

RGPD : Ça ne se passera plus comme ça !



Selon une nouvelle étude de CyberArk, près de deux tiers des organisations françaises (62 %) ayant été victime d'une cyberattaque n'ont pas avoué à leurs clients que leurs données personnelles avaient été compromises. Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, les entreprises qui n'agiront pas pour être plus transparentes s'exposeront à d'importantes sanctions.

« Malheureusement, il n'est pas rare que les organisations décident de cacher l'ampleur des dégâts causés par une cyberattaque. Comme nous l'avons vu lors des violations de données chez Yahoo !, Uber et bien d'autres, les entreprises peuvent soit dissimuler des informations intentionnellement, soit constater que l'attaque a finalement été plus nuisible que précédemment annoncé, déclare Jean-François Pruvot, Regional Director Europe West and South Europe, Sales chez CyberArk. Dès l'année prochaine, ce type de comportement sera lourdement sanctionné, en raison des amendes qui seront infligées en vertu du RGPD en cas de manque de conformité. L'autre point étonnant de cette étude réside dans cette obstination à appliquer des pratiques dépassées en matière de sécurité, et le manque de cohésion entre les leaders commerciaux et les responsables de la sécurité IT, malgré leur capacité à identifier les risques encourus et les cyberattaques qui font sans cesse la une des journaux. »...[lire la suite]

Complément de Denis JACOPINI :

À partir du 25 mai 2018 les entreprises, filiales ou agences françaises ont obligation de signaler à la CNIL tout vol de données ou piratage ayant entraîné une exposition des données détenues auprès de personnes non autorisées.

Pour qu'il y ait violation, 3 conditions doivent être réunies :

- Vous avez mis en œuvre un traitement de données personnelles ;
- Ces données ont fait l'objet d'une violation (destruction, perte, altération, divulgation ou un accès non autorisé à des données personnelles, de manière accidentelle ou illicite) ;
- Cette violation est intervenue dans le cadre de votre activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de votre service de téléphonie ou d'accès à d'internet).

La notification doit être transmise à la CNIL dans les 24h de la constatation de la violation. Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

Une notification initiale dans les 24 heures de la constatation de la violation ;

Puis, une notification complémentaire dans le délai de 72 heures après la notification initiale.

Le formulaire à utiliser est celui-ci :



https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

Besoin d'un **accompagnement pour 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 :

Mise en conformité RGPD : Mode d'emploi

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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données 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 DITET n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : CNIL et *Enquête CyberArk* : 62 % des entreprises françaises n'ont pas signalé des violations de données à leurs clients – *Global Security Mag Online*

Webmaster ou responsables de sites : comment répondre aux demandes d'effacement de données personnelles publiées sur votre site ?

	Webmaster ou responsables de sites : comment répondre aux demandes d'effacement de données personnelles publiées sur votre site ?
---	--

Tout internaute a la possibilité de demander à un responsable de site Internet que ses données personnelles ne soient plus diffusées en ligne, et que les pages diffusant ces données ne soient plus indexées par les moteurs de recherche.

En tant que responsable d'un site internet, comment répondre à ces demandes ?

Le règlement européen sur la protection des données qui entre en vigueur en mai 2018 modifie les modalités d'exercice du droit d'opposition qui sera prévu à l'article 21 et introduit un droit à l'effacement à l'article 17.

• Une demande d'opposition ne sera plus soumise à la justification de motifs légitimes.

• En conséquence, dès qu'il sera saisi d'une telle demande, le responsable de traitement ne devra plus traiter les données, sauf à prouver qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou pour la constatation, l'exercice ou la défense de droits en justice.

• Cette demande devra être traitée « dans les meilleurs délais » et sous 1 mois maximum à compter de la réception de la demande (article 12) contre 2 mois aujourd'hui.

Je reçois un courrier me demandant de supprimer des données personnelles que faire ?

Etape 1 : vérifier que la demande est complète

Une demande d'opposition de la part d'un internaute doit comporter *a minima* :

- Le motif de la demande (jusqu'au 25 mai 2018, date d'entrée en vigueur du règlement européen)
- Un moyen d'identifier le demandeur (ex. copie d'un justificatif d'identité ; une copie noir et blanc du recto suffit, vous ne devez pas conserver cette pièce au-delà du temps nécessaire pour traiter la demande). L'identification du demandeur peut également être réalisée par la mise en place d'une procédure *ad hoc* par le responsable de traitement.

