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 coeur 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, combinés 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 États-Unis »*, souligne l'organisation.
Cette asymétrie des transferts de data avait déjà été constaté dans le cadre du Safe Harbor…[lire la suite]

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)

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 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 (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

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

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

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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

Télétravail et protection des données personnelles

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 aout 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]

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 ?

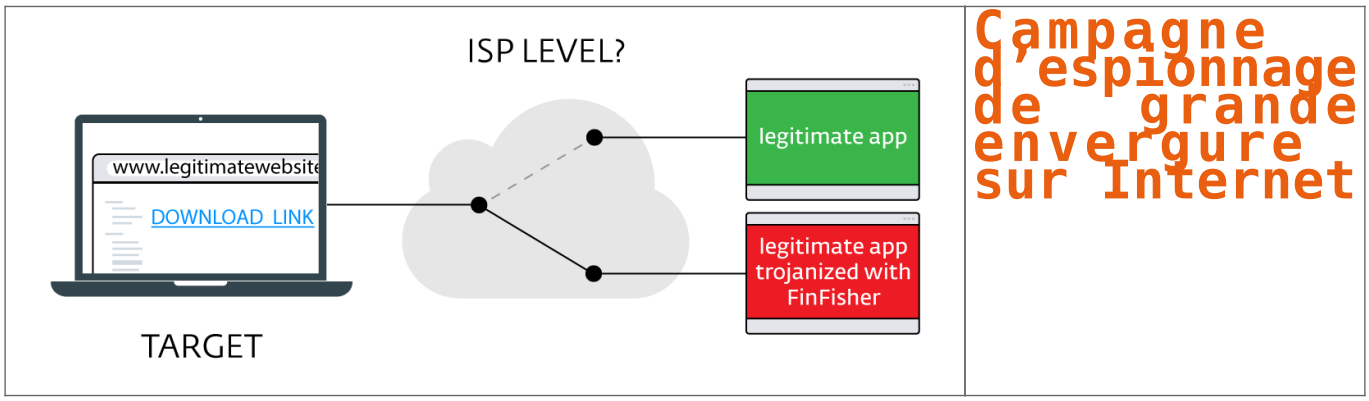
Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Télétravail et protection des données personnelles – LE MONDE DU DROIT : le magazine des professions juridiques*

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 :

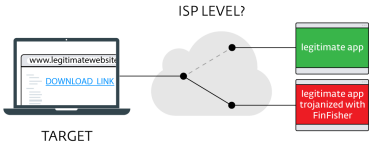
• la surveillance via les webcams et les microphones (images retransmises en direct)

• 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.**



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 Grunemwald 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]

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]

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 maliciel d'installer à son insu un programme informatique destiné à vous espionner. L'ordinateur visé par la manoeuvre 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 patchs 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 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 (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

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

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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

Pirate Bay contamine votre ordinateur pour fabriquer de la monnaie virtuelle

Pirate Bay contamine votre ordinateur pour fabriquer de la monnaie virtuelle

Avec les années, il est devenu de plus en plus difficile pour les sites de torrent et de téléchargement pirates de survivre uniquement grâce aux revenus publicitaires. Mais ils ont su rebondir et trouver de nouvelles techniques pour parvenir à générer suffisamment de revenus, simplement en utilisant les processeurs des visiteurs pour miner des crypto-monnaies.
Le procédé a été découvert **dans un code JavaScript sur The Pirate Bay**, et si ce n'est pas systématique, c'est néanmoins assez fréquent pour devenir problématique, puisqu'il est très facile de se rendre compte **des pics soudains d'utilisation du CPU (jusqu'à 100%)** pour récupérer du **Monero**. Le site avance qu'il s'agit pour l'instant d'une phase de test, qui pourrait cependant mener à une utilisation plus mainstream du procédé qui lui permettrait de rester rentable….[lire la suite]

Réagissez à cet article

Source : *Pirate Bay emprunte les processeurs des visiteurs pour miner de la monnaie virtuelle | KultureGeek*

Alerte : CCleaner compromis par une backdoor

Alerte : L'utilitaire CCleaner compromis par une backdoor

Piriform avertit que son logiciel CCleaner a été compromis. Avec des risques de fuites de données persos de 130 millions d'utilisateurs.

Piriform, l'éditeur de l'utilitaire CCleaner de nettoyage et d'optimisation de Windows, vient de reconnaître qu'il a fait l'objet d'une attaque.

Les versions 5.33.6162 sur poste fixe et 1.07.3191 en mode Cloud de sa solution ont été compromises.

