESET assistent régulièrement à des conférences sur la sécurité. Ils constatent que de nombreux thèmes font leur apparition : Next-gen, IoT, DDoS, plateforme d'administration des alertes complexes…

Le fait que ces mots soient de plus en plus utilisés n'est pas un problème en soi, mais nous nous sommes demandé si le monde de la cybersécurité ne prenait pas le problème dans le mauvais sens et passait alors à côté de sujets qui doivent être abordés.
À travers cette tribune, nous vous proposons 5 règles essentielles pour une sécurité efficace en entreprise.

Leçon 1 : appréhender les risques associés à l'entreprise
La sécurité informatique est complexe, mais son objectif premier est simple. Il s'agit de réduire les risques tout en les rendant visibles pour que l'entreprise puisse les accepter afin de continuer à travailler.
Pour y parvenir de manière efficace, vous devez amener vos éditeurs de solutions de sécurité à comprendre votre entreprise et à ne pas la considérer uniquement du point de vue IT, mais la saisir dans sa globalité.
En débutant un projet avec une entreprise, l'éditeur doit d'abord identifier, cartographier et catégoriser les risques y compris ceux liés spécifiquement à votre secteur d'activité (approche sectorielle). Deuxièmement, vous déterminerez ensemble les risques qui nécessitent d'être traités et dans quel ordre. Une fois cette étape réalisée, le responsable de la sécurité informatique doit mettre en place une conduite de changement avec des objectifs clairs et des délais. Idéalement, ce processus aura été pensé bien en amont et réalisé pas à pas, afin de ne pas s'engager dans trop de projets à la fois.

Leçon 2 : mettre en place une approche sécuritaire avec un but précis
La définition d'une feuille de route est essentielle et doit impliquer les responsables de l'activité de votre entreprise afin de s'adapter si cela est nécessaire. Pendant la création et l'exécution de la feuille de route, les projets définis contribueront à la réduction des risques et à l'atteinte des objectifs. Il est important de ne pas perdre de vue ces derniers pour que les responsables de la sécurité n'entravent pas la bonne marche de l'entreprise avec leurs mesures. L'approche sécuritaire définie doit être comprise par tout le monde, même sans compétences IT. Bien sûr, l'informatique joue un rôle, mais uniquement à la fin du processus lorsque les solutions sont nécessaires à l'exécution des projets de sécurité.

Leçon 3 : garantir l'essentiel avant la mise en œuvre de solutions de sécurité plus avancées
Après avoir fait le point sur les congrès auxquels nous avons assisté, nous constatons que la plupart des entreprises n'ont même pas les mesures de sécurité essentielles telles que la mise en place d'un antivirus et la protection des postes de travail par un mot de passe. Les présentations des entreprises expertes en cybersécurité offrent un contenu intéressant, mais trop avancé pour la plupart des entreprises. En outre, les retours d'expérience montrent que la grande majorité des piratages (environ 90 %) utilisent les méthodes les plus simples ou des vulnérabilités connues : courriers électroniques et phishing, pièces jointes contenant des malwares, etc. Sans oublier le maillon le plus faible : l'être humain. Vous devez donc déployer des solutions de sécurité en rapport avec ces risques connus avant de vous tourner vers des technologies de pointe plus sophistiquées, même si ces dernières sont importantes.

Leçon 4 : choisir ses fournisseurs de cybersécurité comme des partenaires
Le nombre de cybercriminels se multiplie autant que les techniques de cyberattaque (qui peuvent être très avancées). Ainsi, les solutions de sécurité ayant une protection multicouche seront indissociables de l'approche sécuritaire des entreprises. Cependant, une telle stratégie suppose comme pour toute construction de bonnes fondations. Construire un tel édifice implique une réelle coopération entre l'architecte, l'agent immobilier, le maçon, le plâtrier et bien sûr le propriétaire. Cette approche commune pour bâtir quelque chose ensemble, pas à pas, correspond exactement ce qui doit arriver dans le monde de la cybersécurité.

