

La CNIL remet en cause le fonctionnement de la plateforme APB



La CNIL remet en cause le fonctionnement de la plateforme APB

Dans un avis rendu public jeudi 28 septembre, la Commission met en demeure le ministère de l'enseignement supérieur de « cesser de prendre des décisions concernant des personnes sur le seul fondement d'un algorithme ».

C'est un nouveau coup porté à la plate-forme Admission post-bac (APB), qui permet de faire ses vœux d'orientation dans l'enseignement supérieur. Dans une décision du 30 août rendue publique jeudi 28 septembre, la Commission nationale de l'informatique et des libertés (CNIL) met en demeure le ministère de l'enseignement supérieur de « cesser de prendre des décisions concernant des personnes sur le seul fondement d'un algorithme et de faire preuve de plus de transparence » dans l'utilisation de la plate-forme.

Cette décision, qui « n'est pas une sanction », précise la CNIL, oblige cependant le ministère à se mettre en conformité avec la loi « dans un délai de trois mois ». Elle intervient suite aux polémiques qui ont émaillé la session 2017 d'APB. Notamment autour des milliers de candidats n'ayant pas reçu de proposition lors des trois phases de la procédure. Mais surtout en raison de l'utilisation du tirage au sort pour départager les candidats trop nombreux à l'entrée des filières universitaires en tension. Tirage au sort régulièrement remis en cause devant les tribunaux administratifs, qui estiment qu'il ne repose sur aucune base légale...[lire la suite]

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

A Lire aussi :

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.



[Contactez-nous](#)



Réagissez à cet article

Source : *La CNIL remet en cause le fonctionnement de la plateforme APB*

Comment devenir DPO ? (Data Protection Officer)



Quelles seront les missions du DPO ? La principale sera de veiller à l'intégrité et la protection des données personnelles de son organisation, tant sur le plan juridique que technique. Il sera également l'intermédiaire entre son organisation et l'autorité de contrôle, en France la Commission nationale de l'informatique et des libertés (Cnil).

Ce poste est donc assez proche de celui de Correspondant informatique et libertés (CIL), déployé depuis 2005 dans des entreprises et les entités publiques françaises. « *Les fonctions sont très similaires, mais le contexte est différent* », résume Albine Vincent, chef du service des CIL à la Cnil. Même son de cloches à l'AFCDP (*), association française représentant les CIL. « *Les fonctions d'un DPO sont à peu près les mêmes que celles d'un CIL, mais avec le niveau de sanctions prévues par le nouveau règlement, elles prennent une tout autre dimension* », estime son délégué général Bruno Rasle.

D'ailleurs, sur les 4 800 CIL actuellement en poste, une grande majorité d'entre eux devraient devenir DPO d'ici à mai 2018. Cette évolution ne sera pas automatique, mais ce choix sera souvent le plus logique. « *Si le CIL a donné satisfaction dans sa mission, il sera bien placé pour devenir DPO. Il devra bien entendu se former pour connaître parfaitement la nouvelle réglementation* », poursuit Albine Vincent. Elle rappelle que la Cnil propose des ateliers d'information sur le sujet. Des formations longues existent aussi pour se former au poste de DPO, comme le Master CEID de Nanterre ou le master spécialisé de l'Institut supérieur d'électronique de Paris (Isep). « *Ce sera de la responsabilité de l'entreprise ou de l'entité publique de choisir la personne qui sera en mesure d'occuper ce poste* », poursuit Albine Vincent. « *Dans le cadre de ses missions de contrôles, la Cnil pourra vérifier que le DPO est bien en mesure de réaliser sa mission et notamment qu'il n'y a pas de conflits d'intérêts avec d'autres fonctions éventuelles qu'il occupe.* » Concrètement, la nomination du DPO devra être déclarée auprès de la Cnil, via un formulaire en ligne...[lire la suite]

Besoin de vous former au 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 DRIEF 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 : *Data Protection Officer : un gardien pour les données personnelles*

Les Français de plus en plus soucieux de la Protection de leurs données personnelles



33% des Français ont déjà essayé d'effacer des informations les concernant sur internet, dont 17% « plusieurs fois ». Un chiffre qui grimpe à 61% chez les 18-24 ans, dont 33% « plusieurs fois ».