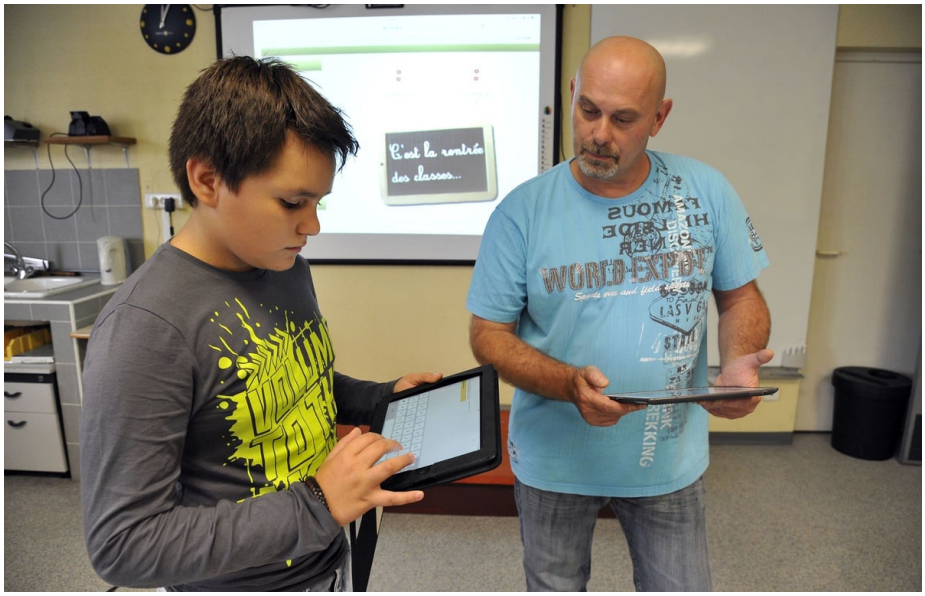
« Une activité suspecte a été identifiée le 12 septembre 2017, où nous avons vu une adresse IP inconnue recevant des données du logiciel trouvé dans CCleaner et CCleaner Cloud sur les systèmes Windows 32 bits », alerte Paul Yung, Vice-Président Produit de Piriform.

Selon l'éditeur, le logiciel a été illégalement modifié avant sa livraison publique. Le pirate a réussi à installer une backdoor à deux niveaux afin d'exécuter du code envoyé à partir d'une adresse IP sur les systèmes affectés…[lire la suite]

Source : *L'utilitaire CCleaner compromis par une backdoor*

Les données personnelles des

écoliers français vont-elles échapper à Google?



Les données personnelles des écoliers français vont-elles échapper à Google?

Une «note interne» diffusée en mai ouvrait la possibilité aux entreprises du numérique de collecter des données scolaires. Les parents d'élèves avaient protesté auprès du ministre de l'Education. Jean-Michel Blanquer compte revoir la politique en la matière.

Pas d'école pour Google, Facebook, et autres géants du numérique, regroupés sous l'appellation Gafa. Jeudi, le porte-parole du gouvernement a indiqué que le ministre de l'Education Jean-Michel Blanquer comptait limiter l'accès de ces entreprises aux données scolaires des élèves.

Le ministre compte « revenir sur une circulaire [en fait, une lettre interne] signée deux semaines avant les présidentielles, qui ouvre très largement, peut-être trop largement l'accès des Gafa dans l'école », a expliqué Christophe Castaner.

Publicités ciblées

Rappel des faits : le 12 mai dernier, Matthieu Jeandron, délégué au numérique éducatif, adresse une lettre aux délégués académiques du numérique. Dans ce courrier, révélé par le Café pédagogique, il explique qu'il n'y a pas « de réserve générale sur l'usage des outils liés aux environnements professionnels chez les grands fournisseurs de service du web ». Un peu plus loin, il indique qu'il ne voit pas de « blocage juridique de principe à la connexion d'un annuaire avec l'un de ses services ».

En clair, cela signifie que Google, Facebook, et autres entreprises du numérique auraient pu collecter des listes d'élèves avec leurs noms, leurs classes, voire même leurs notes dans le cadre de travaux effectués en ligne. Ces données peuvent rapporter de l'argent : par exemple, on peut imaginer que Google, ayant connaissance des difficultés d'un élève, lui « propose » des publicités ciblées sur les cours en lign…[lire la suite]

Source : *Les données personnelles des écoliers français vont-elles échapper à Google?*

Comment pirater un téléphone sans le toucher ?

Comment pirater un téléphone sans le toucher ?

L'exploitation de failles de sécurité se trouvant au niveau du protocole Bluetooth permet de pirater un appareil à distance. La démonstration est faite sur un smartphone Android, mais les vulnérabilités concernent potentiellement d'autres types d'appareils.

Armis, entreprise spécialiste des questions de sécurité informatique, a découvert huit exploits (ces éléments de programme visant à exploiter une faille informatique) réunis sous l'étiquette BlueBorne, et permettant de prendre à distance le contrôle de téléphones, d'objets connectés et même potentiellement d'ordinateurs. *« Nous nous attendons à découvrir beaucoup d'autres vulnérabilités de ce type sur diverses plateformes proposant une connexion Bluetooth. Ces failles sont actuellement ouvertes, et peuvent être exploitées par les hackers. Les attaques via BlueBorne peuvent être utilisées pour réaliser tout un arsenal de piratages différents, autorisant l'exécution de code malveillant à distance ou encore la prise de contrôle des appareils«* , explique Armis….[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, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dansl e but de déposer plainte ou de 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 formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

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

Besoin d'un Expert ? contactez-nous

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

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *BlueBorne : le hack qui permet de pirater un téléphone sans le toucher*