Leçon 5 : impliquer l'ensemble des collaborateurs pour mener à la réussite
Pour améliorer votre sécurité, vous devez avoir le soutien de vos collaborateurs. Le responsable de la sécurité doit être en mesure de fournir des explications brèves et claires à l'ensemble des métiers de la société. Si cela n'est pas réalisé correctement, votre entreprise ne comprendra pas les enjeux et ne pourra soutenir les plans définis. Comme l'a déclaré Albert EINSTEIN : « si vous ne pouvez pas expliquer quelque chose simplement, c'est que vous ne l'avez pas bien compris ! »

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité en entreprise : 5 leçons à retenir pour une sécurité efficace – Global Security Mag Online

---

6 bonnes pratiques pour se protéger du piratage informatique

	6 bonnes pratiques pour se protéger du piratage informatique

---

Par manque de temps ou de ressources, les PME négligent le risque de piratage informatique. Quelques règles de bon sens suffisent pourtant à écarter en partie les menaces.

Perdre ses données suite à une attaque informatique peut avoir de lourdes conséquences pour une start-up ou une PME. L'entreprise peut même ne jamais s'en relever. Piratage de site Internet, clé USB piégée, vol de mot de passe, programme espion caché dans des pièces jointes… Les cyber menaces sont de plus en plus fréquentes. Quelles sont les règles simples pour s'en protéger ? Le point avec Stéphane Dahan, président de Securiview, entreprise spécialisée dans le management de la sécurité informatique.

#1 : Identifier les données les plus sensibles

« *Faites preuve d'une saine paranoïa*, affirme Stéphane Dahan. *C'est-à-dire sachez définir précisément quelles sont les informations à protéger dans l'entreprise* ». Inutile donc de mettre des barrières partout sans discernement. Quelle que soit leur forme (mail, papier, fichier), posez vous donc la question : quelles sont les données les plus sensibles et quelle est la probabilité qu'on me les vole ? « *Ensuite, il faut les localiser. Messagerie, Dropbox, téléphone, autant de pistes de fuite possible pour des informations qui ont de la valeur.* »

#2 : Mettre à jour les systèmes et sauvegarder

« *Ne pas oubliez de mettre à jour régulièrement ses antivirus et ses systèmes d'information. On voit trop souvent des entreprises négliger cet aspect* », soutient Stéphane Dahan. N'oubliez pas non plus de **sauvegarder périodiquement vos dossiers stratégiques**. « *Idéalement, ils doivent être stockés à plusieurs endroits. Si un serveur brûle, que vous soyez capable de les retrouver ailleurs* ».

#3 : Assurer la confidentialité des données clés

A l'intérieur de l'entreprise, assurez-vous que seuls les salariés ayant besoin des informations sensibles puissent y accéder. Par exemple, que les mots de passe ou clés de chiffrement ne soient **attribués qu'aux personnes qui ont besoin de les connaître**.

#4 : Définir et faire appliquer la politique de mot de passe

Attention dans le choix des mots de passe ! C'est trop souvent le talon d'Achille des systèmes d'information. « *Eviter de choisir les plus bateau comme abc123 ou 12345, une mauvaise habitude plus courante qu'on ne le dit* », insiste Stéphane Dahan. Idéalement, fixez des règles de choix et de dimensionnement des mots de passe et **renouveler ces derniers régulièrement**.

#5 : Protéger les terminaux mobiles

Les postes mobiles sont des points d'accès potentiels pour des pirates informatiques. Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ils doivent bénéficier au moins des mêmes mesures de sécurité que les postes fixes. Même si cela représente une contrainte supplémentaire, les conditions d'utilisation des terminaux nomades imposent même le renforcement de certaines fonctions de sécurité.

#6 : Sensibiliser l'équipe au risque de piratage

Périodiquement, rappelez à votre équipe quelques règles élémentaires : ne pas divulguer des mots de passe à un tiers, ne pas contourner les dispositifs de sécurité internes, éviter d'ouvrir la pièce jointe d'un message venant d'une adresse inconnue, etc. La sensibilisation doit également porter sur **l'utilisation des réseaux sociaux**. « *Les comptes Facebook ou Linkedin des collaborateurs sont des mines d'informations pour les pirates*, explique Stéphane Dahan. *Ils s'en servent pour adresser des messages très personnalisés qui vont leur permettre d'entrer dans le système d'information de l'entreprise.* »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : 6 bonnes pratiques pour se protéger du piratage informatique, Marketing et Vente – Les Echos Business

---

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Cette étude analyse les risques de cyberattaques sur des infrastructures énergétiques européennes, ainsi que leurs potentielles conséquences, notamment sur les réseaux électriques. Elle offre également une approche comparative des mesures prises par différents pays d'Europe afin de protéger leur industrie et collaborer à l'échelle de l'Union européenne.