Etape 2 : répondre par écrit à la demande

Vous disposez d'un délai légal de 1 mois à compter de la date de réception du courrier pour répondre à la demande.

3 options s'offrent à vous :

- Demander des compléments si la demande est imprécise ou incomplète (absence du justificatif d'identité par exemple). Vous devez répondre au demandeur en lui précisant les compléments à vous fournir pour pouvoir traiter sa demande. Vous pouvez également lui demander toute précision utile vous permettant de faciliter le traitement de la demande (urls précises faisant l'objet de la demande, inventaire des données à effacer...). Lorsque vous demandez des compléments, le délai est suspendu et court à nouveau une fois ces éléments fournis par le demandeur.
- Refuser de donner suite à la demande de l'internaute. Dans ce cas, vous devez répondre par écrit au demandeur et impérativement motiver votre décision de refus.
- Répondre positivement à la demande. Dans ce cas, vous procéderez en 3 temps :
 1. En supprimant ou modifiant les pages en cause de votre site Internet
 2. En procédant à la mise à jour du cache des moteurs de recherches.
 3. En confirmant la suppression ou la modification au demandeur

Comment répondre favorablement à une demande d'opposition ?

En fonction de la demande de l'internaute (suppression du contenu, correction, anonymisation, désindexation des moteurs de recherches) vous disposez de différentes solutions pour y répondre.

Tout contenu web a par défaut vocation à être indexé par les Moteurs de recherche. Ainsi, la prise en compte effective d'une demande d'opposition à la diffusion en ligne de données personnelles implique, outre la suppression ou modification du contenu, de s'assurer également de sa désindexation par les moteurs de recherche.[lire la suite]

Besoin d'un accompagnement pour 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 :

Mise en conformité RGPD : Mode d'emploi

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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles



Denis JACQUIN est Expert Judiciaire en Informatique spécialisée 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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (partenaire de la CERT INTERPOL)
- Formation de CIL/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 : *Webmaster ou responsables de sites : comment répondre aux demandes d'effacement de données personnelles publiées sur votre site ?* | CNIL

Une victime de piratage de Lunel raconte son « traumatisme »



Une victime de
piratage de
Lunel raconte
son
« traumatisme »

La lutte contre la cybercriminalité se joue aussi en région. Parmi les victimes de ces nouvelles pratiques de fraude numérique, des particuliers mais aussi des entreprises. Bruno a récemment vécu une attaque informatique dans son agence immobilière à Lunel. Il raconte.

C'était il y a un mois, au retour d'un week-end. Bruno rouvre son agence immobilière et se retrouve sans téléphone. La société qui gère son système de téléphonie déportée le prévient alors : « Nous vous avons coupé parce que nous nous sommes rendu compte qu'il y avait un problème. » Les lignes de l'entreprise ont en fait été victimes durant le week-end d'un hacker. Lequel a pu se brancher sur ses lignes et les a dirigées vers un service surtaxé au lieu du bas prix initial choisi par le chef d'entreprise et son opérateur.

« Et s'ils avaient pris nos fichiers ? »

Repérée très rapidement, la fraude n'aura eu que peu d'incidence financière : « 300 à 400 euros de téléphone volé, précise Bruno. Mais c'est un véritable traumatisme ! Quand j'ai appris ça, il y a eu dix minutes de flottement, où je me suis posé beaucoup de questions ! Ce n'est pas tant ce qu'ils m'ont volé, mais ce qu'ils auraient pu faire. Ils ont pu rentrer. Et s'ils avaient pris nos fichiers ? Quasiment toutes nos données sont informatisées... Ils peuvent foutre en l'air une entreprise ! » Cinq cents dossiers de propriétaires et leur historique, toute la comptabilité de l'agence...

Bruno a immédiatement porté plainte à la gendarmerie de Lunel. « Ils ont un super-service. Ils ont été à l'écoute, ont pris le problème au sérieux et très rapidement, ils sont remontés jusqu'à la source, dans un pays lointain. Vers Israël, je crois. Ils ont retrouvé le hacker, même s'il est impossible d'aller le chercher. Vous vous rendez compte de ce que ces gens sont capables de faire ! » Et de saluer le travail d'investigations des militaires.