Soucieux de leur e-réputation, près de 75% des 18-24 ans déclarent par ailleurs rechercher régulièrement sur le net des informations associées à leurs nom et prénom (vs 57% sur l'ensemble des Français).

LA PROTECTION DES DONNÉES PERSONNELLES, UNE PRÉOCCUPATION EN HAUSSE, PARTICULIÈREMENT CHEZ LES JEUNES

En 2017, 85% des Français se disent préoccupés par la protection de leurs données personnelles en général, soit une augmentation de 4 points par rapport à 2014. Une question qui suscite encore plus d'inquiétude dès lors qu'il s'agit de la protection des données sur Internet : 90% se disent préoccupés pour leurs données mises en lignes (+5 pts depuis 2014).

Les 18-24 ans apparaissent particulièrement sensibles à cette question puisqu'ils sont 93% à se dire préoccupés par la protection de leurs données en ligne, dont 48% « très préoccupés » (vs 39% pour l'ensemble des Français).

ALORS QUE LES USAGES EN LIGNE ONT FORTEMENT PROGRESSÉ EN 3 ANS

51% des Français déclarent réaliser « souvent » des paiements en ligne (+12 points depuis 2014), 39% stockent des documents personnels (mails, photos, vidéos, fichiers divers) sur des serveurs, contre 31% il y a 3 ans ; enfin plus d'1 Français sur 2 publie régulièrement des propos ou des photos personnels sur les réseaux sociaux (52%), ils sont 72% chez les 18-24 ans.

SI LES USAGES À RISQUES RECULENT ET QUE LES PRATIQUES VERTUEUSES PROGRESSENT...

23% des Français déclarent saisir leurs coordonnées personnelles sur les forums, soit une baisse de 5 points par rapport à 2014, et seuls 17% des Français partagent par mail des messages types chaînes de lettre (-10 pts).

En parallèle, la protection de l'accès aux « device » a augmenté, l'utilisation d'un mot de passe s'est systématisée pour tous les équipements : 86% des Français utilisent un mot de passe pour leur ordinateur professionnel (+8 pts vs 2014), 76% pour leur ordinateur personnel (+7 pts), 73% pour leur téléphone mobile (+9 pts), 61% pour leur tablette tactile (+10 pts). Comme en 2014, plus de 93% des Français ont le souci de mettre à jour leur anti-virus.

... LES FRANÇAIS N'ONT PAS ENCORE ADOPTÉ TOUS LES BONS REFLEXES

La grande majorité des Français (74%) utilise un seul et même mot de passe pour ses comptes et espaces en ligne, une pratique en augmentation (+5 pts vs 2014), sans doute à relier à la démultiplication du nombre de comptes par internaute et à la difficulté à gérer de nombreux mots de passe différents.

PIRATAGE BANCAIRE ET NON-RESPECT DE LA CONFIDENTIALITÉ DE LEURS DONNÉES : PRINCIPALES CRAINTES DES FRANÇAIS

80% des Français jugent le risque de piratage de leurs données bancaires important dont 47% « très » important. Parallèlement, les craintes des Français sont également vives concernant le respect de la confidentialité de leurs données (42%, +3 pts) et la protection des enfants dans leur usage d'Internet (49%, +4 pts).

A QUI LES FRANÇAIS FONT-ILS CONFIANCE POUR PROTÉGER LEURS DONNÉES ?

Dans ce contexte, le lien de confiance entre les Français et les acteurs qui utilisent leurs données reste à renforcer, et pour certains acteurs, ce lien reste même à construire :

Les banques sont les seuls acteurs à obtenir la confiance de plus de la moitié des Français en matière de protection des données (53%, en augmentation de 3 pts). Comparativement, les opérateurs télécom, les moteurs de recherche ou les acteurs des réseaux sociaux ne recueillent qu'un faible niveau de confiance (respectivement 23%, 20%, et 10%).