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité sur toute la chaîne de valeur énergétique, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné cette industrie : les cyberattaques.

Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique.

La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

LIRE L'ETUDE (PDF)

Original de l'article mis en page : Cyberattaques et systèmes énergétiques: faire face au risque | IFRI – Institut français des relations internationales

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Un collectif Anonymous pirate le site de l’Anssi

Un collectif Anonymous pirate le site de l’Anssi

Cible d'une attaque DDoS, le site Internet de l'Agence nationale de la sécurité des systèmes d'information (Anssi) a été bloqué à plusieurs reprises les 4 et 5 février.
Trois semaines après l'annonce d'une campagne de recrutement, l'Agence nationale de la sécurité des systèmes d'information (**Anssi**) fait les frais de sa popularité grandissante. Cible d'une attaque par déni de service distribué (DDoS), le site Internet de l'Anssi a été bloqué le 4 février au soir, rapporte Zataz, et a été à nouveau perturbé ce vendredi 5 février après-midi jusqu'à 15h30 environ.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Le site de l'Anssi piraté par un collectif Anonymous

---

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Souhaitant mettre rapidement sur le marché leurs produits, les fabricants d'objets connectés ont eu tendance à négliger l'aspect sécurité, contribuant ainsi à la vulnérabilité de leurs utilisateurs face à de possibles attaques.

Atlantico : En septembre et octobre 2016, deux attaques DDOS ont été particulièrement marquantes : la première sur l'entreprise OVH et la deuxième sur DYN. Dans les deux cas, ces attaques ont été rendues possibles par les objets connectés. Malgré l'ampleur de ces attaques, celles-ci sont à relativiser. Dans une récente étude réalisée pour le compte de l'entreprise HSB, on note que seulement 10% des utilisateurs ont été touchés par des problèmes de piratage. Quels sont les risques du piratage des objets connectés ?

Quel peut être le préjudice porté aux particuliers et aux entreprises ?

Yvon Moysan : Une attaque DDoS ou attaque par déni de service massive vise à **rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.** Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément et depuis de multiples endroits. L'intensité de ce « tir croisé » rend le service instable, voire indisponible. **Le risque d'être confronté à ce type d'attaque est important et surtout les tentatives sont nombreuses**. Dans le cas de la société américaine Dyn que vous évoquez, celle-ci a été victime d'une attaque de plus d'un Téra-octet par seconde, ce qui pourrait concerner environ 10 millions d'objets connectés piratés. Ce niveau d'intensité est toutefois très rare.

Le préjudice subi dépend du type d'objets connectés piratés et du caractère sensible des données des particuliers. Si la majorité des objets connectés contiennent rarement des informations aussi sensibles que celles qui sont stockées sur un ordinateur, **il en existe des sensibles comme les voitures connectées ou les fusils intelligents qui, piratés à distance, peuvent représenter un véritable danger, potentiellement mortel pour l'utilisateur.** Et **ce risque s'est d'ores et déjà avéré.** Des experts en sécurité informatique ont ainsi réussi à prendre le contrôle à distance d'une Jeep Cherokee. Ils ont pu agir sur la vitesse, freinant et accélérant à leur guise, envoyant même la voiture dans le fossé alors que pour le fusil intelligent, d'autres experts ont réussi a bloqué le déclenchement du tir.

