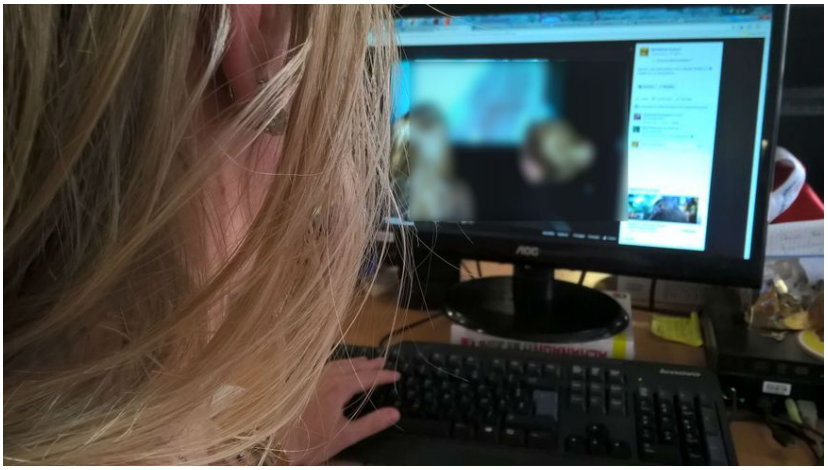
Un lycée met sur pied un projet pédagogique pour sensibiliser les jeunes au cyber-harcèlement

	Un lycée met sur pied un projet pédagogique pour sensibiliser les jeunes au cyber-harcèlement

Ces lycéens s'attaquent à un sujet sensible : montrer comment les jeunes peuvent devenir des cibles sur le net. Ce projet prendra la forme d'une expo photos au printemps prochain.

Facebook, twitter, instagram, snapchat et bien d'autres, il existe une multitude de médias et de réseaux sociaux qu'utilisent parfois avec frénésie les jeunes. Laurine a trouvé la parade pour éviter le cyber-harcèlement : « mes comptes sont protégés. C'est le premier truc que j'ai fait en m'inscrivant. Seuls mes amis peuvent voir mon profil ».
Tanguy, lui, a préféré s'éloigner des réseaux sociaux, les parents de ces lycéens et les enseignants de Rochefeuille les ont prévenus des atouts et des dangers du web : *« oui, ils nous dit que ce sont des réseaux de découverte et d'information mais aussi qu'il peut y avoir des gens qui peuvent nous faire souffrir moralement »*.
Il y a des chiffres qui font froid dans le dos. **40% des 13/17 ans avouent avoir subi une agression en ligne et 61% des ados harcelés disent penser au suicide**. Selon des statistiques publiées en janvier dernier, 3 ou 4 jeunes, victimes d'une agression en ligne, se suicident chaque année.

Pour toute information supplémentaire sur le cyber-harcèlement, le ministère de l'Education Nationale a mis en place un site spécialement dédié à ce sujet : faire face au cyber-harcèlement.

LE NET EXPERT
:
• **SENSIBILISATION / FORMATIONS** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• **MISE EN CONFORMITÉ RGPD / CNIL**
- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**
Besoin d'un Expert ? contactez-nous
Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Dans un lycée d'Ernée, un projet pédagogique pour sensibiliser les jeunes au cyber-harcèlement*

RGPD : Dans quel cas devez-vous désigner un DPO (Data Protection Officer) ?

	**RGPD : Dans quel cas devez-vous désigner un DPO (Data Protection Officer) ?**

L'article 37 du RGDP oblige les opérateurs (responsable de traitement et sous-traitant), dans certains cas, à désigner un DPO. Le G29 [1] encourage, par ailleurs, toutes les entreprises à procéder à la désignation d'un DPO, étant précisé qu'en cas de désignation « volontaire » d'un DPO, l'entreprise devra respecter l'ensemble des dispositions du RGDP y afférentes. Dans quel cas est-il obligatoire de désigner un DPO ?

Selon le RGPD (Réglement Général sur la Protection des Données), il est obligatoire de désigner un DPO dans trois différentes hypothèses :
1. Lorsque le traitement des données personnelles est effectué par une autorité publique ou un organisme public ;
2. Lorsque les *« activités de base »* du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un *« suivi régulier et systématique »* à *« grande échelle »* des personnes concernées ;
3. Lorsque les *« activités de base »* du responsable du traitement ou du sous-traitant consistent en un traitement à *« grande échelle »* des données *« particulières »*, c'est-à-dire sensibles au sens de la réglementation en matière de données personnelles (telles que les données de santé ou relatives à des infractions ou condamnations).