Parallèlement, la confiance des Français envers l'Etat (47%, +7 pts) s'améliore sur cette question, et reste très élevée à l'égard de la CNIL, une instance très positivement perçue (77% + 3 pts)...

QUE PROPOSE LE NET EXPERT, (EXPERT INFORMATIQUE ASSERMÉNTÉ) :

- FORMATIONS (n° formateur Direction du Travail)
- EXPERTISES & AUDITS (certifié ISO 27005)
- RECHERCHE DE PREUVES

NOTRE MÉTIER :

- FORMATIONS :
 - EN CYBERCRIMINALITÉ
 - EN PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - AU MÉTIER DE b
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES

FORMATIONS EN CYBERCRIMINALITÉ, 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 ;

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 ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons 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 ;

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 mettons 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 (Règlement 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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIET n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Une extension qui fait discrètement bosser votre ordi pour faire gagner de la cryptomonnaie à d'autres



Une extension qui fait discrètement bosser votre ordi pour faire gagner de la cryptomonnaie à d'autres

Alors que les cryptomonnaies, Bitcoin et Ethereum en tête, sont de plus en plus appréciées et commencent à prendre de l'ampleur (une rumeur qui n'a pas été confirmée prêterait à Amazon la volonté d'accepter des Bitcoins pour les paiements), il semblerait qu'une de leurs consœurs soit cryptée à l'insu des internautes par des sites plus ou moins sûrs.

Cette cryptomonnaie s'appelle Monero et elle a la particularité de ne pas être minée sur le processeur graphique (le GPU) mais sur le processeur central (le CPU).

Des extensions et du code source pour miner Monero

La particularité de Monero, le fait qu'elle soit minée par le CPU, semble avoir donné des idées à plusieurs sites et entreprises : pourquoi ne pas faire travailler les ordinateurs des internautes ? Ainsi, par exemple, l'extension Chrome SafeBrowse, téléchargée plus de 140.000 fois, utiliserait le CPU des ordinateurs l'ayant installée pour miner de la cryptomonnaie Monero pour le compte de ses créateurs.

Cette utilisation n'a pas manqué d'être vivement critiquée mais elle aurait été reproduite à de nombreuses reprises : sur le site de torrent The Pirate Bay, une phase de test a été menée mi-septembre selon les administrateurs. L'idée serait de remplacer les bannières publicitaires par un script permettant de miner du Monero....[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
- MISE EN CONFORMITE RGPD / FORMATION DPO

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 ;
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 ;

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 ;

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 (Règlement 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.



[Contactez-nous](#)

Réagissez à cet article

Source : Monero : la cryptomonnaie que vous minez sans le savoir

Privacy Shield : Le transfert de données Europe-USA suffisamment sécurisé ?



Privacy
Shield : Le
transfert de
données
Europe-USA
suffisamment
sécurisé ?

Pour Le Conseil national du numérique, le Privacy Shield doit être « renégocié » car l'accord n'offre pas de garanties suffisantes à la protection des données.

A l'occasion du premier bilan annuel du Privacy Shield et de ses garanties, le **Conseil national du numérique** (CNNum) exprime sa divergence. L'accord de transfert d'une partie des données entre l'Union européenne et les Etats-Unis, qui a succédé au dispositif Safe Harbor à partir du 1er août 2016, « doit être renégocié », selon le comité consultatif d'experts en charge d'éclairer les pouvoirs publics sur le numérique. Celui-ci dit partager les inquiétudes d'autres organisations comme les CNIL européennes (fédérées à travers le G29), la commission des libertés civiles du Parlement européen et des associations de défense des droits.

« Le Privacy Shield présente un trop grand nombre de zones d'ombre et ne donne pas suffisamment de garanties à la protection des données personnelles des Européens », souligne par voie de communiqué le CNNum. L'accord en l'état est « faible, susceptible d'annulation sur les mêmes fondements que son prédécesseur ». Le Safe Harbor avait été invalidé fin 2015 par la Cour de justice de l'Union européenne (CJUE).

