Conseils d’un spécialiste RGPD : Comment se mettre en conformité ?

Mettre un établissement en conformité avec le RGPD nécessite la réalisation de certaines tâches plus techniques et organisationnelles que juridiques, même si ce dernier domaine doit aussi être maîtrisé par le DPO (Data Protection Officer).

Une mise en conformité nécessitera donc une excellente connaissance en matière de sécurité informatique, d'analyse de risques, d'organisation des services, de transferts de flux de données et enfin de pédagogie pour que l'ensemble des employés de l'établissement comprenne le but de la démarche pour devenir acteur.

Les étapes à respecter sont :

1. Désigner un élément pilote ;
2. Établir une cartographie de l'ensemble des traitements de données de létablissement ;
3. Vérifier les spécificités et dispenses propres à l'activité ou au statut de l'établissement ;
4. Analyser chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement ;
5. Prioriser ses actions à mener
6. Tenir un registre dans lequel seront référencés les différents traitements des données à caractère personnel conformes et à modifier ;
7. Gérer les risques par une analyse des impacts
8. Mettre en place des procédures
9. Documenter et tenir compte de l'évolutio06n de l'entreprise et s'assurer que la conformité est maintenue.

Ne pas oublier que le RGPD prévoit l'obligation de déclarer une faille, entraînant une fuite ou un vol de données personnelles, auprès de l'autorité de contrôle dans les 72 heures suivant l'incident. Le DPO pourra accompagner l'établissement dans la gestion de ces incidents.

Enfin, le DPO devra traiter les demandes d'accès à ses données personnelles, formulées par exemple par un client.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
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
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)

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

Source : Denis JACOPINI et *Data Protection Officer : un gardien pour les données personnelles*

Des détenteurs de Bitcoins détroussés par un virus

Des détenteurs de Bitcoins détroussés par un virus

« Crypto Shuffler », un virus identifié par la société de sécurité informatique russe Kaspersky Lab, a permis de voler l'équivalent d'environ 140.000 dollars.

La société de sécurité informatique russe Kaspersky Labs a annoncé jeudi avoir identifié un virus qui fait les poches des détenteurs de monnaies virtuelles. Ce virus, nommé « Crypto Shuffler », aurait déjà permis de voler *« l'équivalent d'environ 140.000 dollars en bitcoins. Les montants volés dans d'autres monnaies virtuelles vont de quelques dollars à plusieurs milliers de dollars »*, a mis en garde Kaspersky Labs dans un communiqué, sans préciser où sévissait le virus.

Pour commettre son larcin, le virus s'infiltre sur les ordinateurs de ses victimes puis frappe lorsque qu'un détenteur d'argent virtuel copie-colle le code d'identification du destinataire d'un paiement, lui substituant ses propres coordonnées…[lire la suite]

Réaction de Denis JACOPINI :

Vous ne savez pas si vous êtes infecté ? Utilisez votre antivirus préféré et lancez une vérification de votre ordinateur pour savoir si votre ordinateur ne serait pas infecté par **« Crypto Shuffler »**. Si votre cyberbouclier l'a détecté, il devrait aussi vous en débarrasser. Dans le doute, abstenez-vous de réaliser des transactions en bitcoin pour l'instant.

Réagissez à cet article

Source : *Des détenteurs de Bitcoins détroussés par un virus*

Mise en conformité RGPD : Mode d'emploi

Mettre un établissement en conformité avec le RGPD nécessite la réalisation de certaines tâches plus techniques et organisationnelles que juridiques, même si ce dernier domaine doit aussi être maîtrisé par le DPO (Data Protection Officer).

Une mise en conformité nécessitera donc une excellente connaissance en matière de sécurité informatique, d'analyse de risques, d'organisation des services, de transferts de flux de données et enfin de pédagogie pour que l'ensemble des employés de l'établissement comprenne le but de la démarche pour devenir acteur.

Les étapes à respecter sont :

1. Établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique ;
2. Vérifier les spécificités et dispenses propres à l'activité ou au statut de l'établissement ;
3. Analyser chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement ;
4. Tenir un registre dans lequel seront référencés les différents traitements des données à caractère personnel conformes et à modifier ;
5. Tenir compte de l'évolution de l'entreprise et s'assurer que la conformité est maintenue dans le temps.

Ne pas oublier que le RGPD prévoit l'obligation de déclarer une faille, entraînant une fuite ou un vol de données personnelles, auprès de l'autorité de contrôle dans les 72 heures suivant l'incident. Le DPO pourra accompagner l'établissement dans la gestion de ces incidents.
Enfin, le DPO devra traiter les demandes d'accès à ses données personnelles, formulées par exemple par un client.

Le DPO obligatoire pour qui ?