« Les gens paient. Ils n'ont pas d'autre choix. »

Ces derniers rencontrent d'ailleurs souvent ce type de piratage des autocom ces derniers temps, avec des montants qui peuvent s'envoler à plusieurs dizaines de milliers d'euros si la fraude n'est pas détectée assez tôt. Bruno, lui, a finalement été remboursé par son opérateur. Il a renforcé son système de façon simple.

Ce qui n'empêche pas l'inquiétude de se retrouver un jour avec ses données prises en otage ou chiffrées...

« J'ai plusieurs collègues qui ont répondu à des e-mails et qui se sont retrouvés victimes d'un chantage. Les gens paient. Ils n'ont pas d'autre choix » explique-t-il.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister 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 ».

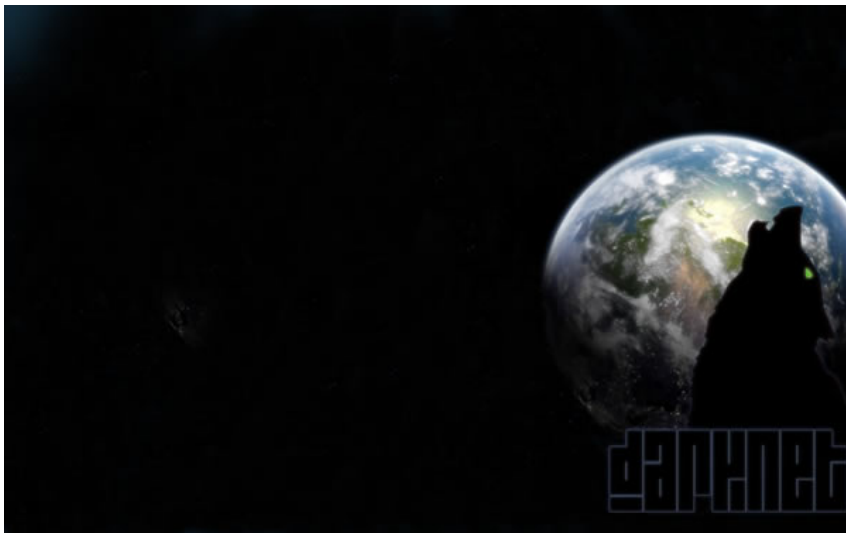
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation 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.



[Contactez-nous](#)

Original de l'article mis en page : Cybercriminalité en région : une victime raconte son « traumatisme »
Réagissez à cet article

DarkNet : Découverte d'une base de données de 1,4 milliards d'identifiants et mots de passe en clair



DarkNet :
Découverte
d'une base de
données de 1,4
milliards
d'identifiants
et mots de
passe en clair

Open data chez les cybercriminels ! La découverte a été annoncée par la société spécialisée en sécurité informatique 4IQ. Il s'agit de la plus importante base de données pirate jamais découverte en ligne. Elle pèse 41 Go. La découverte de 41Q date du 5 décembre et la société indique qu'elle se trouve sur un espace du Dark Web, sans préciser l'endroit (on se doute bien pourquoi). La base de donnée en question contient exactement **1 400 553 869 identifiants et mots de passe en clair**, et un moteur de recherche dédié permet d'y accéder et d'y naviguer. Du vrai open data chez les pirates !..

	Count	Password	Count	Password	
1	8218720	123456	21	370802	000000
2	3103003	123456789	22	354784	123
3	1861380	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1279179	111111	25	311371	1qaz!@WSX
6	1120222	12345678	26	300279	123qwe
7	1085144	abc123	27	299904	12!@12
8	999930	1234567	28	288838	029800
9	952440	00000000	29	291132	a123456
10	879024	1234567890	30	276473	qwe123
11	868640	123123	31	270488	1q2w3e4r
12	834488	12345	32	268121	qwertyui
13	821078	helloworld	33	263805	7777777
14	584344	iloveyou	34	250278	123abc
15	527158	1q2w3e4r5	35	250732	qwerty123
16	470582	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241486	987654321
18	417878	12345678	38	227701	222222
19	398114	123321	39	228786	000000
20	371627	654321	40	220383	112233

N'oubliez pas les règles de sécurité pour réduire les risques de piratage de vos comptes ne ligne : changez régulièrement vos mots de passe, utilisez un générateur de mot de passe sécurisé (ou activez la double authentification lorsque c'est possible) et stockez vos identifiants / mots de passe de manière sécurisée via un gestionnaire de mot de passe.[lire la suite]

- LE NET EXPERT
 - ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVE de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITE
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
 - RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORIGINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
 - EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JURIDIQUES | 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 DORTEFP (Numéro formateur n°93 84 03041 84).