La collecte massive et indifférenciée de données pratiquée par les services de renseignement américain, une pratique mise à jour par les révélations d'Edward Snowden relative au cyberespionnage américain, était au cœur de ce dossier.

Le Privacy Shield n'offrirait toujours pas de garanties satisfaisantes dans ce domaine.

Bouclier percé ?

Lors de négociations qui ont précédé l'adoption du Privacy Shield en juillet 2016, la Commission européenne avait obtenu des autorités américaines une avancée présumée : la collecte de masse de données devait être écartée au profit d'une collecte ciblée.

Mais cette avancée n'est qu'une « simple directive présidentielle » prise par l'ancien locataire de la Maison Blanche, Barack Obama, souligne le CNNum dans son communiqué. Sur le fond, « le droit américain reste largement inchangé » en la matière.

« Les évolutions législatives et jurisprudentielles récentes, combinées à la position affichée par la nouvelle administration [Trump] » sont « un signal politique particulièrement préoccupant. »

Le CNNum fait notamment référence aux évolutions à venir de la législation américaine en matière de données, dont le titre VII du FISA Amendments Act (FAA). Il est censé expirer à la fin de l'année mais pourrait être reconduit.

Ces dispositions incluent la controversée « section 702 », qui autorise la surveillance large de tout ressortissant d'un pays étranger.

Une section qui a notamment servi de fondement aux programmes de surveillance Prism et Upstream de la National Security Agency (NSA) que Snowden avait dévoilés à partir de mi-2013.

Le Conseil national du numérique s'inquiète également de « la vacance de postes clés en charge de la supervision du dispositif côté américain » et de « l'effectivité des mécanismes de recours. »

Des problématiques de souveraineté sont également soulevées par l'organisation.

Les données constituent un actif essentiel de l'économie numérique. Or les flux de données d'Europe sont « massivement captés par les Etats-Unis », souligne l'organisation.

Cette asymétrie des transferts de data avait déjà été constaté dans le cadre du Safe Harbor.[lire la suite]

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

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPEEN 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 ; (Demandeur de la DITET n°10 et 10101 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 : *Transfert de données Europe-USA: le CNNum rejette le Privacy Shield | Silicon*

20% des ordinateurs de la Police de Manchester son sous Windows XP



20% des
ordinateurs de
la Police de
Manchester son
sous Windows
XP

GREATER MANCHESTER POLICE are still using defunct operating system Windows XP on one-in-five machines in active use on the force.

The second biggest police force in the UK joins the Metropolitan Police on the list of shame, according to new findings from a Freedom of Information Act request made by *the BBC*.

« The remaining XP machines are still in place due to complex technical requirements from a small number of externally provided highly specialised applications, » a spokeswoman told Auntie Beeb.

« Work is well advanced to mitigate each of these special requirements within this calendar year, typically through the replacement or removal of the software applications in question. »

Most forces refused to cooperate with the FOI request, citing security reasons. This includes the Met Police who back in June admitted they had 18,000 machines that still run XP (including offline ones) and that only eight machines were running Windows 10...[lire la suite]

NOTRE MÉTIER :

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
 - **MISE EN CONFORMITE RGPD / FORMATION DPO**

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 ;

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 ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons 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 ;

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 mettons 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 (Règlement 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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Manchester Police are using Windows XP on one in five computers*

Télétravail et protection des données personnelles



Le télétravail pose certaines questions concernant d'abord le droit du salarié à la déconnexion mais aussi sur la protection des données. La barrière de plus en plus floue entre outils personnels et outils professionnels avec la collecte d'informations impose de revoir le régime juridique de la protection des données. Explications par François Alambret, Counsel chez Bryan Cave Paris.

L'essor du télétravail a accru la nécessaire protection des données personnelles. Si ces deux sujets se complètent, ils ne doivent éclipser les autres aspects de la digitalisation des relations de travail.