La première hypothèse n'appelle pas de commentaire particulier. En revanche, comment interpréter les notions d'« activités de base », « suivi régulier et systématique » et « grande échelle » des deux autres hypothèses ?

« activités de base »

Le G29 [1] précise qu'il s'agit des activités principales et non accessoires du responsable de traitement ou du sous-traitant. Autrement dit, ce sont les opérations de traitement de données personnelles qui découlent des opérations clés résultant de l'activité du responsable de traitement ou du sous-traitant. Le G29 [1] illustre son propos de plusieurs exemples. Ainsi, par exemple, une société ayant pour activité principale la surveillance d'espaces publics doit nécessairement mettre en œuvre des traitements de données personnelles résultant de cette surveillance, cette société devrait donc désigner un DPO. Au contraire, les opérations de traitement de données personnelles relatives aux salariés de l'entreprise, liées à l'établissement des fiches de paie, des congés, etc., ne seraient que des opérations accessoires.

« grande échelle »

Le G29 [1] ne définit pas plus que le RGDP cette notion et fournit seulement les critères pouvant être pris en compte pour déterminer s'il s'agit d'un traitement à « grande échelle ».
Devront ainsi être pris en compte :
• le nombre de personnes concernées ;
• le volume des données traitées ;
• la durée du traitement ;
• l'étendue géographique du traitement.
Cette notion, dont l'interprétation sera casuistique, place ainsi les entreprises face à une certaine insécurité juridique. Elles devront faire preuve de prudence quant à leur décision de ne pas désigner de DPO.

« suivi régulier et systématique »

Le G29[1] a défini, d'une part, la notion de *« suivi régulier »* comme étant un suivi *« en cours ou se produisant à des intervalles particuliers pour une période donnée »* ou *« récurrent ou répété à des moments fixes »* ou encore *« constant ou périodique »* et, d'autre part, la notion de *« suivi systématique »* comme étant un suivi *« produit selon un système »* ou *« pré-organisé, organisé ou méthodique »* ou *« adopté dans le cadre d'un plan général de collecte de données »* ou encore *« réalisé dans le cadre d'une stratégie globale »*. Cette notion doit nécessairement couvrir toute activité consistant à faire du suivi et du profilage en ligne des personnes.
Exemples d'activités traitant de manière régulière et systématique des données personnelles :
• Recherche et profilage sur Internet ;
• Opérateur de réseau de télécommunication ;
• Fournisseur de services de télécommunication ;
• Publicité comportementale ;
• Géolocalisation ;
• E-mail retargeting ;
• Vidéo surveillance ;
• Appareils connectés ;
• etc.

: Le G29 [1] recommande à toutes les entreprises traitant des données personnelles de désigner un DPO.

[1] : Le G29 est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Son organisation et ses missions sont définies par les articles 29 et 30 de la directive 95/46/CE, dont il tire sa dénomination sur la protection des données

---

Besoin de **vous mettre en conformité avec le RGPD** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Le statut du délégué à la protection des données personnelles. Par Jean-Baptiste Chanial et Cécile Louwers, Avocats.*

Faille de sécurité dans des caméras de vidéosurveillance FLIR

Faille de sécurité dans des caméras de vidéosurveillance FLIR

Un chercheur en sécurité informatique découvre comment accéder aux images de caméras de vidéosurveillance thermiques FLIR.

Infiltration possible dans des caméras de vidéosurveillance ! Étonnante révélation, fin septembre, par un internaute du nom de LiquidWorm. Ce chercheur en sécurité informatique a diffusé un code qui permet de découvrir que les caméras thermiques de vidéo surveillance de marque FLIR pouvaient être espionnées. FLIR Systems a des identifiants de connexion SSH codés en dur dans sa version distribuée sous Linux.

Bref, un accès aux images, via cet accès caché qui ne peut être modifié !

Cette backdoor est dénoncée quelques jours avant le salon Milipol qui se déroulera en novembre à Paris. Flir Systems y sera présent pour présenter son matériel.