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » et Cybercriminalité et est RGPD (Vice-Déan du Données à Caractère Personnel).

- Accompagnement à la mise en place du RGPD
- Cartographie et traitement des données : à la demande ou en lots (Big Data)
- Audits sécurité (ISO 27005)
- Expertises techniques et juridiques :
 - Recherche de preuves numériques, données bancaires, emails, contenus, déclarations de clients...
- Expertise de la preuve de non connaissance



Le Net Expert
INFORMATIQUE
Pratiquant des Données Numériques

[Contactez-nous](#)

Réagissez à cet article

Source : *DarkNet : Découverte d'une base de données de 1,4 milliards d'identifiants et mots de passe en clair | UnderNews*

RGPD : Vol de données : la nouvelle norme



RGPD
Vol de
données :
la
nouvelle
norme

A six mois de l'entrée en vigueur du nouveau règlement européen sur la protection des données personnelles (RGPD) le 25 mai 2018 prochain, Proofpoint, spécialiste de la cybersécurité, dévoile les résultats de son étude paneuropéenne (Royaume-Uni, France, Allemagne) analysant le niveau de préparation des entreprises.

Les cyberattaques sont malheureusement devenues monnaie courante pour les entreprises qui doivent désormais intégrer pleinement les risques associés à leurs stratégies de sécurité pour se protéger. A l'image du piratage d'Equifax exposant les données personnelles de plus de 145 millions de citoyens américains ou du ransomware Wannacry ayant affecté plus de 200,000 ordinateurs dans 150 pays, tout le monde est concerné.

La France, semble particulièrement affectée, avec 61% des entreprises françaises qui déclarent avoir subi un vol de données personnelles durant les deux années écoulées (54% au Royaume Uni et 56% en Allemagne) et 78% d'entre elles qui redoutent un vol de données dans les 12 mois à venir (54% au Royaume-Uni et 46% en Allemagne).

Niveau de préparation RGPD : un décalage évident entre perception et réalité

Si les décideurs IT français semblent mieux préparés que leurs voisins (51% des répondants français pensent que leur organisation est déjà en conformité avec la réglementation RGPD, contre 45% au Royaume-Uni et 35% en Allemagne), l'étude révèle que plus d'une entreprise française sur cinq (22%) ne sera toujours pas en conformité avec la réglementation lors de son entrée en vigueur en mai 2018 (23% au Royaume-Uni et 34% en Allemagne). Un résultat finalement peu surprenant, considérant que seules 5% des entreprises auraient effectivement mis en place toutes les stratégies de gestion de données nécessaires pour garantir cette mise en conformité.

Les décideurs IT semblent pourtant conscients des enjeux, puisque 66% des répondants confient que leur budget a augmenté en prévision de l'entrée en vigueur de RGPD. Plus de sept entreprises sur dix en Europe ont par ailleurs monté des équipes projet dédiées RGPD et plus d'une sur quatre a désigné un responsable de la protection des données. A l'épreuve des faits, et alors que les entreprises avaient deux ans pour se préparer (adoption de la réglementation en avril 2016), seuls 40% des répondants révèlent que leur organisation a rempli un formulaire de mise en conformité RGPD...[lire la suite]

LE NET EXPERT

• MISE EN CONFORMITÉ RGPD / CNIL

- AUDIT RGPD ET CARTOGRAPHIE de vos traitements

- MISE EN CONFORMITÉ RGPD de vos traitements

- SUIVI de l'évolution de vos traitements

• FORMATIONS / SENSIBILISATION :

- 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

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 DORTEPP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

• **RECHERCHE DE PREUVES :**

• Accompagnement à la mise en place de DPO ;

• **Formation** (et sensibilisation) à la **Cybercriminalité** (Assurance n°15 0206 84) ;

• Audit Sécurité (ISO 27005) ;

• Expertises techniques et judiciaires ;