Le développement du télétravail

Le télétravail n'a pas attendu l'émergence d'internet pour exister mais il s'est incontestablement développé par la conjonction de différents facteurs : les progrès des outils technologiques individuels, l'individualisation des relations du travail et l'accroissement des centres urbains et leur congestion concomitante.

Poussé d'abord par les revendications des salariés, le télétravail a été organisé par les entreprises par le biais d'accords collectifs ou de chartes (informatiques ou sur la qualité de vie au travail), puis reconnues par les organisations syndicales au niveau européen et national (accord cadre européen sur le télétravail du 16 juillet 2002 et accord national interprofessionnel du 19 juillet 2005). Enfin, encadré par le législateur par le biais des lois du 22 mars 2012, du 8 août 2016 (Loi travail dite loi « El-Khomri ») et les ordonnances Macron en cours de promulgation.

Cette dernière étape législative vise encore à simplifier le recours au télétravail, notamment par le biais d'un accord ou d'une charte d'entreprise en dispensant ensuite les parties d'un avenant au contrat de travail (voir article 24 de l'ordonnance n°3 du 31 août 2017 modifiant les articles L.1222-9 et suivants du code du travail).

L'employeur n'est plus tenu, non plus, de supporter le coût de ce télétravail, ce qui autorise le salarié « de facto » à utiliser son propre matériel informatique (avec les conséquences afférentes en termes de confidentialité et de sécurité).

La protection des données personnelles

Dès son apparition, le télétravail s'est heurté aux problématiques de la protection des données informatiques. Cette contrainte a d'ailleurs été rappelée expressément par les partenaires sociaux dans leur premier accord européen (point 5 de l'accord cadre du 16 juillet 2002) et national (article 5 de l'accord national interprofessionnel du 19 juillet 2005).

Et de fait, le télétravail accroît les risques sur la protection des données de façon à la fois structurelle et technique. Structurellement, par le mode même d'organisation du travail (qui augmente les communications digitales au détriment de communications directes et orales dans l'entreprise) et techniquement car le salarié demeure à distance des services informatiques de l'entreprise et peut dorénavant utiliser ses propres matériels informatiques avec les risques qui en découlent.

Le règlement communautaire sur la protection des données en date du 27 avril 2016 (souvent dénommé GDPR « Global Data Protection Regulations ») prend acte de la digitalisation croissante de la société et de ses nouvelles formes de travail. Il renforce les mesures de protection à l'égard des personnes et donc vis-à-vis des salariés et des télétravailleurs.

L'imbrication des deux notions/ le rôle de l'entreprise

Ces deux sujets (télétravail et protection des données) s'accompagnent et s'encouragent mutuellement. Le renforcement de la protection des données offre des garanties nécessaires au développement du télétravail.

Toutefois, ce cadre législatif et réglementaire posé, c'est aux acteurs de l'entreprise de s'en saisir et de le façonner.

A eux de négocier et de rédiger un accord collectif ou une charte permettant une mise en œuvre fluide mais aussi sécurisée du télétravail, dans le respect du nouveau règlement communautaire du 27 avril 2016.

Mais traiter ces deux thèmes isolément méconnaît l'ampleur des bouleversements de la digitalisation de la société et des relations du travail...[lire la suite]

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

A Lire aussi :

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 DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