Le risque existe également pour des objets plus communs comme les applications de smart home. Des hackers ont ainsi réussi à bloquer la température de thermostats connectés à une température polaire ou saharienne. Plus préjudiciable, des hackers ont pris le contrôle de caméras de surveillance, récupéré les vidéos enregistrées, et au final les ont diffusées sur le Web. Un baby phone a également été la cible d'un hacker terrorisant un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, celui-ci s'est mis à hurler des insanités sur le nourrisson. **Le risque peut surtout être généralisé si des hackers réussissent à prendre le contrôle des réseaux d'électricité ou de gaz sur un quartier par exemple.** Il devient en effet possible de plonger toute une zone dans le noir ou, en fonction des données récoltées sur la consommation, de savoir quelles habitations sont occupées ou pas, en vue d'éventuels cambriolages.

Cela peut ensuite être contraignant pour la société qui a fabriqué et vendu les objets piratés car cela révèle **la faiblesse du niveau de sécurité**. Dans le cas de l'attaque de la société Dyn, une partie des objets connectés étaient ceux de la société chinoise Xiongmai, qui a dû les rappeler en urgence pour leur appliquer un correctif de sécurité. Cela peut aussi être problématique pour les clients de la société victimes de l'attaque. Dans le cas de Dyn, cela a eu pour conséquence de rendre inaccessible pendant une dizaine d'heures des sites comme Twitter, Ebay, Netflix, GitHub ou encore PayPal.

On peut aussi s'interroger sur certaines pratiques des constructeurs. Le fait de mettre un mot de passe commun à tous les appareils avant une première connexion a déjà été pointé du doigt. Quels autres dysfonctionnements peut-on mettre en avant ? Face à l'augmentation du nombre d'objets connectés, comment s'adaptent précisément les constructeurs en termes de sécurité ?

Tout d'abord il est important de préciser que ce type d'attaques par déni de service n'a rien de nouveau : les cybercriminels utilisent depuis des années des armées d'ordinateurs piratés pour inonder de requêtes les sites ciblés et les rendre inaccessibles.

La nouveauté réside ici dans le nombre croissant des objets connectés qui accroit de manière exponentielle les possibilités d'attaques. Or **la puissance d'une attaque dépend essentiellement du nombre de périphériques piratés, d'où l'intérêt de passer par les objets connectés**. Il existe en effet **plusieurs milliards d'objets connectés dans le monde contre quelques centaines de millions d'ordinateurs.** Pour y faire face, il existe des solutions proposées par les hébergeurs pour protéger leurs serveurs des attaques. Ces solutions permettent, par exemple, d'analyser en temps réel et à haute vitesse tous les paquets, et si besoin d'aspirer le trafic entrant, voire de mitiger, c'est-à-dire repérer tous les paquets IP non légitimes, tout en laissant passer les paquets IP légitimes.

Du côté des constructeurs d'objets connectés, tous les thermostats, toutes les webcams ou les imprimantes ne présentent pas de faille de sécurité, mais il s'agit d'un point préoccupant car **pour la plupart des fabricants, la sécurité n'a pas été la priorité dès le départ**, **ayant souvent été donnée à la rapidité de la mise à disposition du produit sur le marché pour répondre à un nouveau besoin**. Il faudrait que des normes minimales de sécurité puissent être définies comme le cryptage des données échangées sur le réseau ou l'exigence de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance et l'interdiction de mots de passe comme « 123456 » particulièrement vulnérables. Dans cet esprit, la Online Trust Alliance, qui regroupe des éditeurs comme Microsoft, Symantec (Norton) et AVG, a rédigé un guide des bonnes pratiques pour minimiser les risques de piratage. Les constructeurs d'objets connectés peuvent, par ailleurs, faire évaluer leurs systèmes de cryptage par des sociétés spécialisées, pour identifier les éventuelles vulnérabilités.

Comment se prémunir du piratage d'objets connectés ? Quels sont les bons comportements à adopter ? Que faire en cas de doute ?

Du côté des particuliers, il apparait préférable de privilégier les produits de sociétés à la pointe des questions de sécurité informatique, comme Google ou Apple. Il faut également installer régulièrement **les mises à jour de sécurité et les mises à jour logicielles**, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut **changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle.** Pour finir, il faut **limiter l'accès d'un objet connecté aux autres objets connectés dans la maison.** Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau. Par exemple, il n'est pas vraiment nécessaire que l'imprimante soit connectée à la télévision.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Attention danger : apprenez à vous protéger contre le piratage de vos objets connectés du quotidien | Atlantico.fr