• **Recherche de preuves** : téléphones, disques durs, e-mails, contenus, documents de clientèle ;

• **Expertises de systèmes de vote électronique** ;

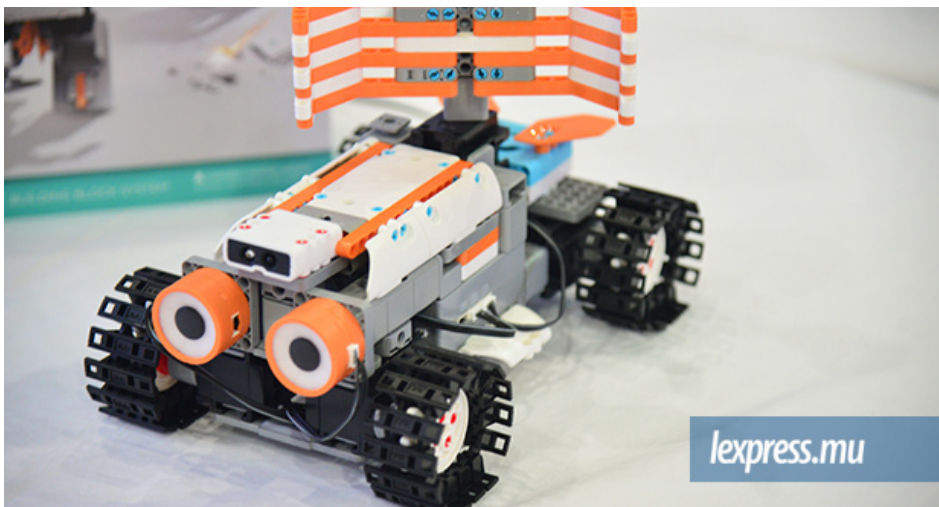
Le Net Expert
INFORMATIQUE
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *RGPD : 1 entreprise française sur 5 ne sera pas en conformité !* | UnderNews

Objets connectés: attention, on vous espionne...



Objets
connectés:
attention,
on vous
espionne...

Montre connectée. Enceintes connectées. Casque connectée. Jouets connectés... Autant d'appareils qui ont besoin d'Internet pour fonctionner correctement. Sauf qu'ils sont susceptibles d'être des espions. La plupart sont, en effet, vulnérables aux menaces.

En France, l'Association européenne de défense des consommateurs a pris les devants pour demander que les poupées connectées soient retirées des étagères pour Noël. Ces poupées connectées, d'un fabricant réputé, répond aux enfants. Les conversations ont été enregistrées au préalable. Toutefois, cela n'est pas conforme aux règles de protection des données des mineurs. En effet, n'importe qui peut s'y connecter à travers le Bluetooth et ainsi intercepter des conversations

Selon un informaticien, les parents ne réalisent pas ce qu'ils achètent. «*Ils ignorent les dangers des poupées ou des jouets connectés. Ils vont en acheter sans réaliser qu'il y a des failles de sécurité*», fait-il valoir.

Pas de vérifications

Le fait est que tous les objets qui ont des fonctions Bluetooth et sont équipés de micros sont de parfaits espions. Grâce à des logiciels espions, des pirates peuvent écouter les conversations. Wikileaks a rendu public des documents, en mars dernier, prouvant que la *National Security Agency*, aux États-Unis, peut effectuer des écoutes...[lire la suite]

LE NET EXPERT

:

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - **FORMATIONS / SENSIBILISATION :**
 - 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

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 RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)

Réagissez à cet article

Source : *Objets connectés: attention, on vous espionne...* | *lexpress.mu*

Alerte ! Un virus «indétectable» pour Windows voit le jour



Alerte ! Un
virus
«indétectable»
pour Windows
voit le jour

Une nouvelle méthode permettant d'esquiver tous les logiciels antivirus a été présentée par les employés de la société enSilo lors de la conférence sur la cybersécurité Black Hat Europe 2017. Ce virus, restant invisible, serait susceptible d'affecter le fonctionnement de toutes les versions de Windows.

Dans le cadre de la conférence sur la cybersécurité Black Hat Europe 2017, les spécialistes de la société enSilo ont décrit une nouvelle méthode permettant d'effectuer une cyberattaque tout en restant indétectable par les antivirus. D'après les programmeurs, ce schéma, baptisé Process Doppelganging, fonctionne sur toutes les versions de Windows.