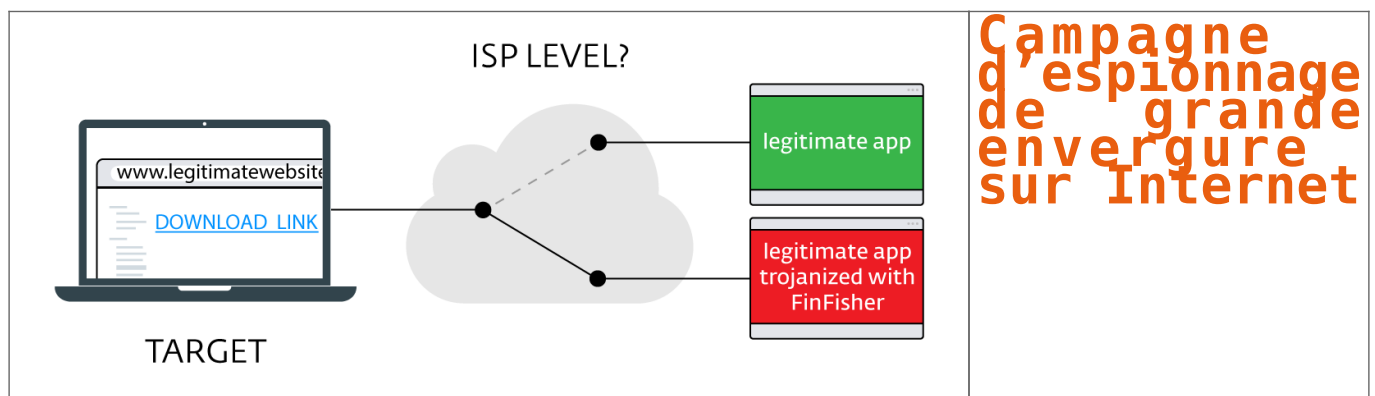


[Contactez-nous](#)



Réagissez à cet article

Campagne d'espionnage de grande envergure sur Internet



Les chercheurs ESET® ont détecté des campagnes d’espionnage liées à FinFisher, le célèbre spyware également connu sous le nom de FinSpy. Sept pays sont infectés. FinFisher est un spyware (logiciel espion) commercialisé en tant qu’outil de surveillance et d’intrusion informatique. Il est vendu à une vingtaine d’organismes gouvernementaux à travers le monde. ESET pense qu’il a également été utilisé par des régimes autoritaires.

Les capacités d’espionnage de FinFisher s’étendent à :

- la surveillance via les webcams et les microphones (images retransmises en direct)
- l’enregistrement de frappe (keylogger)
- l’exfiltration des fichiers

Ce logiciel espion a reçu un certain nombre de modifications via des correctifs dans sa dernière version. Elles améliorent ses fonctions pour se montrer plus intrusif. FinFisher peut ainsi rester sous le radar de détection des solutions de sécurité et empêcher une analyse approfondie de son comportement. L’innovation la plus importante reste la méthode pour pénétrer les machines ciblées.

Lorsqu’un utilisateur ciblé est sur le point de télécharger une application populaire telle que WhatsApp®, Skype® ou VLC Player®, il est automatiquement redirigé vers le serveur de l’attaquant. La victime installe alors une version qui inclut un malware de type Trojan et se trouve ainsi directement infectée par FinFisher.

ISP LEVEL?

TARGET

Mécanisme d’infection de la dernière variante de FinFisher

« Sur deux des sept campagnes menées, les logiciels espions se sont propagés au moyen d’une attaque man-in-the-middle. Autrement dit, les communications sont interceptées à l’insu des parties concernées. Nous pensons que **les principaux fournisseurs d’accès à Internet de ces deux pays ont joué un rôle crucial dans cette infection** », explique Filip Kafka, Malware Analyst chez ESET et à l’origine de cette recherche. Ces campagnes sont les premières à révéler publiquement la probable implication (volontaire ou pas) d’un fournisseur d’accès à Internet dans la diffusion de malwares. « Les campagnes FinFisher sont des projets de surveillance perfectionnés et tenus secrets. Les méthodes utilisées associées à la portée de ces attaques en font une menace sans précédent », poursuit Filip Kafka.

Par le passé, ESET a publié un certain nombre d’articles sur les campagnes FinFisher. Vous pouvez les consulter ici. Les experts ESET ont également rédigé un article détaillé sur cette nouvelle campagne. Pour plus de détails, notre cybersecurity leader Benoit Gruenewald peut répondre à vos questions.

[Note pour les éditeurs.](#)

FinFisher, le soi-disant malware du gouvernement et l’approche de l’industrie de la sécurité sont sous les feux de la rampe. Pour ESET, il n’existe pas de malware dans la mesure où ce programme a été acheté d’une part puis modifié et détourné d’autre part par des individus mal intentionnés.