Le Règlement général sur la protection des données (RGPD), qui sera effectif le 25 mai 2018, rend obligatoire la nomination d'un Data Protection Officer (DPO) pour les entités publiques et certaines entreprises. « *Ce délégué à la protection des données sera au cœur du nouveau cadre juridique européen* », résume le groupe de travail G29, qui réunit les « Cnil européennes ». La nomination d'un DPO sera donc incontournable pour toutes les entités publiques du Vieux Continent, telles que les collectivités locales, les hôpitaux, les universités… Côté entreprises, le DPO sera obligatoire pour celles dont l'activité principale les amènent à réaliser à grande échelle un suivi régulier et systématique des personnes (profiling), ou de traiter des données «sensibles» – santé, opinions politiques ou religieuses, orientation sexuelle, etc. – ou des données relatives à des condamnations et infractions pénales.

Parmi les entreprises qui devraient être concernées par cette obligation : des sociétés d'e-commerce ou de marketing digital, des banques et assurances, des établissements de soins ou encore des entreprises du secteur des télécoms.

« *Même lorsque le RGPD n'exige pas spécifiquement la nomination d'un DPO, les entreprises pourront parfois estimer utile d'en désigner un sur une base volontaire* », poursuit le G29. Car en effet, le nouveau règlement européen renforce très sensiblement les responsabilités des entreprises en matière de protection des données personnelles et surtout les sanctions. En France, le plafond maximal des sanctions de la Cnil est déjà passé de 150000 euros à 3 millions d'euros avec la Loi pour une république numérique de 2016. Les amendes prévues par le RGPD peuvent quant à elles atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial. De quoi inciter de nombreuses entreprises à nommer un DPO pour s'assurer de leur conformité avec le nouveau règlement.

Le DPO comment ?

Le premier travail d'un DPO sera d'établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique. Pour cela, le DPO devra se rapprocher des représentants des différentes instances de l'organisation pour rassembler les informations nécessaires. Une fois cette cartographie réalisée, le DPO analysera chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement.

Le DPO combien ?

Il n'existe pas encore de grille salariale établie pour le DPO, ses revenus devraient être au moins comparables à ceux du CIL, soit environ 50000 euros par an. La pénurie attendue de candidats au poste de DPO devrait même tirer les salaires vers haut. La Cnil prévoit que plus de 80000 organisations, publiques ou privés, devront se doter d'un DPO en France.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

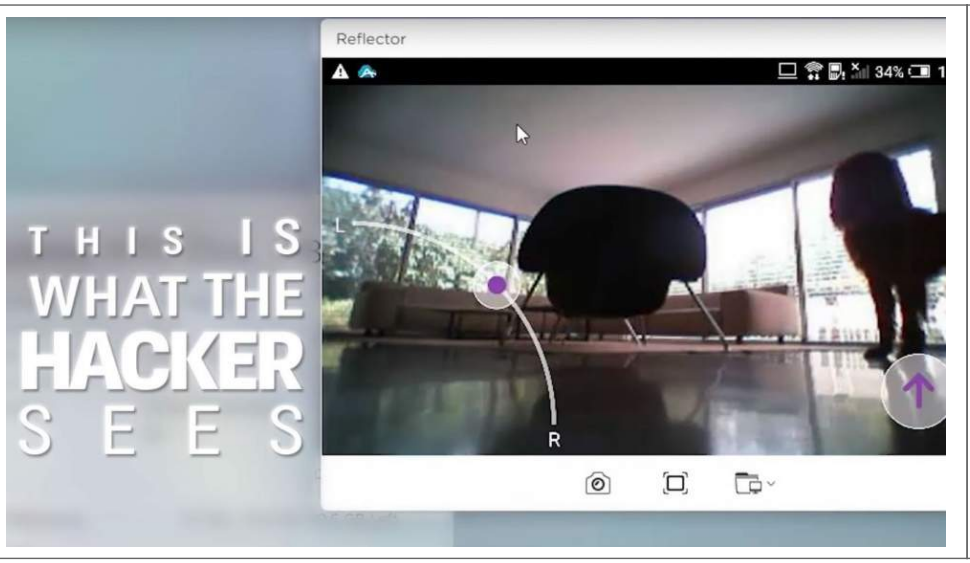
Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
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
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)

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

Source : Denis JACOPINI et *Data Protection Officer : un gardien pour les données personnelles*

Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés



Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés

---

La faille de sécurité « HomeHack » permettait de prendre le contrôle de n'importe quel objet connecté du fabricant coréen LG. Mais appliquée aux robots aspirateurs, elle serait un moyen offert aux hackers d'observer l'intérieur des maisons.