Selon l'information diffusée par « Zero science« , les modèles de caméras incriminées sont les 10.0.2.43 (logiciel F/FC/PT/D) et les versions du micrologiciel 8.0.0.64: □□1.4.1, 1.4, 1.3.4 GA, 1.3.3 GA et 1.3.2 sont concernés par cette porte cachée…[lire la suite]

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :

- **CYBERCRIMINALITÉ**

- **PROTECTION DES DONNÉES PERSONNELLES**

- AU **RGPD**

- À LA **FONCTION DE DPO**

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)

- **MISE EN CONFORMITÉ RGPD** de vos traitements

- **SUIVI** de l'évolution de vos traitements

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)

- TÉLÉPHONES (récupération de **Photos / SMS**)

- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES

- **SÉCURITÉ** INFORMATIQUE

- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *ZATAZ Une porte cachée dans des caméras de vidéosurveillance FLIR – ZATAZ*

Une faille dans le Wifi pourrait compromettre vos données personnelles

	Une faille dans le Wifi pourrait compromettre vos données personnelles

Les réseaux WiFi du monde entier pourraient être piratés par le biais d'une faille de sécurité majeure, ont mis en garde lundi les autorités américaines et des chercheurs en Belgique.

C'est le protocole de chiffrement WPA2, utilisé par quasiment tous les réseaux WiFi pour se protéger des intrusions, qui est vulnérable: il est possible grâce à cette faille de décrypter toutes les données transmises en WiFi depuis des téléphones mobiles, ordinateurs, tablettes, etc.
Cette annonce vient confirmer la vulnérabilité des réseaux WiFi signalée depuis longtemps par les experts en cybersécurité. Mais, pour l'heure, on ne sait pas si des pirates ont effectivement utilisé cette faille à des fins malveillantes.
D'après des chercheurs de l'université belge de Louvain à l'origine de cette découverte, elle rend possible «le vol d'informations sensibles comme les numéros de cartes bancaires, les mots de passe, les messages instantanés, courriels, photos, etc.».
Selon la configuration du réseau, il est aussi possible d'injecter et de manipuler les données.
Par exemple, «un pirate pourrait insérer des « ransomware » (rançongiciels, NDLR) ou d'autres logiciels malveillants dans des sites internet», poursuivent les universitaires, qui ont baptisé la faille «KRACK» (Key Reinstallation Attack), car elle permet aux pirates d'insérer une nouvelle clé de sécurité dans les connexions WiFi…[lire la suite]

LE NET EXPERT
:
• **SENSIBILISATION / FORMATIONS** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• **MISE EN CONFORMITÉ RGPD / CNIL**
- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**
Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84)

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

Source : *WiFi: une faille qui pourrait compromettre vos données personnelles | TVA Nouvelles*

Alerte : Faille Wifi du WPA2. Risques et solutions pour s’en protéger

Alerte : Faille Wifi du WPA2. Risques et solutions pour s’en protéger

---

Dévoilée au public lundi 16 octobre 2017, Krack Attacks est une faille qui permet aux pirates d'espionner votre connexion wifi. Que doit-on craindre ? Comment se protéger ? Denis JACOPINI nous apporte des éléments de réponse.

Que doit-on craindre de cette faille découverte dans le WPA2 ?

Mathy Vanhoef, chercheur à l'université KU Leuven, a découvert une faille permettant d'intercepter des données transmises sur un réseau Wi-Fi, même lorsqu'il est protégé par le protocole WPA2. Pire, il est également possible d'injecter des données, et donc des malwares, en utilisant la technique découverte. Les réseaux domestiques aussi bien que les réseaux d'entreprises sont concernés, c'est donc une découverte majeure dans le domaine de la sécurité informatique.

La technique décrite par Mathy Vanhoef est appelée Key Reinstallation AttaCK, ce qui donne KRACK.

Comment se protéger de cette faille ?

Il n'y a pas de meilleur protocole que le WPA2. Il ne faut surtout pas revenir au protocole WEP. Changer de mot de passe ne sert à rien non plus. Le seul moyen de se protéger de cette faille est de mettre à jour votre système d'exploitation et les appareils concernés. Les acteurs du marché, fabricants ou éditeurs, ont été notifiés de cette faille le 14 juillet 2017. Certains l'ont comblée par avance comme Windows.

Il faut combler la faille à la fois sur les points d'accès et sur les clients, c'est-à-dire que patcher vos ordinateurs et smartphones ne vous dispense pas de mettre à jour votre routeur ou votre box Wi-Fi.