Lire la réponse d’ESET à une lettre ouverte adressée à Bits of Freedom, un groupe de défense des droits numériques...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITÉ, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SÉCURITÉ ET ANALYSE D’IMPACT
- MISE EN CONFORMITÉ RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITÉ, 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 ;

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 ;

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 ;

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 (Règlement 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 ».

- Audite 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 ; (Venez-vous assister ou intervenir)
- Formation de C.I.L.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Contactez-nous

Réagissez à cet article

Source : ESET

Votre appareil
potentiellement piratable par
Bluetooth



Votre appareil
potentiellement
piratable par
Bluetooth

Des failles informatiques présentes sur des milliards d'objets disposant de la technologie Bluetooth viennent d'être dévoilées. Attention : danger.

« On va peut-être atteindre un record d'attaques enregistrées ces dernières années. » Le communiqué de la société américaine Armis, spécialisée dans la sécurité informatique, ne mâche pas ses mots. Pire encore : « Nous craignons que la faille que nous avons découverte ne soit que la partie visible de l'iceberg. » La raison de cette annonce gentiment alarmiste ? Potentiellement 5,3 milliards de terminaux dans le monde pourraient être attaqués. Leur point commun à tous ? Ils disposent du Bluetooth. Tous sont donc exposés aux attaques dites « BlueBorne ».

Freinons un tout petit peu le mouvement de panique : la faille BlueBorne ne fonctionne que si le Bluetooth est préalablement activé sur l'appareil, même si celui-ci est en mode invisible. Selon le terminal piraté, il est possible de prendre son contrôle ou de faire du « *man in the middle* », autrement dit d'intercepter les communications entre plusieurs interlocuteurs sans se faire repérer. L'attaque n'est pas difficile à mener et peut, dans le meilleur des cas, aboutir en dix secondes. On peut bien sûr craindre la main mise sur des documents confidentiels. Mais on peut aussi redouter une opération « rançongiciel » d'envergure, à l'instar de WannaCry...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
- MISE EN CONFORMITE RGPD / FORMATION DPO

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 ;

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 ;

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 ;

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 accompagnerons 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 (Règlement 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 DRTF 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 : Angoisse : des milliards d'appareils sont potentiellement piratables via Bluetooth

Une faille dans Windows 10 utilisée pour vous espionner

!



Une
faille
dans
Windows
10
utilisée
pour vous
espionner
!

Selon un rapport publié sur le blog de la firme de sécurité informatique FireEye, les pirates procédaient comme suit : un fichier Word ouvert innocemment par l'utilisateur activait la faille 0-Day -CVE-2017-8759- et permettait au malicieux d'installer à son insu un programme informatique destiné à vous espionner. L'ordinateur visé par la manœuvre était alors contraint d'installer FinSpy – le spyware en question.

Ce malware est développé par une entreprise anglaise particulièrement controversée qui commercialise ses produits à des gouvernements partout dans le monde : **Gamma Group**. Selon le rapport de FireEye, **FinSpy a déjà été vendu à de multiples acheteurs**, il est donc plus que probable que ceux-ci s'en servent activement pour tenter d'infiltrer de nombreuses cibles.

Selon les experts en cybersécurité de Microsoft, les hackers en question font **partie du groupe NEODYMIUM**, déjà connu pour des pratiques de hacking similaires. Microsoft reste donc très vigilant par rapport à ces failles de sécurité : n'hésitez donc pas à télécharger les patches proposés dès que possible !

On ne le répétera jamais assez, si vous recevez un fichier Word suspect sur votre boîte mail ne l'ouvrez pas, même s'il vous promet de vous révéler la suite de Game Of Thrones !...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
 - MISE EN CONFORMITE RGPD / FORMATION DPO

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 ;

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 ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons 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 ;

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 réaliserons 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 mettons 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 (Règlement 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.



Réagissez à cet article

Source : *Windows 10 : une faille de sécurité permet aux pirates d'y installer un dangereux malware !*