Ainsi, les experts ont établi qu'avec l'utilisation des transactions NTFS, il était possible d'apporter des modifications dans un fichier. Ensuite, Process Doppelganging est capable de masquer le chargement de ce fichier modifié. Pendant tout ce temps-là, l'antivirus ignore que l'ordinateur est la cible d'une attaque puisque le code malveillant utilisé par Process Doppelganging ne laisse pas de traces sur le disque...[lire la suite]

LE NET EXPERT

:

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - **FORMATIONS / SENSIBILISATION :**
 - 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

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 RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;

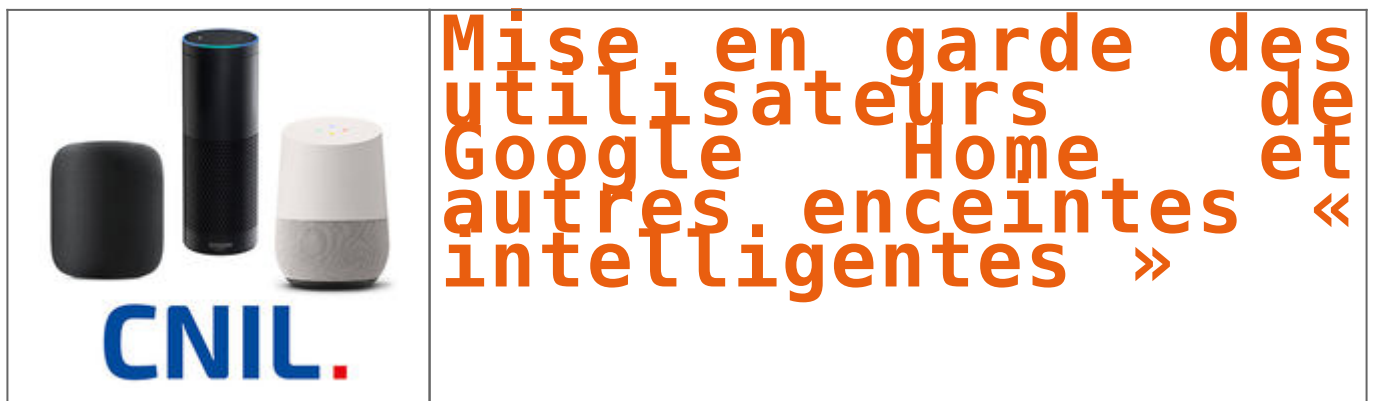


[Contactez-nous](#)

Réagissez à cet article

Source : *Attention, danger! Un virus «indétectable» pour Windows voit le jour – Sputnik France*

Mise en garde des utilisateurs de Google Home et autres enceintes « intelligentes »



Guidée vocalement, une enceinte connectée assiste l'utilisateur dans les tâches de son quotidien. Quels enjeux posent cette technologie au regard de la vie privée des utilisateurs ?

Qu'est-ce qu'une enceinte connectée dite intelligente ?

Une enceinte connectée « intelligente » est un dispositif équipé d'un haut-parleur et d'un micro qui intègre un assistant vocal. Grâce à cet équipement, l'enceinte est capable d'interagir avec l'utilisateur pour lui délivrer un service suite à une requête vocale. L'assistant est en mesure de répondre à une question, donner la météo, régler le chauffage, activer des lumières, réserver un VTC/Taxi, acheter des billets ...

Le principe général de fonctionnement se caractérise par 4 grandes étapes :

Etape 1 – L'utilisateur « réveille » l'enceinte à l'aide d'une expression clé (« Hey Snips » / « Ok Google » / « Hey Alexa »).

Etape 2 – L'utilisateur énonce sa requête.

Etape 3 – La parole prononcée est automatiquement transcrite en texte puis interprétée afin qu'une réponse adaptée soit fournie.