Même si, en tant qu'utilisateur, vous n'avez pas grand chose à faire de plus que de mettre à jour votre système d'exploitation et le firmware de votre point d'accès pour vous protéger contre la faille Krack Attacks, nous vous énumérons une liste de préconisations qui mises bout à bout, rendront plus difficile aux pirates les plus répandus l'intrusion dans votre Wifi.

Les Conseils de Denis JACOPINI pour avoir un Wifi le plus protégé possible :

1. Mettez à jour les systèmes d'exploitation de vos ordinateurs, smartphones, tablettes et objets.
2. Mettez à jour votre point d'accès Wifi (le firmware de votre Box, routeur…)
3. Modifier le SSID ;
4. Modifier le mot de passe par défaut ;
5. Filtrage des adresses MAC (facultatif car peu efficace);
6. Désactiver DHCP ;
7. Désactiver le MultiCast (pour les appareils qui disposent de cette fonction) ;
8. Désactiver le broadcast SSID (pour les appareils qui disposent de cette fonction) ;
9. Désactiver le WPS (pour les appareils qui disposent de cette fonction) ;
10. Utilisez un VPN ou un accès http**s** pour envoyer ou recevoir des informations confidentielles
11. Choisissez un cryptage fort de votre Clé WIFI :

- Technologie WPA 2 (également connu sous le nom IEEE 802.11i-2004) ;
- **Protocole de chiffrement AES** (ou CCMP) : **Important !**

Des personnes peuvent accéder librement à votre Wifi ?

Condition exigée depuis plusieurs années par les touristes et les nomades, il y a de fortes chances que les clients de votre hôtel, de vos chambres d'hôtes, de vos gîtes ou tout simplement des amis vous demandent absolument de disposer du Wifi.

Je tiens à vous rappeler que selon l'article L335-12 du Code de la Propriété Intellectuelle, l'abonné Internet reste le seul responsable des usages de sa connexion.

Ainsi, je ne peux que vous conseiller d'être prudent concernant l'usage de votre connexion Wifi par des tiers et de vous munir de moyens technologiques permettant de conserver une trace de chaque personne se connectant sur votre Wifi afin que si votre responsabilité en tant qu'abonné à Internet était recherchée, vous pourriez non seulement vous disculper mais également fournir tous les éléments permettant l'identification de l'individu fraudeur.

Les personnes intéressées par les détails techniques, et pointus, concernant la découverte de la faille WPA2 peuvent se rendre sur le site du chercheur dédié à ce sujet.

Bulletin d'alerte du CERT-FR

Va-t-on aller vers un WPA 3 ?

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *KRACK Attacks: Breaking WPA2 / KRACK : faille du Wi-Fi WPA2, quels appareils sont touchés ? Comment se protéger ?*

RGPD : quels changements pour les entreprises ?

RGPD : quels changements pour les entreprises ?

À l'occasion du salon des Assises de la Sécurité de Monaco qui a réuni plus de 2500 spécialistes de la sécurité informatique, le nouveau règlement européen sur les données personnelles était dans tous les esprits. Ce dernier, qui entrera en vigueur le 25 mai 2018, constitue une réelle avancée pour les citoyens, mais un sacré casse-tête pour les entreprises du secteur numérique qui n'ont plus que quelques mois pour se mettre en conformité.

« En tant que citoyen, on va avoir l'accès à nos données plus facilement ainsi qu'un droit d'effacement. Le texte a été conçu pour donner du pouvoir aux Européens sur les grands acteurs américains du numérique. S'ils refusent d'appliquer la loi, l'amende sera de 4 % du chiffre d'affaires mondial consolidé, ce qui est énorme même pour des sociétés comme Google. Ensuite, il y aura un certain nombre de choses pour lesquelles le citoyen devra donner son consentement. Les entreprises devront solliciter l'accord des utilisateurs de manière plus explicite et transparente pour chaque changement de règles générales d'usage, de conditions générales de ventes, etc. La loi permettra également de contacter les acteurs du numérique pour demander la suppression de l'intégralité de ses données bien plus facilement qu'à l'heure actuelle. Par ailleurs, les citoyens vont avoir le droit à la portabilité de leurs données. Concrètement, si un jour vous voulez quitter Gmail pour aller chez Hotmail, vous pourrez demander la portabilité de vos emails, les récupérer et les passer sur un autre compte. Cela renforce l'idée que les données que l'on crée nous appartiennent. En tant que citoyen, c'est une avancée extraordinaire qui n'a aucun équivalent dans le monde ».
Des changements dont on ne peut que se réjouir…[lire la suite]