Pratiques parce qu'ils nous simplifient la vie et qu'on peut les piloter depuis une simple application mobile, les objets connectés sont aussi potentiellement de véritables chevaux de Troie dans notre intimité.
Les experts de l'entreprise de cybersécurité Check Point ont révélé une faille de sécurité, « HomeHack », via laquelle il était possible de prendre le contrôle à distance d'un aspirateur LG Hom-Bot et d'espionner l'intérieur d'une maison au moyen de la caméra intégrée, comme le montre cette vidéo :
http://www.youtube.com/embed/BnAHfZWPaCs
Communiqué à LG en juillet dernier, le problème a depuis été corrigé par le constructeur en septembre, mais une question demeure : comment être certain que les objets connectés qui nous entourent sont assez sécurisés ? En effet, il est régulièrement proposé aux clients de synchroniser l'ensemble de leurs appareils sur un même système, ici l'application mobile SmartThinQ de LG, disponible sur Android et iOS…[lire la suite]

Réagissez à cet article

Source : *Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés*

Alerte : 2 applications infectées sous Android et macOS

Alerte : 2 applications infectées sous Android et macOS

Les chercheurs ESET® ont découvert 2 menaces, l'une agissant sous macOS® et l'autre sous Android™. Le malware sous macOS a fait 1 000 victimes. Quant à la menace sous Android, plus de 5 500 téléchargements ont été effectués.

OSX/Proton, ou le voleur de données

Les chercheurs ESET sont entrés en contact avec l'éditeur Eltima®, à la suite de la découverte d'une version de leurs applications compromises. Environ 1 000 utilisateurs auraient été infectés par le kit OSX/Proton, disponible sur les marchés underground.

Les applications Elmedia Player® (lecteur multimédia) et Folx® (gestionnaire de téléchargement) sont concernées. OSX/Proton est une backdoor qui possède de nombreuses fonctionnalités et permet de récupérer :

• les détails de l'OS : numéro de série de l'appareil, nom complet de l'utilisateur actuel…
• les informations provenant des navigateurs : historique, cookies, marque-pages, données de connexion…
• les portefeuilles de cryptomonnaie : Electrum / Bitcoin Core / Armory
• les données contenues dans ./ssh
• le trousseau macOS grâce à une version modifiée de chainbreaker
• la configuration du VPN Tunnelblick®
• les données GnuPG
• les données de 1password
• la liste de toutes les applications installées

ESET fournit la liste des indicateurs de compromission ainsi que la méthode de nettoyage en cas d'infection sur le lien suivant : https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/

Cryptomonnaie : une version compromise de Poloniex® sur Google™ Play

Avec plus de 100 cryptomonnaies au compteur, Poloniex est l'un des principaux sites d'échange de cryptomonnaie au monde. Les cyberpirates ont profité du fait qu'il n'y ait pas d'application officielle de Poloniex pour développer 2 versions malicieuses.

En plus de récolter les identifiants de connexion à Poloniex, les cybercriminels incitent les victimes à leur accorder l'accès à leur compte Gmail™. Les pirates peuvent ensuite effectuer des transactions depuis le compte de l'utilisateur et effacer toutes les notifications de connexions et de transactions non autorisées depuis la boîte de réception.

La première des applications malveillantes se nomme « POLONIEX » et a été installée 5 000 fois, malgré les avis négatifs. La deuxième application, « POLONIEX EXCHANGE », a été téléchargée 500 fois avant d'être retirée du Google store, suite à la notification d'ESET.

Vous trouverez les mécanismes utilisés par les pirates et les moyens de se prémunir contre ce malware en cliquant sur le lien suivant :
https://www.welivesecurity.com/2017/10/23/fake-cryptocurrency-apps-google-harvesting-credentials/

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**

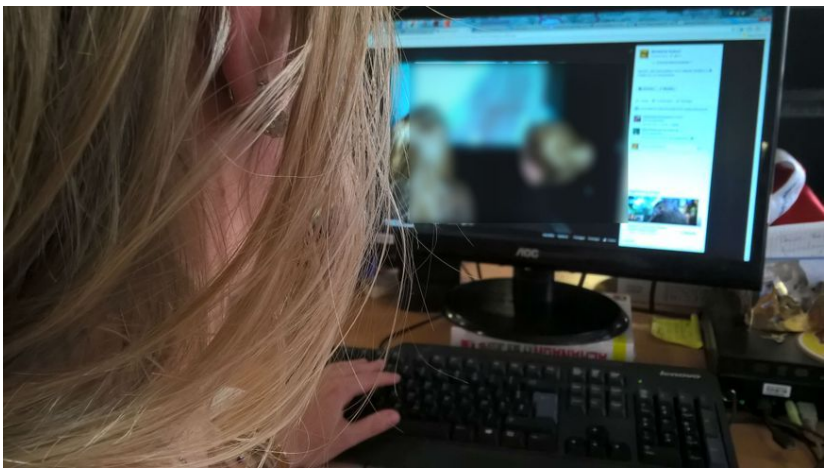
Besoin d'un Expert ? contactez-nous

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 : *Boîte de réception (715) – denis.jacopini@gmail.com – Gmail*

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.

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

---

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]

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 ?

Réagissez à cet article

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