Etape 4 – L'enceinte repasse en « veille »

Certaines de ces enceintes enregistrent localement les requêtes de l'utilisateur de manière à lui laisser la maîtrise de ses données (ex. une enceinte connectée avec l'assistant vocal de Snips). D'autres en revanche, envoient ces requêtes dans le cloud, autrement dit sur les serveurs de traitement de la société (ex. Amazon Echo, Google Home...). Dans les deux cas, l'appareil (ou ses serveurs) peut être amené à conserver :

- Un historique des requêtes transcrites afin de permettre à la personne de pouvoir les consulter et à l'éditeur d'adapter les fonctionnalités du service.
- Un historique des requêtes audio afin de permettre à la personne de les réécouter et à l'éditeur d'améliorer ses technologies de traitement de la parole.
 - Les métadonnées associées à la requête comme par exemple, la date, l'heure, le nom du compte...

[...]

Nos conseils

1. Encadrer les interactions de ses enfants avec ce type d'appareils (rester dans la pièce, éteindre le dispositif lorsqu'on n'est pas avec eux) ;
2. Couper le micro / éteindre l'appareil lorsque l'on ne s'en sert pas ou lorsqu'on ne souhaite pas pouvoir être écouté ;
3. Avertir des tiers/invités de l'enregistrement potentiel des conversations (ou couper le micro lorsqu'il y a des invités)
4. Vérifier qu'il est bien réglé par défaut pour filtrer les informations à destination des enfants.
5. Connecter des services qui présentent réellement une utilité pour vous, tout en considérant les risques à partager des données intimes ou des fonctionnalités sensibles (ouverture porte, alarme...) ;
6. Etre vigilant sur le fait que les propos tenus face à l'appareil peuvent enrichir votre profil publicitaire ;
7. Ne pas hésiter à contacter les services supports en cas de questions et, le cas échéant, la CNIL.
8. Se rendre régulièrement sur le tableau de bord pour supprimer l'historique des conversations/questions posées et personnaliser l'outil selon vos besoins. Par exemple, définir le moteur de recherche ou la source d'information utilisé par défaut par l'assistant...[lire la suite]

LE NET EXPERT

:

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
- CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
- MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION :
 - 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

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 DDRETFP (Numéro formateur n°93 84 83041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »

« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- **Mise en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Cybercriminalité** (et substituts) à la **Cybercriminalité** (Assistance n°93 84 83041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires :
 - **Recherche de preuves** : téléphones, disques durs, e-mails, contenus, documents de données ;
 - **Expertise de systèmes de vote électronique** ;



Contactez-nous



Réagissez à cet article

Source : *Enceintes intelligentes : des assistants vocaux connectés à votre vie privée | CNIL*

Jouets connectés : Dangers pour votre vie privée dit la

CNIL

	Jouets connectés : Dangers pour votre vie privée dit la CNIL
---	---

La Présidente de la CNIL met en demeure la société GENESIS INDUSTRIES LIMITED de procéder à la sécurisation de jouets connectés à destination d'enfants : la poupée « My Friend Cayla » et le robot « I-QUE ».

Le robot « I-QUE » et la poupée « My Friend Cayla » sont des jouets dits « connectés ». Ils répondent aux questions posées par les enfants sur divers sujets tels que des calculs mathématiques ou encore la météo. Les jouets sont équipés d'un microphone et d'un haut-parleur et sont associés à une application mobile téléchargeable sur téléphone mobile ou sur tablette. La réponse est extraite d'Internet par l'application et donnée à l'enfant par l'intermédiaire des jouets.

Alertée, en décembre 2016, par une association de consommateurs sur le défaut de sécurité des deux jouets, la Présidente de la CNIL a décidé de réaliser des contrôles en ligne en janvier et novembre 2017. Elle a par ailleurs adressé un questionnaire en mars 2017 à la société située à Hong-Kong.

Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom...) mais également des informations renseignées dans un formulaire de l'application « My Friend Cayla App ».

Plusieurs manquements à la loi Informatique et Libertés ont été constatés dont notamment :

Le non-respect de la vie privée des personnes en raison d'un défaut de sécurité

Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou « appairer ») un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier (par exemple, avec un code PIN ou un bouton sur le jouet).

La personne située à une telle distance est en mesure d'entendre et d'enregistrer les paroles échangées entre l'enfant et le jouet ou encore toute conversation se déroulant à proximité de celui-ci.

La délégation de la CNIL a également relevé qu'il était possible de communiquer avec l'enfant situé à proximité de l'objet par deux techniques :

- soit en diffusant via l'enceinte du jouet des sons ou des propos précédemment enregistrés grâce à la fonction dictaphone de certains téléphones ;
- soit en utilisant les jouets en tant que « kit main libre ». Il suffit alors d'appeler le téléphone connecté au jouet avec un autre téléphone pour parler avec l'enfant à proximité du jouet.