Besoin de **vous mettre en conformité avec le RGPD** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la 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

Source : *Données personnelles : que va changer le nouveau règlement européen ?*

Propos de Jérôme Billois, Senior Manager chez Wavestone

---

7 conseils pour se protéger les enfants des cyber pédophiles

7 conseils pour se protéger les enfants des cyber pédophiles

Les spécialistes de la cybercriminalité de la police judiciaire niçoise tirent la sonnette d'alarme. Trop d'enfants sont laissés seuls avec un ordinateur dans leur chambre, exposés au danger. Voici quelques conseils pour s'en prémunir.

1. Mettez le moins de photos personnelles possibles sur les réseaux sociaux, de vous, de votre famille ;
2. On ne divulgue pas le vrai nom de l'enfant, ou sa photo sur Internet ;
3. Il ne doit pas accepter de nouveaux contacts inconnus: ni par e-mail, ni sur les réseaux et autres applications sociales ;
4. Les parents doivent se tenir informés des risques ;
5. Sensibiliser les enfants lors d'un dialogue familial constructif ;
6. Ne jamais laisser un ordinateur dans une chambre d'enfant, seul, sans surveillance. *« Il doit se trouver dans la pièce principale, sans code d'accès. » ;*
7. Ne pas laisser les enfants opérer des achats seuls sur le Net.

L'Éducation nationale a publié une étude de 2014: 4,5% des collégiens disaient subir un cyber harcèlement, c'est-à-dire une violence verbale, physique ou psychologique répétée. Un élève sur cinq a déjà été victime de cyberviolence…[lire la suite]

LE NET EXPERT :

• **SENSIBILISATION / FORMATIONS** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA FONCTION DE DPO

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

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

Source : *7 conseils pour se protéger des cyber pédophiles – Nice-Matin*

Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

---

Android est à nouveau visé par un malware vendredi 13 octobre : DoubleLocker, un redoutable ransomware, chiffre les fichiers sur le smartphone et change son mot de passe, même s'il n'est pas rooté. Des chercheurs de ESET à l'origine de la découverte expliquent que ce ransomware se cache dans un APK d'Adobe Flash Player ce qui peut augmenter le risque d'une propagation rapide. La seule façon de s'en débarrasser c'est de réinitialiser le smartphone. Ce serait le pire ransomware détecté à ce jour.

Les chercheurs de ESET viennent de découvrir le premier **ransomware Android** capable de prendre le contrôle total de votre smartphone. Il parvient à obtenir des droits administrateur même sur des smartphone non-rootés, ce qui le rend extrêmement dangereux. Android/DoubleLocker.A est basé sur un trojan bancaire modifié pour changer le code PIN du smartphone sur lequel il est installé et chiffrer ses données. Les chercheurs précisent qu'un tel mode d'action était jusqu'ici du jamais vu.

Android : le pire ransomware jamais détecté, DoubleLocker, bloque et chiffre les smartphones

Le chercheur Lukáš Štefanko à l'origine de la découverte de DoubleLocker ajoute : « *à cause du fait qu'il trouve son origine dans un malware bancaire, DoubleLocker pourrait très bien être modifié pour devenir ce que l'on pourrait appeler un malware bancaire-rançon. Un malware à deux étages, qui essaie d'abord de voler vos données bancaires et/ou vider votre compte ou compte PayPal, puis bloque votre appareil et ses données pour exiger une rançon… spéculation de côté, on a détecté la version test d'un tel malware dans la nature pratiquement en même temps, en mai 2017*« .

On trouve DoubleLocker dans des APK de Flash Player sur de sites compromis méthode déjà utilisée par d'autres malwares. Une fois lancée, l'application lance un service d'accessibilité baptisé Google Play Service. Le malware obtient ensuite tout seul les permissions d'accessibilité, puis les utilise pour activer les droits administrateurs et se définir comme *Launcher* par défaut. Dès que l'utilisateur appuie sur le bouton Home, le malware est activé. Le PIN est alors changé et les fichiers du répertoire principal chiffrés. Le ransomware demande alors de payer 0.013 BTC dans les 24 heures, soit environ 62 euros au moment où nous écrivons ces lignes. Les chercheurs relèvent que les fichiers chiffrés, qui prennent l'extension .cryeye, ne sont pas supprimés à l'issue de ce délai…[lire la suite]

QUE PROPOSE **LE NET EXPERT**, (**EXPERT INFORMATIQUE ASSERMENTÉ**) :

• SENSIBILISATIONS / FORMATIONS (n° formateur)

• RECHERCHE DE PREUVES

• EXPERTISES & AUDITS (certifié ISO 27005)

NOTRE MÉTIER :

• SENSIBILISATION / FORMATIONS :

- **CYBERCRIMINALITÉ**

- **PROTECTION DES DONNÉES PERSONNELLES**

- AU **RGPD**

- À LA FONCTION DE DPO

• RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)

- TÉLÉPHONES (récupération de **Photos / SMS**)

- SYSTÈMES NUMÉRIQUES

• EXPERTISES & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES

- **SÉCURITÉ** INFORMATIQUE

- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

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

Source : *Android : le pire ransomware jamais détecté fait ses premières victimes*

RGPD : Ce que les consommateurs doivent savoir

	**RGPD : Ce que les consommateurs doivent savoir**

Les consommateurs doivent comprendre clairement ce qu'ils acceptent comme traitements sur les sites e-commerce et la portée de leurs consentements.

Les techniques modernes de marketing e-Commerce (retargetting, suggestions de produits…) doivent être explicitement acceptées par les particuliers. Ils disposent également d'un accès direct à leurs informations personnelles. En pratique, ils pourront demander la portabilité de leurs informations (données de commandes, listes d'envie…) et obtenir un double consentement pour leurs enfants. En cas de fuite de données, l'internaute sera informé dans les 72 heures par l'entreprise, la responsabilité pouvant incomber au sous-traitant responsable de la fuite ou à l'hébergeur si ce dernier a été attaqué. Pour s'assurer du respect de ces nouveaux droits, le législateur a rendu possibles les actions collectives via des associations…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la 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

Source : *Le RGPD : 81% des entreprises ne seront pas en conformité en mai 2018 – Global Security Mag Online*

RGPD : Comment le mettre en oeuvre dans le e-Commerce

RGPD : Comment le mettre en oeuvre dans le e-Commerce

D'ici mai 2018 toutes les entreprises devront respecter la nouvelle réglementation. Cette mise en œuvre implique une bonne compréhension à la fois des obligations et des moyens d'y parvenir.

Les sites e-Commerce devront assurer le plus haut niveau possible de protection des données. Pour garantir la sécurité des données personnelles de leurs clients les marchands devront déployer tous les moyens techniques et respecter des règles strictes : la mise en œuvre d'un registre de consentements, la conservation des données, la sécurisation des mails transactionnels, le cryptage des mots de passe…. Un délégué à la protection des données (DPO) sera désigné pour assurer la mise en place et le suivi de ces actions.

On passe dans une logique de responsabilisation totale de l'entreprise, une nécessité au regard des plus de 170 000 sites ne seront pas en conformité avec le règlement européen en mai 2018.

Rappelons que chaque jour des milliers d'attaques visent la totalité des acteurs du e-Commerce. La sécurité des données et des infrastructures techniques sont les enjeux majeurs du monde du web. Le nombre total de cyber-attaques a augmenté de 35% en l'espace d'un an. En France nous en avons recensé plus de 15 millions au 1er trimestre 2017 ce qui représente 4,4% des attaques mondiales. Un cadre contraignant pour les entreprises et des impacts majeurs à court terme Le baromètre RGPD1 démontre qu'à ce jour 44% des entreprises considèrent déjà qu'elles ne seront que partiellement conformes. Les sanctions en cas de manquement aux obligations imposées par la règlementation sont financières et indexées sur le chiffre d'affaires de l'entreprise. Elles peuvent atteindre de 10 à 20 millions d'euros ou 2 à 4% du CA, la sanction la plus élevée sera retenue. Un nouveau concept émerge : le « Privacy By design », un gage de qualité et de réassurance pour les entrepreneurs à la recherche d'une sécurisation optimale des données clients. Un site conçu en « Privacy by Design » garantit qu'aucun module n'a été ajouté à la structure du site et que la solution a été élaborée avec la protection des données comme prérequis à chaque étape de la mise en ligne du site…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la 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

Source : *Le RGPD : 81% des entreprises ne seront pas en conformité en mai 2018 — Global Security Mag Online*