La Présidente a considéré que l'absence de sécurisation des jouets, permettant à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des propriétaires des jouets et d'avoir accès aux discussions échangées dans un cercle familial ou amical, méconnaît l'article 1^{er} de la loi Informatique et Libertés selon lequel l'informatique « ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Le défaut d'information des utilisateurs des jouets

Alors que des informations personnelles sont traitées par la société, les contrôleurs de la CNIL ont constaté que les utilisateurs des jouets ne sont pas informés des traitements de données mis en œuvre par la société...[lire la suite]

LE NET EXPERT

- MISE EN CONFORMITÉ RGPD / CNIL
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- MISE EN CONFORMITÉ RGPD de vos traitements
- SUIVI de l'évolution de vos traitements
- FORMATION / SENSIBILISATION :
 - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (Outils Gendarmier/Police)
 - QUÉRAIRES (Photos / E-mails / Fichiers)
 - TELEPHONES (récupération de Photos / SMS)
 - SYSTEMES NUMERIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES (JUDICIAIRES / ADMINISTRATIVES)
 - SECURITE INFORMATIQUE
 - SYSTEMES DE VOTES ELECTRONIQUES

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 accrédité auprès de la SOUTEP (Numéro formateur n°93 84 0345 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

Principales compétences :

- Accompagnement à la mise en place de **RGPD**
- Audits** de conformité à la **Règlement** (RGPD) (ISO 27005, etc.)
- Enquêtes techniques et judiciaires**
- Appropriation** (Sensibilisation, formation, ateliers, etc.) aux enjeux, réglementations, obligations de confidentialité ;
- Apprentissage** et **formation** aux **nouvelles technologies**

Le Net Expert
INFORMATIQUE
Expertise et Conseil en Informatique

Contactez-nous

Réagissez à cet article

Source : *Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité | CNIL*

Alerte : Faille dans TeamViewer permet de prendre le contrôle de votre ordinateur

Untitled - Notepad
File Edit Format View Help
After injecting with your preferred method press the correct hotkey to initiate the hook routine

TeamViewer Permissions Hook v1
XPL0_7
GELLYN
INFO - Made on Windows 10 using TeamViewer x86 Version 13.0.5058
TeamViewerBaseAddress: 0xEF0000
Press [NUMPAD 1] if you are the Host/Server
Press [NUMPAD 2] if you are the Client

Alerte :
Faille
dans
TeamViewer
permet de
prendre le
contrôle
de votre
ordinateur

Plusieurs millions d'internautes utilisent, de part le monde, l'outil TeamViewer. Un problème de sécurité vient d'être découvert. Il pourrait permettre de détourner l'ordinateur des utilisateurs.

Le logiciel TeamViewer est une sorte de cheval de Troie légal. Je m'explique ! L'outil permet de prendre la main sur un ordinateur dont l'accès a été autorisé. Il permet aussi de filmer l'écran, capture écran, ... Bref, un trojan licite. Seulement, un problème de taille vient d'être découvert dans ce logiciel utilisé par des millions d'entreprises et particuliers.

Tout d'abord, une vulnérabilité critique a été découverte dans le logiciel qui pourrait permettre aux utilisateurs partageant une session de prendre le contrôle total du PC de leur interlocuteur. Pour qu'une session à distance fonctionne sur les deux machines, il faut un présentateur, celui qui affiche son écran et un spectateur, celui qui regarde l'écran du présentateur...[lire la suite]

Lien vers le code et la démo de Gelin

Commentaire de Denis JACOPINI :

Dans la mesure du possible, ne laissez jamais un TeamViewer en l'attente. Autorisez l'accès manuellement. Si vous ne pouvez pas faire autrement, programmez le déclenchement d'une alerte lors des connexions automatiques. En attendant, que Teamviewer corrige cette vulnérabilité au plus vite, prudence !

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **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**

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 RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- **Accompagnement** à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- **Audits Sécurité** (ISO 27005) ;
- **Expertises techniques et judiciaires** ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)



Réagissez à cet article

Source : ZATAZ *Une faille dans TeamViewer permet de détourner l'ordinateur d'un utilisateur* – ZATAZ